

Plataforma central de videovigilància

Plec de prescripcions tècniques



1. CONTEXT I OBJECTIUS DEL PROJECTE	5
1.1. Antecedents	5
1.2. Introducció	6
1.3. Justificació	6
1.4. Objectius	7
1.5. Abast del projecte	7
1.6. Situació actual	8
2. REQUISITS GENERALS I NORMATIUS	9
2.1. Requisits generals	9
2.2. Requisits normatius i de ciberseguretat	13
3. REQUISITS D'ARQUITECTURA	15
3.1. Sistema central	16
3.2. Client de vídeo	18
3.3. Transmissió, control, configuració i monitoratge de vídeo	20
4. REQUISITS FUNCIONALS	22
4.1. Visualització en directe	22
4.2. Reproducció	23
4.3. Enregistrament	24
4.4. Descàrrega d'imatges	25
4.5. Conservació de la cadena o custòdia d'imatges	26
4.6. Enviament a tercers	27
4.7. Interfície de visualització i navegació	29
4.8. Control remot	33
4.9. Informes	34

5. REQUISITS TÈCNICS	35
5.1. Càmeres	36
5.2. Videogravadores	37
5.3. Xarxes i protocols de comunicació	38
5.4. Federació	41
5.5. Planimetria	42
5.6. Monitoratge	43
5.7. Integritat i traçabilitat	44
6. REQUISITS D'INTEGRACIÓ	46
6.1. Gestió d'identitats	46
6.2. GIS	48
6.3. Interfonia G-INFO i G-SOS	51
6.4. Telecomandament d'instal·lacions fixes (CCIF)	53
6.5. API – TMB	55
7. ALTRES REQUISITS	56
8. REQUISITS DE MANTENIMENT, OPERACIÓ I GESTIÓ TECNOLÒGICA	57
9. REQUISITS DE GESTIÓ DEL PROJECTE	64
10. PLANIFICACIÓ I METODOLOGIA	68
10.1. Fases del projecte	68
10.2. Fites Rellevants	69
11. PROVA INICIAL DE VERIFICACIÓ	69
12. EQUIP DE TREBALL	69
13. MEDI AMBIENT	71

Glossari

Concepte	Descripció
CCM	Centre de Control de Metro
CCM2	Centre de Control de Metro d'Emergència
ICOM	Informació i Comunicació de Metro
CST	Centre de Suport Telemàtic
OTS	Operació Tècnica del Servei
ATEC	Àrea de Tecnologia de TMB
SOM	Sistemes d'operació de Metro
TOLA	Tècnic d'Operació de Línies Automàtiques
CCE	Cabina Cap d'Estació
VMS	<i>Video Management System</i>
PCE	lloc de control d'emergència Can Zam
MPLS	<i>Multiprotocol Label Switching</i>
API	<i>Application Programming Interface</i>
AAC	Agent d'Atenció al Client
VMP	Producte Mínim Viable

1. CONTEXT I OBJECTIUS DEL PROJECTE

1.1. Antecedents

El sistema de videovigilància (CCTV) de Transports Metropolitans de Barcelona (TMB) es va implementar de manera progressiva, començant per la xarxa de Metro durant els anys 80 i estenent-se a la xarxa de Bus a finals dels 90. Des d'aleshores, ha experimentat una evolució contínua i ha incorporat avenços tecnològics per satisfer les necessitats operatives i de seguretat creixents de l'organització.

Principals millores implementades:

1. Transició a sistemes digitals migrant la infraestructura analògica a sistemes de videovigilància digital, per millorar la qualitat d'imatge i l'eficiència de l'emmagatzematge.
2. Infraestructura centralitzada basada en servidors virtuals i bases de dades corporatives per optimitzar la gestió i l'accés a la informació de vídeo.
3. Integració amb sistemes corporatius: permet una gestió més eficient i més interoperabilitat.
4. Consolidació de plataformes de vídeo (CVV): per a la unificació de plataformes de vídeo de les línies convencionals en un sistema únic, que simplifica l'operació i el manteniment previ a la creació.
5. Expansió de la videovigilància a trens i autobusos, per ampliar la cobertura i millorar la seguretat al transport públic.
6. Monitoratge avançat en temps real, que permet una resposta ràpida davant d'incidents i situacions crítiques.
7. Incorporació d'anàlítica d'imatges per detectar automàticament esdeveniments i comportaments sospitosos, i millorar així la seguretat proactiva.

La ràpida evolució tecnològica i l'obsolescència d'alguns sistemes actuals fan imprescindible la implementació d'una plataforma unificada i actualitzada de videovigilància que permeti el següent:

1. Optimitzar la gestió de vídeo per simplificar i centralitzar l'operació diària i millorar-ne l'eficiència operativa.
2. Millorar l'efectivitat de la seguretat a les xarxes de Metro i Bus, per garantir un entorn més segur per als usuaris.
3. Control àgil i fiable: Implementació d'un sistema de control més àgil i fiable, que permeti una resposta ràpida i efectiva davant de qualsevol situació.

D'aquesta manera TMB reafirma el seu compromís amb la innovació tecnològica per oferir un sistema de transport públic més segur, eficient i fiable per a tots els ciutadans.

1.2. Introducció

Actualment, el servei de videovigilància de TMB està compost per diverses solucions tecnològiques que permeten la captació de vídeo a temps real, selecció, enregistrament i revisió d'imatges en diferit als principals emplaçaments de **Metro i Bus**, incloses estacions, cotxeres, edificis corporatius i sistemes embarcats en trens i autobusos.

Atès que gestiona informació confidencial, la videovigilància és considerada un **servei crític** i una eina essencial per a l'operació i la supervisió de la seguretat dins de l'empresa.

Els components principals de l'ecosistema de videovigilància de Metro i edificis corporatius són els següents:

1. Línies automàtiques: telecomandament central i clients a cabines de caps d'estació (LA de Marina-Sony).
2. Línies convencionals i edificis corporatius: consolidador de videovigilància Indra (CVV), amb infraestructura basada en videogravadors i clients de vídeo a cabines de Lanaccess. La solució disposa d'una nativa central i clients en cabines de cap d'estació.
3. Sistema embarcat: Telefunken en línies automàtiques i GMV en línies convencionals.

Els components principals de l'ecosistema de videovigilància de Bus són els següents:

1. telecomandament central Marina-Sony a cotxeres.
2. Sistema embarcat GMV a autobusos.

El sistema de videovigilància abasta múltiples centres d'operació i seguretat, com ara:

Infraestructures: estacions de Metro, cotxeres de Metro i Bus, trens i autobusos.

1. Centres de control:
 - a. Centre de Control de Metro (CCM)
 - b. Centre de Control de la Xarxa de Bus (CCXB)
 - c. Centre de Control de Metro d'Emergències (CCME)
 - d. Centre de Control de la L9/L10 (PPC) i el Centre d'Emergències (PCE)
 - e. Centre de Seguretat i Protecció Civil (CSPC)
 - f. Centre de Control d'Estació (CCE)
2. Altres entitats: STM, gerències de línia, Centre de Control de Trànsit Urbà (CCTU), Guàrdia Urbana, entre d'altres.

Aquest ecosistema complex i distribuït fa que calgui avançar cap a una plataforma única i centralitzada que optimitzi la gestió de la videovigilància i garanteixi un servei eficient i segur.

1.3. Justificació

El consolidador de videovigilància (CVV) de línies convencionals de Metro, implementat a inicis de la dècada passada, va permetre **unificar** tecnologies analògiques i optimitzar el flux d'informació i la interoperabilitat entre sistemes dins de la infraestructura fixa de Metro.

Després de més de 10 anys en funcionament, aquest programari de propietat ha quedat **obsolet**, cosa que fa necessari cercar una alternativa més flexible, basada en estàndards i solucions de mercat que permeti una substitució ràpida i segura d'aquest sistema. A més, la nova solució ha de ser escalable i evolucionar tecnològicament per:

1. Integrar-se amb nous sistemes embarcats.
2. Adaptar-se a nous estàndards i avenços del mercat.
3. Incorporar informació i esdeveniments d'altres sistemes.

D'altra banda, la infraestructura de video-gravadors de les línies convencionals continua operativa i no presenta signes d'obsolescència, per la qual cosa no es preveu substituir-la.

No obstant això, la coexistència de múltiples eines de videovigilància als centres de control dificulta l'operativa de seguretat i redueix l'eficiència del servei.

Per aquests motius, TMB ha decidit renovar la plataforma central de videovigilància amb un sistema VMS (*Video Management System*), una solució més moderna, flexible i basada en els estàndards del mercat. Aquest nou sistema garantirà el servei diari, la seguretat i la protecció civil dins de les instal·lacions de TMB, alhora que optimitzarà la seva gestió tecnològica.

Un VMS és un sistema d'administració de vídeo dissenyat per gestionar la informació de càmeres i video-gravadors de manera centralitzada, independentment de la ubicació, la tecnologia o el tipus. Aquest nou VMS serà, a més, el sistema central transversal de TMB, que progressivament anirà integrant tots els sistemes de videovigilància de l'organització.

1.4. Objectius

Aquest plec té com a objectiu definir les especificacions tècniques per a la contractació dels serveis d'enginyeria, subministrament, implementació, configuració i posada en servei del reemplaçament de l'actual consolidador de vídeo per un VMS estàndard i de mercat.

Aquest canvi proporcionarà als equips d'operació, seguretat i manteniment una eina més avançada, dinàmica i amb una visió multimodal, que millorarà la gestió i anàlisi del vídeo en el sistema.

Aquest projecte pretén aconseguir quatre objectius clau:

1. Incorporar millores i eines noves que optimitzin el sistema actual de videovigilància eliminant alhora els problemes d'obsolescència del CVV.
2. Facilitar la presa de decisions mitjançant una plataforma unificada i més eficient.
3. Implementar mesures que reforcin la protecció de la infraestructura davant d'amenaques digitals.
4. Millorar el control i la supervisió de l'estat de la infraestructura, per permetre una gestió més àgil i precisa.

1.5. Abast del projecte

El subministrament objecte d'aquesta licitació comprèn, de manera enunciativa però no limitativa, les prestacions següents:

1. L'anàlisi de la situació del sistema en producció, basat en el consolidador de vídeo d'Indra, com a punt de partida per elaborar el pla de migració al nou VMS
2. Anàlisi de requisits i de seguretat, especificació, disseny, desenvolupaments S'han de tenir en compte els aspectes següents (llista **no** exhaustiva):
 - Anàlisi i requisits de la xarxa de teleprocés
 - Proposta de solució i pla d'acció per a la migració del sistema de videovigilància a les línies convencionals i els edificis corporatius
 - Integració amb els NVR de Lanaccess
 - Integració amb GIS i API de TMB
 - Integració amb altres sistemes requerits: INFO, SOS, CCIF i LDAP/KEYCLOAK
 - Adaptacions del programari a la plataforma VMS de mercat d'acord amb els punts anteriors
3. Subministrament de llicències
4. Instal·lació del VMS, inclosa la configuració, validació i posada en marxa
5. Elaboració de la documentació tècnica
6. Formació per als usuaris i administradors del sistema
7. Garantia del subministrament
8. Bossa d'hores per a desenvolupaments evolutius no previstos
9. Auditoria de ciberseguretat

Es consideraran incloses dins del subministrament totes aquelles tasques, elements, treballs o serveis que, tot i no estar expressament indicats, siguin imprescindibles per garantir el compliment integral de les funcionalitats, requisits i objectius establerts en aquest plec de condicions tècniques.

Es consideren prescripcions tècniques mínimes aquelles que, en cas de no complir-se, fan incompatible la solució aportada amb els sistemes distribuïts o centrals de TMB, que no permetin oferir el servei extrem a extrem o oferir totes les funcionalitats i requisits descrits en aquest plec de prescripcions tècniques.

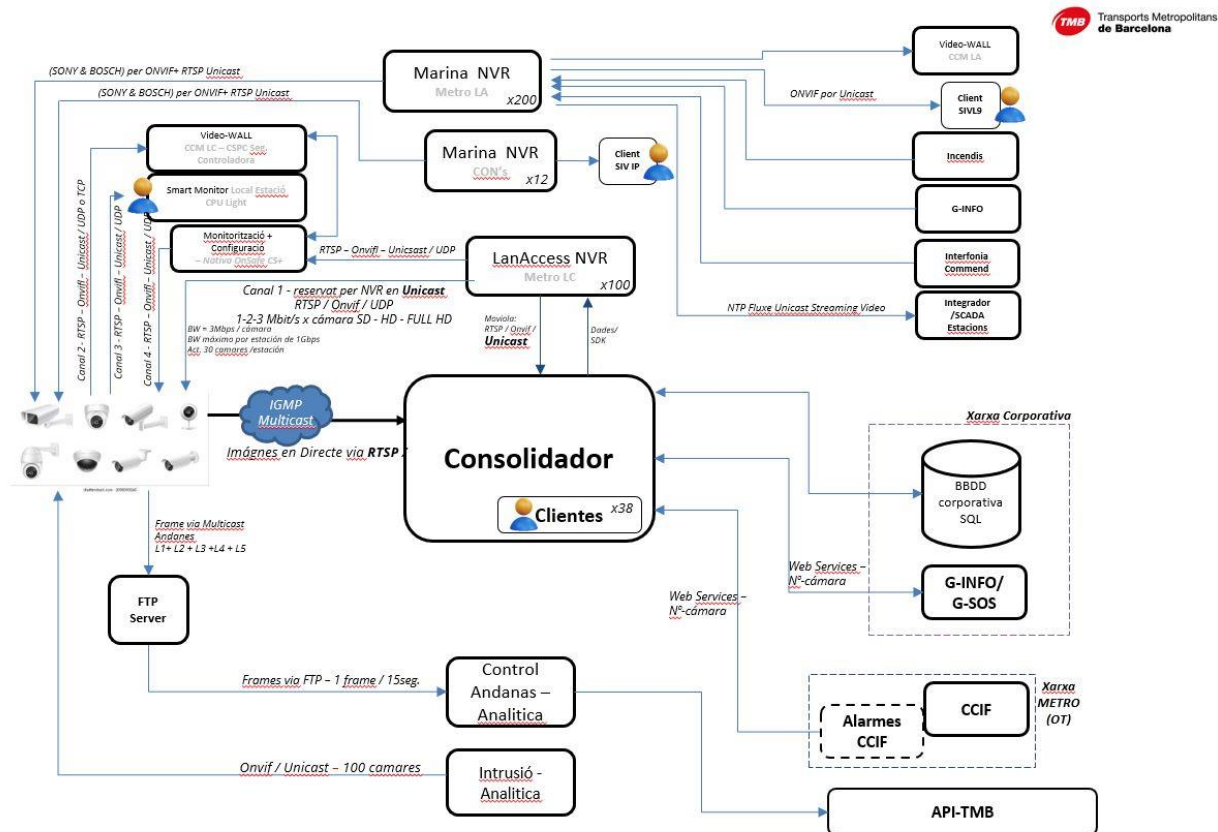
1.6. Situació actual

La videovigilància de TMB està composta per diversos sistemes tecnològics, que es descriuen més detalladament a continuació:

1. Consolidador de vídeo d'Indra: utilitzat a les línies convencionals i els edificis corporatius.
2. Sistema natiu de Marina: implementat a les línies automàtiques i a les cotxeres de Bus.
3. Sistema natiu de GMV: destinat a la videovigilància embarcada a Metro i Bus.
4. Sistema natiu de Lanaccess: emprat a l'edifici de Miramar, Telefèric i al *videowall* de les sales de control.

La nova plataforma VMS ha d'integrar la infraestructura de vídeo existent a les instal·lacions de TMB. Tot i això, en aquesta **primera fase**, la licitació s'enfocarà exclusivament al punt 1 esmentat anteriorment.

L'esquema de funcionament del sistema actual és el següent:



L'esquema anterior s'ha de revisar a l'inici del projecte per poder actualitzar alguna divergència que l'esquema no reflecteixi correctament.

2. REQUISITS GENERALS I NORMATIUS

2.1. Requisits generals

A continuació, es presenten de manera general els requisits que el sistema VMS ha de complir i en els apartats següents, s'oferiran detalls més específics de la majoria.

REQUISITS GENERALS		
ID	Concepte	Descripció
RGEN1	Àmbit	La solució i el projecte han de satisfer els requisits i les necessitats descrites en tots els apartats d'aquest plec de prescripcions.
RGEN2	Qualitat	La solució ha de tenir la màxima qualitat, fiabilitat i disponibilitat, considerant la videovigilància com un servei crític per a l'operació i la seguretat de TMB.

RGEN3	Programari	A l'oferta s'indicarà la marca i els productes base que integren la solució proposada. TMB es reserva el dret de rebutjar productes del tipus VMS que no ofereixin prou garanties o no compleixin els requisits d'aquest plec.
RGEN4	Escalabilitat i obertura	El VMS ha de permetre que múltiples <i>partners</i> homologats pel fabricant puguin personalitzar i adaptar el producte base i la resta de desenvolupaments del projecte en un futur, per garantir la flexibilitat, l'evolució contínua de la solució i una personalització específica per a TMB.
RGEN5	Modes d'operació i entorns	La solució disposarà de dos entorns de manera simultània 24 x 7: ○ PRODUCTIU: Entorn principal que ha de complir totes les funcionalitats i requisits del plec. Aquí s'implantaràn, s'integraran i es configuraran tots els elements necessaris del sistema, tant clients distribuïts com sistemes centrals. ○ DESENVOLUPAMENT: Rèplica de l'entorn productiu per validar noves versions i configuracions abans de la implementació. Els dispositius de laboratori es poden integrar en aquest entorn o en el productiu amb canvis de configuració remots, ràpids i desatesos. La volumetria d'elements de camp (per exemple, càmeres) a integrar-se en aquest entorn serà la mínima necessària que garanteixi la possible validació de la solució i les noves versions.
RGEN6	Temps d'arrencada i robustesa	El VMS ha de ser completament operatiu després d'un reinici en menys de dos minuts per a l'entorn central i 45 segons addicionals per a clients finals.
RGEN7	Talls de tensió	La plataforma VMS i tots els seus components han de ser robustos davant de talls abruptes d'alimentació, per garantir una arrencada normal en restablir l'energia.
RGEN8	Integritat de fixers	Ha de tenir una arquitectura que minimitzi el risc de fallada per corrupcions del sistema de fixers i ha de proveir eines autònomes que permetin revisar i reparar els sistemes de fixers en cas necessari.
RGEN9	Interoperabilitat	La solució proposada ha de garantir la interoperabilitat amb els sistemes i elements de camp de CCTV de tercers actualment desplegats a les línies convencionals, que en permeti la integració completa sense necessitat de substituir la infraestructura d'enregistrament ni les càmeres existents. Així mateix, ha d'assegurar que té capacitat per a futures integracions amb la resta de sistemes de videovigilància

		implementats a Bus i Metro de TMB i garantir una arquitectura flexible i escalable.
RGEN10	Compatibilitat amb NVR actuals	El sistema s'ha d'integrar amb les gravadores existents de la marca Lanaccess, que suporten ONVIF perfil G, i permetre la integració completa de funcionalitats com la gestió d'enregistraments a <i>failover</i> i la supervisió d'estat mitjançant un SDK o API específic d'aquest fabricant.
RGEN11	Compatibilitat amb les càmeres actuals	El sistema s'ha d'integrar amb les càmeres actualment implantades a Metro i integrades al consolidador de vídeo.
RGEN12	Compatibilitat amb els protocols estàndard	Compatibilitat amb els protocols ONVIF (<i>Profile S, G i T</i>), RTSP, H.264, H.265 per garantir la interoperabilitat amb dispositius actuals i futurs.
RGEN13	Flexibilitat <i>unicast/multicast</i>	Optimització de l'amplada de banda amb suport per a alta densitat de càmeres. Gestió de fluxos de vídeo en <i>unicast</i> i <i>multicast</i> , assegurant a <i>multicast</i> una transmissió directa des de la font fins al client final per a una distribució eficient.
RGEN14	Transmissió de vídeo	El sistema ha de ser compatible amb transmissions <i>multicast</i> per a la visualització en temps real i amb <i>unicast</i> per a la reproducció de vídeo gravat, i optimitzar així l'ús de l'amplada de banda i garantir una qualitat de servei adequada en tots dos casos. TMB definirà en fase de projecte si finalment la transmissió de les càmeres en temps real es fa per <i>multicast</i> o <i>unicast</i> .
RGEN15	Enregistrament	Tot i que la solució aprofitarà els NVR actuals de TMB, el VMS ha de possibilitar l'enregistrament dins del seu propi entorn tecnològic. En qualsevol d'aquests dos modes d'enregistrament, ha de garantir la màxima flexibilitat i seguretat en la gestió de les imatges, implementant mecanismes redundants i enregistrament en <i>failover</i> per assegurar la continuïtat operativa davant de possibles errors.
RGEN16	Disponibilitat i fiabilitat	La solució s'ha de basar en una arquitectura de microserveis que garanteixi un nivell alt de disponibilitat i fiabilitat.
RGEN17	Disponibilitat i fiabilitat	La solució s'ha d'implantar sobre els servidors virtuals disponibles a la infraestructura de TMB. Addicionalment, el VMS a implantar ha de basar-se en una arquitectura d'execució mitjançant contenidors, que permeti l'aïllament de processos, la portabilitat entre entorns i l'escalabilitat horitzontal. El proveïdor ha d'aportar tota la solució, inclosa la capa de contenidors i la seva orquestració. Aquesta arquitectura ha d'assegurar capacitats de redundància, <i>failover</i> i balanceig de càrrega.

RGEN18	Arquitectura centralitzada	El sistema ha d'estar dissenyat sota un model client-servidor en estructura centralitzada, que garanteixi una connexió eficient i segura entre els clients (estacions de treball, dispositius mòbils) i els servidors centrals.
RGEN19	Arquitectura distribuïda	Tot i que la solució serà centralitzada, ha de permetre l'operació amb gravadors, servidors i càmeres en ubicacions distribuïdes dins d'estacions o edificis, per garantir una ampliació o reconfiguració del sistema en un futur.
RGEN20	Gestió i configuració	La solució ha de permetre una gestió centralitzada mitjançant una única interfície, que faciliti la configuració, monitoratge i supervisió de tots els components del sistema de manera eficient.
RGEN21	Gestió d'identitats	El sistema ha de ser compatible amb els sistemes de gestió d'identitats de TMB per a l'autenticació d'usuaris i la sincronització de grups. La configuració de rols es gestionarà des de la interfície d'administrador, per assegurar un control granular i específic sobre les funcionalitats del sistema.
RGEN22	Encriptació	El sistema VMS ha de garantir l' encriptació extrem a extrem de les imatges , tant en trànsit com en repòs, per minimitzar el risc de ciberatacs que puguin comprometre la seguretat de la infraestructura i la reputació de TMB.
RGEN23	Priorització jeràrquica	El VMS ha de permetre la configuració de diferents nivells d'accés per als usuaris i reflectir la jerarquia organitzacional. A cada nivell d'accés cal assignar una prioritat a les diferents funcionalitats del sistema. Els usuaris amb funcions jeràrquiques superiors (per exemple: CCM, personal de seguretat o gerents de línia, entre d'altres) han de tenir prioritat per accedir a fluxos de vídeo i a la resta de funcionalitats. Cal garantir que aquests perfils tinguin aquesta informació en forma d'imatges de vídeo perquè puguin prendre decisions ràpidament en situacions crítiques.
RGEN24	Analítica de vídeo	El sistema ha de ser capaç d'integrar i gestionar analítiques de vídeo de tercers en temps real o diferit.
RGEN25	Monitoratge i salut del sistema	La solució ha d'incloure eines per al monitoratge en temps real de l'estat del sistema, amb alertes automàtiques davant d'errors o anomalies.
RGEN26	Virtualització del sistema	Tots els components del sistema, inclòs el VMS i els seus mòduls associats, han de ser compatibles amb els entorns virtualitzats en la infraestructura actualment disponible de TMB. No es permeten solucions al núvol; el desplegament ha de ser cent per cent on-premise .

RGEN27	Suport i manteniment	El fabricant o integrador ha d'oferir un suport tècnic continu i garantir la disponibilitat d'actualitzacions i pedaços durant tota la vida útil del sistema que, com a mínim, ha de ser de 15 anys a partir de la posada en marxa del sistema a les instal·lacions de TMB.
RGEN28	Llicenciamnt flexible	Les llicències han de ser modulars i ajustades a l'ús real del sistema perquè es puguin fer ampliacions en el futur.
RGEN29	Socis homologats	La solució ha de permetre que múltiples socis homologats pel fabricant facin personalitzacions i adaptacions sobre el producte base, per garantir-ne la flexibilitat, la interoperabilitat i l'evolució contínua de la plataforma.

2.2. Requisits normatius i de ciberseguretat

En el context d'un disseny i la implementació d'un sistema de gestió de vídeo en una corporació ferroviària i de transport públic com és la de TMB, cal complir normatives específiques per garantir la seguretat, la privadesa i l'operativitat d'aquest sistema catalogat com a crític. Aquestes regulacions no només protegeixen la infraestructura i els passatgers, sinó que també asseguren que el sistema compleixi estàndards de ciberseguretat, protecció de dades i qualitat operativa.

L'aplicació de la normativa ha de mitigar al màxim els riscos greus, com ara els següents:

- Filtracions de dades personals de passatgers i empleats.
- Atacs cibernètics que deshabilitin càmeres o en permetin la manipulació.
- Multes i sancions legals per incompliment de regulacions de privadesa.
- Problemes d'interoperabilitat amb altres sistemes crítics (control d'accés, senyalització ferroviària, etc.).

La ciberseguretat en un sistema VMS ferroviari com el que s'especifica en aquest document, no només ha de protegir la privadesa i la infraestructura, sinó que també ha de **garantir la seguretat dels nostres passatgers i la continuïtat del servei**. Implementar mesures de protecció avançades és clau per evitar atacs i complir normatives de seguretat. A continuació, es presenten els requisits normatius i de ciberseguretat:

REQUISITS NORMATIUS I DE CIBERSEGURETAT		
ID	Concepte	Descripció
NCB1	Compliment RGPD	La solució ha de complir amb el Reglament general de protecció de dades (RGPD) de la Unió Europea, així com la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD). Així mateix, s'ha de garantir que el sistema VMS respecta en tot moment les normatives vigents en matèria de protecció de dades, tant a

		escala europea com nacional. Cal adjuntar la declaració de conformitat GRPD del fabricant / Política de Privadesa.
NCB2	Gestió de vulnerabilitats	La solució ha de proporcionar un llistat detallat i exhaustiu de les <u>contramesures</u> avançades implementades per mitigar les vulnerabilitats, prevenir els accessos no autoritzats i establir el <u>procediment de resposta</u> davant de possibles ciberatacs dirigits a la infraestructura del VMS de TMB.
NCB3	Mesures avançades de ciberseguretat	El sistema ha d'incorporar mesures avançades de ciberseguretat, com ara l'autenticació multifactorial, l'encryptació de dades en trànsit i en repòs, i actualitzacions regulars de microprogramari i programari.
NCB4	Xifratge i protecció de l'emmagatzematge de vídeo	El flux de vídeo ha de fer servir protocols d' encryptació segurs, com TLS i SRTP , per xifrar i protegir la transmissió. A més, combinarà protocols d'autenticació com OAuth 2.0 o autenticació basada en certificats , per assegurar que només els usuaris autoritzats puguin accedir al contingut. A més de xifrar el trànsit, també s'ha d'encriptar l'emmagatzematge de vídeo i els registres associats, per assegurar que, fins i tot en cas que un dispositiu sigui compromès o robat, la informació està protegida.
NCB5	Integritat de les dades i segmentació de la xarxa	La integritat del flux de vídeo extrem a extrem s'ha de fer mitjançant HMAC i MAC, per evitar així modificacions no desitjades. La solució final ha de córrer en una VLAN específica de vídeo per reforçar la seguretat.
NCB6	Registre d'accessos i logs	El sistema ha d'implementar un control d'accés robust, limitant les funcionalitats i les dades als usuaris segons els seus rols. A més, s'exigirà un registre detallat de totes les accions rellevants (accessos, configuracions, visualització de vídeos, etc.) a <i>logs</i> d'auditoria. Aquests <i>logs</i> seran essencials per al següent: - Investigació d'incidents: Facilitar la identificació de possibles filtracions de seguretat o d'accessos no autoritzats. - Auditories internes i externes: Permetre la verificació del compliment de normatives i procediments de seguretat.
NCB7	Actualitzacions i pedaços de seguretat	La solució ha de proporcionar pedaços o mesures contra vulnerabilitats detectades, cosa que pot implicar actualitzacions regulars del programari VMS.
NCB8	Protecció contra atacs	El VMS ha de comptar amb mecanismes de defensa contra atacs DDoS (<i>distributed denial of service</i>) i implementar mesures que protegeixin la disponibilitat de la infraestructura de videovigilància de TMB.

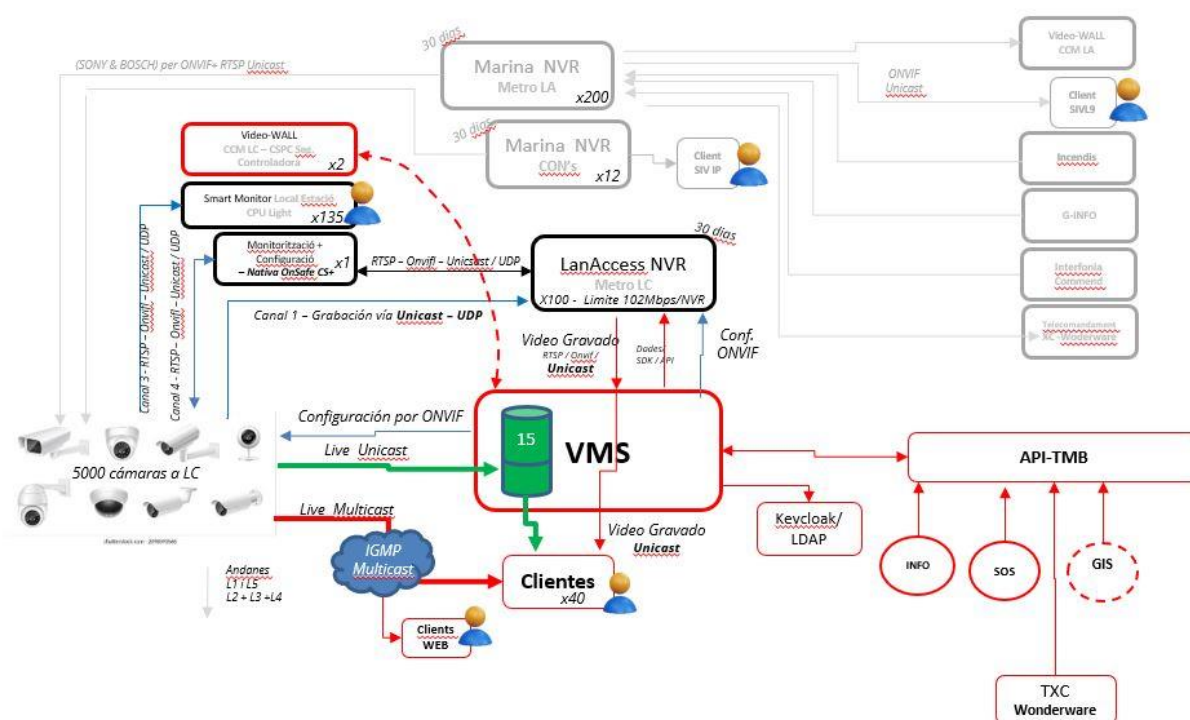
NCB09	Pla de recuperació davant de desastres	La solució ha de comptar amb un <u>pla de recuperació davant de desastres</u> que asseguri la disponibilitat del sistema en cas d'incident greu, inclosos suports regulars i l'ús d'infraestructura redundant per garantir la continuïtat del servei.
NCB10	Protecció contra <i>malware</i>	Per garantir la seguretat del sistema VMS, s'han d'incorporar mecanismes de protecció contra <i>malware</i> , que incloguin antivirus i sistemes de detecció d'intrusions, amb l'objectiu de prevenir tant atacs externs com amenaces internes.
NCB11	Consultoria i auditoria	S'ha de fer un servei de consultoria i auditoria de seguretat informàtica i de comunicacions/xarxes de la solució.

3. REQUISITS D'ARQUITECTURA

A continuació, es presenta una arquitectura de referència per al nou sistema de gestió de vídeo (VMS). És important destacar que aquesta arquitectura és orientativa i no limitant. Els licitadors podran proposar solucions alternatives, sempre que compleixin amb tots els requisits tècnics i funcionals especificats en aquest plec i TMB ho accepti.

Aquesta licitació se centra exclusivament en la implementació d'un sistema de videovigilància fixa per a línies convencionals i edificis corporatius. No es preveuen altres tipus de videovigilància en aquesta fase. La solució proposada ha de permetre la substitució estructurada i eficient del consolidador de vídeo actual, que s'allotja en servidors físics i suporta clients pesants com Workstation i *videowall*. El procés de migració s'ha de fer sense interrupcions significatives al servei.

S'espera que l'arquitectura de la nova solució sigui similar a la descrita a l'apartat següent, encara que es valoraran positivament les propostes innovadores i optimitzades que compleixin els requisits establerts.



Per a la integració dels diferents protocols de funcionament dels sistemes de videovigilància i la gestió des d'una única interfície de control, la solució VMS s'ha de basar en la implementació d'interfícies de comunicació amb cada sistema. Això s'ha de fer de la manera següent:

- Mitjançant el desenvolupament d'interfícies de comunicació basades en les API facilitades pel fabricant o integrador responsable de cada sistema per a la comunicació de control (sol·licitar imatges, entre altres coses) i la implementació de descodificadors (estàndard o desenvolupats segons les especificacions dels diferents fluxos de vídeo);
- mitjançant l'ús de SDK proporcionats pel fabricant o integrador responsable de cada sistema (inclosa la comunicació de control i la descodificació de vídeo),
- o mitjançant l'ús de controls ActiveX proporcionats per cada fabricant o integrador (inclosa la comunicació de control i la descodificació de vídeo).

3.1. Sistema central

SISTEMA CENTRAL		
ID	Concepte	Descripció
ARQ1	Centralització	El VMS ha de suportar una arquitectura centralitzada amb dos centres de processament de dades (CPD) ubicats en edificis separats: un CPD principal i un CPD secundari en configuració de <i>failover</i> .
ARQ2	Federació	El VMS ha de suportar una arquitectura federada que permeti l'administració centralitzada de múltiples sistemes independents sense comprometre la seva autonomia operativa, complint els criteris següents:

		○ Connectivitat federada: interconnexió d'instàncies independents per a supervisió i gestió unificada ○ Autonomia entre centres: funcionament independent de cada emplaçament davant de la pèrdua de comunicació amb el sistema central ○ Accés i permisos centralitzats: administració centralitzada d'usuaris i permisos ○ Transmissió segura i optimitzada: comunicació segura i optimització d'amplada de banda ○ Compatibilitat i escalabilitat: expansió sense canvis disruptius i compatibilitat entre versions
ARQ3	Microserveis	El VMS ha de tenir una arquitectura basada en microserveis, en què cada servidor pugui allotjar una o més funcions. La instal·lació ha de tenir la capacitat per permetre als administradors: ○ Instal·lar un o més servidors al llarg de la xarxa abans d'activar les funcions. ○ Activar i desactivar funcions segons calgui en tots i cadascun dels servidors. ○ Centralitzar la configuració i administració de la funció. ○ Suport de configuració remota. ○ Moure les funcions des d'un servidor a un altre.
ARQ4	Monitoratge	El VMS ha d'incorporar un servei de monitoratge de servidors (<i>watchdog</i>) robust i autònom. Aquest servei supervisarà de manera continuada i proactiva l'estat de tots els servidors i PC que executin mòduls de la plataforma VMS. El monitoratge ha d'abastar aspectes crítics com l'ús de CPU, memòria RAM, espai en disc, estat dels serveis i la latència de la xarxa.
ARQ5	Servei Windows	El servei de monitoratge s'ha d'implementar com un servei de Windows, configurat per iniciar-se automàticament en engegar el sistema. Ha de funcionar independentment de la sessió d'usuari per garantir el monitoratge continu fins i tot sense usuaris connectats. El servei de monitoratge ha d'estar instal·lat a tots els servidors i PC que executen mòduls del VMS.
ARQ6	<i>On-premise</i>	Tots els components del sistema s'han d'implementar a la infraestructura local (<i>on-premise</i>) de TMB, sense dependència de serveis o recursos ubicats al núvol públic o privat. S'exceptua d'aquest requisit el procés específic de postproducció per a l'emascament d'imatges gravades que s'hagin de cedir a

		tercers. Aquesta excepció es limita estrictament a aquesta funcionalitat i no implica la dependència de serveis al núvol per a cap altra part del sistema.
ARQ7	Integració	L'arquitectura de la solució ha de ser fàcilment integrable mitjançant API i permetre la integració de les tasques del control central i els dispositius finals amb altres sistemes corporatius.
ARQ8	Virtualització de components	Tots els components del VMS (tret dels clients) han de ser instal·lables en màquines virtuals amb un aïllament adequat entre serveis crítics. Els servidors han de ser compatibles amb la virtualització a la plataforma VMware disponible a TMB.
ARQ9	Dimensionament	El licitador ha de proporcionar una llista detallada dels recursos necessaris per a cada màquina virtual (CPU, RAM, emmagatzematge, xarxa).
ARQ10	Còpia de seguretat	El licitador ha d'incloure recomanacions sobre la configuració de <i>snapshots</i> i còpies de seguretat de les màquines virtuals.
ARQ11	Disponibilitat	El VMS ha de suportar clústers d'alta disponibilitat per garantir la continuïtat del servei davant d'errors de maquinari o programari.
ARQ12	Balanceig de càrrega	La solució ha de distribuir la càrrega de processament de vídeo per evitar colls d'ampolla en servidors virtualitzats.
ARQ13	Redundància i <i>failover</i>	S'han d'implementar mecanismes de redundància i <i>failover</i> als servidors crítics (gestió, retransmissió de vídeo, etc.).
ARQ14	Escalabilitat	La solució ha de ser escalable horitzontalment i verticalment, per permetre futures evolucions del servei mitjançant modificacions de programari o de configuració. El licitador ha d'explicar la capacitat d'escalabilitat i les limitacions del sistema.
ARQ15	Monitoratge de la plataforma	La solució ha d'oferir eines integrades per monitorar l'estat dels servidors (CPU, memòria, emmagatzematge). El sistema ha d'estar preparat per proporcionar dades a la plataforma Centreon de monitoratge de TI instal·lada a TMB.
ARQ16	Actualitzacions	La solució ha de permetre actualitzacions de programari sense interrupcions als serveis principals.

3.2. Client de vídeo

El sistema de gestió de vídeo ha de comptar amb els següents tipus de clients per a l'accés i operació del sistema:

1. Client pesant (*thick client / desktop client*)
2. Client web (*web client / thin client*)
3. Client mòbil (*mobile client*)

CLIENTS		
ID	Concepte	Descripció
CLV1	Instal·lació	Ha de ser una aplicació nativa instal·lada en equips amb sistema operatiu Windows.
CLV 2	Funcionalitats	Funcionalitats completes de visualització en viu, reproducció de vídeo, exportació d'evidències, gestió d'alarmes, configuració avançada, cerca forense, etc.
CLV3	Descodificació	Compatibilitat amb targetes gràfiques dedicades per a descodificació per programari.
CLV4	Autenticació	Compatibilitat amb autenticació centralitzada (LDAP, SAM, OAuth) i integració amb plataformes com Keycloak.
Client web i mòbil		
CLW1	Navegadors	- El client web ha de ser compatible amb navegadors moderns i estàndard: Chrome, Edge, Firefox i Safari. - S'ha de garantir la independència de la plataforma, que permeti l'execució dins dels navegadors esmentats.
CLW2	Tauleta i mòbil	El client web ha de suportar la visualització en format tauleta i <i>smartphone</i> .
CLW3	Accés segur	- Capacitat per definir un URL única per a l'accés al client web i reforçar la seguretat - Comunicacions encriptades per a totes les transaccions
CLW4	Instal·lació	- El client web ha de ser realment lleuger, sense requerir instal·lació al dispositiu de l'usuari. - La funcionalitat només ha de dependre d'un navegador web i connectors estàndard del navegador.
CLW5	Funcionalitats	- Visualització de vídeo en viu i gravat en diverses resolucions: 320 x 240, 640 x 480 i 1280 x 1024 a 15 FPS - Visualització en mosaics: 1, 4, 6 o 9 mosaics - Control PTZ bàsic: panoràmica, inclinació, zoom, preajustaments i patrons - Capacitat per reproduir vídeo gravat - Exportació de vídeo - Accés a informes
CLW6	Funcionalitats addicionals	Capacitat per carregar i visualitzar plànols GIS-TMB
CLW7	Autenticació	- Nom d'usuari i contrasenya - Directori actiu - Proveïdor d'identitat OpenID Connect

		○ Compatibilitat amb autenticació centralitzada: LDAP, SAML, OAuth ○ Integració amb plataformes de gestió d'identitat: Keycloak
CLW8	Tecnologia	Preferiblement ús de tecnologies web modernes: HTML5 i WebRTC
CLW9	Connexions concurrents	○ Suport per a un mínim de 100 connexions web concurrents per a vídeo en viu (H.264, 640 x 480, 15 FPS, 500 KBps) ○ Suport per a 60 connexions concurrents per a vídeo en format MJPEG (640 x 480) ○ Nombre de connexions mòbils mínimes concurrents per a una transmissió de vídeo en viu amb una qualitat mínima de vídeo de càmera: H264 (640 x 480) a 15 FPS a 500 KBps, o 60 per a un format MJPEG (640 x 480), o 100 per a un format H.264 (640 x 480) ○ Suport de visualització de fluxos H.265 al client web
CLW10	Latència	Latència màxima de 800 ms per a flux de vídeo H.264 natiu

3.3. Transmissió, control, configuració i monitoratge de vídeo

En el disseny de la solució VMS, la transmissió de vídeo des de les càmeres fins als diferents components del sistema ha de seguir un esquema basat en *unicast* per a l'enregistrament i la recuperació de vídeo, per garantir un ús eficient de l'amplada de banda i la correcta gestió dels fluxos de vídeo.

El VMS s'ha d'integrar amb els NVR existents sense reemplaçar la funció d'emmagatzematge, actuant com a intermediari en la sol·licitud i distribució del vídeo tant en viu com enregistrat.

Per a l'**enregistrament**, les càmeres han de transmetre un **flux de vídeo per unicast** cap als NVR de Lanaccess, en què s'emmagatzemarà el vídeo sense que el VMS hi intervingui. L'accés al vídeo gravat s'ha de fer sota demanda: quan un client amb permisos especials sol·liciti la reproducció d'un esdeveniment, el VMS ha de gestionar la sol·licitud al NVR corresponent, el qual ha de respondre enviant el flux de vídeo gravat per *unicast* al VMS. Posteriorment, el VMS ha de distribuir aquest mateix flux als clients que l'hagin sol·licitat i assegurar-se que cada sessió de reproducció sigui independent i sense consum innecessari d'amplada de banda.

Pel que fa a la visualització en temps real, el client ha de sol·licitar al VMS l'accés al vídeo en viu d'una càmera específica. En aquest cas, el VMS no ha de consultar el NVR, sinó que pot gestionar directament la sol·licitud amb la càmera. La càmera ha de poder transmetre el flux de vídeo en viu, tant per *unicast* com per *multicast* al VMS (el mecanisme final l'ha de decidir TMB en fase de projecte), que alhora s'ha de redistribuir als clients sol·licitadors, assegurant-se que el vídeo arriba amb la qualitat i latència adequades.

El VMS ha de ser capaç d'administrar múltiples fluxos de vídeo provinents de cada càmera, seleccionant-ne dinàmicament la resolució i la taxa de bits adequades segons el cas (visualització en viu, enregistrament o reproducció de vídeo emmagatzemat). A més, la integració amb els NVR ha de permetre que el VMS accedeixi a les gravacions sense interferir en el seu funcionament ni duplicar emmagatzematge.

Aquesta arquitectura garanteix una transmissió controlada en què el VMS gestiona les sol·licituds sense sobrecarregar la xarxa amb trànsit innecessari. La solució ha d'optimitzar el consum de recursos i assegurar una interoperabilitat correcta entre les càmeres, els NVR i el VMS sense comprometre la qualitat del servei ni l'estabilitat del sistema.

Les càmeres de la xarxa de vídeo de les línies convencionals ja disposen de diferents perfils d'*streaming* configurats, de manera que **no** cal fer la configuració inicial d'aquests paràmetres (aquesta acció es fa a través del *web service* de la càmera en el moment de la instal·lació) des de la interfície VMS, tot i que ha de suportar els protocols adequats amb les càmeres per assumir el rol d'administrador de la configuració en cas necessari.

Fluxos de comunicació i protocols

1. Enregistrament als NVR (ja implementat)

- Origen: càmeres
- Destí: NVR
- Protocol de control: ONVIF (configuració i gestió) o *driver* específic de la càmera
- Protocol de transmissió: RTSP
- Mode de transmissió: *unicast*

2. Visualització de vídeo gravat

- Origen: NVR
- Destí: VMS (servidor central)
- Protocol de control: ONVIF G o *driver* específic del NVR (per cercar i recuperar enregistraments)
- Protocol de transmissió: RTSP
- Mode de transmissió: *unicast*
- Distribució final: el VMS rep el vídeo i el reenvia en *unicast* als clients sol·licitadors

3. Visualització de vídeo en viu

- Origen: càmera
- Destí: VMS
- Protocol de control: HTTP, ONVIF o *driver* específic de la càmera per a sol·licitud i configuració de l'*stream*
- Protocol de transmissió: RTSP
- Mode de transmissió *unicast* i, opcionalment, *multicast*, si ho decideix TMB
- Distribució final: el VMS redistribueix el flux en *unicast* als clients sol·licitadors

En qualsevol cas, i tot i que la transmissió de vídeo es considera *unicast* tant per al vídeo en directe com gravat, així com la visualització i reproducció als llocs client, el VMS ha de ser compatible amb solucions ***multicast***.

4. REQUISITS FUNCIONALS

4.1. Visualització en directe

Actualment, la xarxa de vídeo de les línies convencionals de Metro té aproximadament **6.000 càmeres** distribuïdes per les seves instal·lacions. Aquestes càmeres transmeten vídeo en directe a *multicast* amb els paràmetres següents:

- Resolució: 1080p (VBR màxim 3 Mpx)
- Freqüència d'imatge: 25 FPS
- Còdec de compressió: H.264
- Taxa de bits estimada: 2,5 MBps per flux

El sistema de visualització de vídeo actual suporta 40 clients de vídeo actius, encara que per a efectes de dimensionament s'ha de considerar una capacitat de fins a 50 clients simultanis.

Cada client tindrà un límit de visualització de fins a 10 canals de vídeo simultàniament, cosa que implica que la infraestructura VMS ha de gestionar un màxim de 500 *streams* simultanis en viu.

Els requisits funcionals que ha de complir un sistema de videovigilància del tipus VMS són, com a mínim, els següents:

DIRECTE		
ID	Concepte	Descripció
VD1	<i>Unicast</i>	El sistema ha de gestionar eficientment la transmissió d'aquests 500 <i>streams</i> simultanis exclusivament per <i>unicast</i> .
VD2	Amplada de banda i trànsit de xarxa	Ha d'implementar mecanismes d'optimització d'amplada de banda i trànsit de xarxa per evitar congestió i garantir una transmissió fluida.
VD3	Escalabilitat horitzontal i vertical	Ha de ser escalable horitzontalment i verticalment per permetre l'ampliació futura de clients o càmeres sense comprometre'n el rendiment.
VD4	Mecanismes de <i>failover</i>	El VMS ha de comptar amb mecanismes de <i>failover</i> que assegurin la continuïtat operativa en cas de fallada d'algun servidor o component crític.
VD5	Preparació per a <i>multicast</i>	El VMS ha d'estar preparat per operar en <i>multicast</i> si fos necessari, per permetre'n l'habilitació sense canvis estructurals en la solució.

4.2. Reproducció

La interfície d'usuari del lloc client ha d'implementar botons que permetin dur a terme les accions següents de manera àgil:

REPRODUCCIÓ		
ID	Concepte	Descripció
REP1	Normal	Reproducció normal a velocitat 1x
REP2	Pausa	Pausa en la reproducció
REP3	Salt cap enrere	La reproducció ha de fer un salt cap enrere un temps, configurat prèviament, amb cada clic al botó o una drecera via teclat (combinació de tecles).
REP4	Salt cap endavant	La reproducció ha de fer un salt cap endavant un temps, configurat prèviament, amb cada clic al botó o una drecera via teclat (combinació de tecles).
REP5	Frame anterior	Amb el vídeo en pausa es pot saltar al <i>frame</i> anterior o al següent.
REP6	Rebobinar	Permet invertir la reproducció. Cada clic d'aquest botó ajusta la velocitat de reproducció inversa des de -1x a -2x, -4x, -8x, -16x, -32x, -64x i -128x (en funció del que permeti el NVR).
REP7	Avançar	Avança ràpidament la reproducció. Cada clic en aquest botó augmenta la velocitat de reproducció de 1x a 2x, 8x, 16x, 32x, 64x i 128x (en funció del que permeti el NVR).
REP8	Transició entre viu i reproducció	Canvi de vídeo en viu a reproducció i viceversa: ha de permetre alternar entre la vista en viu i la reproducció d'enregistraments de manera fluida.
REP9	Càmera lenta	Reproducció a càmera lenta: permet canviar entre la velocitat de reproducció normal (1x) i la càmera lenta (1/8x, 1/4x o 1/2x) en funció del que permeti el NVR.
REP10	Reproducció en bucle	Reproducció en bucle: ha de permetre establir marcadors d'inici i fi en la línia de temps per repetir un segment de vídeo.
REP11	Instantània	Desar una instantània: ha de permetre capturar i emmagatzemar una imatge fixa del vídeo en un fitxer local. El nom del fitxer ja ha d'incloure per defecte el codi de la càmera i la data i hora del moment de l' <i>snapshot</i> .
REP12	Marcadors	Desplaçar-se entre marcadors: ha de permetre la navegació ràpida entre punts predefinits en la línia de temps.

REPRODUCCIÓ		
ID	Concepte	Descripció
REP13	Zoom	Zoom digital: ha de permetre ampliar una zona específica de vídeo sense modificar la transmissió original.
REP14	PTZ	Controlar la càmera de manera remota per canviar-ne l'angle de visió i nivell de zoom. - Control i ajustament manual de la velocitat de moviment <i>Presets</i>: selecció ràpida de posicions predefinides - Zoom: ajustament manual del zoom òptic o digital - Moviments específics: fer una volta de 180° - Posicions preestablertes i rondes: canvi de posicions preestablertes, inici i detenció rondes
REP15	Transició	Alternança fluida entre vídeo en viu i reproducció.
REP16	Commutació càmera en viu	El temps de retard entre la petició de commutació de la càmera en viu i la presentació a la pantalla serà com a màxim de dos segons.

4.3. Enregistrament

El sistema VMS no reemplaçarà el sistema d'enregistrament existent, que es basa en NVR de Lanaccess distribuïts a cada estació. La interfície d'usuari del lloc client ha de permetre realitzar les accions següents de manera àgil implementant botons que permetin:

GRAVACIÓ		
ID	Concepte	Descripció
GRB1	Integració	El sistema VMS no reemplaçarà el sistema d'enregistrament existent, que es basa en NVR de Lanaccess distribuïts a cada estació. La interfície d'usuari del lloc client ha de permetre la interacció eficient amb aquest sistema.
GRB2	Gestió i reproducció	Ha de suportar sol·licituds de vídeo gravat en <i>unicast</i> .
GRB3	Enregistrament natiu escalable	El VMS ha d'estar dissenyat i llicenciat de manera que permeti l'addició futura de noves càmeres i fonts de vídeo per a enregistrament natiu sense incórrer en costos addicionals de llicència o despeses associades a l'increment de la capacitat d'enregistrament. Això inclou escenaris d'expansió del sistema, com ara l'ampliació d'estacions existents o la incorporació de nous edificis corporatius.

4.4. Descàrrega d'imatges

La interfície d'usuari del lloc client ha de permetre dur a terme les accions següents de manera àgil implementant botons que permetin:

DESCÀRREGA		
ID	Concepte	Descripció
DES1	Formats d'exportació	Els formats d'exportació de vídeo que han d'estar disponibles a la solució són els següents: ○ Format de vídeo natiu del reproductor de la solució VMS, compatibles amb àudio, informació de data i hora, indicadors de moviment i marcadors, que hereten de manera automàtica la signatura digital del vídeo original. ○ PPA. ○ Format MP4 compatible amb H.264 i MPEG-4 i d'àudio AAC. ○ L'aplicació ha de permetre convertir fitxers exportats prèviament a format natiu del reproductor de vídeo del VMS a formats ASF o MP4.
DES2	Retenció de vídeo	La solució ha de poder exportar el vídeo en els formats desitjats als servidors habilitats per TMB. La solució ha de comptar amb el seu propi servidor repositor de vídeo (servidor de descàrregues) per emmagatzemar exportacions de vídeo i captures (<i>snapshot</i>). En aquest servidor es podrà configurar el temps de retenció o l'opció que els vídeos no s'eliminin automàticament.
DES3	Gravacions Protegides	En cas que una gravació hagi de ser judicialitzada, l'operador de Seguretat (o un grup específic d'usuaris, segons es configuri) podrà marcar-la com a "protegida", assignant-li un temps addicional de conservació definit en dies. Tot i que tècnicament seria possible mantenir aquestes gravacions protegides als NVR de Lanaccess, aquesta opció no és recomanable, ja que podria comprometre la capacitat d'emmagatzematge destinada a la retenció estàndard de 30 dies. Per evitar aquest risc, la proposta és que, en marcar un vídeo com a "protegit", aquest es descarregui automàticament en un servidor propi del sistema, o en un NAS de TMB, garantint que l'emmagatzematge dels NVR no es vegi afectat. Les gravacions protegides podran gestionar-se amb flexibilitat, definint polítiques com: 1. Esborrat automàtic després de x dies.

		2. Conservació indefinida fins que un usuari autoritzat decideixi esborrar-les. 3. Delegació de permisos d'eliminació únicament a un grup específic amb privilegis sobre enregistraments protegits. El sistema ha d'assegurar tant la conservació d'evidències judicials com la disponibilitat de l'emmagatzematge principal per a les gravacions regulars.
DES4	Privilegis d'usuari	Les funcionalitats d'exportació i descàrrega de vídeo han d'estar restringides a usuaris amb privilegis adequats.
DES5	Xifratge	La solució ha de disposar de la capacitat de xifrar vídeos exportats per defecte o a voluntat de l'operador amb permisos. L'encriptació es farà mitjançant contrasenya.
DES6	Empaquetatge	Per compartir fitxers exportats en format del reproductor de vídeo natiu del VMS, hi ha d'haver l'opció d'empaquetar els fitxers amb el reproductor de vídeo del VMS i després copiar-los a un format físic (USB, CD o DVD).
DES7	Clip de vídeo	La solució ha de permetre la creació de clips de vídeo a partir de les exportacions.
DES8	Retalls/truncament de descàrregues	A partir d'una descàrrega ja feta se n'ha de poder extreure parts (períodes concrets més curts) mantenint la integritat de les imatges de manera segura, sense considerar manipular-les.

4.5. Conservació de la cadena o custòdia d'imatges

La integritat de l'evidència de vídeo és fonamental en investigacions i procediments legals. El nou VMS ha de proporcionar un flux de treball complet per a la recopilació, la gestió, la revisió i la compartició segura d'evidència amb parts internes i externes, mantenint un registre d'auditoria complet i garantint la integritat de la cadena de custòdia. D'aquesta manera la plataforma central de videovigilància ha de complir amb les següents funcionalitats per garantir i demostrar la cadena de custòdia:

DESCÀRREGA		
ID	Concepte	Descripció
CCI1	Signatures digitals	El sistema pot aplicar signatures digitals als enregistraments de vídeo per detectar qualsevol alteració posterior. Si el vídeo ha estat manipulat, la signatura digital s'ha d'invalidar per alertar sobre la possible manipulació.
CCI2	Marques d'aigua	Cal aplicar marques d'aigua visibles (amb informació de l'usuari, estació de treball, data i hora) o invisibles als vídeos en viu i enregistrats. Aquesta mesura dissuasiva ha de mitigar el risc per

		fuga d'informació i ajudar en cas necessari a rastrejar l'origen de les còpies.
CCI3	Encriptació <i>end-to-end</i>	El VMS ha d'oferir xifratge de vídeo, comunicacions i metadades per protegir la confidencialitat de l'evidència durant l'emmagatzematge i la transmissió.
CCI4	Control d'accés i permisos	S'han de poder definir rols i permisos d'usuari granulars per controlar qui pot accedir, veure, exportar o eliminar enregistraments de vídeo. Això assegurarà que només el personal autoritzat pugui interactuar amb l'evidència.
CCI5	Registres d'auditoria	El sistema ha de mantenir registres detallats de totes les accions fetes al sistema, inclòs qui va accedir a quin vídeo, quan es va exportar, si s'hi van fer anotacions, etc. Aquests registres d'auditoria són fonamentals per demostrar la cadena de custòdia.
CCI6	Gestió segura d'exportacions	En exportar vídeos, s'ha de poder aplicar mesures de seguretat com ara la protecció amb contrasenya i la inclusió de registres d'auditoria de l'exportació.
CCI7	Conservació a llarg termini	Ha d'oferir opcions d'arxivament de vídeo configurables per complir els requisits normatius i les polítiques de retenció d'evidència. S'han de poder definir polítiques per moure automàticament els enregistraments a emmagatzematge a llarg termini i gestionar-ne el cicle de vida.

4.6. Enviament a tercers

CESSIÓ DE VIDEO A TERCERS		
ID	Concepte	Descripció
FVT1	Reenviament	El sistema ha de gestionar peticions de flux de vídeo i permetre l'accés temporal i restringit a un nombre limitat de càmeres. Els tercers autoritzats seran cossos de seguretat de l'estat, els ajuntaments i altres entitats governamentals o privades designades per TMB. Hi ha d'haver un registre de les càmeres que se cedeixen, el temps de visionat i el motiu de la cessió. Cal un contracte de cessió d'imatges, que defineixi els usos i les finalitats de la cessió.
FVT2	Emmascarament	El sistema ha de permetre compartir imatges en directe amb tercers, aplicant tècniques d'emascarament per protegir la privadesa. S'ha de poder triar quina part de la imatge s'emascara i el grau d'aquest emmascarament.

FVT3	Priorització local	El sistema ha de permetre la limitació precisa de l'amplada de banda per a vídeos en viu i reproduccions i prioritzar el rendiment òptim a la xarxa local de TMB. La gestió de l'amplada de banda ha d'assegurar que les operacions crítiques de Metro i Bus no es vegin afectades per la distribució de fluxos a tercers.
FVT4	Control de l'amplada de banda	Un cop satisfetes les peticions d'amplada de banda local, el VMS ha d'oferir la capacitat de regular l'amplada de banda destinada a l'enviament de fluxos de vídeo a sistemes externs. Això permetrà controlar l'impacte en l'amplada de banda disponible entre els diferents llocs connectats.
FVT5	Autenticació	El VMS ha d'implementar l'autenticació de doble factor per verificar la identitat de tercers (policia, ajuntaments, etc.) abans de cedir imatges. El sistema ha de maximitzar la seguretat i prevenir accessos no autoritzats, per reduir el risc de robatori de credencials i atacs de pesca.
FVT6	Autorització	S'han d'establir mecanismes d'autorització per regular l'accés a les imatges que garanteixin el compliment legal i la protecció de dades confidencials.
FVT7	Comunicació xifrada	S'han de fer servir protocols xifrats com TLS/SSL per protegir la transmissió de dades que han de garantir la confidencialitat i integritat de les imatges durant la transferència d'imatges a tercers.
FVT8	Registre i auditoria	Cal mantenir un registre detallat de totes les activitats relacionades amb la cessió d'imatges. S'han d'incloure <i>logs</i> sobre qui va accedir a quines imatges, quan i per què.
FVT9	Protecció de dades i compliment legal	El sistema ha de complir totes les lleis i regulacions de protecció de dades aplicables (per exemple, RGPD). S'han d'implementar polítiques de privadesa clares i transparents per a la cessió d'imatges.
FVT10	Integritat de les imatges	Cal implementar marques d'aigua digitals i metadades per protegir la integritat de les imatges i facilitar-ne la identificació.
FVT11	Disponibilitat	El sistema ha de garantir la disponibilitat contínua de les imatges per a tercers autoritzats, amb un mínim temps d'inactivitat. S'ha de tenir un sistema d'alertes, que avisi en cas que hi hagi problemes amb la cessió d'imatges.

4.7. Interfície de visualització i navegació

La interfície d'usuari del lloc client ha de permetre dur a terme les accions següents de manera àgil implementant botons i finestres que permetin:

- Navegar entre els diferents nivells de cada estació (vestíbul, planta, andana, etc.).
- Desplaçar, fer zoom, rotar i escalar els plànols de manera intuïtiva.
- Superposar capes d'informació amb dispositius de seguretat (càmeres, sensors o punts d'accés).
- Visualitzar esdeveniments de seguretat en temps real, associant alarmes amb ubicacions als plànols.
- Seleccionar dispositius al mapa per accedir a informació, activar accions o visualitzar vídeo en viu.

VISUALITZACIÓ I NAVEGACIÓ		
ID	Concepte	Descripció
VSN1	Estructura i personalització	El VMS ha d'incloure una llista en forma d'arbre que mostri les càmeres i els dispositius organitzats jeràrquicament, que en permeti l'accés per ubicació, zona o tipus de dispositiu.
VSN2	Estructura jeràrquica	El sistema ha de permetre la personalització de la jerarquia de l'arbre, amb la possibilitat de modificar l'estructura i assignar etiquetes personalitzades a càmeres o grups de càmeres, adaptant-se a l'estructura organitzativa de TMB. Per exemple: ○ línia de Metro ○ estació ○ vestíbul ○ andana ○ càmera
VSN3	Cerca avançada	El VMS ha de comptar amb una funció de cerca avançada per localitzar ràpidament dispositius a l'arbre, fent servir filtres com ara el nom, tipus, ubicació, estat operatiu o una combinació de filtres.
VSN4	Vistes personalitzades	El sistema ha de permetre desar configuracions de vistes personalitzades per a accés ràpid a grups de càmeres o àrees d'interès.
VSN5	Informació contextual	En seleccionar una càmera de l'arbre, el VMS ha de mostrar detalls com ara la ubicació geogràfica, model, l'estat d'enregistrament i l'última connexió.
VSN6	Previsualització d'imatges	En passar el cursor o fer clic sobre una càmera de la llista tipus arbre, el sistema ha de mostrar una previsualització en miniatura d'un <i>frame</i> en temps real d'aquesta càmera.

VISUALITZACIÓ I NAVEGACIÓ		
ID	Concepte	Descripció
		S'ha d'activar sense afectar la configuració principal de la visualització o el <i>layout</i> , per poder comprovar ràpidament l'estat de la càmera i l'activitat a la seva àrea de cobertura.
VSN7	Resolució de problemes	La configuració ha d'incloure una varietat d'eines per a la solució de problemes que hi pugui haver relatius a la infraestructura de videovigilància parametritzada al VMS.
VSN8	Informes d'activitat	La configuració ha de permetre extreure històrics basats en l'activitat de les imatges. L'usuari serà capaç d'exercir accions com imprimir un informe i solucionar un problema d'un esdeveniment específic d'accés des de la vista de la generació d'informes.
VSN9	Interfície adaptativa i dinàmica	Interfície adaptable de manera dinàmica que s'ajusta en temps real al qual està fent l'operador. La interfície d'usuari per a l'operació s'ha d'adaptar de manera dinàmica a allò que l'operador està fent. Això es pot aconseguir a través de l'agrupació de <i>widgets</i> en la secció de controls.
VSN10	Àrea de treball personalitzable	L'usuari ha de tenir el control complet sobre l'àrea de treball de l'usuari a través d'una varietat d'opcions de personalització seleccionades per l'usuari. Els administradors també han de poder limitar el que els usuaris i operadors poden modificar a la seva àrea de treball a través de privilegis.
VSN11	Disseny de llistes d'esdeveniments/alarms i patrons de mosaics de visualització	Les llistes d'esdeveniments i alarmes es podran col·locar a qualsevol part de la pantalla, des de només una part de la pantalla fins a la pantalla completa, i l'usuari podrà canviar-ne la mida. L'usuari ha de definir la longitud de les llistes d'esdeveniments o alarmes. Les barres de desplaçament han de permetre a l'usuari navegar a través de llargues llistes d'esdeveniments i alarmes. La interfície d'usuari per a l'operació ha de suportar diversos patrons de mosaics de visualització, com ara un mosaic de visualització (matriu 1 x 1), 16 mosaics (matriu 8 x 8) i altres variacions.
VSN12	Suport multimonitor de la interfície	La interfície d'usuari per a l'operació ha de suportar tants monitors com adaptadors de vídeo tinguin el PC i el sistema operatiu Windows sigui capaç d'acceptar.
VSN13	Interfície d'operació	La interfície d'usuari per a l'operació ha de proporcionar una interfície per suportar les següents funcions i activitats sobre el vídeo i l'anàlisi de vídeo:

VISUALITZACIÓ I NAVEGACIÓ		
ID	Concepte	Descripció
		○ Monitorar esdeveniments des d'un sistema de seguretat en viu. ○ Generar informes, inclosos informes personalitzats. ○ Monitorar i reconèixer alarmes. ○ Crear i editar incidents i generar informes d'incidents. ○ Visualitzar mapes gràfics dinàmics i plans de pis igual que executar accions des de mapes i plans de pis gràfics i dinàmics. ○ Administrar i executar accions i macros actuals.

NAVEGACIÓ		
ID	Concepte	Descripció
NAV1	Mosaics i multipantalla	El sistema ha de suportar la visualització en múltiples pantalles i pantalla completa, per permetre l'extensió de la interfície per controlar múltiples càmeres simultàniament a mosaics configurables (1 x 1, 2 x 2, 3 x 3, 4 x 4 i fins a 10 x 10). També es podran configurar mosaics amb distribució a demanda i finestres de diferents mides.
NAV2	Limitació de mosaics per usuari	S'ha d'implementar un sistema de permisos per limitar la creació de matrius de mosaics que superin un nombre determinat de càmeres simultànies per prevenir la sobrecàrrega de la xarxa i els sistemes de descodificació.
NAV3	Perfils d'usuari i layouts	El sistema ha de permetre la creació de perfils de <i>layouts</i> configurables per a diferents torns o tipus d'operadors. Les configuracions d'usuari i els <i>layouts</i> personalitzats han de ser accessibles en iniciar sessió des de qualsevol client compatible i garantir una experiència consistent.
NAV4	Arrossegat i deixar anar	El sistema ha de permetre la reconfiguració del <i>layout</i> arrossegant i deixant anar des de l'arbre de càmeres o el pla/mapa sinòptic, i permetre la personalització en temps real.
NAV5	Videowall	El client de vídeo ha de ser compatible amb configuracions de <i>videowall</i> i multipantalla, l'operador ha de poder distribuir vistes de càmeres a diverses pantalles o monitors.

NAVEGACIÓ		
ID	Concepte	Descripció
NAV6	Configuracions	Les configuracions d'usuari han de ser accessibles en iniciar sessió des de qualsevol client compatible perquè l'experiència sigui personalitzada sense importar el dispositiu d'accés.
NAV7	Configuracions	El sistema ha de desar configuracions personalitzades de <i>layout</i> per a usuaris específics, de manera que l'operador pugui recuperar <i>layouts</i> predefinits i optimitzats en qualsevol moment.
NAV8	Etiquetes i descripcions	Opcions per mostrar etiquetes personalitzades a cada mosaic, com ara: ○ nom de la càmera ○ font (<i>multicast/unicast</i>) ○ nombre de <i>frames</i> emesos en temps real durant la connexió ○ còdec utilitzat ○ pèrdua de paquets ○ resolució ○ <i>biterate</i> ○ estat actual (connectada/desconnectada) Aquesta informació pot estar superposada o pot ser accessible des d'alguna pestanya habilitada per a cada mosaic.
NAV9	Indicadors visuals	El sistema ha de mostrar informació d'estat mitjançant codis de color als mosaics: ○ Verd: emissió en viu ○ Vermell: reproducció d'enregistrament ○ Groc: sense connexió o advertiment ○ Blanc: mosaic no assignat
NAV10	Opcions del mosaic	Cada mosaic ha de disposar de botons o mecanismes per al següent: ○ Tallar l'emissió en directe o reproducció del canal de vídeo que estiguin mostrant. ○ Mostrar el vídeo anterior o següent que s'estava mostrant prèviament en aquest mosaic. ○ Canviar entre modes d'emissió en directe a reproducció de vídeo gravat i viceversa.
NAV11	Selecció múltiple de mosaics	Es podrà fer una selecció del nombre de mosaics que es desitgin. La selecció ha de quedar clarament realçada dins del mosaic del <i>layout</i>. Calen les opcions següents: ○ Selecció de mosaics fent-hi clic a sobre

NAVEGACIÓ		
ID	Concepte	Descripció
		Selecció de tots els mosaics
NAV12	Gestió múltiple de mosaics	S'ha de disposar d'un comandament general amb botons que permetin la gestió de múltiples mosaics simultanis seleccionats prèviament, que permeti el següent: - Tancament i tall de l'emissió als mosaics seleccionats. - Arrossegat i deixar anar càmeres des de l'arbre o pla interactiu sobre els mosaics seleccionats. - Opcions de reproducció iguals sobre els mosaics seleccionats. - Canviar entre emissió en directe i reproducció.
NAV13	<i>Multistreaming</i> en un mosaic	Ha d'oferir la possibilitat de visualitzar diversos fluxos (per exemple: alta resolució i baixa resolució) d'una mateixa càmera en mosaics diferents.
NAV14	Rotació de càmeres	Ha de permetre la configuració de rotació o rondes automàtiques de càmeres en una cel·la o grup de mosaics segons un interval definit.
NAV15	Zoom digital	Ha de proporcionar la capacitat de fer zoom digital al canal de vídeo seleccionat. Això vol dir que els operadors han de poder ampliar la imatge de vídeo digitalment per obtenir una vista més detallada d'àrees específiques dins del quadre de vídeo.

4.8. Control remot

En el context d'una empresa ferroviària, el control efectiu dels llocs client distribuïts és vital per diverses raons que impacten directament en la seguretat, l'eficiència operativa i la resposta davant d'incidents. A continuació, es detallen els requisits següents:

CONTROL REMOT		
ID	Concepte	Descripció
CR1	Estacions de treball	El VMS ha de proporcionar capacitats per controlar remotament el contingut d'altres estacions de treball que executen la interfície d'usuari de monitoratge i formen part del mateix sistema.
CR2	Detall de funcionalitats	Les principals funcionalitats que ha de complir aquest mode remot són les següents: Capacitat per intercanviar càmeres, portes i zones de manera remota als requadres de visualització

CONTROL REMOT		
ID	Concepte	Descripció
		○ Capacitat per controlar el vídeo en viu i en reproducció de manera remota ○ Capacitat per canviar el patró del requadre de manera remota ○ Capacitat per crear i eliminar tasques de manera remota ○ Capacitat per iniciar i aturar els cicles de les tasques de manera remota ○ Capacitat per anar al mode de pantalla completa de manera remota ○ Capacitat per desar i tornar a carregar l'àrea de treball de manera remota
CR3	Suport de paret de vídeo	El VMS ha de suportar aplicacions per a <i>videowalls</i> que permetin connectar i controlar múltiples estacions de treball i monitors de manera simultània.
CR4	Interfície gràfica de replicació	L'operador ha de tenir accés a una interfície gràfica que mostra la replicació de les estacions de treball remotes que executen la interfície d'usuari de monitoratge.
CR5	Seguretat i auditoria	S'ha de mantenir un registre d'auditoria dels usuaris que fan ús de les funcionalitats de monitoratge remot i quines accions fan. S'ha de poder definir quins usuaris tenen permisos per exercir el monitoratge remot. Cal assegurar la privadesa dels usuaris monitorats i que el monitoratge remot es faci de manera legal.
CR6	Rendiment i fiabilitat	La funcionalitat de monitoratge remot ha de ser fiable i no ha d'afectar el rendiment del sistema. S'ha de poder monitorar la latència del monitoratge remot.

4.9. Informes

La generació d'informes en un sistema de gestió de vídeo (VMS) no només optimitza la gestió i la seguretat, sinó que també facilita enormement les auditories posteriors en què la traçabilitat, integritat i compliment normatiu són pilars fonamentals de compliment obligat per a TMB. El nou VMS ha de ser una eina completa per generar informes personalitzats, programats i fàcils de compartir, que permetin analitzar i gestionar la informació de vídeo de manera eficient i segura. A continuació, es detallen els requisits funcionals i tècnics que ha de complir el VMS respecte del mòdul d'informes:

INFORMES		
ID	Concepte	Descripció
INF1	Generació	El VMS ha de generar informes de l'estat i el funcionament del sistema. Heu de suportar informes d'alarmes, vídeo (arxius, moviment, etc.) i activitat de la infraestructura. Els informes han de ser federats per poder consolidar dades de múltiples sistemes VMS (per exemple: línies automàtiques, cotxeres de Bus i línies convencionals).
INF2	Personalització	Els usuaris han de poder generar informes genèrics, fer servir plantilles o crear informes personalitzats. La personalització ha d'incloure filtres, extensió, període de temps i columnes visibles. També han d'incloure gràfics (línies, barres, circulars, etc.). Important: no ha de requerir programari extern per generar aquests informes.
INF3	Accés controlat	Cada tipus d'informe (per exemple, informe d'alarmes o informe d'activitat) ha de tenir els seus propis permisos. Això vol dir que només les persones amb els permisos adequats podran veure o generar aquests informes.
INF4	Taulers de control	El VMS ha de permetre la creació de taulers dinàmics amb ginyes personalitzables. L'accés i la modificació de taulers es controlarà mitjançant privilegis. Els taulers es guardaran en carpetes públiques o privades.
INF5	Widgets i personalització	Els <i>widgets</i> han de permetre configurar la ubicació, la mida, el títol i el color de fons. Tipus de <i>widgets</i> : imatge, text, mosaic, pàgina web, quantitat d'entitats i informes. El VMS ha de permetre ampliar els <i>widgets</i> amb un SDK. S'ha de poder imprimir el tauler i exportar a format PNG. S'ha de poder enviar de manera automàtica per correu electrònic.

5. REQUISITS TÈCNICS

A continuació, es detallen les condicions i especificacions tècniques que ha de complir la solució VMS per assegurar el seu òptim funcionament, integració i escalabilitat dins l'entorn operatiu de TMB, un operador públic de transport de viatgers que gestiona una infraestructura de més de 10.000 càmeres en funcionament 24 x 7.

Es consideren prescripcions **tècniques mínimes** les que, si no es compleixen, fan incompatible la solució aportada entre els seus propis elements/mòduls o els sistemes centrals de TMB. De manera que, a banda de les valoracions dels aspectes tècnics, per verificar que es compleixen les especificacions mínimes, serà obligatori passar una verificació a l'entorn preproductiu i productiu de TMB per validar la viabilitat funcional i tècnica de la solució proposada.

5.1. Càmeres

Es disposa dels següents models de càmera a la xarxa de CCTV de línies convencionals:

1. Càmeres analògiques:
 - a. Models: Siemens (al voltant de 2.000 càmeres)
 - b. Codificadora IP H264 Sony Lanaccess
2. Càmeres IP
 - a. Sony EB630 i EB640 (al voltant de 1.000 càmeres en total)
 - b. Bosch DINION NBN-65023-B (al voltant de 1.000 càmeres)
 - c. Avigilon 2.0C-H5A-B2 (al voltant de 60 càmeres)

A efectes de dimensionament i disseny del sistema es considerarà l'existència d'un total de 5.000 càmeres a la xarxa de vídeo fix de línies convencionals. Es consideraran mecanismes d'escalabilitat davant de futures integracions dels sistemes de vídeo fix de línies automàtiques i sistemes embarcats a les línies de Bus i Metro.

La solució ha de complir els requisits següents:

CÀMERES		
ID	Concepte	Descripció
CAM1	Dispositius	Ha d'assegurar la compatibilitat amb les càmeres i codificadores instal·lats a la xarxa de vídeo fix de línies convencionals ja sigui a través de <i>drivers</i> nadius de les càmeres o per mitjà de protocols i estàndards suportats.
CAM2	Protocols i estàndards suportats	Ha de suportar ONVIF als perfils S, G, T i M per a compatibilitat amb càmeres i assegurar, per tant, la interoperabilitat amb els equips de TMB: ○ càmeres IP de Sony, Bosch, Avigilon ○ còdecs de Lanaccess instal·lats a les càmeres de Siemens
CAM3	Formats de compressió	Per a la transmissió de vídeo en viu: ○ H.265 (HEVC), per optimitzar l'amplada de banda sense sacrificar qualitat ○ H.264 (AVC) ○ MJPEG, per a fluxos de baixa latència en aplicacions crítiques
CAM4	Resolucions i FPS mínims	Per visualitzar l'estat de les càmeres: ○ Suport per a càmeres amb resolucions des de D1 (720 x 576) fins a 4K (3840 x 2160) ○ Mínim 25/30 FPS en temps real i compatibilitat amb modes d'enregistrament a FPS reduïts

CÀMERES		
ID	Concepte	Descripció
CAM5	Compatibilitat amb funcions de les càmeres	Des del VMS ha de poder controlar i gestionar el següent: ○ PTZ (Pan-Tilt-Zoom) en càmeres motoritzades mitjançant ordres estàndard ONVIF o de propietat (inclou trucades a preposicions i la seva configuració) ○ Paràmetres de configuració de les càmeres ○ WDR (<i>wide dynamic range</i>) i control d'exposició a càmeres avançades ○ Àudio bidireccional, que permeti la transmissió i recepció d'àudio des del client ○ Entrades i sortides de relé, per a la gestió d'esdeveniments (per exemple: activació d'alarmes)
CAM6	Gestió de <i>streaming</i> i connectivitat	○ Suport per a <i>dualstreaming</i> ○ Possibilitat de configuració d'un <i>timeout</i> de connexió per alliberar recursos quan una càmera no està en ús ○ Mecanisme de reconexió automàtica en cas de pèrdua de comunicació
CAM7	Monitoratge	○ SNMP o <i>driver</i> natiu per a monitoratge de l'estat de les càmeres ○ Verificació de l'estat de connexió (<i>online/offline</i>, latència) ○ Detecció d'errors d'<i>streaming</i> o pèrdua de paquets ○ Notificacions automàtiques en cas d'errors o canvis a la configuració ○ Detecció de canvi d'imatge de la càmera (<i>tampering</i>) ○ Altres

5.2. Videogravadores

El sistema d'enregistrament de les estacions de línies convencionals i edificis corporatius està format per NVR (*net video recorder*) del fabricant Lanaccess models:

- HM Cluster de tres targetes CPU i tres ports Gigabit Ethernet. Perfil ONVIF G
- HM Cluster de tres targetes CPU i cinc ports Gigabit Ethernet. Perfil ONVIF G

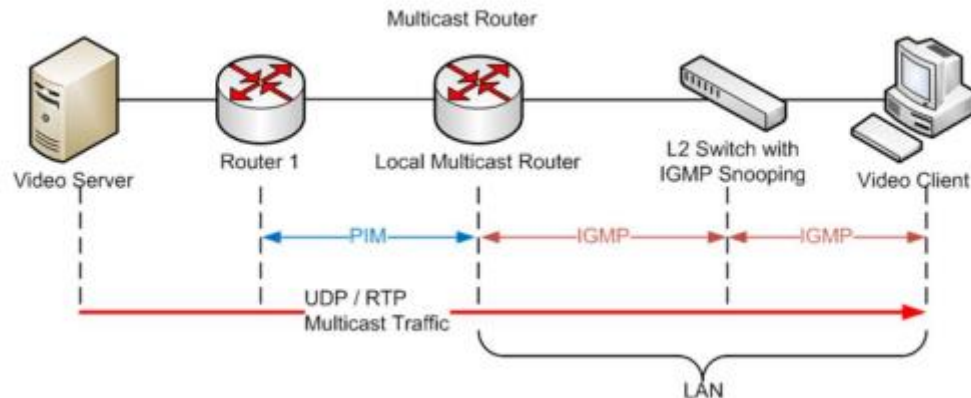
La solució proposada s'ha d'integrar amb aquests equips sense necessitat de modificar la infraestructura existent:

VIDEOGRAVADORES		
ID	Concepte	Descripció
NVR1	Integració	Suport per buscar, recuperar i reproduir enregistraments emmagatzemats als NVR sense necessitat de duplicar-los al VMS.
NVR2	Protocol	Accés a enregistraments mitjançant ONVIF Profile G o SDK de propietat.
NVR3	Cerca	Capacitat per cercar enregistraments per metadades, esdeveniments o <i>timestamp</i> . Capacitat d'establir marques de cerca al NVR.
NVR4	Format dels fitxers de vídeo	Suport per a recuperació de fitxers de vídeo en formats MP4, MKV o AV.
NVR5	Monitoratge de salut	La solució ha de poder integrar, rebre i processar esdeveniments generats pel NVR (errors de disc, pèrdua de vídeo, detecció de moviment, etc.).
NVR6	Xifratge de vídeo en trànsit	La solució ha de garantir que les connexions amb els NVR siguin segures. Pot ser a través de protocols com RTSP sobre TLS o configuracions HTTPS per accedir als <i>streams</i> de vídeo.
NVR7	Xifratge en repòs	El VMS ha de ser capaç de reconèixer i treballar amb NVR que tinguin xifratge habilitat en el seu emmagatzematge. A més, ha de permetre la desxifratge dels fitxers de vídeo quan calgui, per visualitzar-los o exportar-los.

5.3. Xarxes i protocols de comunicació

Aquest apartat detalla els requisits tècnics per a la integració del sistema de videovigilància a la infraestructura de la xarxa MPLS existent a TMB les característiques de la qual són les següents:

1. La xarxa de dades actual és una xarxa MPLS amb equipament del fabricant Cisco Systems.
2. La xarxa està configurada en mode MVPN (*multicast* VPN mitjançant túnels GRE) i utilitza el protocol PIM Sparse Mode (PIM-SM) per al maneig del trànsit *multicast*.
3. El transport *multicast* sobre MPLS es basa en el perfil **Rosen Profile 0** (mVPN GRE, conforme a la RFC 6037), utilitzant:
 - ASM (*any source multicast*) per a l'arbre Default MDT
 - SSM (*specific source multicast*) per a l'arbre de dades MDT
4. La comunicació entre rúters i *switches* d'estacions i oficines es fa mitjançant el protocol IGMP V3.



5. El sistema de videovigilància es troba desplegat en un VRF autocontingut amb suport per a *multicast*. A cada estació, hi ha una VLAN específica d'accés en què es connecten càmeres i videogravadores. Els servidors de vídeo estan ubicats als centres de processament de dades (CPD).

Limitacions d'infraestructura

1. Cada rúter d'estació té una plantilla configurada per a la reserva de recursos de memòria (TCAM) optimitzada per al trànsit de vídeo. Aquesta configuració imposa les limitacions següents:
 - Un màxim de 2.000 rutes *multicast* IPv4 en ubicacions estàndard.
 - Un màxim de 4.000 rutes IPv4 *multicast* a la instal·lació de la Sagrera, on es concentren la majoria dels clients de vídeo.
2. Els enllaços de xarxa tant a estacions com a oficines estan limitats a una capacitat d'**1 GBps**, compartida per tots els serveis presents a cada ubicació.
3. Tot i que la xarxa MPLS permet la implementació de polítiques de qualitat de servei (QoS) i *traffic engineering*, **actualment no està configurada** aquesta funcionalitat, ni se'n preveu la implementació durant el desplegament del nou sistema. Per tant, **el sistema VMS ha d'estar dissenyat per funcionar sense dependència de QoS** i garantir un rendiment equivalent al sistema actual.

Requisits funcionals de comunicació de vídeo

El nou sistema VMS ha de reproduir com a mínim la funcionalitat de transmissió actual, d'acord amb els paràmetres següents:

1. Cada càmera ha d'emetre:
 - Un flux *multicast* cap als centres de control.
 - Un flux *unicast* cap a la videogravadora corresponent.
2. El sistema local de cada estació s'ha de poder subscriure al flux *multicast* de les càmeres per a la visualització en temps real.
3. La videogravadora ha de transmetre flux *unicast* per a la visualització d'enregistraments a demanda.

Requisits d'implantació i transició

L'adjudicatari ha de tenir en compte que el sistema actual de videovigilància està en funcionament (entorn de producció), per la qual cosa la integració del nou sistema s'ha de fer garantint la mínima afectació al servei. Serà necessària la coordinació amb el departament de xarxes de TMB per a les tasques següents:

- El disseny inicial de la integració.
- La realització de proves tècniques conjuntes.
- La validació del transport *multicast* i del funcionament del sistema VMS sobre la xarxa existent.

Les intervencions que puguin afectar el servei s'han de planificar preferentment en horari nocturn o en franges de baixa demanda. No es permet emprendre accions que puguin comprometre el funcionament d'altres serveis sobre la xarxa.

Per tal de garantir la compatibilitat i integració del nou sistema de videovigilància (VMS) a la infraestructura existent de xarxa, l'adjudicatari ha de tenir en compte a més els requisits tècnics següents:

XARXES I PROTOCOLS DE COMUNICACIÓ		
ID	Concepte	Descripció
RED1	Compatibilitat amb VLAN	El sistema ha de ser compatible amb VLAN per a la segmentació del trànsit per poder separar el trànsit de càmeres, clients i servidors. Això millorarà la seguretat i el rendiment de la xarxa.
RED2	Suport per a IGMP Snooping i PIM-SM	Es requereix suport per a IGMP Snooping i PIM-SM per a la gestió eficient del trànsit <i>multicast</i> i per optimitzar l'amplada de banda i reduir la càrrega a la xarxa.
RED3	Priorització de trànsit amb QoS	El sistema ha de suportar la priorització de trànsit mitjançant QoS (DSCP o 802.1p) per garantir la qualitat de vídeo i la transmissió sense interrupcions, especialment en moments d'alta demanda.
RED4	Xifratge TLS 1.2/1.3:	S'exigeix el xifratge del senyal de vídeo i les credencials mitjançant TLS 1.2 o 1.3 per protegir la integritat i confidencialitat de les dades transmeses.
RED5	Protecció amb SRTP	El sistema ha d'implementar SRTP (Secure RTP) per a la protecció de les transmissions de vídeo en viu i prevenir la intercepció i manipulació de les imatges.

RED6	Autenticació segura	Es requereix suport per a autenticació mitjançant certificats digitals i credencials encriptades, per garantir l'accés segur al sistema i la protecció contra accessos no autoritzats.
RED7	Buffer dinàmic de reproducció	El sistema ha d'incloure un <i>buffer</i> dinàmic de reproducció per minimitzar els talls de vídeo en connexions inestables, que assegurï una visualització fluida de les imatges.
RED8	Emmagatzematge a <i>cache</i> local	Es requereix suport per a emmagatzematge en <i>cache</i> local als clients per evitar interrupcions en la reproducció de vídeo i reduir la càrrega a la xarxa central.
RED9	Taxa de bits adaptativa (ABR)	El sistema ha d'implementar ABR (<i>adaptive bitrate streaming</i>) per ajustar dinàmicament la qualitat del vídeo en funció de l'amplada de banda disponible, de manera que s'optimitzi la transmissió i es garanteixi una visualització òptima en diverses condicions de xarxa.

És crucial que el sistema VMS sigui escalable per suportar el creixement futur de la xarxa de videovigilància. La solució proposada ha de ser compatible amb els estàndards de la indústria per assegurar la interoperabilitat amb altres sistemes existents o futurs.

5.4. Federació

La solució proposada s'ha de basar en una arquitectura federada que permeti la unificació de múltiples sistemes VMS independents a una plataforma centralitzada. A continuació, es detallen els requisits funcionals i tècnics que ha de complir el VMS respecte a aquest tipus d'arquitectura:

XARXES I PROTOCOLS DE COMUNICACIÓ		
ID	Concepte	Descripció
FED1	Visió global unificada	Per garantir l'eficiència i seguretat màximes en entorns complexos i distribuïts geogràficament, com és la xarxa de transport de TMB, el sistema de videovigilància (VMS) ha d'oferir una visió global unificada. Això implica la capacitat de supervisar i controlar de manera centralitzada múltiples sistemes VMS independents des d'una única interfície intuïtiva.
FED2	Escalabilitat i flexibilitat	El VMS ha de facilitar la incorporació d'ubicacions o sistemes VMS nous a la plataforma centralitzada de manera senzilla.

FED3	Gestió centralitzada d'alarmes i esdeveniments	El sistema ha de permetre la gestió global d'alarmes i esdeveniments generats a diferents ubicacions o sistemes VMS per facilitar la resposta ràpida i coordinada davant d'incidents de seguretat.
FED4	Generació d'informes consolidats	També ha de permetre la generació d'informes globals que consoliden dades de múltiples ubicacions o sistemes VMS, cosa que facilitarà l'anàlisi de tendències i patrons de seguretat a tota l'organització.
FED5	Operació simplificada	Ha de permetre als operadors de TMB fer accions en entitats remotes (càmeres, alarmes, etc.) des d'una única interfície, per simplificar l'operació i millorar l'eficiència.
FED6	Consideracions addicionals:	S'han d'implementar mecanismes robusts per protegir l'accés als sistemes i les dades. També s'ha de tenir en compte l'amplada de banda necessària, per poder gestionar una arquitectura federada, i es garantirà en tot moment que hi hagi prou amplada de banda. La latència de la xarxa s'ha de garantir perquè els temps de resposta siguin tan baixos com sigui possible.

5.5. Planimetria

Aquest apartat descriu els requisits per a la integració del sistema d'informació geogràfica de TMB amb el nou sistema de gestió de vídeo (VMS), cosa que assegura una visualització precisa i en temps real dels dispositius de videovigilància sobre la cartografia de la xarxa de metro. La integració entre el servei GIS-TMB i el VMS s'ha de fer mitjançant una API que proporcioni els serveis següents:

- Lliurament de dades en format GeoJSON per a la representació vectorial de plànols.
- Geometries estàndard (polígons, línies i punts) per definir estructures i ubicacions de dispositius.
- Propietats d'objectes georeferenciats (nom d'estació, ID de dispositiu, metadades addicionals).
- Jerarquització de nivells o plantes dins una mateixa estació.
- Consultes i filtres per a nivells específics d'una estació.
- Sincronització de dades periòdica o sota demanda de les dades GIS amb el VMS.

Les funcionalitats clau per a la integració són les següents:

- Visualització en temps real de dispositius de videovigilància sobre plànols georeferenciats actualitzats.

- Accés a vídeo en viu i gravat des de la interfície del VMS, amb la ubicació exacta de cada càmera.
- Gestió d'esdeveniments de seguretat des d'una interfície unificada.
- Importació i actualització dinàmica de la informació des del servei GIS-TMB.

Consideracions addicionals:

- La solució VMS ha de garantir la precisió i la integritat de les dades georeferenciades durant la importació i l'actualització.
- El sistema haurà de tenir de forma nativa eines de visualització i anàlisi geoespacial dins del seu VMS.

5.6. Monitoratge

En aquest apartat es defineixen les accions de supervisió contínua de la salut del VMS i els components que conformen el servei de videovigilància de TMB. L'objectiu del monitoratge és conèixer de manera immediata el grau de prestació d'aquest servei, per la qual cosa ha d'estar preparada per generar esdeveniments, alarmes i contraalarmes.

- Esdeveniment: qualsevol fet que passa en un moment determinat que pot alimentar les eines de monitoratge disponibles a TMB.
- Alarma: qualsevol esdeveniment la presència del qual significa o pot significar l'inici d'un període de no prestació o una prestació degradada del sistema de videovigilància.
- Contraalarma: esdeveniment la presència del qual significa la finalització d'un període de no prestació o una prestació degradada d'aquest servei a les instal·lacions de TMB.

Els requisits que ha de complir un sistema de videovigilància VMS quant a monitoratge són, com a mínim, els següents:

MONITORATGE		
ID	Concepte	Descripció
MTZ1	Provisió d'inventari dinàmic	El sistema ha de proporcionar, de manera dinàmica, l'inventari de les tipologies de càmeres i NVR que conformen el sistema, juntament amb totes les característiques necessàries.
MTZ2	Accessibilitat directa	Tots els elements del VMS han de ser accessibles directament a través de la xarxa MPLS de TMB i mitjançant un protocol estàndard com ara SSH, WMI o HTTPS. Addicionalment, els esdeveniments de l'estat de salut seran accessibles a través de l'SDK (es pot fer servir per crear captures de SNMP).
MTZ3	Monitoratge continu	El VMS ha de permetre la supervisió contínua de la salut de les càmeres i NVR per assegurar un funcionament correcte i detectar errors ràpidament.

MONITORATGE		
ID	Concepte	Descripció
MTZ4	Integritat de les càmeres	El VMS ha de comprovar de manera automàtica les transmissions de les càmeres per detectar si hi va haver alteracions en aquest cas aixecarà una alarma. S'hi ha d'incloure informes sobre esdeveniments d'alteració detectats.
MTZ5	Detalls de la integritat	Pel que fa al punt anterior, el VMS permetrà definir la sensibilitat de detecció de les transmissions de cada càmera: baixa, mitjana o alta. Ha de ser possible definir la quantitat de càmeres que s'analitzen alhora. Per utilitzar la mínima quantitat de recursos, caldrà definir la freqüència d'anàlisi de les transmissions de les càmeres. Ha de ser possible conèixer les càmeres configurades per a una anàlisi posterior.
MTZ6	Definició de paràmetres	El VMS ha de disposar de mètriques que es faran servir per monitorar el sistema, com ara la disponibilitat de la càmera, la qualitat de la imatge i la confirmació d'enregistrament.
MTZ7	Generació d'alarmes	El sistema ha de ser capaç de generar alarmes automàticament en cas de detectar problemes, com ara càmeres fora de línia o errors a l'enregistrament. També contra alarmes quan detecti restabliment o reconexió amb l'element.
MTZ8	Interfície d'usuari intuïtiva	Ha de comptar amb una interfície d'usuari accessible i intuïtiva que permeti als operadors de manteniment de TMB, gestionar i monitorar fàcilment el sistema de videovigilància.
MTZ9	Capacitats de report:	El sistema ha de permetre la generació d'informes sobre l'estat i el rendiment del sistema de videovigilància, inclosa l'activitat de les càmeres i la taxa de falses alarmes.

5.7. Integritat i traçabilitat

La solució ha de garantir la responsabilitat i la transparència en la gestió de la seguretat i la integritat de les dades per a la seva traçabilitat i posterior auditoria, per això en aquest apartat es detallen els requisits següents:

INTEGRITAT		
ID	Concepte	Descripció

INT1	Encriptació de dades	Tant en trànsit com en repòs, les dades de vídeo i esdeveniments s'han de xifrar per protegir-los contra accessos no autoritzats i manipulacions. Això ha de garantir a TMB que la informació es mantingui íntegra i confidencial.
INT2	Seguretat dels logs:	Els <i>logs</i> han d'estar protegits contra qualsevol alteració o manipulació. Cal assegurar que, un cop generat un <i>log</i> , no es pugui modificar.
INT3	Emmagatzematge de logs	Els <i>logs</i> han de ser emmagatzemats durant un període determinat (a definir en fase de projecte).
INT4	Detall dels logs	Cada esdeveniment registrat ha de tenir un identificador únic que faciliti la cerca, correlació i auditoria dels esdeveniments.
INT5	Accés restringit	Només els usuaris autoritzats han de poder accedir, visualitzar o exportar els <i>logs</i> . L'accés als <i>logs</i> ha de ser auditat i controlat.
INT6	Vídeos exportats	El VMS ha de garantir que els vídeos exportats no puguin ser alterats durant el procés d'exportació i han de conservar les metadades:

TRAÇABILITAT		
ID	Concepte	Descripció
TZ1	Registres d'auditoria detallats	El VMS ha de registrar totes les accions realitzades pels usuaris, inclosos els inicis de sessió, canvis de configuració, visualització i exportació de vídeo i gestió d'alarmes. Això permetrà a TMB rastrejar qui va fer què i quan.

TZ2	Traçabilitat de vídeo	S'han de generar registres d'esdeveniments del sistema, com ara fallades de maquinari, errors de programari i alarmes, cosa que facilitarà la identificació i la resolució de problemes.
TZ3	Gestió de <i>logs</i> centralitzada	El VMS ha de permetre la visualització i l'anàlisi de <i>logs</i> , cosa que facilitarà la cerca d'informació rellevant i la generació posterior d'informes d'auditoria.
TZ4	Exportació de registres	El sistema ha de permetre l'exportació de registres d'auditoria, i esdeveniments en diferents formats (com ara CSV perquè aquest és fàcil de crear i editar amb qualsevol editor de text), cosa que en facilitarà l'anàlisi i presentació com a evidència en investigacions.
TZ5	Marques d'aigua en vídeo	El sistema ha d'implementar uns mecanismes d'estampació de marques d'aigua als vídeos enregistrats, amb l'objectiu de validar l'autenticitat del material visual extret de les instal·lacions de TMB.

6. REQUISITS D'INTEGRACIÓ

La solució VMS ha d'integrar les solucions de TMB següents:

- **Gestió d'identitats** i rols
- **TMB-GIS**: servei de mapes geolocalitzats
- **G-INFO i G-SOS**, sistemes de classificació de trucades d'interfonia
- **CCIF**, telecomandament d'infraestructures fixes d'estació

A continuació, es descriuen les més significatives.

6.1. Gestió d'identitats

En el disseny de la solució VMS, la gestió centralitzada d'identitats i accessos és un aspecte clau per garantir la seguretat i el control sobre els usuaris del sistema.

Per això, el VMS ha de desenvolupar una integració SSO basada en SAML 2.0 i OpenID Connect (OIDC) i integrar-se amb el proveïdor d'identitat corporatiu.

Els permisos de cada usuari al VMS estaran definits per rols gestionats a través de LDAP corporatiu i l'aplicació hi accedirà a través de *claims* o *assertions* (segons es faci servir OIDC o SAML2).

S'exigeix compatibilitat amb protocols estàndard d'autenticació com ara OAuth2, OpenID Connect i SAML 2.0, que facilitin un accés Single Sign-On (SSO) per als usuaris ja autenticats en altres sistemes de l'organització.

Per tal de garantir una integració fluida amb Keycloak, es coordinarà una reunió tècnica amb els equips responsables. En aquesta sessió es definiran els paràmetres específics d'autenticació, es resoldran dubtes per a aquesta integració.

GESTIÓ D'IDENTITATS		
ID	Concepte	Descripció
ID1	Autenticació centralitzada	S'ha d'implementar una autenticació d'usuaris basada en SAML 2.0 i OpenID Connect (OIDC) i integrar-se amb el proveïdor d'identitat corporatiu. Per a "dispositius" / "elements no interactius" / "sense usuaris", es podrà fer servir un mecanisme d'API-Key, o un <i>client credentials grant</i> d'OIDC per comunicar-se amb els sistemes corporatius, sempre a través de l'API de TMB.
ID2	Seguretat de credencials	El VMS no ha d'emmagatzemar contrasenyes d'usuaris localment; tota l'autenticació s'ha de delegar a Keycloak per garantir la seguretat de les credencials.
ID3	Inici de sessió	La integració ha d'implementar els fluxos de SSO i SLO corresponents segons l'estàndard utilitzat, per millorar l'experiència i la usabilitat de la solució.
ID4	Xifratge	Totes les comunicacions amb sistemes externs han d'estar protegides mitjançant TLS (xifratge de dades en trànsit). Cal utilitzar protocols segurs i evitar versions obsoletes (TLS 1.0, 1.1 i anteriors).
ID5	Grups i rols	Les autoritzacions granulars es poden aplicar al VMS i s'han de fer a base de rols definits internament a l'Active Directory de TMB, que arribaran en forma de <i>claim</i> o <i>assertion</i> per via estàndard a OIDC o SAML, respectivament.
ID6	Rols i permisos personalitzats	El VMS ha de ser capaç de definir rols que incloguin permisos granulars, com ara: ○ Accés a càmeres específiques o grups de càmeres ○ Visualització en temps real o accés a enregistraments/reproduccions ○ Capacitat de controlar càmeres PTZ o iniciar enregistraments manuals

GESTIÓ D'IDENTITATS		
ID	Concepte	Descripció
		○ Exportació de clips de vídeo ○ S'ha de limitar l'accés per horari o ubicació física de l'usuari

6.2. GIS

El servei TMB-GIS és una plataforma d'informació geoespacial que centralitza i gestiona la cartografia digital i les dades georeferenciades de tota la xarxa de Metro. Aquest sistema no només emmagatzema els plànols detallats d'estacions, túnels, accessos i altres infraestructures, sinó que també conté capes d'informació específiques sobre els sistemes implantats a la xarxa, com ara el circuit tancat de televisió (CCTV), control d'accessos, *beacons* Bluetooth, *access point* wifi, senyalització i altres elements de seguretat.

El servei TMB-GIS és clau perquè permet la integració amb el VMS, per tant, facilita la visualització en temps real dels dispositius de videovigilància sobre plànols georeferenciats actualitzats. Gràcies a aquesta integració, els operadors del centre de control podran consultar la ubicació exacta de cada càmera, accedir al vídeo en viu o gravat, i gestionar esdeveniments de seguretat des d'una interfície unificada.

TMB-GIS també és la font oficial de dades espacials de TMB, la solució VMS ha de poder importar i actualitzar dinàmicament la informació des d'aquest sistema, per assegurar una gestió eficient i centralitzada dels recursos de videovigilància a tota la xarxa de Metro.

A més de la integració de les dades que ofereix aquesta aplicació, la solució VMS ha de ser compatible amb altres formats de plànols estàndard que serviran de suport mentre no es disposi de la integració amb la font principal (TMB-GIS).

Integració de cartografia del servei TMB-GIS al VMS

En el marc de la licitació per a la implantació d'un nou sistema de gestió de vídeo (VMS), es requereix la integració de cartografia provinent del servei GIS de TMB. Aquesta integració es farà mitjançant un mecanisme d'importació de capes en format GeoJSON, per assegurar la correcta representació dels plànols dins del motor gràfic del VMS.

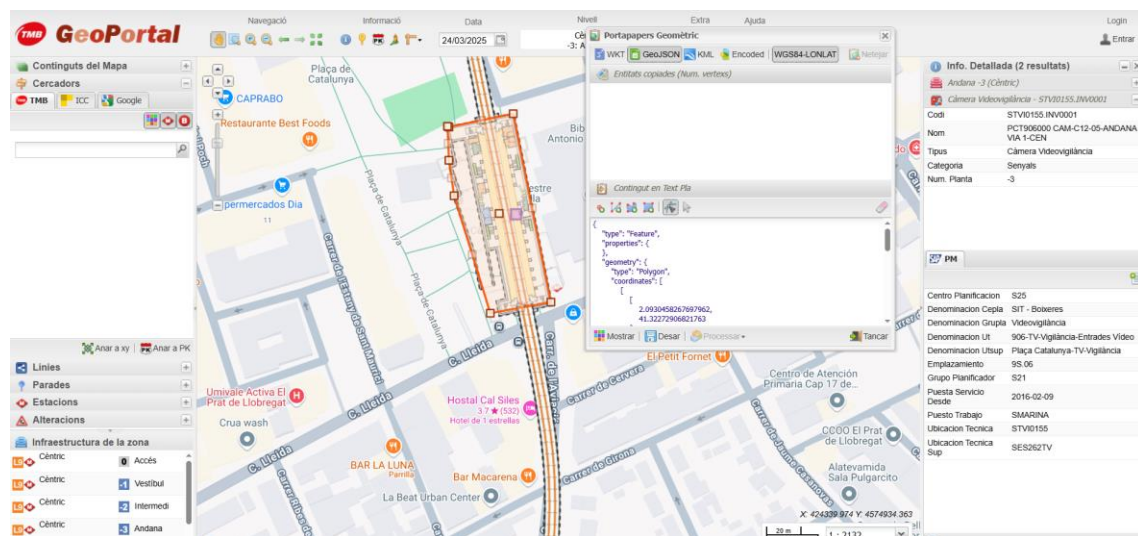
Des del servei TMB-GIS es disposarà d'una API que podrà servir les dades al VMS. La solució ha de comptar amb la següent infraestructura per a la integració:

VMS-GIS		
ID	Concepte	Descripció
GIS1	Interpretació	El VMS ha de ser capaç d'interpretar dades en el format GeoJSON, com a representació vectorial del pla sol·licitat.
GIS2	Geometries	La solució ha de suportar geometries estàndard com ara polígons, línies i punts per definir estructures i ubicacions d'elements i dispositius en format GeoJSON. Les entitats tindran informació (planta, estació, tipus d'entitat, etc.) per facilitar-ne la simbolització i el filtratge en client.
GIS3	Sincronització	El VMS ha d'actualitzar periòdicament o sota demanda les dades GIS per reflectir canvis en la cartografia.
GIS4	Implementació	El VMS podrà consultar les dades de plànols d'infraestructura de manera actualitzada mitjançant una API REST de descàrrega de GeoJSON per estació.
GIS5	Cache	El sistema ha de tenir mecanismes de <i>cache</i> per optimitzar el rendiment i evitar sobrecàrrega en la consulta de plànols.
GIS6	Parser	El VMS ha de desenvolupar un <i>parser</i> de GeoJSON que converteixi les dades rebudes en estructures compatibles amb el motor gràfic del VMS, inclòs el mapatge automàtic de nivells i jerarquies espacials dins de cada estació.
GIS7	Normalització	El sistema ha d'incorporar mecanismes de normalització i validació de dades per garantir coherència als plànols importats.

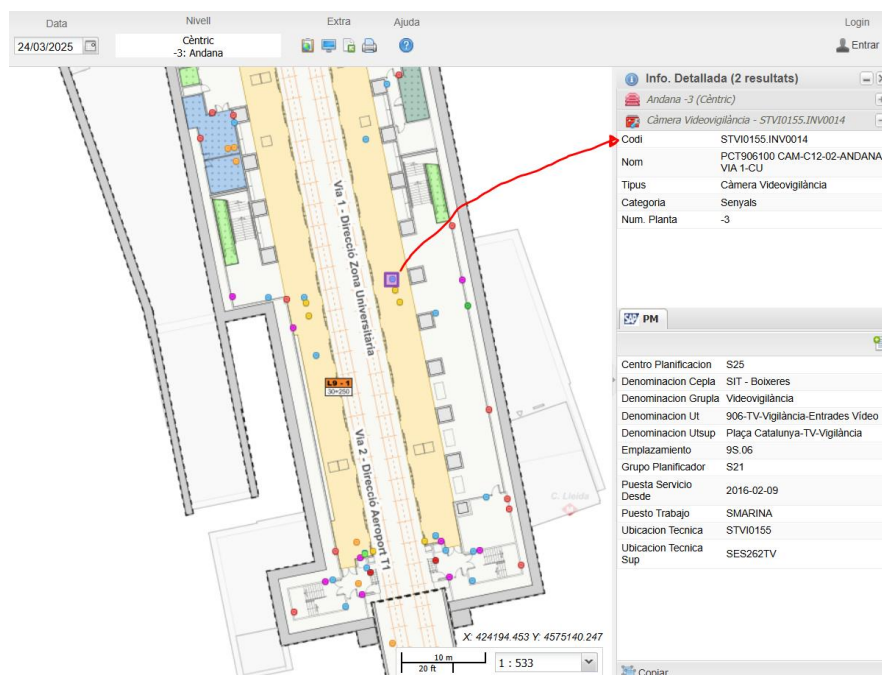
Exemple del codi GeoJSON resultant del contorn d'estació:

```
{
  "type": "Feature",
  "properties": {
  },
  "geometry": {
    "type": "Polygon",
    "coordinates": [
      [
        [
          2.0930458267697962,
          41.32272906821763
        ],
        [
          2.0935125311382747,
          41.3228015845978
        ]
      ]
    ]
  }
}
```

```
[
  2.0937861164578173,
  41.32177426168569
],
[
  2.0933462341794216,
  41.32171383042217
],
[
  2.0930833776959656,
  41.32235439896753
],
[
  2.0930458267697962,
  41.322547776913815
],
[
  2.093035097933709,
  41.32273309690765
],
[
  2.0930458267697962,
  41.32272906821763
],
]
}
}
```



Exemple d'ubicació tècnica d'una càmera de videovigilància ubicada a l'andana.



6.3. Interfonia G-INFO i G-SOS

En aquest apartat es descriu la integració entre el sistema G-INFO/G-SOS i el sistema VMS a través de l'API-TMB, que permet la transferència d'informació necessària perquè el VMS commuti la càmera que enfoca millor l'interfón de l'estació. En aquesta integració G-INFO/G-SOS actua com a productor i el VMS com a consumit de la informació.

La volumetria de peticions des dels diferents interfons repartits per les estacions és la següent:

- Interfonia G-INFO: 1.500 interfons. Es registra una mitjana de 485 trucades al dia.
- Interfonia G-SOS: 1.200 interfons. Es registra una mitjana de 710 trucades al dia.

G-INFO i G-SOS		
ID	Concepte	Descripció
INTGS1	G-INFO/G-SOS (Productor)	El sistema G-INFO/G-SOS ha de publicar les dades següents a través de l'API: ○ Data i hora de la petició per a l'inici de la commutació de la càmera ○ Número de la càmera i visor o <i>layout</i> ○ Data i hora de la petició per a la fi de la commutació de la càmera Nota: La durada mitjana d'una trucada s'estima en 30 segons.

INTGS2	API	○ L'API ha de fer servir el format JSON per transferir dades. ○ S'implementarà un mecanisme d'autenticació segur per protegir l'accés a l'API. ○ Es definirà un <i>end point</i> específic per accedir a aquesta informació. ○ L'API suportarà el protocol HTTPS.
INTGS3	Flux d'integració	○ El sistema G-INFO/G-SOS detecta l'inici d'una trucada d'interfonia al camp. ○ G-INFO/G-SOS registra la data i l'hora d'inici, i el número de la càmera. ○ G-INFO/G-SOS publica aquestes dades mitjançant l'API. ○ El sistema VMS consumeix les dades de l'API. ○ El sistema G-INFO/G-SOS detecta la fi d'una trucada. ○ G-INFO/G-SOS registra i publica la data i l'hora de fi. ○ G-INFO/G-SOS publica aquestes dades a través de l'API, actualitzant la informació de cada trucada. ○ El sistema VMS actualitza la informació de la trucada al seu sistema. ○ El VMS podrà utilitzar aquesta informació per al seu ús intern, com ara la generació d'esdeveniments o la visualització de la informació de les trucades.
INTGS4	Logs	○ El VMS ha de generar <i>logs</i> detallats que proporcionin una traçabilitat completa dels esdeveniments relacionats amb la visualització de càmeres commutades. Aquests registres són essencials per a l'auditoria, l'anàlisi d'incidents i la millora continua del sistema. ○ Cal registrar la recepció de cada esdeveniment incloent: ○ Data i hora de recepció de cada esdeveniment ○ Identificador del número de càmera que va generar l'esdeveniment ○ Informació addicional rellevant de l'esdeveniment, si n'hi hagués ○ Identificador del client que va visualitzar les càmeres ○ Confirmació del client ○ Els <i>logs</i> han d'incloure marques de temps precises i detallades. ○ Cal implementar un mecanisme de rotació de <i>logs</i> per gestionar l'espai d'emmagatzematge. ○ El VMS ha de proporcionar una interfície per a la cerca i el filtratge de <i>logs</i>. ○ Els <i>logs</i> han de poder ser exportables en format CSV.

		Es valorarà positivament la integració amb sistemes de gestió de <i>logs</i> centralitzats.
INTGS5	Escalabilitat	El sistema ha de suportar la càrrega habitual de peticions d'interfonia diària sense afectar el rendiment del VMS i ser fàcilment escalable davant un volum més gran de trucades o càmeres.
INTGS6	Latència	Ha de garantir una latència mínima ($\leq 0,5$ segons) des de la recepció de l'esdeveniment fins a la visualització de la càmera corresponent.

6.4. Telecomandament d'instal·lacions fixes (CCIF)

Hi ha aproximadament 240 portes de sortida d'emergència, l'obertura de les quals es vol monitorar mitjançant les càmeres que cobreixen la seva àrea d'influència. La freqüència dels esdeveniments és baixa.

La integració actual funciona de la manera següent:

1. El CCIF d'Emte Sistemas envia un missatge d'alarma de porta oberta (per exemple, la cadena E0111SIN01ALA006V) mitjançant un servidor web. Per redundància, l'alarma s'envia duplicada des de dos servidors diferents.
2. El consolidador de videovigilància (CVV) d'Indra rep aquest missatge.
3. El CVV localitza la càmera associada a l'alarma mitjançant una taula interna (per exemple, associa l'alarma a la càmera FL11180).
4. El CVV ordena a les estacions clients seleccionades la commutació a aquesta càmera.

Per millorar aquest procés i fer que passi per l'API de TMB, es proposa el següent:

1. L'API TMB hauria de ser el punt de recepció dels missatges d'alarma enviats pel CCIF.
2. L'API de TMB transmet aquests missatges al VMS.
3. El VMS serà l'encarregat de fer la commutació de les càmeres als clients seleccionats.

Aquesta modificació permetrà centralitzar la gestió d'alarmes a través de l'API de TMB i el VMS i optimitzar-ne la integració i millorar la fiabilitat del sistema de videovigilància.

TELECOMANDAMENT D'INSTAL·LACIONS FIXES (CCIF)		
ID	Concepte	Descripció
CCIF1	Recepció d'esdeveniments	El VMS ha de poder rebre esdeveniments a temps real des de l'API-TMB.
CCIF2	Integració	El VMS ha de comptar amb una API d'integració que permeti la recepció i el processament d'esdeveniments des de l'API-TMB mitjançant protocols estàndard (REST API, WebSockets, MQTT, Syslog, etc.).

CCIF3	Gestió d'esdeveniments	El sistema ha de poder gestionar diversos esdeveniments simultanis per poder visualitzar múltiples obertures de portes a diferents monitors o <i>videowalls</i> segons la configuració.
CCIF4	Taula de correspondència porta-càmera	El VMS ha de proporcionar una taula de correspondència configurable per mapar la ID de porta rebuda des de l'API-TMB amb la càmera o càmeres corresponents al VMS.
CCIF5	Configuració editable des d'interfície VMS	S'ha de poder modificar aquesta associació des de la interfície d'administració del VMS sense necessitat de canvis a l'API-TMB.
CCIF6	Assignació múltiple de càmeres per porta	L'associació ha de suportar l'assignació d'una o diverses càmeres per porta i permet visualitzar diferents angles segons calgui.
CCIF7	Selecció de clients per a visualització	El VMS ha de permetre seleccionar els llocs de client que visualitzaran la càmera associada a la porta de l'estació. No tots els clients requeriran aquesta funció automàticament.
CCIF8	Visualització automàtica en base a esdeveniments	En rebre un esdeveniment d'obertura de porta d'emergència, el VMS ha de poder mostrar automàticament la càmera assignada a un monitor o <i>videowall</i> segons les regles definides.
CCIF9	Regles de prioritització d'esdeveniments	Ha de permetre definir regles de prioritització que assegurin que els esdeveniments més crítics no se sobreescrueixen amb esdeveniments de menys importància.
CCIF10	Confirmació manual d'esdeveniments	Ha de tenir una opció de confirmació d'esdeveniment que permeti a l'operador marcar manualment un esdeveniment com a revisat o tancat.
CCIF11	Registre detallat d'esdeveniments a logs	El VMS ha de registrar a <i>logs</i> cada esdeveniment rebut de l'API-TMB i incloure: ○ ID de la porta d'emergència activada ○ Data i hora exacta de l'esdeveniment (<i>timestamp</i>) ○ Càmera activada en resposta a l'esdeveniment ○ Usuari que va revisar o gestionar l'esdeveniment ○ Temps de resposta entre l'esdeveniment i la visualització de la càmera
CCIF12	Capacitat	El sistema ha de suportar la recepció d'esdeveniments des de 240 portes sense afectar el rendiment del VMS.
CCIF13	Latència	La latència màxima entre la recepció de l'esdeveniment i la visualització de la càmera no ha de superar els dos segons.

CCIF14	Tolerància a esdeveniments concurrents sense errors	Heu de permetre la gestió d'esdeveniments simultanis sense que el sistema experimenti degradació en la resposta o col·lisió de visualitzacions.
--------	---	---

6.5. API – TMB

Aquest apartat descriu els requisits tècnics per a la integració del sistema VMS amb l'API propietària de TMB. Aquesta integració és fonamental per permetre, entre altres coses, la visualització en temps real de càmeres vinculades a esdeveniments específics: com ara trucades d'interfons o obertures de portes, directament des dels llocs clients del VMS. A continuació, es detallen els mecanismes d'autenticació, els *end points* i els requisits per al *front end* i *back end* del VMS.

API		
ID	Concepte	Descripció
API1	Autenticació	L'autenticació i l'autorització s'ha de fer mitjançant algun dels mecanismes de l'API de TMB (OpenID Connect o API-keys).
API2	<i>End point</i>	El VMS ha de consumir dades de l'API prèviament publicades per G-INFO per visualitzar en els clients de vídeo i en temps real la càmera vinculada a l'interfon de l'estació, restringint la visualització exclusivament al període de comunicació activa entre el client i l'ICOM-CCM. El format de resposta ha de ser JSON.
API3	<i>End point 2</i>	El VMS ha de consumir dades de l'API prèviament publicades per G-SOS per visualitzar en els clients de vídeo i en temps real, la càmera vinculada a l'interfon de l'estació, restringint la visualització exclusivament al període de comunicació activa entre el client i l'ICOM-CCM i CSPC-Seguretat. El format de resposta ha de ser JSON.
API4	<i>End point 3</i>	El VMS consumirà dades de l'API prèviament publicades per CCIF/Telecomandament IF, per visualitzar a les parades clients de CCM i en temps real, la càmera vinculada a la porta de l'estació, restringint la visualització exclusivament al període d'obertura/tancament de la porta. El format de resposta ha de ser JSON.

API5	Interfície d'usuari	Per a la interfície web del sistema VMS s'ha d'implementar un disseny de tipus <i>responsive</i> per garantir compatibilitat amb diferents mides de pantalla i dispositius. El <i>front end</i> ha de ser compatible amb les versions més recents dels navegadors següents: • Microsoft Edge • Mozilla Firefox • Google Chrome
API6	<i>Back end</i>	El <i>back end</i> ha d'incloure els aspectes clau següents: • Registre d'esdeveniments i transaccions • Generació de <i>logs</i> detallats de totes les accions fetes, incloses les transaccions amb l'API i esdeveniments dins de l'aplicació • Mecanismes de reintents i generació d'alertes • Implementació d'estratègies de reintent automàtic en cas de fallades de comunicació amb els <i>end points</i> • Generació d'alarmes i notificacions en cas de manca de resposta o errors crítics

7. ALTRES REQUISITS

Altres Requisits		
ID	Concepte	Descripció
OR1	Onvif	El sistema VMS proposat haurà d' estar certificat conforme als estàndards ONVIF Profile S, G i T, garantint la interoperabilitat amb dispositius de tercers.
OR 2	Failover	La plataforma haurà d'estar específicament dissenyada per operar en entorns d'alta disponibilitat, i incloure de forma nativa funcionalitats de redundància, commutació per error (failover) automàtica i balanceig automàtic de càrrega entre servidors.
OR 3	Federació	El sistema haurà de permetre la gestió centralitzada i federada del vídeo, amb control unificat des d' un centre d' operacions i possibilitat d' administració distribuïda.

OR 4	Integració NVR	Serà requisit imprescindible que el sistema proposat disposi d' integració comprovada amb els NVR de Lanaccess actualment implantats en les línies convencionals de TMB assegurant la interoperabilitat i continuïtat del servei.
OR 5	Modulo PSIM	El sistema de gestió de vídeo VMS objecte de la present licitació haurà de disposar d'un mòdul de gestió integral de seguretat tipus PSIM (Physical Security Information Management).
OR 6	Equip Projecte	L' integrador del sistema haurà de garantir que el seu equip de projecte estigui certificat pel fabricant en el producte VMS ofertat, per tal d' assegurar que disposa de les competències necessàries per implementar, gestionar i mantenir la solució de forma eficaç

8. REQUISITS DE MANTENIMENT, OPERACIÓ I GESTIÓ TECNOLÒGICA

Els requisits de manteniment, operació i gestió tecnològica són els següents:

REQUISITS DE MANTENIMENT, OPERACIÓ I GESTIÓ TECNOLÒGICA		
ID	Concepte	Descripció
RMOGT1	Disponibilitat	El sistema estarà sempre actiu i operatiu (24 x 7), excepte per causes tècniques justificades (per exemple: actualitzacions de parts <i>core</i> del sistema, intervenció a servidors per part de TMB, etc.) o operatives de TMB. L'interval de fora de servei sempre serà el mínim dispensable i mai no ha d'afectar l'operativa del servei de Metro.
RMOGT2	Gestió	La proposta de solució inclourà els sistemes i mecanismes necessaris per gestionar i administrar remotament tots els elements de la solució tècnica proposada. Aquest sistema ha de ser monitorable, parametrizable i gestionable de manera remota.
RMOGT3	Monitoratge	S'ha de monitorar l'estat, les alarmes, el funcionament i el versionat dels sistemes centrals, així com de qualsevol altre element rellevant del sistema i integració.
RMOGT4	Monitoratge i registre	Ha de disposar de mecanismes de monitoratge, supervisió i registre que permetin la seva correcta operació i manteniment de la solució extrems a extrem. Entre altres coses, s'ha de poder fer un monitoratge tècnic del sistema i un registre de <i>logs</i> .

RMOGT5	Monitoratge i registre	Qualsevol activitat feta al sistema i clients (de visualització <i>online</i> i diferida, descàrrega de fitxers, etc.) ha de quedar registrada i s'ha de poder verificar mitjançant <i>logs</i> accessibles només per l'administrador del sistema.
RMOGT6	Monitoratge i registre	Es disposarà d'un registre en <i>logs</i> analítics de la seva activitat, monitoratge, KeepAlive, versionat, etc.
RMOGT7	Monitoratge i registre	Tot fitxer de registre ha de vetllar perquè la informació sigui autocontinguda i contextualitzada perquè es pugui gestionar posteriorment de manera simple i ràpida. Per exemple, incloent-hi data, hora, ubicació, tipus, etc.
RMOGT8	Registres	Disposarà de <i>logs</i> (tècnics i analítics) que permetin a posteriori analitzar, detectar i fer un seguiment i <i>debug</i> de tots els mòduls, processos, les tasques que fan els usuaris i l'anàlisi de possibles anomalies del funcionament.
RMOGT9	Registres	La solució ha de tenir diferents nivells de <i>log</i> i proporcionar alta informació per a les tasques de <i>debug</i> , optimització i anàlisi.
RMOGT10	Actualitzacions	Totes les actualitzacions del programari i les aplicacions relacionades amb el sistema han d'estar autoritzades i validades per TMB.
RMOGT11	Actualitzacions	Les actualitzacions sobre el sistema es distribuïran segons una planificació acordada per totes dues parts i sempre garantint la disponibilitat del servei.
RMOGT12	Mantenibilitat	Un dels requisits bàsics del disseny del sistema és una bona mantenibilitat, definida com a 'facilitat per executar tasques de manteniment preventiu i correctiu'. El licitador ha d'indicar quines facilitats són proveïdes pel sistema en aquest àmbit (alarmes preventives, indicadors i alarmes, eines d'autodiagnòstic i proves de modularitat de la solució, actualització de mòduls en calent, etc.).
RMOGT13	Mantenibilitat	S'han d'explicitar els requisits de manteniment programat, així com els derivats de les necessitats de mantenir la funcionalitat requerida o els que poguessin derivar de la legislació de telecomunicacions, seguretat o altres en vigor. El conjunt ha de permetre avaluar el nivell de disponibilitat del sistema des d'aquest punt de vista. A més, s'han d'indicar els coeficients de fallada esperables (MTBF o similars) i la dotació d'elements redundants previstos per mantenir el nivell de disponibilitat compatible amb les necessitats de funcionament i actualització del sistema.

RMOGT14	Preventiu	S'han d'automatitzar tots aquells manteniments preventius necessaris per al funcionament correcte del sistema que ho permetin. S'entén per manteniment preventiu qualsevol acció periòdica amb freqüència inferior a cinc anys.
RMOGT15	Manteniment	La solució s'ha d'adequar als requisits de manteniment i implantació de TMB per assegurar que encaixa en els procediments i normatives de TMB.
RMOGT16	Fiabilitat	Els equips, sistemes/serveis i el seu disseny han de garantir una alta fiabilitat (mínim 99,7 %) i una alta disponibilitat. Així mateix, cal que sigui una solució robusta i precisa.
RMOGT17	Operativitat	El sistema ha d'estar totalment operatiu de manera desatesa després d'un reinici sense necessitat d'intervenció per part d'un operador o usuari.
RMOGT18	Disponibilitat	El disseny del sistema i les característiques dels seus components han de permetre una disponibilitat del 99,99 %. Les prestacions de fiabilitat dels elements crítics han de requerir un disseny amb elements tolerants a errors. L'oferent ha d'indicar els aspectes de la seva arquitectura que garanteixen una alta fiabilitat del sistema i una alta disponibilitat dels serveis: arquitectura resistent a errors, redundància d'elements crítics, funcionaments degradats d'operació, etc. El licitador ha d'explicitar els modes de funcionament degradats.
RMOGT19	Obsolescència	S'ha de garantir durant un període mínim de 10 anys la mantenibilitat, actualització i evolució de la solució proposada pel licitador.
RMOGT20	Acords de nivell de servei	Els serveis tecnològics que proveeixi el contractista o qualsevol actor del sistema s'han de regir mitjançant acords de nivell de servei. Durant la fase d'enginyeria es definiran els serveis tecnològics i conseqüentment i com a mínim: 1. Els ANS (és a dir, SLA) 2. Els indicadors relacionats (és a dir, FOM)
RMOGT21	Històric	Per a totes les dades d'aplicació que s'utilitzen i versionats de programaris, s'ha de presentar un pla de gestió d'històrics (arxivat o eliminació).

RMOGT22	Pla de formació	L'adjudicatari ha d'elaborar, durant la fase de disseny, un pla de formació que contemplarà tots els aspectes relatius a la formació dels usuaris, gestors i mantenidors del sistema. Aquesta formació ha de garantir el nivell de formació suficient per garantir que el personal involucrat en TMB té el coneixement suficient del sistema, la seva operació i manteniment. Aquest ha de ser revisat i aprovat per TMB.
RMOGT23	Pla de formació	La formació s'ha d'impartir de la manera següent: • Previ al VMP: formació necessària perquè els rols de TMB i tercers puguin complir les seves funcions mínimes a partir de la posada en marxa del VMP del sistema. • Posterior a la VMP: completar la formació no impartida en el punt anterior. També formacions que apliquin a ampliacions posteriors al VMP fins a assolir el cent per cent dels requisits i funcionalitats del sistema. Aquesta formació ha de ser teoricopràctica per assimilar millor el temari. Addicionalment, s'ha de lliurar tota la documentació relacionada amb aquesta formació, de la qual s'haurà d'entregar una versió audiovisual per fer-la servir a TMB. Aquesta documentació ha de ser revisada i aprovada per TMB.
RMOGT24		Hi ha tres formacions diferenciades amb, com a mínim, el temari següent: • Formació a mantenidors de nivell 1 (tres sessions): ○ Descripció del sistema i arquitectura ○ Gestió del sistema vertical ○ Interpretació d'alarmes del sistema ○ Procediments de diagnosi centralitzats i resolució d'incidències ○ Gestió i inventariat del sistema ○ Instal·lació de clients ○ Altres • Formació gestors i responsables del sistema (tres sessions sota la mateixa formació): ○ Descripció del sistema, arquitectura i integracions del sistema ○ Descripció de funcionalitats, modificació de configuració/paràmetres, altes/baixes d'equips i usuaris, compartició amb tercers, etc. ○ Procediments de diagnosi centralitzats i resolució

		d'incidències ○ Gestió i inventariat del sistema ○ Gestió avançada del sistema ○ Instal·lació de clients i ús general de les natives (incloses interfícies d'administració, entre d'altres) ○ Altres • Formació a usuaris de les natives de vídeo (nou sessions) ○ Descripció general del sistema i les seves funcionalitats ○ Ús dels clients de vídeo La formació s'ha de basar en tot moment en una documentació prèviament redactada i aprovada per TMB i la direcció tècnica del projecte. La documentació completa, en format digital i en paper, s'ha d'entregar al començament de la formació de cada grup. Així mateix, atès que els usuaris de les natives treballen en tres torns (matí, tarda i nit), i que cobreix les 24 hores, s'han d'impartir aquestes formacions repartides a totes les franges horàries segons criteri de TMB. Com que els usuaris poden tenir diferents nivells d'accés/permisos sobre l'aplicació, les formacions han de començar per les parts comunes i, posteriorment, les específiques de cada rol per poder unir en una mateixa sessió de formació a diferents rols d'usuari que siguin usuaris de la nativa de vídeo. L'adjudicatari ha d'adaptar-se a les dates i horaris establerts per TMB per impartir els cursos de formació, en funció de la disponibilitat del personal.
RMOGT25	Pla de manteniment	L'adjudicatari ha d'elaborar durant la fase de disseny un pla de manteniment que contempli els aspectes relatius al manteniment preventiu, correctiu, predictiu i gestió de l'obsolescència de la solució oferta. El pla ha de ser d'acord amb l'explotació prevista, ha de ser revisat i aprovat per TMB.
RMOGT26	Pla de manteniment	El pla de manteniment ha de recollir totes les mesures per mantenir en perfecte estat operacional els sistemes.
RMOGT27	Pla de manteniment	Durant l'execució del projecte i del període de garantia l'adjudicatari ha de dur a terme les tasques definides en el pla de manteniment (correctiu, preventiu, etc.) de la solució completa.

RMOGT28	Garantia	La solució ha de tenir una garantia de quatre anys. La garantia començarà a comptar després de l'acceptació provisional del sistema per part de TMB. L'acceptació provisional es donarà després de complir-se totes les condicions següents després de la posada en marxa de la versió final que integri totes les funcionalitats i cobreixi el cent per cent dels requisits d'aquest plec: • 30 dies seguits sense cap incidència • Correcció els problemes o incidències detectades fins aquest moment del sistema complet • Lliurament i acceptació de la documentació Les correccions que impliquin canvis en la configuració o nous versionats implicaran el reinici dels 30 dies sense incidències. Les noves versions posteriors derivades d'utilitzar la bossa d'hores no implicaran reinici de la garantia, però aquestes modificacions sí que estaran incloses fins a la finalització de la garantia global o sis mesos després de la seva posada en producció (el que passi més tard). L'acceptació final del sistema es farà quan s'acabi el període de garantia.
RMOGT29	Garantia	La garantia ha d'incloure el suport i solució sense cap cost addicional per a TMB de les incidències i errors del sistema. La resolució d'incidències s'ha de fer de manera ràpida i eficaç per tal d'assegurar la disponibilitat immediata dels sistemes.
RMOGT30	Manteniment	El licitador ha d'assumir totes les tasques del pla de manteniment durant la implantació i garantia del sistema amb les següents excepcions que farà TMB: • El primer nivell bàsic de la solució a escala central i SW el farà el personal de TMB amb prèvia formació/documentació i habilitats amb el monitoratge corresponent. El seu abast serà seguir els procediments establerts als documents de lliurament d'entorn del sistema al departament de TLC o que consideri TMB. De manera general, les accions que podran fer serà revisió d'alarmes, reinicis de servidors, reinici de serveis, etc. En cas que la incidència no pugui o hagi de ser resolta per TMB segons el que descriu el paràgraf anterior, s'avisarà el nivell 1 o 2 del licitador que depenent de l'impacte ha d'activar el servei 24 x 7 o solucionar amb el servei 8 x 5. El servei de 24 x 7 o 8 x 5 dependrà de com de crítica sigui la incidència/avaria. A continuació, es descriuen les avaries segons el nivell i la gestió: - o Nivell 1: quan impacta greument en el sistema, de manera que es perden les principals funcionalitats del sistema a la xarxa, línia, tram o grup d'estacions o lloc central. Són avaries que afecten greument l'explotació i l'operació.

		• Disponibilitat 24 x 7. • Temps màxim de resposta remota: immediata. • Temps màxim de diagnòstic: dues hores. • Temps màxim de restabliment del sistema: quatre hores. o Nivell 2: quan es perden les funcionalitats principals del sistema i pot afectar totalment o parcialment una estació. • Disponibilitat 24 x 7. • Temps màxim de resposta remota: dues hores. • Temps màxim de diagnòstic: quatre hores. • Temps màxim de restabliment del sistema: vuit hores. o Nivell 3: quan no impacten greument en el sistema implicat i només es perden funcionalitats secundàries del sistema a la xarxa, línia, tram o grup d'estacions o lloc central. • Disponibilitat 8 x 5. • Temps màxim de resposta remota: immediata. • Temps màxim de diagnòstic: vuit hores. • Temps màxim de restabliment del sistema: 24 hores. Es considera horari laborable (8 x 5) de dilluns a dijous de 8.00 a 17.00 i divendres de 8.00 a 14.00, excepte els dies festius oficials. Per poder fer aquest manteniment el proveïdor facilitarà els mitjans de comunicació necessaris (per exemple: telèfon i correu electrònic de contacte). El temps màxim de resposta i resolució començaran a comptar des de la primera comunicació al proveïdor (respongui o no).
RMOGT31	Propietat intel·lectual	TMB tindrà en exclusiva la propietat intel·lectual de tot el material que sigui elaborat per l'adjudicatari en execució del contracte i, en particular, de tots els drets de propietat intel·lectual patrimonial, industrial i d'imatge que se'n derivin. Això també inclou tots els dissenys, desenvolupaments, personalitzacions, adaptacions i instàncies. El contractista ha de lliurar tots els codis font que elabori específicament per al projecte i la documentació relativa a l'especificació, disseny i implementació, a més de documentar i facilitar els entorns de desenvolupament i llibreries necessaris per a la seva compilació i enllaç de tots els desenvolupaments directes i indirectes. Serà propietat de TMB el resultat dels serveis, així com material i documents que es facin en compliment del contracte. A l'efecte dels paràgrafs anteriors, l'adjudicatari es compromet al lliurament de tota la documentació tècnica i funcional, així com materials i lliurables generats durant la prestació del servei i en el procés d'anàlisi, disseny, desenvolupament, implementació i proves. Tota la documentació elaborada i els resultats obtinguts per l'adjudicatari en execució del contracte seran propietat de TMB. Per als elements de programari que es desenvolupin específicament dins del projecte, caldrà lliurar les eines necessàries amb el codi font del sistema (per exemple, en una màquina virtual de TMB) i el seu corresponent entorn de desenvolupament, tot això correctament configurat. També cal lliurar un document que expliqui els passos que cal seguir per, partint del codi font, es pugui arribar a obtenir el paquet de distribució de l'aplicació.

RMOGT32	Llicències	Tota la solució que estigui desenvolupada o subministrada dins del projecte ha d'estar correctament llicenciada a nom de Ferrocarril Metropolità de Barcelona, SA, amb llicències que en permetin la reutilització posterior en cas de substitució d'elements o ampliació. Hi ha llicències que han de cobrir tot el període del projecte (implantació i garantia).
RMOGT33	Fiabilitat	Els sistemes dissenyats i oferts en aquest àmbit han de garantir la precisió i la robustesa de tots els sistemes que el componen i la traçabilitat de la informació relativa. S'han d'indicar els aspectes de l'arquitectura que garanteixen una alta fiabilitat del sistema i una alta disponibilitat dels serveis.

9. REQUISITS DE GESTIÓ DEL PROJECTE

REQUISITS DE GESTIÓ DEL PROJECTE		
ID	Concepte	Descripció
RGP1	Fases	L'especificació, el disseny, la implementació i, en general, qualsevol etapa/fase han de ser acordats amb TMB. No es pot passar d'una etapa a l'altra fins a l'aprovació de TMB per a la solució global o parcial en cas de dividir-se en blocs. TMB es reserva el dret d'aprovació de totes les etapes/fases.
RGP2	Pilot MVP	L'adjudicatari ha de fer un pilot basat en la primera versió mínima producte (MVP) del sistema proposat. Durant la fase d'enginyeria, TMB definirà detalladament l'abast del pilot. El MVP ha d'incorporar, com a mínim, les funcionalitats essencials establertes per TMB a l'inici del projecte, i incloure: • Clients pesants i lleugers accessibles via interfície web amb funcionalitats principals. • Un nombre determinat de càmeres i videogravadores integrades, segons les especificacions inicials de TMB. • Transmissió <i>multicast</i> entre VMS i càmera en directe. La validació i acceptació del pilot MVP per part de TMB serà condició indispensable per començar al desplegament generalitzat del sistema. Així mateix, aquesta validació marcarà l'inici de les accions de formació al personal de TMB, en cas que encara no s'hagin iniciat.
RGP3	Lliurament entorn	El projecte ha de passar el conjunt de les fases ITIL que componen la transició del servei. Aquestes fases inclouen el lliurament del servei al departament d'operacions de l'àrea de tecnologia.

RGP4	Control de qualitat	Tots els lliurables de programari i documentals que es deriven del projecte, han de passar els controls de qualitat que TMB apliqui. Aquests lliuraments no es donaran per tancats fins que no tinguin la qualitat necessària i siguin aprovats per TMB.
RGP5	Control de versió	El sistema ha de tenir una gestió de versionat del programari que en permeti el control, la gestió i el manteniment. Un cop versionat ha de seguir les polítiques de TMB en cas de ser elaborat ad hoc per al projecte.
RGP6	Nomenclatura	L'adjudicatari ha de seguir i respectar l'estructura i la nomenclatura de tots els lliurables, ja sigui documentació o programari elaborat ad hoc, basant-se en les directrius de TMB.
RGP7	Ubicació dels treballs	Els serveis s'han de prestar de manera prioritària des de les instal·lacions de l'adjudicatari. TMB habilitarà un servei de connexió externa. Per a aquells serveis que TMB consideri que s'han de fer a les seves dependències (reunions complexes, validació de lliuraments, formacions, etc.), se sol·licitarà a l'adjudicatari que es desplaci amb una antelació mínima suficient i tindrà l'obligació l'aportació de les eines i altres aspectes relacionats que siguin necessaris per a la prestació d'aquest servei.
RGP8	Pla d'acceptació i proves	L'adjudicatari ha d'elaborar, durant la fase de disseny, el pla d'acceptació i proves (unitàries, integració, funcionals, extrems a extrem o d'estrès, entre d'altres) necessàries que permetin garantir el funcionament correcte de tots els elements. Aquest pla ha de concretar tot l'esquema d'acceptació especificat als plecs, amb la descripció de les fites més significatives i els procediments associats. Cada conjunt de proves ha de tenir la documentació corresponent, així com el resultat de la seva execució (seguiment i control dels errors trobats, per exemple). Ha de ser revisat i aprovat per TMB.
RGP9	Seguiment i control	L'adjudicatari ha de proposar i executar un pla de seguiment i control del projecte (reunions i informes en format digital periòdics, etc.) que TMB ha d'aprovar. L'objectiu principal serà conèixer l'avenç del projecte tenint en compte l'estat de la planificació i els possibles riscos i desviacions, etc.
RGP10	Comunicació	La comunicació durant fase de disseny, implementació, proves i posada en marxa de la solució, sobre aspectes tecnològics del projecte, es podrà fer directament amb els especialistes del licitador per a una millor coordinació i agilitat en aquestes fases.
RGP11	Lliurables	Llista detallada de la relació de documents que s'han de lliurar. Es consideren lliurables obligatoris mínims els següents documents i arxius tècnics: Especificació de requisits

		• Especificació funcional i de disseny detallat: utilitzant diagrames de casos d'ús, escenaris, diagrames de seqüència, model de processos, model de dades, disseny tècnic gràfic de les aplicacions, plànols, esquemes elèctrics, etc. • Projecte constructiu • Documentació <i>as build</i> de la solució • Plans: pla de conformitat, pla d'acceptació, pla d'instal·lació, pla de qualitat, pla de manteniment, pla de formació, pla de seguretat, etc. • Manuals d'operació, administració, manteniment i instal·lació i usuari. El manual d'usuari ha d'incloure no només la instal·lació de l'aplicació, sinó també si es fan personalitzacions al servidor/PC (per exemple: forçar un idioma o una zona horària concreta, excepcions de l'antivirus, etc.). • Document de lliurament d'entorn • Protocols de proves FAT, SAT, pilot i seguiment • Procediments d'anàlisi de fallades • Tota la documentació involucrada en la gestió control i seguiment del projecte (planificació, informes de progrés, actes, etc.) • L'adjudicatari ha de lliurar la totalitat del codi font del programari desenvolupat específicament (ad hoc) per al projecte de TMB. Aquest codi font ha de ser funcional, compilable i estar degudament documentat. Com a part del lliurament, el codi font s'ha de publicar en un dipòsit designat dins de l'organització de TMB a la plataforma GitHub. S'ha de garantir que TMB tingui control total i accés exclusiu a aquest repositori, així com qualsevol a altre document generat durant el projecte. El projecte no es considerarà com a finalitzat fins que no s'entregui la documentació i les fonts dels desenvolupaments fets específicament per a TMB.
RGP12	Documentació	El licitador pot adjuntar a la seva oferta tota la informació complementària que consideri d'interès.
RGP13	Organització	L'adjudicatari garanteix que els recursos humans destinats per fer els treballs derivats d'aquest contracte són suficients en nombre, coneixements i experiència i que aquest es pot executar totalment segons els temps i dates límit descrits en aquest plec.
RGP14	Recursos materials i tècnics	L'adjudicatari posarà a disposició del projecte tots els recursos tècnics necessaris per desenvolupar-lo i implantar-lo. Les empreses licitadores han de presentar una relació dels recursos tècnics que es posaran a disposició de l'obra, sobre la base de les necessitats

		plantejades al present plec. Es valorarà negativament la inclusió d'elements i recursos superflus.
RGP15	Planificació	El licitador ha de planificar i prioritzar tasques. Aquesta planificació ha de ser consensuada i aprovada per TMB.
RGP16	Valor afegit	Descripció de les millores aportades pel licitador: El licitador ha d'indicar les prestacions que ofereix que no estiguin especificades o no estiguin sol·licitades al plec i que consideri rellevants per desenvolupar millor el servei.
RGP17	Beca d'hores evolutives	El licitador ha d'incloure a la seva oferta una bossa mínima de 200 hores destinada al desenvolupament, la validació i la implantació d'evolutius del sistema durant l'execució del projecte. La gestió i el consum d'aquesta bossa serà definida per TMB durant el transcurs del projecte i es durà a terme de manera aproximada segons el procediment següent: • Sol·licitud: TMB sol·licitarà una millora o evolució concreta del sistema i requerirà al proveïdor una estimació d'hores necessàries. • Estimació: el proveïdor ha de presentar una estimació detallada en hores i incloure-hi totes les fases implicades (anàlisi, desenvolupament, validació, posada en marxa als diferents entorns, etc.), així com una data estimada per disposar d'una versió funcional en entorn de desenvolupament. • Aprovació: TMB avaluarà l'estimació presentada i podrà: a) Aprovar-la b) Sol·licitar aclariments o ajustaments c) Desestimar la petició • Execució: un cop aprovada la sol·licitud per TMB, el proveïdor durà a terme el desenvolupament i es coordinarà amb TMB per validar-la i posar-la en marxa. Només es podran executar i facturar aquelles hores i conceptes prèviament aprovats i validats per TMB. No s'admetran facturacions per hores no executades o no validades dins del marc del projecte. El control del consum d'aquesta bossa s'ha de fer conjuntament entre TMB i el proveïdor, per garantir la traçabilitat i la transparència en el seu ús.
RGP18	Preus	El licitador ha de garantir el manteniment del preu de les llicències durant la vigència del contracte en cas que TMB vulgui ampliar les inicialment previstes en aquest plec.
RGP19	Preus	Cadascun dels preus de les ofertes ha d'incloure la verificació, posada en marxa dels serveis, formació tècnica, documentació, garantia del sistema i qualsevol altre servei necessari perquè el sistema funcioni correctament.
RGP20	Preus	Tots aquells costos que es generin per dur a terme el bon funcionament del projecte s'entenen que estan inclosos en els preus unitaris indicats a l'oferta.

RGP21	Preus	No s'accepta cap increment de cost en concepte de costos imprevistos.
RGP22	Seguiment	Durant tota la fase de projecte s'han de fer reunions setmanals de seguiment i control, a les instal·lacions que TMB designi.

10. PLANIFICACIÓ I METODOLOGIA

10.1. Fases del projecte

L'adjudicatari ha de presentar un pla detallat de les fases i tasques necessàries per a la correcta execució del projecte que inclogui, com a mínim, les etapes següents (les quals han de ser acordades i aprovades per TMB). Cada fase individual requerirà l'aprovació de TMB abans de procedir a la següent.

1. Enginyeria i disseny:
 - Anàlisi i definició de requisits del projecte
 - Disseny detallat de l'arquitectura i les integracions del sistema VMS i el seu desenvolupament
 - Disseny i desenvolupament de la solució i integracions amb sistemes existents
 - Elaboració i execució de plans de proves i validació
2. Replanteig i preinstal·lació. Pot incloure visites tècniques a les instal·lacions: estacions, CCM, sala de seguretat a la Sagrera i Sagrada Família.
3. Desplegament i instal·lació:
 - Desenvolupament d'un pla de migració del sistema consolidador al VMS, que en garanteixi la coexistència durant la transició
 - Instal·lació de l'arquitectura central a la granja de servidors virtuals de TMB
 - Instal·lació del programari en llocs de clients pesants, web i mòbils
 - Verificació i acceptació de cada tasca mitjançant llistes de control (*checklist*)
 - Posada en marxa progressiva del sistema VMS
4. Migració i apagat ordenat del sistema consolidador de videovigilància
5. Documentació completa del sistema VMS, inclosos els manuals d'usuari, les guies d'instal·lació i configuració, la documentació tècnica, etc.
6. Formació al personal de TMB
7. Garantia i manteniment
8. Coordinació, seguiment i control del projecte:
 - A l'inici del projecte, l'adjudicatari ha de presentar un pla detallat amb les fases, les dependències, la durada de tasques i les fites.
 - Coordinació, seguiment i control continu del projecte i les seues fases i fites
 - Informes de progrés regulars a TMB

10.2. Fites Rellevants

A continuació, s'indiquen a grans trets les fites més rellevants que hi ha al projecte i ha de complir l'adjudicatari. Els mesos són relatius a la formalització de l'adjudicació.

- Abans de començar amb els treballs, caldrà aixecar acta CAE de PRL.
- 5è mes: posada en marxa pilot MVP.
- 8è mes: posada en marxa en producció de l'última versió del programari en entorn central i clients que inclogui tots els requerits en aquest plec.
- 12è mes: completar totes les tasques i requisits del plec a les tasques relacionades amb la garantia i el manteniment.

11. Prova inicial de verificació

A l'inici del contracte, màxim en un mes des de la formalització del contracte, el proveïdor haurà d'haver lliurat amb èxit una prova inicial de verificació per a la seva revisió per part de FMB.

FMB disposarà d'un termini d'una setmana per revisar-la i validar-la amb els següent punts:

- a) Clients pesants i lleugers accessibles via interfície web,
- b) Un nombre determinat de càmeres integrades, segons les especificacions inicials de TMB.
- c) Verificació del correcte funcionament del sistema amb transmissió de vídeo a la xarxa MPLS de TMB, tant en unicast com en multicast.

En cas que la prova no sigui aprovada per FMB en el termini indicat, l'adjudicatari disposarà d'un termini d'una setmana per presentar una proposta amb les modificacions sol·licitades per a FMB. En cas de no complir amb les modificacions sol·licitades en el termini indicat, no serà aprovat per FMB.

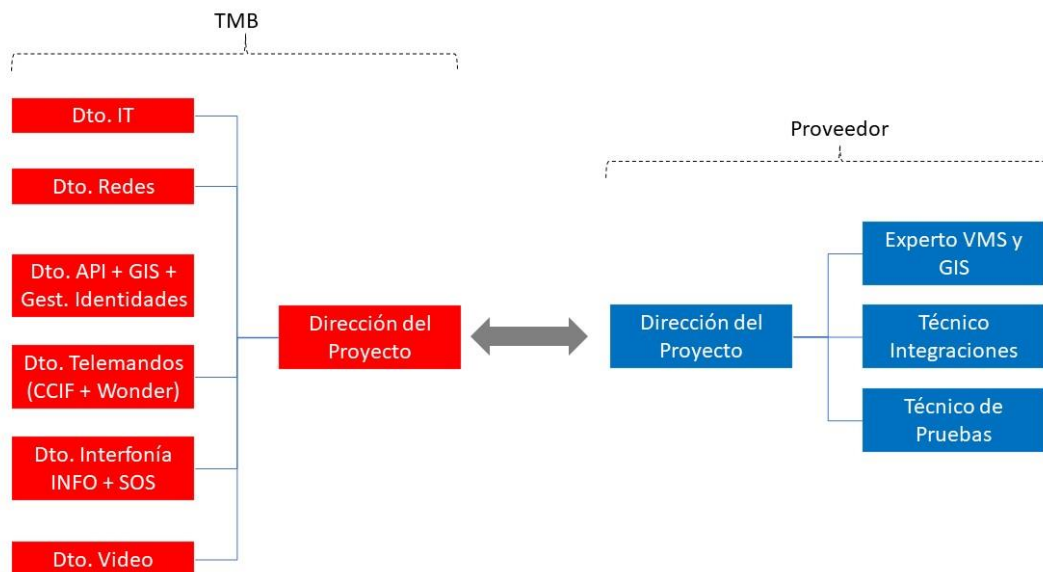
Si, una cop transcorreguts els terminis indicats la prova continua sense ser aprovada per FMB es considerarà que el contracte no ha estat formalitzat, sense que el inicial adjudicatari tingui dret a indemnització ni compensació alguna per cap concepte i reservant-se FMB el dret a reclamar una indemnització de fins al 3% de l'import d'adjudicació de licitació. Així mateix, és procedirà a adjudicar el contracte al licitador que hagi presentat la següent oferta amb millor relació qualitat-preu, prèvia presentació de la documentació exigida a la clàusula 22.8 del PCP

12. EQUIP DE TREBALL

L'equip assignat al projecte ha de tenir un coneixement molt ampli i experiència necessària per donar resposta a tots els requisits i abasts de les tasques especificades al present plec.

En l'arrencada del projecte el licitador ha de desenvolupar els perfils i el nombre de persones que han de formar l'equip de projecte evolucionant la proposta de l'oferta. Aquesta proposta ha de ser consensuada i validada per TMB. L'equip s'ha de definir en un organigrama. El contractista ha d'explicitar amb detall el personal facultatiu que, sota la seva dependència, durà a terme els diferents treballs del projecte.

La proposta d'organigrama ha de comptar com a mínim amb els perfils i equips següents que el licitador ha d'ampliar amb els recursos necessaris per a la correcta consecució del projecte en abast, qualitat i temps:



A continuació, s'indiquen alguns comentaris d'alguns dels perfils/rols de l'organigrama mínim anterior (**no** és una llista **exhaustiva** de funcions ni característiques):

- **Expert en VMS i GIS:** es tracta de la persona o persones encarregades de la parametrització de la plataforma VMS a les necessitats de TMB quant a diferents marques de càmeres, NVR locals en estació, xarxa MPLS i altres condicionants esmentats en aquest plec. També s'encarrega de la integració amb el GIS de TMB basat en el protocol GeoJSON.
- **Tècnic de proves:** la persona o persones encarregades de confeccionar la *checklist* de proves abans de la posada en servei en producció de cadascuna de les versions centrals i de clients, etc.
- **Gestor de projecte:** la persona o persones responsables de la planificació, supervisió, execució i tancament del projecte del nou sistema de videovigilància. Això inclou la gestió de l'abast, el temps, els costos, la qualitat, els recursos humans, les comunicacions, els riscos i les adquisicions del projecte, així com assegurar la consecució dels objectius definits dins de les restriccions establertes.

TMB valorarà la idoneïtat de les persones assignades a l'execució del projecte i podrà exigir, quan ho consideri oportú, la substitució de part o de la totalitat del personal assignat a l'execució de l'obra. El contractista ha d'acceptar i complir aquesta substitució en el termini de les dues setmanes següents a la comunicació feta per TMB.

Qualsevol canvi en el personal assignat a l'execució de l'obra ha de ser comunicat i acceptat prèviament per TMB.

13. MEDI AMBIENT

En aquest apartat es defineixen de manera general algunes premisses relacionades amb la gestió mediambiental de l'activitat licitada que el proveïdor ha de complir en cas que apliqui segons la naturalesa de cada tasca del projecte:

Criteri	Descripció	Condicionants
Impressió d'informes (documents de treball o documents finals)	En cas que sigui necessària la impressió de qualsevol document de treball, s'ha d'acordar amb TMB si s'imprimeix o no i prioritzar els punts següents: - Reduir el màxim possible el nombre d'impressions, tot ajustant-les a les necessitats. - Utilitzar paper cent per cent reciclat (excepte per a plànols no imprimibles en DIN A4 o DIN A3). - Imprimir els documents a doble cara i en blanc i negre (el color només s'utilitzarà en casos en què no es pugui interpretar en blanc i negre).	En cas que calgui imprimir documents.
Embalatges no primaris, material reciclat	Els embalatges no primaris* dels productes estaran fabricats al completament a partir de materials reciclats. * Embalatge addicional al del material mateix per a la distribució final del producte.	En cas que el servei se serveixi de productes amb embalatges no primaris.
Etiqueta ambiental dels vehicles	Els vehicles (turismes o furgonetes) que donin el servei en aquest contracte han de tenir adjudicada l'etiqueta ambiental tipus C, com a mínim.	Per a serveis que requereixin l'ús de vehicles (turismes o furgonetes). Aquest criteri és aplicable quan es tinguin previstos almenys 20 serveis l'any.
Vessament i abocament de líquid	S'han de prendre les mesures necessàries durant el servei perquè en cap cas hi hagi cap mena d'abocament o vessament de líquid directe al medi ambient.	En cas d'utilització de líquids.

	Si el servei implica l'ús o manipulació de productes líquids perillosos s'ha de disposar de mitjans de contenció i absorció davant de possibles vessaments.	
Residus. Productor de residus	Amb caràcter general, el contractista ha d'actuar com a productor del residu generat derivat de l'activitat objecte d'aquest contracte, per tant, ha de complir els requisits legals d'aplicació derivats de la legislació ambiental aplicable, especialment la Llei 7/2022, de 8 d'abril, de residus i sòls contaminats per a una economia circular; el Decret legislatiu 1/2009, de 21 de juliol, pel qual s'aprova el Text refós de la Llei reguladora dels residus; el Reial decret 553/2020, de 2 de juny, pel qual es regula el trasllat de residus a l'interior del territori de l'Estat, i el Decret 152/2017, de 17 d'octubre, sobre la classificació, la codificació i les vies de gestió dels residus a Catalunya; entre altres normes concordants. El contractista es fa càrrec dels residus i en cap cas no els pot deixar en dependències de TMB.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Codificació, separació i classificació de residus	El contractista ha de caracteritzar, codificar, separar i classificar els residus que produeixi o tingui de conformitat amb les determinacions del <i>Catàleg de residus de Catalunya</i> (CRC).	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Emmagatzematge de residus	El contractista ha d'emmagatzemar els residus abans de cedir-los al transportista autoritzat, en condicions adequades d'higiene i salut, i sempre fent servir envasos adequats i zones d'emmagatzematge d'acord amb la legislació. El període d'emmagatzematge mai no podrà superar els sis mesos per als residus perillosos (a excepció de disposar d'una autorització especial per superar aquest temps) o en el cas dels residus no perillosos	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).

	aquest període serà inferior a dos anys en cas que es destinin a valorització, i un any quan es destinin a eliminació.	
Residus. Etiquetatge de residus	El contractista ha d'etiquetar els residus abans de cedir-los al transportista autoritzat de manera clara i visible, llegible i indeleble, seguint la normativa aplicable i, en el cas dels residus peril·losos, ha d'identificar la naturalesa dels riscos mitjançant els pictogrames aplicables segons les normatives vigents.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Documentació de gestió de residus	El contractista ha de formalitzar la documentació de control de la gestió de residus (notificacions prèvies, contractes particulars, fitxes d'acceptació, fitxes de destinació, fulls de seguiment).	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Transport de residus	El contractista ha de fer servir empreses transportistes autoritzades per al transport dels residus. En cap cas es farà un trasllat de residus per part d'un transportista no autoritzat. Els residus generats a les instal·lacions de TMB han de ser transportats directament al gestor autoritzat mitjançant un transportista autoritzat.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Gestió de residus	El contractista ha de gestionar els residus mitjançant un gestor autoritzat i sempre a través d'una via de gestió autoritzada per a residus que es produeixen o gestionen a Catalunya.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Registre propi de residus	El contractista ha de portar al dia un registre propi de residus (arxiu cronològic) amb la informació de les retirades de residus efectuades, en el qual han de constar, com a mínim, les dades especificades per la normativa vigent.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Procediments de gestió de residus	El contractista ha de disposar de procediments i pautes de treball per gestionar correctament els residus a les seves instal·lacions i el personal que treballa n'ha de ser coneixedor.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-

		los (se'ls emporta i els gestiona).
Residus. Inspecció aleatòria	El contractista ha d'accedir al fet que TMB pugui inspeccionar i vigilar en tot moment, de manera mostral i aleatòria, els seus treballs com a adjudicatari del contracte, així com el compliment de les seves obligacions. Queda obligat a facilitar tota la col·laboració necessària per dur a terme aquestes tasques d'inspecció (facilitarà documentació, donarà lliure accés a les instal·lacions, etc.).	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Subcontractacions	En cas que el contractista subcontracti part de la seva activitat a un tercer que inclogui la generació de residus, és responsabilitat del contractista principal indicar al contracte qui ha d'actuar com a productor del residu generat (contractista o subcontractista). En cas de no indicar res, el contractista principal assumirà aquesta funció, així com les responsabilitats que se'n deriven.	Si el servei contractat suposa la generació de residus i el proveïdor s'encarrega gestionar-los (se'ls emporta i els gestiona).
Residus. Contenedors TMB	Els residus es gestionaran respectant la normativa aplicable i els procediments interns de gestió de residus i sistemes de recollida selectiva establerts per TMB. En cap cas, els residus poden ser abandonats o dipositats en llocs que no siguin habilitats per a aquesta funció. Els residus sempre es dipositaran als llocs especialment habilitats per a la seva recollida i posterior gestió. Referència: procediment 502 de TMB.	Si el servei contractat suposa la generació de residus i TMB n'assumeix la gestió.
Direcció d'obra. Supervisió ambiental per direcció d'obra	La direcció d'obra ha d'incorporar en el pla de treball la supervisió de les mesures ambientals recollides al pla d'ambientalització i assegurar-ne el compliment durant l'execució.	Només aplicable al servei de direcció d'obra.
Direcció d'obra. Informe ambiental en modificacions d'obra	En cas que es facin modificacions al projecte, la direcció d'obra ha d'emetre un informe ambiental específic sobre l'impacte d'aquestes modificacions abans d'aprovar-les.	Només aplicable al servei de direcció d'obra.

Direcció d'obra. Control ambiental de materials	La direcció d'obra ha de revisar i validar que els materials emprats compleixin els criteris ambientals establerts (ecoetiquetes, reciclats, fusta certificada, etc.).	Només aplicable al servei de direcció d'obra i si hi ha prescripció ambiental de materials al PPT.
Direcció d'obra. Informe final ambiental de l'obra	La direcció d'obra elaborarà un informe final que indiqui el grau de compliment dels criteris ambientals establerts, amb evidències documentals i conclusions.	Només aplicable al servei de direcció d'obra.

David Vicente Oliva

RESP. SISTEMES TECNOLÒGICS OPERACIÓ