Barcelona

Institut Municipal Barcelona Innovació i Tecnologia
Direcció de Serveis d'Innovació i Tecnologies de Ciutat

Plec de prescripcions tècniques que regeix el contracte de serveis de manteniment de càmeres perimetrals, de seguretat ciutadana i control d'accessos de la Gerència d'Àrea de Seguretat, Prevenció i Convivència de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible

ÍNDEX

0. INTRODUCCIÓ 4
ANTECEDENTS 4
1. OBJECTE 7
2. ABAST 8
2.1. SERVEIS INCLOSOS 14
2.1.1. AUDITORIA INICIAL I AUDITORIES ADDICIONALS 14
2.1.2. MANTENIMENT PREVENTIU 16
2.1.3. MANTENIMENT CORRECTIU 19
2.1.4. SERVEI DE REPARACIÓ I GESTIÓ DE GARANTIES 22
2.1.5. SERVEI DE SUPORT I GESTIÓ D'INCIDÈNCIES (HELPDESK) 23
2.1.6. SERVEI DE REPORTING 24
2.1.7. SERVEI D'ACTUALITZACIÓ DE LA INFORMACIÓ I INVENTARI 26
2.1.8. REUNIONS DE SEGUIMENT 27
3. FASES DE PRESTACIÓ DEL SERVEI 29
3.1. INICI DEL CONTRACTE 29
3.2. FASE D'EXECUCIÓ 30
3.2.1. LLOC DE PRESTACIÓ DEL CONTRACTE 30
3.2.2. HORARI DE LA PRESTACIÓ DELS SERVEIS 31
3.2.3. IDIOMA 31
3.3. PLA DE CONTINGÈNCIA 31
3.4. PLA DE DEVOLUCIÓ DEL SERVEI 32
PLA DE TRANSICIÓ DEL SERVEI 33
4. MODEL DE PRESTACIÓ DEL SERVEI 38
4.1. MODEL DE RELACIÓ BIT/ADJUDICATARI 38
4.2. MODEL DE GESTIÓ D'INCIDÈNCIES 41
4.3. ACORDS DE NIVELL DE SERVEI 42
5. MARC DE TREBALL 43
5.1. EINES CORPORATIVES DE SEGUIMENT 43
5.2. EINES DE MONITORITZACIÓ 43
6. RECURSOS HUMANS 44
1. FUNCIONS PER PERFIL 45
2. CARACTERÍSTIQUES PROFESSIONALS 47
3. DIMENSIONAMENT 48
7. FACTURACIÓ 49
8. PERÍODE DE GARANTIA DEL CONTRACTE 50
9. PROPOSTA TÈCNICA I ECONÒMICA 50
10. CLÀUSULES GENERALS DE SEGURETAT 50
10.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓDE DADES I COMPLIMENT NORMATIU 50
10.2. CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT 51
10.3. RESPONSABLE DE SEGURETAT 52
10.4. CLÀUSULA PER ACCESSOS POTENCIALS 53
10.5. CONFIDENCIALITAT 53
10.6. CLÀUSULES DE SEGURETAT D'ACCÉS A SISTEMES DE L'AJUNTAMENT 54
10.6.1. AUDITORIA 54
10.6.2. GESTIÓ D'INCIDENTS 55

10.6.3. ACCÉS A LA INFORMACIÓ 55
10.6.4. DIMENSIONAMENT/GESTIÓ DE CAPACITATS 55
10.6.5 ANÀLISIS FORENSES 55
10.6.6. CONTROL D'ACCÉS 55
10.6.7. GESTIÓ DEL PERSONAL 56
10.6.8. PROTECCIÓ DEL LLOC DE TREBALL 58
10.6.9. CLÀUSULA DE COMUNICACIONS EXTERNES 58
10.6.10. PROTECCIÓ DELS SUPORTS INFORMÀTICS 59
10.6.11. PROTECCIÓ DE LA INFORMACIÓ 59
10.6.12. PROTECCIÓ DE LES INSTAL·LACIONS 61
10.6.13 GESTIÓ D'EXCEPCIONS 61
10.7 CLÀUSULES DE SEGURETAT D'ADMINISTRACIÓ DE SISTEMES 61
10.7.1 GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS 61
10.7.2 AUTORITZACIÓ DELS USUARIS ALS SISTEMES 62
10.7.3 INVENTARI D'ACTIUS 63
10.7.4 CONFIGURACIÓ DE SEGURETAT 63
10.7.5 MANTENIMENT 64
10.7.6 XIFRATGE DE DADES 66
10.7.7 CERTIFICATS 66
10.7.8 ANTIMALWARE 66
10.7.9 CÒPIES DE SEGURETAT 66
10.7.10 CONTROL D'ACCÉS 67
10.7.11 EXPLOTACIÓ 67
10.7.12 PROTECCIÓ DELS SERVEIS 68

11. ANNEX 1: INFORMACIÓ ADDICIONAL I ACLARIMENTS 70

0. INTRODUCCIÓ

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

Concretament, BIT participa en el disseny i execució de l'estratègia TIC de l'Ajuntament, ofereix assessorament i suport en tots aquells projectes o programes que requereix una estratègia de sistemes d'informació i telecomunicacions, i, impulsa i executa projectes tecnològics de diversa índole.

Entre les seves funcions BIT és responsable del desenvolupament, manteniment i evolució de solucions TIC eficients i productives per a la ciutadania i els empleats municipals.

Dins del BIT, i com a part de l'estratègia d'evolucionar les TIC per millorar la vida de la ciutadania, es troba la Direcció de Serveis d'Innovació i Tecnologies de Ciutat, que té com a objectiu impulsar la transformació digital i la modernització tecnològica del municipi, promovent l'ús estratègic de la tecnologia per millorar la gestió pública, la seguretat ciutadana, la sostenibilitat urbana i la qualitat de vida de les persones.

Entre les seves responsabilitats hi ha el disseny, la implementació i l'administració de les infraestructures i solucions que conformen les tecnologies de ciutat; és a dir, el conjunt d'eines digitals i sistemes intel·ligents que permeten gestionar de manera eficient i sostenible els serveis municipals i l'espai públic. Aquestes tecnologies inclouen, entre d'altres, les xarxes de sensors urbans, les plataformes de gestió de dades, els sistemes d'informació geogràfica i les aplicacions per a la presa de decisions basada en dades. També en formen part els sistemes de videovigilància i seguretat ciutadana, que integren càmeres instal·lades a la via pública o en equipaments municipals, centres de control, xarxes de comunicacions i altres components que contribueixen a una ciutat més segura i connectada.

ANTECEDENTS

L'Ajuntament de Barcelona ha consolidat una estratègia de seguretat urbana basada en la innovació tecnològica, la prevenció i la protecció dels drets fonamentals. En aquest context, els sistemes de videovigilància esdevenen una eina essencial per garantir la seguretat de l'espai públic, reforçar la capacitat operativa dels cossos de seguretat i millorar la convivència ciutadana.

La videovigilància no es concep únicament com un instrument de control, sinó com una infraestructura crítica per a la detecció precoç d'incidents, la gestió eficient de situacions d'emergència i el suport a les tasques d'investigació. Aquesta visió s'alinea amb els estàndards europeus de seguretat urbana intel·ligent i amb iniciatives com el projecte Secur'Cities, en què Barcelona va participar activament.

A més, la ciutat aposta per un model de videovigilància avançat, basat en tecnologies de darrera generació com càmeres amb capacitat de seguiment dinàmic (PTZ), sistemes de vídeo analítica i integració amb plataformes de gestió d'incidents. Aquest enfocament permet una cobertura més eficient del territori, l'eliminació de punts cecs i una optimització dels recursos humans i materials.

La implantació d'aquests sistemes es fa sota criteris estrictes de legalitat, proporcionalitat i transparència, amb protocols específics per garantir la protecció de dades personals i la supervisió institucional. Així, la videovigilància esdevé una eina al servei de la ciutadania, orientada a reforçar la confiança col·lectiva en la capacitat de resposta de les institucions públiques.

Dins del marc del Pla Endreça, i en coherència amb els objectius estratègics de la Gerència d'Àrea de Seguretat, Prevenció i Convivència, s'ha plantejat una transformació tecnològica integral del sistema de videovigilància per tal d'alinear-lo amb els estàndards de seguretat urbana del segle XXI. Aquesta transformació prioritza la prevenció d'incidents, la protecció de la ciutadania i la millora de la capacitat operativa dels serveis de seguretat.

Durant l'any 2025 es va començar a treballar una reorganització de la xarxa de càmeres de videovigilància, identificant zones cegues mitjançant criteris de seguretat, vulnerabilitat i densitat de trànsit de persones. El projecte preveu la instal·lació progressiva d'unes 1.100 càmeres noves distribuïdes en 69 espais i agrupades en 9 fases d'execució. Actualment, està en execució la Fase 1, 2, 3 i 4.

BIT, està liderant, de la mà de Barcelona Infraestructures Municipals S.A. (BIMSA), el desplegament i la gestió de la nova xarxa de càmeres de videovigilància. Aquest concepte, no és únicament ajudar en la posada en marxa de l'equipament si no definir i dimensionar el conjunt de serveis associats a aquesta xarxa de càmeres, que es defineixen en els següents apartats.

És en aquest context que el BIT, mitjançant la Direcció de Serveis d'Innovació i Tecnologies de ciutat, a l'empara del que es preveu a la Llei 9/2017, de 8 de novembre, de contractes del sector públic, decideix impulsar un plec que doni cobertura a la contractació de serveis vinculats al manteniment de la xarxa de càmeres de

videovigilància amb mesures de contractació pública sostenible. Però no disposa de mitjans ni recursos tècnics adients per realitzar aquestes actuacions, motiu pel qual cal procedir a l'auxili mitjançant la contractació amb tercers, tot d'acord amb l'objectiu d'estabilitat pressupostària i control de despesa i amb total respecte als principis d'eficàcia, eficiència, publicitat, transparència, no discriminació i igualtat de tracte.

Actualment, el servei de manteniment dels sistemes de videovigilància, control d'accessos i videogestió de la Gerència de Seguretat i Prevenció de l'Ajuntament de Barcelona es troba cobert per dos contractes vigents, que donen resposta a diferents àmbits funcionals i tecnològics:

1. Contracte núm. 20224187

Corresponent als *serveis de manteniment integral dels sistemes de vigilància perimetrals i interiors (CCTV) i control d'accessos (CCAA) dels edificis de la Guàrdia Urbana i de la Gerència de Seguretat i Prevenció*, amb data de finalització prevista el **13 de desembre de 2026**.

2. Contracte núm. 20224346

Relatiu als *serveis de manteniment integral dels sistemes de càmeres de videovigilància de seguretat pública i dels equips de videogestió associats*, amb data de finalització prevista el **19 d'abril de 2027**.

1. OBJECTE

El present document té per objecte establir les condicions tècniques que han de regir la contractació, l'execució i el control del servei de manteniment integral de la xarxa de càmeres de videovigilància i de tots els seus sistemes i components complementaris, amb la finalitat de garantir la seva operativitat contínua, fiabilitat, qualitat d'imatge i disponibilitat en tot moment. Així com dels elements de la xarxa de control d'accessos a les dependències municipals objecte d'aquest contracte, amb mesures de contractació pública sostenible.

El contracte inclou el manteniment del conjunt de càmeres que conformen la infraestructura completa de videovigilància gestionada per la Gerència d'Àrea de Seguretat, Prevenció i Convivència, tant a la via pública com als edificis municipals titularitat de la mateixa, així com els equips i subsistemes que asseguren la captació, transmissió, processament, enregistrament i visualització de les imatges. També dels dispositius i software que controla l'accés als emplaçaments corresponents.

A data de redacció d'aquesta licitació la xarxa de videovigilància està formada per un conjunt d'elements distribuïts al territori municipal segons el següent llistat aproximat:

- Càmeres de seguretat ciutadana instal·lades a via pública:
  - 97 càmeres actualment operatives.
  - 730 càmeres addicionals previstes per a la fase 2025–2027.
  - Possibilitat d'ampliació amb 500 càmeres addicionals en fases posteriors.
- Càmeres perimetrals instal·lades en edificis municipals:
  - 214 càmeres repartides en diverses seus.
- Cartelleria càmeres perimetrals:
  - 98 cartells repartits en diverses seus.
- Elements de control d'accés:
  - 29 dispositius.
  - 1 software de gestió dels controls d'accessos.
- Cartelleria a via pública.
  - 184 cartells repartits per diverses ubicacions.
  - Creixement pel desplegament de noves càmeres de seguretat ciutadana. Estimació en Fase 1: 91 addicionals. Estimació Fase 2 i 3: 183. Pendents de Fase 4.
- Elements de seguretat via pública (pilones)
  - 5 dispositius.

El servei proposat està especialment orientat al treball de camp, entenent com a tal, totes les actuacions preventives, correctives, tècniques i operatives que cal dur a terme sobre la xarxa de càmeres per preservar-ne l'estat, la qualitat i l'operativitat. Aquestes actuacions inclouen els manteniments periòdics, la reparació i reposició d'equips, les intervencions en la infraestructura de xarxa i alimentació, la verificació de gravació i transmissió, els ajustos i alineacions d'imatge, la reconfiguració de dispositius i la integració de nous elements.

La finalitat del contracte és assegurar que la xarxa de càmeres i els seus elements complementaris es mantenen en condicions òptimes de servei, evitant-ne el deteriorament, detectant i corregint fallades, i garantint una disponibilitat màxima del sistema, minimitzant els temps d'inactivitat i mantenint la qualitat tècnica i operativa necessària per als serveis que en depenen.

L'adjudicatari haurà de disposar de personal tècnic especialitzat en sistemes de seguretat i videovigilància, amb experiència en tasques de manteniment, reparació i suport tècnic dels equips i instal·lacions objecte del contracte.

Aquest personal haurà d'estar capacitat per a la detecció i diagnosi d'incidències, l'execució d'actuacions preventives i correctives sobre la infraestructura física i lògica del sistema, incloent-hi reparacions, substitucions i integracions d'equips nous, així com per a garantir el compliment dels procediments operatius, protocols de coordinació i nivells de servei (ANS) establerts en el present document.

2. ABAST

Tal com s'ha indicat en l'apartat anterior, els serveis a contractar s'engloben en un conjunt de serveis estipulats que es descriuen a continuació:

- Auditoria inicial i auditories addicionals ad-hoc
- Manteniment preventiu
- Manteniment correctiu
- Servei de reparació i gestió de garanties
- Servei de suport i gestió d'incidències
- Servei de reporting
- Servei d'actualització de la informació i/o inventari
- Reunions de seguiment

Els sistemes objecte d'aquest contracte seran les càmeres de videovigilància, els sistemes de control d'accessos i els sistemes de control industrial associats a la seguretat i al control de l'espai públic, incloent-hi, entre d'altres, els controladors PLC, pupitres d'operació, elements de comunicació, equips de xarxa, armaris de control i

la resta d'elements que permetin la gestió remota o local de pilones, o altres dispositius equivalents que hi pugui haver instal·lats a la ciutat de Barcelona o a les dependències municipals de la Gerència d'Àrea de Seguretat, Prevenció i Convivència objecte d'aquest contracte.

No només formaran part de l'abast els equips principals, sinó també tots els seus accessoris, components auxiliars, programari associat, sistemes d'alimentació, comunicacions, cartelleria vinculada i qualsevol altre element necessari per al seu correcte funcionament. Dins de les dependències municipals també s'inclourà l'equipament necessari per a la visualització, enregistrament i operació dels sistemes (servidors, enregistradors, estacions de treball, PLC, conversors, equips de comunicació i similars).

Igualment, formaran part de l'abast tots els equips que componguin la xarxa de videovigilància, els sistemes de control d'accessos a les dependències policials i els sistemes PLC de control de pilones associats a seguretat ciutadana o altres accessos urbans que siguin incorporats, substituïts o ampliats durant la vigència del contracte. Aquests equips s'incorporaran automàticament a l'inventari del servei i quedaran subjectes a les mateixes condicions de manteniment, suport, actualització documental i nivell de servei establertes en aquest plec.

L'empresa adjudicatària haurà de disposar de vehicle propi per poder realitzar els desplaçament necessaris per dur a terme les tasques objecte d'aquest contracte.

L'inventari actual del que es disposa del servei es mostra a continuació:

SEGURETAT CIUTADANA

UBICACIÓ	No_Càmeres	Marques	Models	Tipus
Allada Vermell	1	Hanwha	XNP-9300RW	Domo
Avinyó	2	Hanwha	PNB-A9001	Box
Boqueria	4	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Drassanes	4	Pelco	SRXE4-6X31-EBT-IR1	Bullet
Escudellers	1	Hanwha	XNP-9300RW	Domo
Ferran Rauric	4	Hanwha	PNB-A9001	Box
George Orwell	2	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Hospital/Robadors	3	Hanwha	PNB-A9001	Box

Maria Cristina	5	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Montcada	4	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Passeig de Gràcia	17	Hanwha	PNB-A9001	Box
Plaça del Teatre	6	Hanwha	PNB-A9001, XNB-8000, XNP-9300RW	Box, Bullet, Domo
Portal de l'Àngel	4	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Portal de la Pau	10	Hanwha	PNB-A9001, XNO-6123R/RW, XNP-9300RW	Box, Bullet, Domo
Princesa	3	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Pérez Pulgar	1	Hanwha	XNP-9300RW	Domo
Rambles	7	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Riera Baixa	3	Hanwha	PNB-A9001, XNP-9300RW	Box, Domo
Sant Oleguer	2	Hanwha, Pelco	PNO-A9311R, SRXE4-6X31-EBT-IR1	Bullet
Sobradiel /Avinyó	1	Hanwha	PNB-A9001	Box
Tàpies	2	Pelco	SRXE4-6X31-EBT-IR1	Bullet
Via Barcino	1	Hanwha	XNP-9300RW	Domo
Via Laietana/Av Catedral	8	Dahua, Hanwha	ITC413-PW4D-Z3, PNB-A9001, XNO-6123R/RW, XNP-9300RW	Box, Bullet, Domo
Total				**97**

PERIMETRALS I INTERIORS

Nº Comissaria	**Nom Comissaria**	**Nº càmeres**	**Marca**	**Models**	**Tipus**
C01	Edif 5 Zona Franca (USP, UIPA, UP i USD)	16	ACTi, Hanwha, Bosch	TCM-7811, QNV-6082R, EX36N, TNV-C7013RC	Domo, Bullet, Corner-mount
C02	Edifici 5 Zona Franca	1	Hanwha	QNV-6082R	Domo

	(USP, UIPA, UPAS...)				
C03	Edif 2 Zona Franca (UI)	19	Bosch, Hanwha, HikVision	EX36N, TNV-C7013RC, DS-2CD2610F-I	Domo, Bullet, Corner-mount, 360º
C04	Galeria de Tir Zona Franca	6	Dahua	HDBW2231RP-ZS-S2, HFW2431T-ZS-S2	Domo, Bullet
C05	UT3 Sants-MontjuÃ¯c	11	Dahua, Hanwha, Samsung	HFW2320RP-ZS, QNO-6082R, SNV-5080R	Bullet, Domo, Fish-eye
C06	Dipòsit A	8	HikVision, Dahua, Hanwha	DS-2CD1643G0-Z, QNO-6082R	Bullet
C07	Prefectura Galeria de Tir	6	Axis, Samsung, Hanwha	M3113, SNV-5080R, QNV-6082R	Domo
C08	Prefectura Sants-Montjuïc	14	HikVision, Axis	DS-2CD2646G2-IZS, P1435-LE, P1467-LE	Bullet
C10	Comissaria Rambla 43	30	Bosch, Panasonic, Hanwha	EX36N, WV-CP280G, QNV-6082R/VEU	Domo, Bullet
C11	UT1 Districte Ciutat vella	32	HikVision, Hanwha	DS-2CD2643G0-IZS, QNO-6082R1	Bullet, Domo
C12	UDAI	1	Samsung	SNO-L5083RP	Bullet
C13	UT Platges	19	Samsung, Bosch	SNO-L5083RP, SNV-5084R, Corner 9000 MP	Domo, Bullet
C14	UT2 Eixample	24	Hanwha, Samsung, HikVision, Bosch	QNV-6082R, DS-2CD2646G2-IZS, QNV-5080R, DS-2CE56D0T-IRMF, XNV-6080R, EX36N, TNV-C7013RC	Domo, Bullet
C15	Unitat Muntada	6	Hanwha, HikVision	QNV-6082R, DS-2CD2646G2-IZS, DS-2CD2610F-I	Bullet
C16	UT8 Nou Barris	13	Samsung, Hanwha, Hikvision	SNV-6084R, QNV-6082R, QND-7080RP, DS-2CD2143G0-IS, DS-2CD2646G2-IZS	Domo, Bullet
C17	Tànger	8	Dahua	IPC-HFW2431T-ZS-S2	Bullet
Total		214			

SERVIDORS PLATAFORMA VIDEO

Nº Comissaria	Nom Comissaria	Versió Milestone	Tipus

C01	Zona Franca UIPA	XProject Smart Client	Servidor
C03	Zona Franca UI	Xprotect Essential v2.1a	Servidor
C04	Zona Franca Galeria Tir	N/A	Servidor
C05	UT3 Sants-Montjuïc	XProject Smart Client 2016	Servidor
C06	Dipòsit A	Grabador Dahua	Servidor
C07	Prefectura Galeria Tir	Web Client 2020 R3	Servidor
C08	Prefectura Sants-Montjuïc	Smart Client 2020 R3	Servidor
C10	Rambla 43	Smart Client 2020 R3	Servidor
C11	UT1 Tàpies (Districte Ciutat Vella)	Smart Client 2020 R3	Servidor
C12	UDAI	Smart Client 2020 R3	Servidor
C13	UT Platges	Smart Client 2020 R3	Servidor
C14	UT2 Eixample	Smart Client 2020 R3	Servidor
C15	Unitat Muntada	Smart Client 2020 R3	Servidor
C16	UT8 Nou Barris	Smart Client 2020 R3	Servidor
Total			**14**

CONTROL PILONES

Ubicació	Unitats	Marca	Tipologia Equipament
Via Laietana	1	Schneider	TM241CE40U
Portal de la Pau	3	Schneider	TM241CE40U
Sant Jaume	1	Schneider	TM241CE40U
Total			**5**

CONTROL ACCESSOS

Nº Comissaria	Nom Comissaria	Unitats	Marca	Tipologia Equipament
C01	Zona Franca UIPA	1	SUPREMA	BioEntryPlus BEPL-OC
C02	Zona Franca UPAS	1	SUPREMA	BioEntryPlus BEPL-OC
C03	Zona Franca UI	4	SUPREMA	3× BioEntryPlus BEPL-OC + 1× BioMini Plus 2
C04	Zona Franca Galeria de Tir	2	SUPREMA	BioEntry P2 BEP2-OD
C05	UT3 Sants-Montjuïc	1	SUPREMA	BioEntryPlus BEPL-OC
C06	Dipòsit A	0	—	—

C07	Prefectura Galeria de Tir	2	SUPREMA	BioEntry P2 BEP2-OD
C08	Prefectura Sants-Montjuïc	1	SUPREMA	BioEntryPlus BEPL-OC
C09	Sala Conjunta	1	SUPREMA	BioEntry P2 BEP2-OD
C10	Rambla 43	3	SUPREMA	1× BST-OC + 2× BioLite Net BEPL-OC
C11	UT1 Tàpies	4	SUPREMA	BioEntryPlus BEPL-OC
C12	UDAI	2	SUPREMA	BioEntryPlus BEPL-OC
C13	UT Platges	3	SUPREMA	2× BioEntryPlus BEPM-OC + 1× BioLite N2 BELN2ODB
C14	UT2 Eixample	2	SUPREMA	BioEntryPlus BEPL-OC
C15	Unitat Muntada	0	—	—
C16	UT8 Nou Barris	2	SUPREMA	BioEntry BIO CSW
C17	Espai Formatiu Tànger	0	—	—
Total				**29**

El software que s'utilitza pel control d'accés, i que haurà de ser part del contracte, és l'IP Biostar, propietat de la Gerència d'Àrea de Seguretat, Prevenció i Convivència.

Aquest inventari és orientatiu. En el moment de l'auditoria inicial s'aixecarà un inventari definitiu per posar en marxa el servei.

Com s'ha comentat anteriorment, aquest inventari serà viu i anirà creixent durant la vigència del contracte amb els desplegaments de càmeres que s'estan realitzant actualment. El servei s'anirà dimensionant any rere any.

El plantejament de creixement en tecnologia s'està definint amb càmeres de tipologies diverses. Hi ha tant càmeres bullet (fixes), com domo (PTZ), 180º, 270º o 360º. Càmeres de tecnologia molt nova que aporta una visió molt més complerta en un únic dispositiu. En funció de l'emplaçament, la proposta combina tipologies diverses per aconseguir visualitzar les àrees requerides per Guardia Urbana.

En termes de control d'accessos no hi ha un plantejament de creixement previst. Però pot donar-se el cas de que s'hagi d'instal·lar algun dispositiu addicional en les dependències mantingudes i que aquest equipament entri dintre de l'abast del manteniment.

A continuació, i als efectes de selecció, es descriuen per a cadascuna de les agrupacions el conjunt de serveis i activitats que conformen el seu abast, d'acord amb la seva naturalesa i definició.

2.1. SERVEIS INCLOSOS

2.1.1. AUDITORIA INICIAL I AUDITORIES ADDICIONALS

L'adjudicatari haurà d'executar, dins dels **primers dos mesos** a comptar des de la formalització del contracte, una **auditoria tècnica** de tots els sistemes de videovigilància (CCTV), tant perimetrals com de seguretat ciutadana, i control d'accessos (CCAA) i de tota la infraestructura associada als sistemes objecte del present contracte.

Aquesta auditoria té com a finalitat establir una línia base de referència tècnica i operativa de totes les instal·lacions, a partir de la qual es realitzarà el servei de manteniment i l'avaluació de la seva qualitat, així com identificar possibles millores d'eficiència, seguretat i sostenibilitat tecnològica.

L'auditoria inicial tindrà com a objectius principals:

- Verificar l'estat real, funcional i normatiu de tots els sistemes i equips objecte del contracte.
- Actualitzar l'inventari de tots els sistemes de CCTV i CCAA, amb identificació unívoca de cada equip i ubicació.
- Comprovar el compliment de la normativa aplicable en matèria de seguretat privada, protecció de dades, seguretat elèctrica i compatibilitat electromagnètica.
- Detectar deficiències, vulnerabilitats i riscos potencials, tant en l'àmbit físic com en el digital.
- Definir, si es creu adient en alguna instal·lació, un pla de millora amb recomanacions prioritzades segons la seva criticitat, cost i impacte operatiu.

L'auditoria haurà d'abastar la totalitat de dispositius i sistemes existents i previstos dins l'àmbit del contracte, amb el nivell de detall mínim següent:

- <u>Sistemes de videovigilància (CCTV)</u>
  - Inventari físic i funcional de totes les càmeres, indicant:
  - Identificador únic, ubicació exacta, model, número de sèrie i estat actual.
  - Tipologia (fixa, domo, PTZ, tèrmica o analítica).
  - Resolució, configuració de gravació (4K / 10 fps i 2K / 8 fps) i compressió utilitzada (H.265/H.264).

- Estat d'òptiques, carcasses, suports, alimentació, connexions i proteccions IP/IK.
- Verificació de gravació i retenció: comprovació del correcte enregistrament d'imatges segons la política establerta en el moment de l'adjudicació (actualment 30 dies a 4K / 10 fps i 60 dies addicionals a 2K / 8 fps).
- Avaluació de la qualitat d'imatge i cobertura, amb comprovació de focus, angle, il·luminació i absència de zones mortes.
- Anàlisi de configuració del programari de gestió (VMS): canals actius, llicències, versions, registres d'alarma i configuració de perfils d'usuari.

- <u>Servidors i emmagatzematge</u>
  - Inventari complet dels servidors locals de les dependències municipals on hi ha CCTV tancats amb dades de:
  - Ubicació, model, processador, capacitat d'emmagatzematge, tipus de RAID i estat dels discos.
  - Capacitat de retenció efectiva, ús actual i marge disponible.
  - Verificació del funcionament dels SAIs associats, si correspon, i comprovació d'autonomia.
  - Versions del sistema operatiu i del programari de gravació o gestió.
  - Configuració de còpies de seguretat i mecanismes de redundància.
- <u>Sistemes de control d'accessos (CCAA)</u>
  - Revisió dels lectors i enregistradors associats:
  - Estat físic
  - Versió de firmware
  - Validació de perfils d'usuari, permisos i sistemes d'autenticació biomètrica o per targeta.

- <u>Cartelleria</u>
  - Inventari complert de les ubicacions dels cartells.
  - Revisió dels cartells
  - Integritat física
  - Ubicació

- <u>Sistemes Pilones (PLC)</u>
  - Inventari complert de les ubicacions dels dispositius.
  - Integritat física
  - Ubicació
  - Càmera associada, si escau.

- Documentació i planificació
    - Elaboració d'un inventari digitalitzat en format Excel o base de dades, amb camp d'identificació únic per equip.
    - Incorporació de plànols actualitzats amb ubicació de càmeres, punts de connexió, servidors.
    - Reportatge fotogràfic de tots els sistemes objecte de aquest contracte.
    - Taula resum d'incidències, deficiències i propostes de correcció, classificades per nivell de criticitat (alta, mitjana, baixa).
    - Proposta d'un pla de manteniment i millora tecnològica de tots els elements objecte d'aquest contracte.

L'auditoria s'haurà de lliurar en format electrònic (PDF signat i fulls de càlcul editables), incloent-hi:

- Informe executiu amb conclusions generals, grau de compliment i recomanacions prioritzades.
- Annex tècnic detallat amb dades de tots els equips, proves realitzades i resultats.
- Plànols, gràfics i fotografies georeferenciades per a la identificació ràpida dels elements.

L'informe haurà d'estar validat pel responsable tècnic de l'adjudicatari i es lliurarà al responsable del contracte del BIT per a la seva aprovació.

Si el responsable del contracte de BIT ho considera oportú, es podran realitzar auditories ad hoc.

2.1.2. MANTENIMENT PREVENTIU

El manteniment preventiu té com a finalitat assegurar que totes les instal·lacions i equips de la xarxa de càmeres de videovigilància es trobin en òptimes condicions de funcionament, evitant avaries i allargant la seva vida útil. Aquest manteniment es realitzarà amb una periodicitat mínima de caràcter semestral (dues intervencions anuals) sobre totes les càmeres i els equips associats a la xarxa de videovigilància.

L'execució d'aquest servei tindrà com a referència tècnica els resultats de l'auditoria inicial. Aquesta periodicitat podrà incrementar-se si així ho determinen els resultats de l'auditoria inicial o les necessitats detectades durant el servei.

Tasques mínimes incloses dins del manteniment preventiu:

- Sistemes de videovigilància (CCTV)
  - Inspecció física:
    - Neteja d'òptiques, carcasses i proteccions.
    - Verificació de fixació, orientació, inclinació i focus.
    - Revisió d'estanquitat i protecció IP/IK.
    - Revisió de cablejat, connectors i punts d'alimentació PoE.
    - Comprovació de temperatura interna i ventilació.
    - Inspecció funcional:
    - Prova de visió diürna i nocturna, amb verificació de WDR i IR.
    - Comprovació de transmissió en temps real i latència del flux.
    - Validació de paràmetres de gravació (4K/10fps i 2K/8fps).
    - Verificació de sincronització horària i configuració de zones d'interès.
    - Reajustament de configuracions o neteja de memòries locals si cal.

- Servidors i emmagatzematge
  - Verificació de la integritat de discs durs i estat del RAID.
  - Comprovació del volum d'emmagatzematge disponible i temps de retenció real.
  - Revisió del rendiment d'escriptura/lectura per assegurar gravació contínua 4K.
  - Validació del correcte funcionament de SAIs i sistemes d'alimentació redundant.
  - Revisió de ventiladors, filtres, temperatura i senyals d'alarma.
  - Test de còpia de seguretat i recuperació (restore test).
  - Actualització de firmware i sistema operatiu, amb registre de versions.

- Sistemes de control d'accessos (CCAA)
  - Neteja i comprovació dels lectors i terminals biomètrics o de targeta.
  - Prova de lectura i autenticació d'usuaris.
  - Revisió de sincronització horària i registre d'esdeveniments.
  - Test de comunicació amb servidor i integració amb CCTV.
  - Verificació d'alimentacions, bateries i connexions.

  - Cartelleria

- Garantir el correcte estat i visibilitat de tota la cartelleria informativa vinculada al sistema de videovigilància, d'acord amb la normativa vigent.
- Neteja per assegurar-ne la llegibilitat.

- Sistemes de Pilones (PLC)
  - Garantir el correcte estat i funcionament del sistema.
  - Neteja i comprovació dels dispositius.
  - Verificació dels PLC, mòduls d'entrada/sortida i equips de comunicació.
  - Comprovació de les comunicacions amb els sistemes de supervisió i control.
  - Revisió d'alarmes, registres i esdeveniments del sistema.
  - Verificació de les seqüències d'accionament i dels mecanismes de seguretat de les pilones.
  - Comprovació de les còpies de seguretat i de la configuració dels equips.

- Documentació i planificació
  - Actualització d'inventaris, plànols i configuracions conforme als canvis detectats.
  - Revisió de coherència entre l'auditoria inicial i la situació actual.
  - Elaboració d'un informe de manteniment amb conclusions i recomanacions.

Després de cada actuació preventiva, l'adjudicatari haurà d'emetre **un Informe de Manteniment Preventiu**, que inclourà com a mínim:

- Data i ubicació de la intervenció.
- Relació detallada d'equips revisats.
- Tasques realitzades i resultats obtinguts.
- Estat general dels equips i anomalies detectades.
- Comparativa amb la línia base de l'Auditoria Inicial.
- Fotografies, gràfics o captures de proves.

Els informes es lliuraran en format digital (PDF signat) dins dels 10 dies posteriors a la intervenció i s'incorporaran al registre del contracte.

2.1.3. MANTENIMENT CORRECTIU

El manteniment correctiu té per objecte resoldre qualsevol incidència, avaria o anomalia detectada en el sistema objecte d'aquest contracte, restablint el servei en el menor temps possible i garantint la continuïtat de la gravació, la transmissió i la seguretat.

Aquest servei inclou tant les reparacions físiques, com la substitució temporal o definitiva dels equips avariats, i, quan sigui necessari, la incorporació de nous dispositius per substituir o ampliar el sistema, mantenint la compatibilitat amb la infraestructura existent.

Tipus d'avaria	Descripció
Crítica	Interrupció total o parcial del servei de gravació o transmissió en més de 5 càmeres en una agrupació
Important	Fallada parcial amb afectació moderada a la qualitat o cobertura en la transmissió o gravació de 2 a 5 càmeres en una única agrupació
Lleu	Pèrdua d'una càmera en una única agrupació

En cas d'avaries **crítiques i importants**, l'adjudicatari haurà d'activar un protocol d'intervenció d'emergència, amb disponibilitat tècnica immediata, mantenint un servei 24x7.

L'Ajuntament tindrà la potestat de modificar la classificació d'una avaria o incidència atenent a criteris operatius i de seguretat pública.
Tasques mínimes incloses dins del manteniment correctiu:

Recepció i registre

- Recepció de les incidències des de la plataforma Helpdesk que l'Ajuntament tingui activa en el moment de la posta en marxa del servei.
- Assignació de codi únic, prioritat i tècnic responsable.
- Comunicació immediata al responsable del contracte.

Diagnosi tècnica

- Anàlisi inicial remota (diagnosi VMS, ping, logs, etc.).
- En cas necessari, desplaçament tècnic per diagnosi in situ.

- Determinació de la causa arrel (elèctrica, òptica, de xarxa, programari o alimentació).
- Emissió d'informe de diagnosi i pla d'actuació amb terminis previstos.
- Coordinació, en cas necessari, amb el mantenidor de la plataforma VMS.

Intervenció tècnica

- Reparació física, substitució o reconfiguració segons la diagnosi.
- Instal·lació d'equip de substitució temporal si no és possible reparar immediatament o no hi ha stock del mateix element disponible. En aquest cas, l'adjudicatari haurà de córrer amb els costos derivats de la nova actuació per tornar a instal·lar l'equipament definitiu (operaris, grua, etc.).
- Validació de la compatibilitat amb la plataforma VMS.
- Actualització de configuracions i proves completes de gravació i visualització.

Validació i tancament

- Proves finals de transmissió, gravació, reproducció i alarmes.
- Validació pel responsable del servei del BIT.
- Actualització de la plataforma d'incidències i de l'inventari.
- Emissió d'informe complet amb causes, solucions, materials i temps d'intervenció.

L'adjudicatari haurà de mantenir un **estoc tècnic mínim disponible** per garantir la qualitat del servei i la substitució immediata de components objecte del contracte. Tots els equips de substitució temporal hauran de ser equivalents o superiors en prestacions i compatibles amb el sistema existent. L'adjudicatari dimensionarà l'estoc com ell consideri adient per assegurar un servei òptim en cas d'incidències.

Cada actuació correctiva, inclosa la substitució o incorporació d'equips, haurà d'estar documentada amb:

- Identificador de la incidència.
- Equip o ubicació afectada.
- Data, hora i tècnic actuant.
- Diagnosi, acció realitzada i materials emprats.
- Temps de resposta i resolució.
- Fotografies o captures de validació, si cal.

- Comparació amb l'auditoria inicial i estat previ.
- Vist i plau per part del responsable del servei del BIT.

Tota aquesta informació s'integrarà en la plataforma d'incidències, per permetre la traçabilitat completa del cicle de vida dels equips i la generació d'indicadors de rendiment (KPI).

2.1.3.1. Incorporació o substitució de nous dispositius

Quan sigui necessària la incorporació d'un nou dispositiu, ja sigui per substitució o per ampliació del parc de càmeres es requerirà:

- Informe tècnic justificatiu amb descripció del motiu i la ubicació.
- Autorització prèvia del responsable del contracte.
- Instal·lació i configuració, en coordinació amb qui sigui oportú, seguint els estàndards UNE-EN 50132-7 i el Reglament Electrotècnic de Baixa Tensió.
- Verificació d'integració i funcionalitat, comprovant transmissió, gravació, fps, resolució i sincronització horària.
- Actualització d'inventari, plànols i configuracions.
- Acta de verificació i recepció signada pel tècnic i el responsable municipal del contracte del BIT.
- Incorporació automàtica a l'inventari per al manteniment preventiu en revisions futures.

En el cas de noves incorporacions, la instal·lació inclourà la configuració de la càmera tant en termes de gestió dels requeriments d'informació necessaris a nivell de xarxa per configurar-la i donar-li connectivitat (IP, DNS, etc.) com en termes d'alta o coordinació necessària per incloure-la a la plataforma VMS que en aquell moment disposi l'Ajuntament de Barcelona. Un cop la càmera està configurada i compta amb connectivitat s'hauran de gestionar les configuracions següents:

- Emmascarament de les zones privades.
- Validació amb Guardia Urbana dels camps de visió.
- Coordinació per incloure l'element en els sistemes de monitorització de l'Ajuntament de Barcelona.
- AS-Built de la instal·lació i alta de la càmera (planimetries, imatges del prompter, paràmetres de configuració de les càmeres, etc.).,

2.1.4. SERVEI DE REPARACIÓ I GESTIÓ DE GARANTIES

El present servei té per objecte la gestió integral de totes les reparacions i substitucions d'equips, components i accessoris coberts per garantia de fabricant o proveïdor, així com la coordinació tècnica i logística necessària per garantir que qualsevol actuació en aquest àmbit es realitzi de manera eficient, documentada i sense interrupció del servei.

L'adjudicatari actuarà com a interlocutor únic davant fabricants i distribuïdors, assumint totes les gestions tècniques i administratives associades a les garanties dels equips instal·lats o subministrats dins l'àmbit del contracte.

El servei de reparació i gestió de garanties inclourà:

- Identificació i registre dels equips que es troben dins el període de garantia, d'acord amb la informació obtinguda en l'Auditoria Inicial i els inventaris actualitzats.
- Verificació de les condicions de garantia (temps, cobertura, modalitat i limitacions).
- Coordinació amb el servei tècnic autoritzat del fabricant o distribuïdor per a la reparació o substitució.
- Gestió completa de la logística de recollida, enviament, seguiment i restitució de l'equip afectat.
- Instal·lació i configuració de l'equip retornat o del nou subministrament.
- Instal·lació d'equips provisionals de substitució per garantir la continuïtat operativa mentre duri la reparació.
- Emissió d'informe final de reparació o substitució, amb indicació de les actuacions realitzades i del nou període de garantia resultant.
- Actualització de l'inventari i de l'historial de manteniment per a cada equip.
- Coordinació amb el mantenidor de la plataforma VMS per a validar el funcionament de l'equip reparat i la configuració realitzada.

Com a mínim, l'adjudicatari haurà de fer les següents tasques dins del procediment de gestió de les garanties.

- <u>Detecció i diagnosi:</u>
  - Quan una incidència afecti un equip en període de garantia, el tècnic designat haurà de confirmar la causa i verificar que la fallada està coberta pel fabricant.

- Comunicació i autorització:
  - L'adjudicatari informarà el responsable del contracte del BIT, indicant model, número de sèrie, descripció de la fallada i termini estimat de gestió. Cap tramesa o intervenció externa podrà realitzar-se sense aquesta comunicació prèvia.

- Tramitació amb el fabricant:
  - L'adjudicatari realitzarà la sol·licitud de reparació o substitució al servei tècnic autoritzat, assegurant el compliment de les condicions de garantia i el subministrament d'equips equivalents o superiors.

- Equip provisional:
  - En cas que la reparació o substitució no pugui efectuar-se dins dels terminis de manteniment correctiu, s'instal·larà un equip provisional de substitució per garantir la continuïtat del servei.

- Reinstal·lació i validació:
  - Un cop reparat o substituït, l'equip serà reconfigurat i integrat al sistema, verificant la seva plena operativitat (imatge, gravació, connexió i configuració). En cas de que l'equip que s'hagi posat no sigui provisional i sigui definitiu, l'equipament passarà a formar part de l'estoc per quan el servei ho requereixi. Sempre que s'hagi validat que el seu funcionament és correcte.

- Documentació:
  - Tota gestió quedarà registrada mitjançant un informe de gestió de garantia, que inclourà el número de sèrie, fabricant, data d'enviament i de retorn, descripció de l'avaria i validació final del seu funcionament.

A més, l'adjudicatari haurà de garantir la traçabilitat completa de cada equip durant tot el procés i en cas que un fabricant o proveïdor no compleixi els terminis o subministri un equip no equivalent, l'adjudicatari haurà d'assumir la responsabilitat de garantir la continuïtat del servei i la integritat funcional del sistema.

2.1.5. SERVEI DE SUPORT I GESTIÓ D'INCIDÈNCIES (HELPDESK)

El servei de suport i gestió d'incidències té per objecte garantir un sistema d'atenció tècnica permanent, centralitzat i estructurat que permeti registrar, analitzar,

prioritzar, atendre i resoldre de manera eficient totes les incidències que afectin la xarxa de càmeres de videovigilància i els seus components complementaris, incloent-hi els equips de camp, els servidors d'enregistrament objecte d'aquest contracte i el sistema de control d'accés amb el software associat.

L'adjudicatari rebrà i gestionarà totes les incidències mitjançant l'eina corporativa de gestió d'incidències que el BIT tingui activa en el moment de la posta en marxa del servei, que actuarà com a plataforma única de registre, control i seguiment del mateix.

El servei pot requerir la coordinació directa amb la resta de serveis de manteniment municipals i amb els equips tècnics municipals implicats, com podem ser: servei d'enllumenat, d'urbanisme, espai urbà, etc., per tal de garantir una resposta àgil, eficient i alineada amb els procediments corporatius.

Característiques del servei (Helpdesk):

- Horari d'atenció ordinària: de dilluns a divendres, de 8:00 h a 18:00 h.
- Servei d'urgències 24x7 per a incidències crítiques i importants.
- Temps de resposta: El temps de resposta estarà determinat pel nivell de gravetat de la incidència.
- Atenció multicanal:
    - Telèfon directe.
    - Accés remot de l'empresa al sistema de gestió d'incidències del BIT.
    - Correu electrònic o sistema de ticketing per a incidències o consultes generals.

El BIT facilitarà a l'adjudicatari els permisos i credencials necessaris per accedir al sistema corporatiu de gestió d'incidències, garantint en tot moment la seguretat, la traçabilitat i la confidencialitat de la informació.

2.1.6. SERVEI DE REPORTING

Aquest servei té per objecte establir un sistema de seguiment, control i comunicació periòdica que permeti al BIT conèixer, de manera objectiva i verificable, l'estat real del sistema de videovigilància i l'eficiència del servei prestat per l'adjudicatari.

L'adjudicatari haurà d'elaborar els següents informes:

Tipus d'informe	Freqüència	Contingut principal
Informe mensual	Cada mes	Seguiment operatiu del servei, incidències i tasques realitzades.
Informe Semestral	Cada 6 mesos	Avaluació global de qualitat, fiabilitat i evolució tècnica.
Informe Anual	Un cop a l'any	Síntesi general, valoració de rendiment i propostes de millora.

A més, el BIT podrà sol·licitar informes específics o extraordinaris en cas d'incidències greus, canvis tecnològics o revisions internes.

Tots els informes hauran de contenir, com a mínim:

- Dades generals del servei: període, ubicacions i volum d'equips revisats.
- Resum d'activitats:
  - Manteniment preventiu: tasques executades, resultats i anomalies detectades.
  - Manteniment correctiu: incidències ateses, temps de resposta i resolució, peces substituïdes i equips nous incorporats.
- Indicadors de rendiment (KPI):
  - Taxa de resolució en primer nivell, segon nivell o tercer nivell.
  - Temps mitjà de resposta per severitat.
  - Temps mitjà de resolució per severitat.
  - Volum de tiquets gestionats mensualment.
  - Índex de reincidència d'avaries.
  - Percentatge d'incidències resoltes dins dels terminis ANS.
- Compliment dels terminis i de la qualitat del servei.
- Anàlisi de desviacions respecte a la línia base (auditoria inicial).
- Propostes de millora: optimització tècnica, actualitzacions de programari, substitució d'equips obsolets, mesures d'eficiència energètica, entre d'altres.
- Conclusions i recomanacions: valoració qualitativa del servei i accions previstes pel següent període.

Els informes s'entregaran en format electrònic (PDF signat digitalment pel responsable del servei) per a la seva integració en els sistemes de gestió del BIT.

Els terminis de lliurament seran:

- Informe mensual: dins dels cinc (5) primers dies hàbils del mes següent.

- Informe semestral: dins dels quinze (15) dies següents al període corresponent.
- Informe anual: dins del primer mes del nou exercici.

2.1.7. SERVEI D'ACTUALITZACIÓ DE LA INFORMACIÓ I INVENTARI

El servei d'actualització de la informació i inventari té per objecte mantenir, durant tota la vigència del contracte, la traçabilitat, la coherència i la vigència de la informació tècnica, documental i gràfica del conjunt d'equips i instal·lacions que conformen el sistema de videovigilància (CCTV) i control d'accessos (CCAA).

L'objectiu és disposar en tot moment d'un registre actualitzat i verificat que permeti a l'Ajuntament conèixer de manera precisa:

- Quins equips existeixen.
- On estan ubicats.
- Quin és el seu estat funcional.
- Quines intervencions s'hi han realitzat.

L'actualització de la informació inclourà:

- Actualització immediata de l'inventari després de qualsevol actuació de manteniment preventiu, correctiu o incorporació de nous equips.
- Manteniment dels plànols de connectivitat de les instal·lacions actuals i/o noves.
- Incorporació de canvis de configuració, ubicació o número de sèrie.
- Gestió de versions dels fitxers tècnics i còpies de seguretat documentals.
- Revisió semestral completa d'inventari i documentació.
- Integració amb la base de dades de l'auditoria inicial per garantir la traçabilitat històrica.

L'inventari haurà d'estar disponible en format digital editable (p.ex: Excel) i compartit amb el responsable de contracte del BIT. Haurà d'incloure, com a mínim, les següents dades per a cada element:

- Codi d'identificació únic.
- Tipologia d'equip (càmera, servidor, switch, lector, etc.).
- Marca, model i número de sèrie.
- Ubicació exacta (edifici, planta, zona).

- Estat funcional (operatiu, avariat, substituït, en garantia).
- Data d'instal·lació o d'última intervenció.
- Responsable tècnic o empresa subministradora.
- Data i tècnic de la darrera revisió preventiva.
- Referència a informes associats (preventiu, correctiu o garantia).

A més, haurà d'incloure una versió gràfica complementària, en format CAD o GIS, que mostri la ubicació de càmeres i equips principals sobre plànols d'edificis o mapes de la via pública.

Com a mínim, cada semestre l'adjudicatari haurà de lliurar una versió actualitzada de l'inventari i de la documentació tècnica, que substituirà l'anterior com a referència oficial del contracte, i que haurà de ser validada pel responsable de contracte del BIT.

L'empresa adjudicatària serà responsable de garantir la seguretat, la confidencialitat i la custòdia de tota la informació gestionada, especialment aquella sensible relacionada amb la seguretat.

En finalitzar el contracte, l'adjudicatari haurà d'entregar al BIT tota la documentació i inventari actualitzats en format digital, degudament estructurats i organitzats segons criteris arxivístics normalitzats que en facilitin la consulta i la conservació.

2.1.8. REUNIONS DE SEGUIMENT

Les reunions de seguiment tècnic tenen com a finalitat garantir una coordinació fluïda entre el BIT i l'adjudicatari, afavorir la millora contínua del servei i assegurar el compliment dels objectius de qualitat, seguretat i disponibilitat establerts al present Plec.

Aquestes reunions són un element essencial per garantir la traçabilitat i transparència en la prestació del servei, així com per facilitar una comunicació fluïda i coordinada entre les parts.

Tipus de reunió	Freqüència	Contingut principal
Mensual	Cada mes	Revisió operativa i incidències obertes i tancades durant el mes.
Semestral	Cada 6 mesos	Avaluació global de qualitat, fiabilitat i evolució tècnica del servei.

Extraordinària	Quan sigui necessari	Resolució d'incidències crítiques.

El BIT podrà convocar reunions addicionals en funció de necessitats específiques.

De cada reunió, l'adjudicatari realitzarà un acta formal, signada pel responsable del contracte del BIT i pel responsable de l'adjudicatari, que haurà d'incloure:

- Ordre del dia i temes tractats.
- Acords adoptats i decisions tècniques.
- Responsables assignats i terminis d'execució.
- Resultats d'indicadors i propostes de millora.

Les actes s'incorporaran al registre documental del contracte i seran de compliment obligatori per a l'adjudicatari en els terminis establerts.

L'adjudicatari serà responsable de:

- La direcció global extrem a extrem de les tasques del contracte.
- La interlocució amb la direcció responsable del servei del BIT.
- La coordinació dels diferents actors que intervenen al contracte.
- La supervisió i seguiment de les tasques detallades en aquest plec.

També serà responsable de dotar el servei amb els recursos adients, tant humans com materials, que permetin el correcte desenvolupament de les tasques necessàries.

3. FASES DE PRESTACIÓ DEL SERVEI

L'adjudicatari haurà de desenvolupar un pla detallat que tingui en compte les característiques i fases específiques que es detallen a continuació:

- **Prestació actual**: en aquesta fase opera únicament l'adjudicatari actual.
- **Execució**: un cop finalitzi la fase de transició, l'adjudicatari haurà de prestar el servei amb el nivell de servei requerit al present plec.
- **Devolució:** La devolució és el període final del contracte en què l'adjudicatari sortint ha de garantir la correcta transferència del servei, dels coneixements i dels actius associats al mateix, assegurant la continuïtat operativa i minimitzant qualsevol impacte en la prestació.

  Durant la fase de devolució es duran a terme les següents activitats:

  - **Transició**: és el període que va entre l'entrada en vigor del contracte i la presa de control del servei per part del nou adjudicatari.

    Durant la transició es duran a terme les següents activitats:

    - **Transferència**: El nou adjudicatari rebrà suport dels adjudicataris actuals, que facilitaran i col·laboraran en el traspàs de coneixement així com en l'habilitació de l'operació. En aquest moment, l'adjudicatari actual continua realitzant la prestació del servei i assolint els ANS actuals. Aquesta fase tindrà una duració màxima de 3 setmanes.
    - **Prestació en transició**: El nou adjudicatari comença a prestar el servei amb els seus propis mitjans, encara que els ANS segueixen sent els de la prestació actual.

3.1. INICI DEL CONTRACTE

Aquest contracte tindrà vigència des del dia1 d'abril de 2027 o del dia següent a la seva formalització, si aquesta fos posterior.

Tal com s'ha indicat als antecedents del contracte, aquest servei dona continuïtat a altres contractes actualment vigents. En conseqüència, a l'inici del contracte s'establirà un període de transició amb l'adjudicatari sortint, durant el qual es produirà un solapament en la prestació del servei.

Durant aquest període, l'adjudicatari sortint haurà de facilitar el traspàs de coneixement necessari sobre el parc d'instal·lacions, els sistemes en servei i els

processos operatius, amb la finalitat de garantir la continuïtat del servei i permetre la correcta presa de control per part del nou adjudicatari.

3.2. FASE D'EXECUCIÓ

La fase d'execució s'inicia a la finalització de cada un dels trams de la fase de transició i s'estén fins a la devolució.

Un cop finalitzada la fase de transició i verificat pel responsable de contracte que el nou adjudicatari està en condicions de prestar el servei amb garanties, s'inicia aquesta etapa, durant la qual l'adjudicatari assumeix la responsabilitat total del servei de manteniment de la xarxa de càmeres de videovigilància i dels seus components complementaris.

En aquesta fase, l'adjudicatari haurà de garantir el compliment estricte dels Acords de Nivell de Servei (ANS) definits, mantenint sempre la màxima disponibilitat de la xarxa de càmeres de videovigilància.

Durant la fase d'execució, l'adjudicatari haurà d'organitzar els seus recursos humans i materials de manera que pugui respondre amb agilitat a totes les incidències i necessitats operatives del servei. Això implica disposar d'equips tècnics capacitats per realitzar actuacions de camp sobre tot l'equipament objecte del present contracte. Igualment, haurà de mantenir disponible un estoc suficient de recanvis i equips provisionals que permetin la substitució immediata d'elements que provoquin incidències crítiques.

3.2.1. LLOC DE PRESTACIÓ DEL CONTRACTE

El contracte es prestarà principalment a les oficines de l'empresa adjudicatària.

Sense perjudici de l'anterior, i en funció de les necessitats del servei, l'òrgan responsable del contracte podrà requerir puntualment la presència d'un o més membres de l'equip adscrit al contracte a:

- Les dependències del BIT, i/o
- Les diferents dependències municipals de l'Ajuntament de Barcelona que disposin de sistemes de videovigilància objecte del contracte, incloent-hi edificis, instal·lacions, equipaments municipals i centres de treball dels òrgans i serveis usuaris, i/o

- Emplaçaments situats a la via pública on hi hagi instal·lats sistemes de videovigilància municipals, principalment càmeres de seguretat ciutadana.

Aquesta presència podrà ser necessària per a tasques de coordinació, suport tècnic, verificació d'incidències, actuacions de manteniment preventiu o correctiu, validacions in situ, o qualsevol altra activitat directament relacionada amb l'objecte del contracte.

3.2.2. HORARI DE LA PRESTACIÓ DELS SERVEIS

L'horari ordinari de prestació del servei serà de 10 × 5, de dilluns a divendres, entre les 08.00 h i les 18.00 h, incloent totes les activitats de manteniment preventiu, correctiu programat i suport tècnic associades al contracte. Aquest horari garanteix la cobertura de la càrrega de treball habitual i l'atenció de les incidències que no afecten de manera directa l'operativitat dels sistemes.

Tanmateix, i d'acord amb els criteris de criticitat establerts al plec vigent, les incidències classificades com a crítiques o importants, és a dir, aquelles que impacten de manera significativa en la funcionalitat dels sistemes de videovigilància, hauran de tenir un servei d'atenció 24x7 i poder ser ateses amb disponibilitat 24 × 7, incloent diagnosi remota i desplaçament tècnic immediat quan sigui necessari, per tal de preservar la continuïtat del servei i la seguretat operativa.

3.2.3. IDIOMA

Obligatòriament l'adjudicatari desenvoluparà el servei en català.

Això inclou també la documentació de gestió, la documentació tècnica requerida i lliurada durant l'execució del servei.

3.3. PLA DE CONTINGÈNCIA

El Pla de Contingència és el mecanisme que ha de garantir la continuïtat i estabilitat del servei davant situacions excepcionals que puguin comprometre el funcionament de la xarxa de càmeres de videovigilància. El seu objectiu és assegurar que qualsevol fallada greu és gestionada de manera immediata, coordinada i eficient, evitant interrupcions del servei i assegurant en tot moment la disponibilitat operativa de les càmeres en la mida que sigui possible per tot allò que estigui a l'abast de l'adjudicatari.

Aquest pla haurà de contemplar tots els escenaris de risc identificats. L'adjudicatari haurà d'establir procediments d'actuació clars, definint rols, responsables, circuits d'escalat i mesures immediates per minimitzar l'impacte, d'acord amb els criteris de seguretat i operativitat.

El Pla de Contingència haurà d'incorporar la disponibilitat immediata d'un estoc mínim de recanvis crítics (càmeres i elements associats que es decideixi al inici del contracte), així com la capacitat de desplegar equips provisionals per garantir la continuïtat del servei en punts sensibles. Igualment, haurà d'establir els procediments per a la restauració del servei, incloent la coordinació adient amb la plataforma de videovigilància, la validació de gravació i visibilitat, i la verificació final de tot.

Tota activació del Pla de Contingència requerirà la generació d'un informe tècnic complet, que inclogui la causa de la incidència, les mesures adoptades, el temps de recuperació i les accions preventives proposades, mantenint la traçabilitat i coherència documental.

3.4. PLA DE DEVOLUCIÓ DEL SERVEI

El Pla de Devolució del Servei té com a finalitat assegurar una finalització ordenada, transparent i sense interrupcions del contracte, garantint que la xarxa de càmeres de videovigilància i tots els components associats continuen operatius i plenament funcionals un cop l'adjudicatari finalitzi la seva prestació. Aquesta fase constitueix un moment crític per a la preservació de la continuïtat del servei, la integritat de la informació i la transferència de coneixement cap al futur adjudicatari o cap al BIT i s'ha d'executar amb el mateix rigor i professionalitat que la fase d'entrada al servei.

L'adjudicatari haurà de presentar aquest pla amb una antelació mínima de tres mesos abans de la data de finalització del contracte, per tal que BIT pugui revisar-lo, validar-lo i, si escau, requerir ajustos o ampliacions. Durant aquesta fase, l'adjudicatari continuarà sent responsable de la prestació del servei i del compliment dels ANS fins al moment exacte de la finalització contractual.

El procés de devolució s'iniciarà amb una revisió conjunta, entre BIT i l'adjudicatari, de l'estat general de les càmeres i de tots els components complementaris. A més l'inventari haurà d'estar completament actualitzat i reflectir fidelment a la realitat de totes les càmeres i equips complementaris. Aquest inventari haurà d'incloure informació sobre ubicacions exactes, funcionalitat, numeració física, estat operatiu i qualsevol incidència rellevant detectada durant el contracte.

L'adjudicatari haurà de lliurar totes les configuracions i còpies de seguretat necessàries perquè el sistema pugui continuar operant sense interrupció.

També serà necessari lliurar un històric complet de les incidències i manteniments realitzats durant la vigència del contracte, incloent l'estat de resolució de cadascuna, les reparacions efectuades, els equips substituïts, les incidències recurrents i qualsevol actuació de caràcter crític.

En paral·lel, l'adjudicatari haurà d'elaborar un Informe final de situació, que descrigui l'estat general del servei en el moment de la finalització del contracte i el nivell de compliment dels ANS.

Si durant la vigència del contracte l'adjudicatari ha rebut material o equipament propietat del BIT, aquest haurà de ser retornat en perfectes condicions, acompanyat d'un inventari signat i validat per ambdues parts. Qualsevol equip substituït o retirat haurà d'estar documentat amb correspondència precisa i rastreig d'intervenció.

Durant la fase de devolució es duran a terme les següents activitats:

PLA DE TRANSICIÓ DEL SERVEI

El Pla de Transició té per finalitat garantir una presa de control ordenada, segura i sense interrupcions del servei per part del nou adjudicatari, assegurant la continuïtat operativa de la xarxa de càmeres de videovigilància i de tots els sistemes i infraestructures associades. Aquesta fase, amb una durada màxima de sis setmanes des de la data d'adjudicació del contracte, constitueix un període crític en què es duen a terme totes les activitats necessàries perquè el nou adjudicatari disposi del coneixement, els recursos, els accessos i les capacitats operatives imprescindibles per iniciar la prestació del servei amb garanties plenes.

Durant la transició, l'adjudicatari sortint manté íntegrament la prestació del servei i el compliment dels ANS vigents, mentre que el nou adjudicatari es va incorporant progressivament a les tasques de coneixement i preparació operativa. Aquesta convivència temporal garanteix que no hi hagi cap afectació sobre la disponibilitat del sistema ni sobre la seguretat de les instal·lacions. El Pla de Transició haurà d'estar degudament planificat i aprovat per BIT abans de la seva execució i haurà d'incloure, com a mínim, les activitats següents:

Coordinació inicial i definició de rols

- Reunió d'inici entre BIT, l'adjudicatari sortint i el nou adjudicatari per establir el calendari de treball, els interlocutors tècnics i operatius i els canals oficials de comunicació.
- Definició dels responsables de cada línia d'activitat: xarxa, servidors, VMS, manteniment de camp i Helpdesk.
- Validació del procediment de seguiment, informes preliminars i metodologia de comunicació de riscos.

Transferència de coneixement i informació tècnica

L'adjudicatari sortint haurà de facilitar al nou adjudicatari tota la informació necessària per garantir una transició completa i segura, incloent:

- Estat actual de les càmeres, servidors, dispositius de xarxa i alimentació.
- Configuracions detallades del VMS (perfils d'imatge, retencions, alarmes, llicències, mapes i canals).
- Informació sobre topologia de xarxa, enllaços LAN-to-LAN, punts d'accés i infraestructura física, si cal.
- Històrics d'incidències, avaries recurrents, manteniments pendents i punts crítics detectats.
- Informació sobre equips en garantia o en procés de substitució.

Aquesta activitat inclourà sessions tècniques, reunions operatives i visites conjuntes a les instal·lacions més rellevants.

Validació d'inventaris i comprovació sobre el terreny
Durant la transició, el nou adjudicatari haurà de:

- Validar l'inventari proporcionat, comprovant-lo sobre el terreny.
- Verificar la identificació física de càmeres, components de xarxa, armariades i punts de connexió.
- Comprovar l'estat real del cablejat, alimentacions, SAIs i elements estructurals que puguin ser objecte del contracte o puguin afectar als sistemes.
- Detectar possibles desviacions entre inventaris i situació real.

Aquesta validació serà una base essencial per a l'auditoria inicial que es realitzarà posteriorment.

Habilitació d'accessos i integració amb els sistemes corporatius
BIT facilitarà al nou adjudicatari:

- Les credencials i permisos per accedir al sistema corporatiu de gestió d'incidències (Helpdesk).
- Els permisos per accedir a la plataforma VMS, tant a nivell de supervisió com de configuració tecnològica.
- L'accés segur als servidors d'enregistrament, estacions de visualització, videowalls i eines de control operatiu, en cas necessari.
- Els permisos per accedir als edificis, sales tècniques, quadres de comunicacions i espais on hi hagi equipament objecte d'aquest plec.

Coordinació entre adjudicataris per a la continuïtat del servei
El Pla de Transició haurà de contemplar un acompanyament operatiu entre l'adjudicatari sortint i el nou adjudicatari per:

- Compartir criteris d'atenció d'incidències i gestió de talls de servei.
- Revisar la configuració dels equips considerats més crítics.
- Garantir que qualsevol incidència durant la transició es gestiona responsablement i sense impacte a la xarxa de càmeres de videovigilància.

Validació tècnica del sistema durant la transició
Abans de finalitzar el període de transició, el nou adjudicatari haurà de validar:

- que totes les càmeres es visualitzen i enregistren correctament al VMS.
- que els servidors compleixen amb els paràmetres d'ús, rendiment i retenció.
- que el Helpdesk funciona correctament com a plataforma única de registre i comunicació
- que no hi ha alarmes actives no resoltes o incidències recurrents pendents.

Aquesta validació s'haurà de documentar i comunicar al responsable de contracte del BIT.

El Pla de Transició finalitzarà quan BIT consideri que el nou adjudicatari disposa de tota la informació, accés i capacitat necessàries per assumir la prestació del servei amb garanties, i sempre que la continuïtat operativa del sistema estigui degudament

assegurada. Aquesta validació s'acreditarà mitjançant una acta formal de finalització de la transició.

El pla de transició consta de 2 parts: transferència del servei i prestació en transició.

Transferència del servei

El Pla de Transferència del Servei té per objecte assegurar el traspàs ordenat, complet i fiable de tota la informació tècnica, documental i operativa necessària perquè el nou adjudicatari pugui assumir el servei de manteniment de la xarxa de càmeres de videovigilància amb garanties des del primer dia. Aquest procés constitueix una etapa crítica dins la fase de transició i assegura que el coneixement necessari per a la prestació del servei no es perd ni queda fragmentat, preservant la continuïtat operativa.

El Pla de Transferència s'executarà durant les tres primeres setmanes de la fase de transició i es realitzarà amb la col·laboració directa entre el BIT, l'adjudicatari sortint i el nou adjudicatari.

La transferència s'iniciarà amb una reunió tècnica específica convocada pel responsable del contracte, on s'establiran els continguts, el calendari i la metodologia de les sessions de traspàs. Aquesta reunió definirà els interlocutors responsables de cada àmbit i fixarà els criteris de qualitat i validació de la informació que s'haurà de lliurar.

En el marc del Pla de Transferència, l'adjudicatari sortint facilitarà tota la informació operativa associada al servei, incloent-hi l'estat actual de cada càmera i equips complementaris, plànols, el detall de les configuracions de les càmeres, entre d'altres que puguin ser necessaris.

Un element fonamental del Pla de Transferència és la validació d'inventaris. L'adjudicatari sortint entregarà l'inventari més recent, però el nou adjudicatari haurà de verificar-lo sobre el terreny mitjançant inspecció física dels equips, comprovació de numeracions, etiquetatge i ubicacions.

El Pla de Transferència també inclourà la cessió estructurada de la documentació relativa a incidències recurrents, avaries crítiques, treballs pendents, mesures correctives aplicades i recomanacions del servei sortint.

Paral·lelament, es realitzaran sessions d'acompanyament tècnic en què els equips de manteniment del servei sortint mostraran sobre el terreny la ubicació de les instal·lacions més rellevants, punts de connexió, armaris, alimentacions, SAIs, suports, racks i sistemes associats. Tot aquell equipament vinculat a la xarxa de càmeres de videovigilància objecte d'aquest contracte.

Un dels aspectes més importants del Pla de Transferència és la habilitació i comprovació dels accessos als sistemes corporatius, incloent el Helpdesk municipal i la plataforma VMS. El nou adjudicatari haurà de validar que pot:

- gestionar incidències al sistema corporatiu.
- accedir a la plataforma VMS amb els rols assignats.
- visualitzar i gestionar càmeres, configuracions i servidors.
- consultar alarmes, reproduccions i arxius.
- accedir als servidors físics o virtuals necessaris per al servei.

Aquesta validació d'accessos s'haurà de completar dins la fase de transferència i és imprescindible per iniciar la fase posterior de prestació en transició.

Finalment, el Pla de Transferència haurà de concloure amb la redacció d'un informe de transferència, aprovat pel responsable de contracte, que reculli:

- la documentació tècnica rebuda.
- els inventaris validats.
- els accessos habilitats.
- les sessions d'acompanyament realitzades.
- els punts crítics detectats.

Prestació en Transició

La Prestació en Transició és la fase en què el nou adjudicatari inicia la prestació efectiva del servei amb els seus propis mitjans, mentre es consoliden les eines, els processos i les coordinacions necessàries per garantir una assumpció plena i estable del contracte. Aquesta fase té una durada màxima de tres setmanes.

Durant aquesta etapa, el nou adjudicatari és el responsable únic del servei i ha de garantir que totes les actuacions es realitzen amb la màxima diligència, utilitzant els sistemes corporatius establerts pel BIT.

Aquesta fase actua com un període d'estabilització on els ANS es mantenen en el nivell actual però no s'aplica el règim de penalitzacions, sempre que l'adjudicatari acrediti actuació diligent i sense afectació significativa al servei. Durant aquest temps, l'adjudicatari haurà de validar:

- la correcta configuració de totes les càmeres.
- la documentació adquirida relativa al servei.
- la correcta operativa del Helpdesk.

Garantia de nivell de servei durant la transició

Durant tota la fase de transició, tant en el període de transferència com en la prestació en transició, l'adjudicatari haurà de garantir el manteniment del nivell de servei, assegurant que la disponibilitat, fiabilitat, seguretat i qualitat de les càmeres de videovigilància no es veuen alterades per cap de les activitats associades al canvi d'adjudicatari.

En aquesta etapa, les càmeres i els seus elements complementaris han de mantenir-se plenament funcionals, sense degradació en la captació, transmissió, gravació o retenció de les imatges. Les incidències crítiques i importants hauran d'atendre's i resoldre's dins els temps establerts pels ANS vigents, i totes les actuacions hauran de quedar registrades al la eina de gestió d'incidències, garantint la traçabilitat i supervisió per part del responsable del contracte.

Així mateix, qualsevol desviació operativa, risc o incidència rellevant detectada durant el procés haurà de ser comunicada immediatament al responsable del contracte amb el seu pla d'acció proposat.

4. MODEL DE PRESTACIÓ DEL SERVEI

4.1. MODEL DE RELACIÓ BIT/ADJUDICATARI

L'adjudicatari, durant els primers quinze dies naturals, a comptar des de l'inici del contracte, en base al seu model organitzatiu, dissenyarà de la manera més exhaustiva possible un model de relació amb el BIT, dissenyat de manera que s'asseguri el correcte acompliment de les seves funcions. L'esmentat model de relació haurà de fer explícita l'estructura i el funcionament dels comitès de relació i coordinació que siguin precisos per a mantenir una interlocució permanent amb els actors involucrats en el procés.

Tots els comitès hauran de poder ser gestionats mitjançant una eina de gestió configurada i mantinguda per l'adjudicatari, accessible des d'Internet, amb autentificació i complint la normativa de seguretat municipal definida pel BIT, possibilitant la generació, publicació de l'acta per part de l'adjudicatari, que haurà de ser validada pel responsable del contracte, en base a la proposta organitzativa.

El model de govern del servei i el contracte hauran d'ajustar-se als requisits mínims que s'especifiquen als següents apartats.

Pel correcte funcionament del servei, cal definir un marc de governança que ajudi a tenir diferents espais d'interlocució per l'equip del servei i interessats, contant també amb les eines per reportar, fer seguiment i presa de decisions.

Hi haurà d'haver, com a mínim, els següents comitès, permetent les agrupacions coherents entre comitès:

COMITÈ DE DIRECCIÓ

Les funcions del Comitè de Direcció són les d'inspeccionar la marxa del servei i prendre les decisions oportunes per adaptar i millorar aquells aspectes que afecten l'objectiu i abast d'aquest.

El Comitè de Direcció tindrà les següents atribucions:

- Validar la planificació del servei i els calendaris d'execució.
- Aprovar formalment els lliurables i informes de seguiment.
- Autoritzar les fites de facturació segons el grau d'execució.
- Fer seguiment del servei en temps, cost i abast, incloent l'estat dels sistemes crítics.
- Gestionar riscos i definir mesures correctores.
- Prendre decisions contractuals relatives a modificacions, ampliacions o incidències greus.
- Validar el compliment dels Acords de Nivell de Servei (ANS) establerts al contracte.
- Impulsar millores evolutives per garantir la continuïtat i l'eficiència del servei.

El Comitè de Direcció es reuneix cada mes així com en els moments d'assoliment de cadascuna de les fites, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

Els components mínims del Comitè seran:

- Responsable del contracte de l'adjudicatari.
- Responsable del contracte per part del BIT.
- Representant de l'Ajuntament (Gerència d'Àrea de Seguretat, Prevenció i Convivència).
- Altres assistents que BIT estimi oportuns.

L'adjudicatari serà el responsable de l'elaboració de la documentació de seguiment del contracte i del servei i també d'aixecar l'acta de les reunions.

Es consideraran reunions del Comitè de Direcció les reunions de llançament i tancament del servei.

La reunió de llançament o Kick-Off tindrà, com a mínim, els següents objectius:

- Presentar la planificació del servei.
- Presentar l'Equip del servei.
- Presentar el Pla de Riscos del servei.
- Identificar dependències, integracions i recursos.
- Consensuar el model de seguiment del servei.

La reunió de tancament tindrà els següents objectius:

- Validar l'entrega de tots els lliurables contractats.
- Confirmar la satisfacció del client amb el servei prestat.
- Documentar evolutius i millores per a futures licitacions o manteniments.

COMITÈ DE CRISI

En cas que el BIT ho consideri necessari es podrà convocar un Comitè de Crisi. L'objectiu d'aquest comitè serà la posada en comú i solució d'una problemàtica o situació crítica.

La sol·licitud del Comitè de Crisi la realitzarà únicament el BIT, qui establirà els assistents, l'hora i localització de la reunió, així com l'agenda i punts a tractar.

Aquest comitè es podrà convocar amb una antelació mínima de 4 hores a l'adjudicatari. El Comitè de Crisi s'anirà reunint amb la periodicitat que estableixi el BIT mentre duri la contingència.

Li corresponen al Comitè de Crisi les funcions de:

- Analitzar el problema o situació i establir-ne la gravetat.
- Definir un pla de contingència per a la resolució immediata de la situació i fer seguiment.
- Definir un pla d'acció, si escau, per implantar mesures que impedeixen que el problema o situació torni a succeir i fer seguiment.
- Designar els responsables de l'execució de les accions definides.
- Designar els responsables encarregats de fer una investigació del succés i fer seguiment.
- Si fossin necessàries, definir les penalitzacions a aplicar sobre els responsables del succés.
- Establir les responsabilitats.

Li correspon al responsable de l'empresa adjudicatària la preparació de la documentació necessària per a la realització del Comitè de Crisi i aixecar acta dels temes i acords de la reunió.

SEGUIMENT OPERATIU DEL SERVEI

El proveïdor estarà obligat a proporcionar al BIT i als seus òrgans de gestió tota la informació relativa a l'estat real del servei sempre que sigui requerit.

4.2. MODEL DE GESTIÓ D'INCIDÈNCIES

El model de gestió d'incidències al manteniment correctiu com a mínim, ha de considerar 3 nivells:

- Nivell 1: Registre d'incidències mitjançant el servei corporatiu d'incidències (aquest nivell és proveeix des del BIT i serà qui escali els incidents a l'adjudicatari sense cap mena de diagnòstic).
- Nivell 2: Anàlisi i diagnòstic inicial de la incidència per part de l'adjudicatari. En cas necessari, també el suport superior i resolució remota.
- Nivell 3: Derivació a tècnics de camp per part de l'adjudicatari.

El seu objectiu principal és garantir una atenció eficient i escalonada, assegurant la restauració ràpida dels serveis afectats i la correcta traçabilitat del procés.

Per tal d'assegurar el correcte funcionament del servei de gestió d'incidències, i garantir una operativa homogènia i alineada amb els procediments corporatius, el responsable del contracte del BIT coordinarà i gestionarà les sessions de formació necessàries relatives a:

- L'eina corporativa de registre i seguiment d'incidències, que constitueix el mecanisme oficial de comunicació, classificació, assignació i tancament de totes les incidències del servei.
- La plataforma VMS (Vídeo Management System) que estigui en funcionament en el moment de l'execució del contracte.

Aquestes formacions tenen com a objectiu assegurar que el personal adscrit per l'adjudicatari:

- Coneix i utilitza adequadament les eines corporatives, garantint la traçabilitat completa de totes les actuacions i el compliment dels protocols de resolució establerts.
- Disposa de competències tècniques suficients per dur a terme una resolució remota eficient de les incidències, minimitzant desplaçaments innecessaris i reduint els temps de resposta i resolució.
- S'integra de manera fluida en els fluxos de treball corporatius, mantenint la coherència operativa entre tots els equips municipals implicats en la gestió de la videovigilància i la seguretat.

Així mateix, i sempre que sigui necessari, el coordinador del servei de l'adjudicatari haurà de garantir l'assistència del seu personal a les formacions convocades.

4.3. ACORDS DE NIVELL DE SERVEI

L'empresa adjudicatària haurà de complir amb uns Acords de Nivell (ANS) mínims de servei que garanteixin la qualitat i eficiència en la gestió de les incidències i peticions. Aquests ANS s'aplicaran al conjunt del servei, incloent suport remot i presencial, i es calcularan mensualment:

Tipus d'avaria	Temps màxim de resposta	Temps màxim de resolució	Disponibilitat del servei	Percentatge mínim de compliment
Crítica	< 4 hores	< 8 hores	24x7	99%
Important	< 12 hores	< 48 hores	24x7	95%
Lleu	Següent dia hàbil	< 7 dies	Següent dia hàbil	90%

La definició d'incidència crítica, important o lleu es troba a l'apartat 2.1.3. Manteniment correctiu.

Els següents indicadors clau de rendiment seran mesurats de forma mensual i inclosos als informes de seguiment com s'ha comentat amb anterioritat:

- Taxa de resolució en primer nivell, segon nivell o tercer nivell.
- Temps mitjà de resposta per severitat de la averia.
- Temps mitjà de resolució per severitat de la averia.
- Volum de tiquets gestionats mensualment.
- Índex de reincidència d'avaries ≤ 5%.
- Percentatge d'incidències resoltes dins dels terminis ANS.

5. MARC DE TREBALL

5.1. EINES CORPORATIVES DE SEGUIMENT

Les eines corporatives de BIT per al seguiment de l'execució del servei són Easyvista i JIRA.

El proveïdor estarà obligat a informar i mantenir actualitzada, com a mínim, la següent informació:

- La planificació global del servei validada pel responsable del contracte.
- L'avanç de cadascuna de les tasques del servei.
- Els riscos identificats.
- Les reunions de seguiment dels serveis amb les actes adjuntes.

El BIT es reserva el dret de modificar aquestes eines amb el previ avís suficient perquè l'adjudicatari pugui adaptar-se a les mateixes i deixant un període de transició raonable.

5.2. EINES DE MONITORITZACIÓ

El sistema Zabbix de monitorització és l'eina corporativa utilitzada per a la supervisió contínua de tots els equips i dispositius integrats en el sistema de videovigilància i de la Sala Conjunta de Comandament, incloent-hi tant els equips instal·lats en dependències municipals, com l'equipament situat a la via pública. Aquest sistema és indispensable per al correcte manteniment del servei i es troba actualment en funcionament, formant part essencial de l'operativa diària de supervisió tècnica.

L'adjudicatari haurà d'operar, gestionar i mantenir Zabbix i tots els seus components, assegurant la correcta configuració, supervisió i actualització dels elements que formen part de l'abast del contracte. Igualment, haurà de garantir que l'eina manté un seguiment en temps real dels dispositius, així com la generació i enviament dels avisos configurats, amb l'objectiu d'anticipar avaries i reduir els temps de resposta i resolució d'incidències.

Funcionalitats mínimes exigides del sistema Zabbix

- Consulta periòdica d'estat de càmeres i dispositius, incloent detecció de pèrdues de comunicació i degradacions de servei, per tal d'avançar-se al diagnòstic d'avaries.
- Monitoratge de paràmetres de rendiment dels servidors i equips clau (capacitat de memòria, disc, càrrega de CPU, etc.), permetent anticipar necessitats de reposició o actuacions preventives.
- Enviament d'alertes automàtiques per correu electrònic a les adreces que determini el personal tècnic del client, segons nivells de criticitat i criteris definits.
- Definició de nivells de criticitat i llindars d'alerta basats en el tipus d'equip, temps de resposta o grau d'afectació del servei.
- Generació de gràfics, tendències i informes, que permetin una revisió analítica del comportament dels sistemes i facilitin el seguiment del servei, així com la presa de decisions tècniques.

Tot nou equipament que s'incorpori a l'abast del contracte —ja sigui de reposició, ampliació o renovació— haurà de ser configurat i integrat a Zabbix per part de l'adjudicatari, garantint que la monitorització del servei es manté completa i actualitzada en tot moment.

Aquesta obligació inclou la creació de nous ítems, triggers, mapes, gràfics i alertes necessàries per assegurar la supervisió correcta d'aquests nous elements, mantenint la coherència amb els criteris i estàndards definits pel responsable de servei del BIT.

6. RECURSOS HUMANS

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis. Cal que els licitadors detallin a les seves propostes quina és l'organització que proposen per al projecte, tenint en compte que hauran de dotar el personal necessari per assegurar la correcta prestació del servei objecte d'aquest contracte i que permeti mantenir una fluïdesa amb els agents que participen en el procés.

El BIT considera que es necessiten, com a mínim, els perfils que es detallen a l'apartat següent:

1. FUNCIONS PER PERFIL

El BIT estima que els perfils mínims necessaris a aportar per part de l'adjudicatari hauran de ser:

Perfil	Responsabilitat
Responsable del contracte/Coordinador del servei	És el màxim responsable del resultat positiu del servei i del compliment de les condicions descrites en aquest plec. Les seves principals tasques són: • Aportar un equip amb les capacitats requerides per a desenvolupar els serveis del contracte. • Garantir una estabilitat dels membres de l'equip per afavorir un bon rendiment i la millora continua. • Donar seguiment al rendiment de l'equip i solucionar eventuals mancances. • Ser el interlocutor oficial envers el BIT, assistint com a mínim a les reunions del Comitè de Direcció del Projecte, i identificant les accions correctives respecte eventuals problemes detectats.
Tècnic CCTV de camp	El tècnic de camp és responsable de la intervenció directa en els emplaçaments on es produeixen incidències relacionades amb càmeres o altres elements de la xarxa de videovigilància objecte d'aquest contracte. El seu objectiu principal és garantir la resolució ràpida i efectiva dels problemes in situ, assegurant la continuïtat del servei i la correcta operativitat dels sistemes. Les seves funcions principals són: • Desplaçament als emplaçaments necessaris: Realitza visites tècniques als llocs afectats per incidències per dur a terme les accions correctives de manera presencial.

	• Realitza els manteniments preventius a camp. • Resolució d'incidències en càmeres i equips de xarxa: Diagnostica i repara problemes físics o de configuració que no poden ser resolts de forma remota. • Coordinació amb el HelpDesk i el tècnic superior: Manté una comunicació fluida amb els equips de suport per informar sobre l'estat de les incidències i confirmar la seva resolució.
Tècnic Superior sistema VMS i helpdesk	El tècnic superior de sistemes VMS i HelpDesk té un paper clau en la gestió i manteniment dels sistemes de videovigilància i en el suport tècnic avançat. Les seves funcions principals són: • Recepció, registre i resolució o derivació d'incidències o peticions de servei. • Verificació del funcionament del sistema: Comprova que els dispositius afectats (càmeres, enllaços de xarxa, equips associats) funcionin correctament després de qualsevol intervenció. • Suport a l'usuari; instal·lació i configuració de programari. • Suport en l'elaboració d'informes mensuals del servei: Col·labora en la preparació i revisió dels informes que reflecteixen l'estat del servei, les incidències gestionades i les accions correctives aplicades. • Participació en reunions de seguiment: Intervé en reunions periòdiques per informar sobre l'evolució del servei, compartir incidències rellevants i proposar millores. • Actualització de l'inventari: Manté actualitzat el registre dels equips i dispositius, assegurant la traçabilitat i el control dels recursos disponibles.

	• Configuració remota de noves càmeres: S'encarrega de la configuració inicial i posada en marxa de les càmeres de videovigilància, garantint la seva integració correcta al sistema VMS. • Suport remot en tasques de manteniments preventius.

2. CARACTERÍSTIQUES PROFESSIONALS

Perfil	Experiència/Coneixements
Responsable del contracte/Coordinador del servei	Cal que acrediti, durant els darrers 10 anys com a mínim 5 anys d'experiència com a responsable de projectes TIC i responsable de negoci, Haver gestionat serveis amb equips de mínim 3 persones en l'àmbit de l'Administració pública i/o sector privat. Està en disposició de la certificació ITIL Foundation, com a mínim.
Tècnic CCTV de camp	Haurà de tenir experiència almenys de 3 anys en entorns d'instal·lació i manteniment de sistemes de videovigilància (CCTV) i control d'accessos. Haurà de poder demostrar coneixement en l'entorn de xarxes IP (switchos, routers, etc.). Experiència en intervencions en camp, reparació d'equipament i manteniments preventius dels sistemes de videovigilància i control d'accessos.
Tècnic Superior sistemes VMS i helpdesk	Haurà d'acreditar experiència en: • Administració de sistemes VMS (Video Management System): Experiència en configuració, monitoratge i integració de càmeres. Mínim 3 anys en els darrers 5. • Capacitat d'atenció a l'usuari: Instal·lació de programari, assistència remota i

	comunicació efectiva. Mínim 3 anys d'experiència. • Suport tècnic avançat (HelpDesk): Almenys 3 anys en resolució d'incidències de segon nivell en els últims 5 anys. • Coneixements de xarxes i sistemes operatius: Configuració remota, diagnòstic i seguretat. Mínim 2 anys. • Gestió d'informes i seguiment: Experiència en elaboració d'informes tècnics i participació en reunions de seguiment. Mínim 3 anys en els darrers 5.

BIT es reserva el dret de verificar les capacitats del personal que participa en el projecte en qualsevol moment i rebutjar-lo en cas que no compleixin amb els requisits exigits. Les despeses que es derivin com a conseqüència de canvis en l'equip de projecte aniran a càrrec de l'adjudicatari.

3. DIMENSIONAMENT

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

A més, en cas de substituir algun membre de l'equip de treball, s'exigirà el següent:

- Un període de formació, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.
- Un període de coexistència, d'un mínim de quinze dies, entre la persona que causa baixa i la persona que s'incorpora.

En cas de que l'oferta de l'adjudicatari millori els mínims exigits en aquest plec, serà aquesta la que prevaldrà, de cara als mínims exigits als posteriors perfils que puguin substituir als recursos humans assignats inicialment.

7. FACTURACIÓ

L'adjudicatari facturarà els serveis i subministraments associats objecte del contracte un cop per cada exercici de vigència del contracte. S'ha previst un model de facturació anual atesa la naturalesa del contracte, basat en la prestació continuada de serveis de manteniment, suport tècnic, gestió de l'estoc de reposició i disponibilitat permanent dels recursos humans i materials necessaris per garantir l'operativitat de la infraestructura de videovigilància.

La facturació anual no implica que l'execució dels treballs sigui lineal durant l'any. La càrrega real de treball pot variar en funció de les incidències, actuacions correctives, renovacions d'equipament o necessitats operatives que es produeixin en cada moment. Es tracta únicament d'un mecanisme de liquidació econòmica, mantenint-se en tot cas l'obligació de l'adjudicatari de prestar els serveis contractats, garantir la disponibilitat dels recursos compromesos i complir els nivells de servei establerts durant tota la vigència del contracte.

Dit això, la facturació es realitzarà segons el següent quadre, aplicant la corresponent baixa licitatòria efectuada per l'empresa adjudicatària:

ANY	MES FACTURACIÓ	IMPORT*
2027	Setembre**	33.315,61 €
2027	Desembre	270.906,90 €
2028	Desembre	594.380,91 €
2029	Desembre	813.253,45 €
2030	Abril***	191.331,60 €
TOTAL		1.903.188,47 €

*A les diferents fites de facturació s'aplicarà la baixa licitatòria efectuada per l'empresa contractista. Tots els imports assenyalats són sense IVA inclòs.

**L'auditoria inicial, com a part de servei independent i amb abast limitat, es cobrarà de manera independent un cop s'hagin finalitzat les tasques i s'hagi entregat l'informe corresponen i hagi sigut validat pel referent de servei.

En el mes de desembre de l'any 2027 es facturarà l'import corresponent al servei de manteniment des de l'entrada en vigor del contracte fins el dia 31/12/2027.

En el mes de desembre de l'any 2028 es facturarà els imports corresponents al servei de manteniment de tot l'any 2028 i el mateix en el mes de desembre del 2029.

***La facturació de l'any 2030 es farà al més següent del mes corresponent en relació a l'entrada en vigor del contracte.

8. PERÍODE DE GARANTIA DEL CONTRACTE

Ateses les característiques i objecte del contracte no s'estableix addicionalment un període de garantia del contracte un cop recepcionat aquest, més enllà de la garantia pròpia de l'equipament per part del fabricant.

9. PROPOSTA TÈCNICA I ECONÒMICA

Les empreses licitadores presentaran la seva proposta d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen aquesta contractació.

Les empreses licitadores l'hauran de presentar a través de la plataforma electrònica, conforme s'estableix al plec de clàusules administratives que regeix la present licitació. A l'oferta en suport electrònic tots els arxius hauran d'estar en format **OpenDocument (.odt, .ods, .odp), Word, Excel, Power Point, MSProject o PDF**, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.

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

Es presentarà un sobre electrònic denominat **BC**, que haurà de contenir l'oferta econòmica i les referències tècniques per a la ponderació dels criteris avaluables de forma automàtica d'acord amb el model que s'annexa al plec de clàusules administratives particulars que regeixen per aquesta contractació.

A l'interior del sobre s'haurà d'incorporar una relació, en arxiu independent, dels documents que hi conté ordenats numèricament.

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

10. CLÀUSULES GENERALS DE SEGURETAT

10.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓDE DADES I COMPLIMENT NORMATIU

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

BIT, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven del REGLAMENT (UE) 2016/679 DEL PARLAMENT EUROPEU I DEL CONSELL, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, així com de la resta de l'ordenament jurídic que sigui d'aplicació. Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat.

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

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

10.2. CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT

Pel que fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS).

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

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

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

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

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

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

10.3. RESPONSABLE DE SEGURETAT

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

- Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.
- Garantir que tots els serveis prestats pel proveïdor a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per BIT i seguint la normativa de seguretat vigent.
- Garantir i liderar dins la seva organització la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives i jurídiques), així com les directrius en matèria de seguretat establertes per BIT.
- Assegurar que tot el personal de l'empresa adjudicatària que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.
- Informar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en les polítiques i instruccions de l'Administració Municipal en cas que els sigui d'aplicació i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat

de la informació i protecció de dades de caràcter personal de l'Administració Municipal.

- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

10.4. CLÀUSULA PER ACCESSOS POTENCIALS

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

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

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

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

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

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

10.5. CONFIDENCIALITAT

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

L'empresa adjudicatària queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment

del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'empresa adjudicatària serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

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

10.6. CLÀUSULES DE SEGURETAT D'ACCÉS A SISTEMES DE L'AJUNTAMENT

10.6.1. AUDITORIA

BIT auditarà que l'empresa adjudicatària vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

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

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

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

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

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

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

10.6.2. GESTIÓ D'INCIDENTS

L'empresa adjudicatària informarà al Departament de Seguretat de BIT de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per BIT.

Les notificacions s'hauran de realitzar pels canals establerts a tal efecte a través del SAU o en el seu defecte, per mitjà del responsable del contracte.

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

10.6.3. ACCÉS A LA INFORMACIÓ

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

10.6.4. DIMENSIONAMENT/GESTIÓ DE CAPACITATS

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

10.6.5 ANÀLISIS FORENSES

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

10.6.6. CONTROL D'ACCÉS

10.6.6.1. Accés local

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

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

10.6.6.2. Accés remot

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

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

10.6.7. GESTIÓ DEL PERSONAL

10.6.7.1. 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 integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

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

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

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

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

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

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

10.6.7.2. Formació i conscienciació

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

Es recordarà regularment:

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

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

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

10.6.8. PROTECCIÓ DEL LLOC DE TREBALL

10.6.8.1. ***Protecció d'equips***

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

Sense perjudici de les mesures generals que els afectin, es requereix a l'empresa adjudicatària que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Els usuaris hauran de disposar d'un canal de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a BIT.

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

L'empresa adjudicatària garantirà que els seus equips es bloquegin al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de la persona usuària per reprendre l'activitat.

Addicionalment, els equips hauran de disposar:

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

10.6.9. CLÀUSULA DE COMUNICACIONS EXTERNES

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

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

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

10.6.10. PROTECCIÓ DELS SUPORTS INFORMÀTICS

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

10.6.10.1. Etiquetat

L'empresa adjudicatària es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

10.6.10.2. Transport

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

10.6.10.3. Esborrat i destrucció

L'empresa adjudicatària haurà de seguir els estàndards i normes de BIT respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut.

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

10.6.11. PROTECCIÓ DE LA INFORMACIÓ

10.6.11.1. Neteja de documents

L'empresa adjudicatària disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults,

metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

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

10.6.11.2. Protecció del correu electrònic

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

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'empresa adjudicatària.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:
- Correu no sol·licitat (spam)
- Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
- Codi mòbil de tipus applet.

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

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

El responsable del contracte de l'Ajuntament avaluarà si el contracte ha de gestionar informació sensible, especialment protegida en relació a la protecció de dades personals, confidencial de l'Ajuntament o de les tecnologies municipals (adreces IP, usuaris, credencials,...).
En cas afirmatiu, l'Ajuntament facilitarà a l'empresa adjudicatària un correu electrònic de l'Ajuntament (@ext.bcn.cat) el qual es convertirà en la via de comunicació entre l'empresa adjudicatària i l'Ajuntament.
Aquesta mesura vol evitar que les empreses externes retinguin informació confidencial de l'Ajuntament en servidors de correu aliens a l'entorn municipal, durant i sobretot, un cop finalitzat el contracte.

10.6.12. PROTECCIÓ DE LES INSTAL·LACIONS

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

- En cas d'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.

10.6.13 GESTIÓ D'EXCEPCIONS

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

10.7 CLÀUSULES DE SEGURETAT D'ADMINISTRACIÓ DE SISTEMES

10.7.1 GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS

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

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

Autenticació interna
Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per BIT basats en protocols estàndards de seguretat. L'empresa adjudicatària haurà d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant, IDP) per a l'autenticació dels usuaris.

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

- Integració mitjançant l'estàndard OpenID Connect (OAuth 2.0), utilitzant el flux d'autenticació de codi d'autorització amb PKCE (intercanvi de clau codificada)

- En cas que l'aplicació no suporti l'ús del protocol OpenID Connect, la integració es farà mitjançant l'estàndard SAML 2.0.

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

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

10.7.2 AUTORITZACIÓ DELS USUARIS ALS SISTEMES

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

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

Aquesta integració podrà ser de dos tipus:

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

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats.

Perfilat d'usuaris
Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i per la Direcció de Seguretat de la Informació de BIT.
El model proposat haurà de complir amb els següents principis:

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

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

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant rols de seguretat, entenent com a rol una entitat que dona accés a una sèrie d'operacions.

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

10.7.3 INVENTARI D'ACTIUS

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

10.7.4 CONFIGURACIÓ DE SEGURETAT

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

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
    - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.

- No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
- S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.

- S'aplicarà la regla de "seguretat per defecte":
  - Les mesures de seguretat seran respectuoses amb la persona usuària i protegiran a aquest, tret que s'exposi conscientment a un risc.
  - Per reduir la seguretat, la persona usuària ha de realitzar accions conscients.
  - L'ús natural, en els casos que la persona usuària no ha consultat el manual, serà un ús segur.

10.7.5 MANTENIMENT

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

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

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

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

	6 < CVSS <=8	1 dia	5 dies	5 dies	5 dies
	CVSS > 8	1 dia	2 dies	1 dia	5 dies

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

10.7.6 XIFRATGE DE DADES

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

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

10.7.7 CERTIFICATS

La Direcció de Seguretat de la Informació de BIT serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de la Direcció de Seguretat de la Informació de BIT. S'entén per certificats digitals corporatius: els de servidor segur, els d'aplicatiu per autenticació o signatura digital, de signatura de codi, de xifratge, etc.

Tots els certificats hauran de ser sol·licitats a través del procediment establert per la Direcció de Seguretat de la Informació de BIT per al seu control i gestió.

El proveïdor haurà de seguir l'estàndard establert per la protecció i custòdia dels certificats digitals a l'hora d'incorporar el certificat pel seu ús.

10.7.8 ANTIMALWARE

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

BIT obtindrà indicadors de la bona gestió de proteccions antimalware i en qualsevol moment tindrà accés i visió de l'estat de la seguretat global de les proteccions.
La Direcció de Seguretat de la Informació de BIT tindrà accés en consulta a la consola de gestió d'aquests programaris del proveïdor.

10.7.9 CÒPIES DE SEGURETAT

L'empresa adjudicatària serà responsable de realitzar còpies de seguretat als sistemes dels quals és administrador per tal de poder recuperar les dades en cas de pèrdua

accidental o intencionada. La freqüència de les còpies de seguretat vindrà donada pel nivell de sensibilitat de les dades que conté, segons el recollit a les guies de BIT.

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

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

10.7.10 CONTROL D'ACCÉS

10.7.10.1 Segregació de funcions i tasques

L'empresa adjudicatària s'encarregarà de que el sistema de control d'accés s'organitzi de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
En concret, se separaran almenys les següents funcions:

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

10.7.11 EXPLOTACIÓ

10.7.11.1 Gestió de la configuració

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

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

10.7.11.2 Gestió de canvis

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

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

10.7.11.3 Protecció de claus criptogràfiques

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

10.7.12 PROTECCIÓ DELS SERVEIS

10.7.12.1 Protecció enfront de la denegació de servei

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

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.
- Es desplegaran tecnologies per prevenir els atacs coneguts.

Aquest plec de prescripcions tècniques ha estat emès per la Sra. Virginia Espinosa Guerrero, tècnica adscrita a la Direcció de Serveis d'Innovació i Tecnologies de ciutat del BIT, amb el vistiplau de,

Patricia Moreno Atanasio
Directora de Serveis d'Innovació i Tecnologies de ciutat

11. ANNEX 1: INFORMACIÓ ADDICIONAL I ACLARIMENTS

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

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

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

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