Servei de Sistemes Elèctrics i Electromecànics
Unitat de Projectes de Sistemes i Equipaments d'Estacions

PLEC DE CONDICIONS TÈCNIQUES

SERVEI DE MANTENIMENT DEL SISTEMA DE CONTROL CENTRALITZAT D'INSTAL·LACIONS FIXES DE XARXA CONVENCIONAL PER FERROCARRIL METROPOLITÀ DE BARCELONA

Xarxa	Línia	Àmbit	Ubicació
METRO	TOTES	TES	MÚLTIPLE

Terme Municipal

BARCELONA I ÀREA METROPOLITANA

Documents	Exemplar	Tom	Data de redacció
PPTE_MANTENIMENT INST. FIXES LC	1	1	10/06/2026

ÍNDEX GENERAL

MEMÒRIA, PRESSUPOST I ANNEXOS

1. ANTECEDENTS 4
2. OBJECTE 4
3. PRESCRIPCIONS REGLAMENTÀRIES 5
4. ABAST DELS TREBALLS 6
5. PRESCRIPCIONS TÈCNIQUES PEL MANTENIMENT DEL TELECOMANDAMENT D'INSTAL·LACIONS FIXES I DELS CENTRES DE TRANSFORMACIÓ 6
5.2 ABAST DEL SERVEI DE MANTENIMENT 6
5.2.1. Serveis inclosos 7
5.2.2 Hardware actual inclòs dins del contracte i evolució del sistema 9
5.2.3 Software inclòs dins del contracte 9
5.3 DURADA DEL SERVEI DE MANTENIMENT 10
5.4 DESCRIPCIÓ DEL SERVEI DE MANTENIMENT 10
5.4.1 Organització del Servei 10
5.4.2 Coordinació del Servei 11
5.4.3 Servei d'atenció d'incidències 11
5.5 MANTENIMENT PREVENTIU 12
5.5.1 Actuacions de Manteniment Preventiu 12
5.6 MANTENIMENT CORRECTIU 14
5.7.1 Temps de resolució funcional 15
5.7.2 Temps de resposta telefònica 16
5.8 MANTENIMENT EVOLUTIU 17
5.7 LÍMITS DEL SISTEMA 17
5.8 COMUNICACIONS ENTRE LES PARTS 18
5.8.1 Comunicació de les incidències 19
5.8.2 Comunicació del manteniment preventiu efectuat 19
5.8.3 Comunicació de d'inici i final dels treballs 20
5.8.4 Comunicació de Situacions de Risc 20
5.8.5 Seguiment del Manteniment 20
5.9 RESPONSABILITATS OBLIGACIONS TRANSVERSALS I GESTIÓ DEL RISC 21
5.10 OBLICACIONS DE TMB 22
5.11 ACCÉS A LES INSTAL·LACIONS 22
5.10.1 Dipòsit i utilització de les claus i codis d'accés a les instal·lacions 23
5.11 PREUS I CONDICIONS 23
6. DISPOSICIONS GENERALS 23
6.1 PERSONAL DESTINAT AL SERVEI 23
6.2 CONFRONTACIÓ DE LA DOCUMENTACIÓ/PLÀNOLS 24

6.3 PROTECCIÓ I NETEJA 24
6.4 DURACIÓ DEL SERVEI 24
6.5 RESCISSIÓ DEL CONTRACTE 24
6.6 RECEPCIÓ PROVISIONAL 24
6.7 GARANTÍA 24
6.8 RECEPCIÓ DEFINITIVA 25
6.9 PROVES I POSADA EN SERVEI 25
6.10 DOCUMENTACIÓ 26
6.11 PENALITZACIONS 26
6.12 CONTRACTES, ACCIDENTS DE TREBALL I PROTECCIÓ A LA INDÚSTRIA 26
6.13 MESURES D'ORDRE I SEGURETAT 26
6.14 DESPESES A CÀRREC DEL CONTRACTISTA 26
7. CRITERIS AMBIENTALS 27
8. REQUERIMENTS DE CIBERSEGURETAT 27
8. SEGURETAT I SALUT LABORAL 52
8.1. ASPECTES GENERALS 52
8.2. COORDINACIÓ D'ACTIVITATS EMPRESARIALS (CAE) 52
8.3. VIGILÀNCIA I CONTROL PER PART DE L'ADJUDICATARI 53
8.4. CENTRE DE TREBALL 54
8.5. PLA DE SEGURETAT I SALUT I LLIBRE DE REGISTRE DE SUBCONTRACTES 54
PRESSUPOST 56

PLECS

Plec de Prescripcions Tècniques i Funcionals del Control Centralitzat de instal·lacions fixes de la Xarxa de Metro

1. ANTECEDENTS

El Control Centralitzat d'Instal·lacions Fixes (CCIF) està desplegat a tota la xarxa d'estacions de Ferrocarril Metropolità de Barcelona (en endavant, FMB). Permet el control i l'operació remota dels equipaments de transport vertical (escales mecàniques, tapissos rodants i ascensors PMR i de gran capacitat), dels equipaments electromecànics (portes d'accés a estació, pous d'esgotament, bombes auxiliars i sistema de ventilació) i de la instal·lació de baixa tensió (control de l'enllumenat, monitorització del subministrament de baixa tensió i monitorització de les proteccions elèctriques del QGBT i dels sistemes d'alimentació ininterrompuda).

La informació que generen tots aquests dispositius es fa arribar fins al telecomandament. Actualment el telecomandament suporta més de 2000 dispositius entre els quals existeixen escales, ascensors, ventiladors, quadres de baixa tensió, pous, foses, portes d'accés a estació, tapissos rodants i sistemes d'alimentació ininterrompuda, així com els PLC's mestres encarregats de reportar tota la informació cap als centres de control. La previsió d'aquest número de dispositius es que vagi creixent tant per adaptació d'estacions com per l'automatització de nous elements.

Actualment el manteniment de primer nivell i suport davant d'una incidència el donen els Enginyers de Manteniment que estan físicament al propi CCM amb cobertura 24x7x365d. A la xarxa de FMB s'està treballant en controlar remotament les estacions i els seus equipaments, fet que provoca que l'obertura-tancament d'estacions en determinats escenaris es remota mitjançant el CCIF i aquest telecomandament passa a ser un telecomandament crític pel servei condicionant l'obertura i tancament d'estacions. Atès aquesta nova condició de criticitat es fa necessari disposar d'un 2n nivell de manteniment per incidències complexes i garantir la disponibilitat i fiabilitat del sistema amb manteniments preventius.

2. OBJECTE

L'objecte de la present especificació és la definició de les característiques tècniques per la contractació del manteniment de 2n nivell del telecomandament d'instal·lacions fixes de línies convencionals.

La modalitat de manteniment a contractar és un 24 x 7 els 365 dies de l'any. Amb aquesta cobertura s'assegura el suport de personal tècnic extern en qualsevol horari d'explotació de FMB.

L'objectiu del servei de manteniment de 2n nivell és garantir la disponibilitat del telecomandament de manera continuada, assegurant la fiabilitat del sistema davant d'incidències complexes amb actuacions de manteniment periòdiques. Per assolir aquest propòsit, el servei s'articula mitjançant tres eixos d'actuació:

- Manteniment Correctiu: Orientat a la resolució d'incidències i avaries per assegurar el restabliment del servei en el menor temps possible, maximitzant la taxa de disponibilitat de la infraestructura.

- Manteniment Preventiu: Basat en actuacions programades i sistemàtiques destinades a minimitzar el risc de fallades i a incrementar la fiabilitat i la vida útil dels equips.
- Manteniment Evolutiu: Amb l'objectiu d'adaptar els sistemes a noves necessitats operatives, aquest servei inclou la realització d'estudis tècnics, el disseny de solucions i l'execució de modificacions o configuracions de programari de manera àgil i eficient.

3. PRESCRIPCIONS REGLAMENTÀRIES

En les prestacions d'aquest manteniment i en la realització de qualsevol tipus d'actuació dins del present contracte, s'aplicaran com a mínim, i sense caràcter limitador, les reglamentacions:

- Tots els plecs, instruccions i normes que siguin legalment obligatòries durant tota la durada del contracte seran així mateix obligatòries per a la realització dels treballs, encara que no hagin estat inclosos de forma explícita en la relació normativa anterior.
- Cap paràgraf d'aquest document alliberarà a l'ADJUDICATARI de la seva responsabilitat en el compliment de tots els codis i normes nacionals i locals aplicables. En cas de discrepància entre normes, s'entendrà que és vàlida la prescripció més restrictiva.
- L'ADJUDICATARI complirà, en tots els sentits, els Reglaments i/o Normatives, Procediments i requeriments interns de FMB que els siguin aplicables, tant per a les instal·lacions, com pels materials, maquinària, elements per desenvolupar el servei i personal implicat.

TERMINOLOGIA DEL MANTENIMENT

La interpretació de les definicions dels termes tècnics inclosos en aquest Plec estan recollits en la Norma UNE-EN 13306 "Terminologia del manteniment" de febrer de 2002 , i en les normes especifiques que en cada cas es citin en el document.

SEGURETAT I SALUT EN EL TREBALL

Prevenció de riscos laborals. Llei 31/1995.

- Reial Decret 39/1997, reglament dels serveis de prevenció.
- Reial Decret 780/1998, por el que es modifica el Reial Decret 39/1997
- Disposicions mínimes de seguretat i salut a els llocs de Treball. Reial Decret 486/1997.
- Disposicions mínimes en matèria de senyalització de seguretat i salut en el Treball. Reial Decret485/1997.
- Disposicions mínimes de seguretat i salut relatives a la manipulació manual de càrregues que comporti riscos, en particular dorso-lumbars, per a els treballadors. Reial Decret 487/1997.
- Disposicions mínimes de seguretat i salut relatives a la utilització per els treballadors d'equips de protecció individual. Reial Decret 773/1997.
- Protecció de els treballadors contra a els riscos relacionats amb l'exposició a agents cancerígens durant el Treball. Reial Decret 665/1997.

- S'estableixen les disposicions mínimes de seguretat i salut per a la utilització per a els treballadors dels equips de Treball. Reial Decret 1215/1997.
- Protecció de la salut i seguretat de els treballadors contra els riscos relacionats amb l'exposició a agents químics durant el Treball. Reial Decret 374/2001.

NORMES GENERALS DE SEGURETAT DEL FMB

- Normes per a l'execució de treballs per personal extrem a la xarxa del FMB.
- Normes de seguretat per a treballs a la zona de vies de la xarxa de FMB.
- Normes per a la realització d'operacions de tall i reposició de tensió a la xarxa del FMB.
- Ús detector presència de tensió en corrent continu per a línies de tracció.
- Normes per la posada a terra de la catenària.
- Circulació vehicles auxiliars/trens de treball amb tensió de línies tracció.
- I totes aquelles disponibles en la biblioteca Controllar Achilles o plataforma PRL equivalent a disposició de l'adjudicatari.

4. ABAST DELS TREBALLS

L'abast de les especificacions compren els següents capítols principals:

- Manteniment telecomandament instal·lacions fixes → Capítol 5
  - Assistència telefònica
  - Manteniment correctiu
  - Manteniment preventiu
  - Manteniment evolutiu

5. PRESCRIPCIONS TÈCNIQUES PEL MANTENIMENT DEL TELECOMANDAMENT D'INSTAL·LACIONS FIXES I DELS CENTRES DE TRANSFORMACIÓ

En aquest document es defineix l'abast i condicions per el manteniment dels telecomandaments d'instal·lacions fixes (CCIF). L'abast a considerar és:

- Servei d'Atenció telefònica.
- Servei de Manteniment Preventiu.
- Servei de Manteniment Correctiu.
- Servei de Manteniment Evolutiu

5.2 ABAST DEL SERVEI DE MANTENIMENT

L'execució de les tasques s'han d'encomanar a un contractista que posseeix el know-how d'aquests sistemes i per tant s'han de contractar amb un procediment negociat sense publicitat. Per aquesta raó la execució de les tasques no es separa en diferents lots.

Dintre d'aquest apartat es recull un resum del nivell de servei requerit pel manteniment de tots dos telecomandaments, i les seves aplicacions externes.

5.2.1. Serveis inclosos

1. Organització del servei.

2. Centre de recepció d'incidències amb disponibilitat 24x7 els 365 dies de l'any.

3. Manteniment preventiu de la totalitat d'equips i sistemes objecte de les especificacions, amb periodicitat anual.

4. Disponibilitat de personal en la modalitat de 24x7

5. Manteniment correctiu que inclou:

   L'adjudicatari assumeix la responsabilitat plena de proporcionar els recursos humans, tècnics i materials necessaris per garantir la prestació integral del servei de manteniment correctiu.

   - Trasllat del personal tècnic al punt de l'avaria.
   - Actuacions necessàries per garantir la operativitat del telecomandament (commutació de servidors)

   - HARDWARE:
     - Llocs d'operador: reposició del servei utilitzant el PC de reserva.
     - Substitució de discos durs de servidors pels discos de backup.
     - NO INCLOU: Materials o serveis de reparació necessaris per a la resolució de la incidència. Tampoc inclou la reposició del Hardware.

   - SOFTWARE:
     - Correcció d'errors dels aplicatius objecte del manteniment.
     - Assistència per resoldre incidències amb Microsoft SQL Server, Microsoft Office i drivers relacionats.
     - Actualització de versions de software i Service Pack de Microsoft Windows i Windows Server així com SQL Server quan aquestes:
       - Solucionin un problema existent en l'abast del manteniment.
       - Siguin compatibles amb el software ja instal·lat (Certificat per el fabricant).

        - No impliquin un canvi en el codi de l'aplicatiu actual.
    - NO INCLOU: Canvis de funcionalitat en els aplicatius.

6. **Documentació i informes** periòdics amb informació del servei de manteniment incloent-hi:
    - Informes de manteniment correctiu
    - Resum d'intervencions
    - Estadístiques

5.2.2 Hardware actual inclòs dins del contracte i evolució del sistema

La relació dels equips i elements inclosos dins del servei de manteniment és:

DESCRIPCIÓ	QUANTITAT
Servidors CCIF	2
WEB CCIF	1
PONT CCIF	1
SQLSERVER	1
PAE_BACKUP	1
Equipament Xarxa (xarxa A, xarxa B)	2
Llocs operació Sagrera (CCIF)	17
Llocs operació Sagrada Família (CCIF)	3
Llocs operació Santa Eulalia (CCIF)	4
Llocs operació Gerència (CCIF)	5
Llocs operació Boixeres (CCIF)	2
Llocs operació Hondures	1

Nota: L'abast d'aquest manteniment respecte a la xarxa A i xarxa B, serà únicament a nivell de detecció i diagnosis de possibles incidències.

El hardware llistat anteriorment és susceptible de ser modificat donada l'obsolescència del sistema complert.

5.2.3 Software inclòs dins del contracte

DESCRIPCIÓ	QUANTITAT
Software servidor CCIF	1
Software servidor SQLSERVER	1
Software GPS	1
Software servidor PAE_Backup	1
SCADA client dels llocs d'operador (segons detall del hardware)	1
Software servidor de Gestió d'Alarmes CCIF	1
Software (tipus) dels PLCs del Concentrador Xarxa Local (CXL)	1
Software de Operador Local Estació	1

Donada l'obsolescència del sistema complert, el software llistat anteriorment és susceptible de ser modificat tot i que la plataforma de SCADA i el core del projecte continuaran sent els mateixos.

5.3 DURADA DEL SERVEI DE MANTENIMENT

La durada del Servei de Manteniment és la següent:

- Organització del Servei: tres (3) ANYS - prorrogable dos (2) ANYS
- Servei d'atenció d'incidències: tres (3) ANYS - prorrogable dos (2) ANYS
- Manteniment Preventiu: tres (3) ANYS - prorrogable dos (2) ANYS
- Manteniment Correctiu: tres (3) ANYS - prorrogable dos (2) ANYS
- Manteniment Evolutiu: tres (3) ANYS – prorrogable dos (2) ANYS
- Documentació i informes: tres (3) ANYS - prorrogable dos (2) ANYS

5.4 DESCRIPCIÓ DEL SERVEI DE MANTENIMENT

La finalitat del Servei de Manteniment a contractar és:

- Assegurar la marxa continuada dels diferents equips, en les millors condicions de seguretat i economia, evitant qualsevol situació que pugui incidir en el seu correcte funcionament.
- Procurar el millor estat de conservació de totes les parts i elements que integren cadascú dels equips del sistema, objecte de l'especificació.
- Solucionar qualsevol incidència, conservant els nivells de qualitat i seguretat establerts.

Aquest manteniment es realitzarà de tal manera que les funcions i activitats de cada dependència o unitat es pugui desenvolupar de la forma més operativa possible per part dels seus usuaris.

5.4.1 Organització del Servei

Amb l'objectiu de mantenir la qualitat del servei, garantint la fiabilitat, eficiència i seguretat de l'equipament, es posarà a disposició de FMB un equip de professionals que reuneixen les qualificacions necessàries per realitzar els treballs amb total garantia de qualitat.

FMB tindrà controlat el llistat de persones autoritzades a realitzar aquest servei. La inclusió o eliminació d'alguna persona en aquest llistat caldrà notificar-lo per l'aprovació formal de FMB.

El màxim responsable del servei "**Cap de Manteniment**" serà un enginyer amb experiència en els diferents sistemes a mantenir.

Les funcions principals del Cap de Manteniment seran:

- Relació administrativa amb FMB
- Establiment d'un Pla General de Manteniment
- Supervisió del procés d'execució del servei de manteniment

El Cap de Manteniment contarà amb el suport de l'equip de intervencions per donar suport en cadascú dels diferents camps d'actuació del projecte:

- Tecnologia IP: Servidors del Centre de Control i xarxa IP

- Tecnologia PLC: Software PLCs CXL
- Tecnologia SW: Aplicació SW CCIF, GPS, WEB, POINT_BRIDGE, gestió d'Alarmes CCIF.

5.4.2 Coordinació del Servei

Un dels requeriment fonamentals per a l'èxit del servei de manteniment és que existeixi una correcta coordinació dels diferents treballs i una transferència d'informació àgil i transparent. Per aconseguir aquesta transferència d'informació es mantindran reunions de seguiment amb periodicitat mínima trimestral. A l'agenda es tractaran entre d'altres els següents punts:

- Informació de l'estat actual del projecte
- Resolució de problemes puntuals
- Coordinació del manteniment preventiu
- Actuacions especials requerides per FMB

A les reunions de seguiment participaran persones que, pels seus coneixements en temes concrets o per la situació del servei o assumptes a tractar, aconsellin la seva participació.

5.4.3 Servei d'atenció d'incidències

Es posarà a disposició de FMB un **servei d'atenció d'incidències amb disponibilitat 24 x 7 els 365 dies de l'any.** La confirmació de recepció d'avís d'incidència es farà de forma immediata, mitjançant telèfon. A la confirmació de la recepció es subministrarà el "número d'incidència" obert. Dins l'horari d'oficina, les incidències es notificaran directament via centraleta telefònica o via telèfon de guàrdia.

El temps màxim per tal de que el tècnic encarregat del manteniment doni suport telefònic es de **(1) hora**.

Si aquest suport telefònic no es viable o no es efectiu caldrà que el tècnic encarregat del manteniment es presenti en les instal·lacions de FMB per tal de resoldre la incidència. Caldrà tenir en compte **els temps de resolució** d'incidències definits en l'apartat 5.7.1 (veure taula). Per el cas més crític, que seria una pèrdua de servei en horari nocturn amb un volum d'estacions >= al 10%, caldrà que el tècnic responsable solucioni la incidència en un temps màxim de **(4) hores**.

Poden existir incidències on la seva correcció queda fora de l'abast d'aquest manteniment, p.exemple un problema en la xarxa de camp dels CXL. En aquestes situacions els temps de resolució seran temps per diagnosticar la incidència.

5.4.3.1 Seguiment de les incidències

Caldrà informar a FMB sobre l'estat de l'avaria, generant un informe amb la descripció de la solució, el material emprat i els temps de resposta i resolució.
El registre de tancament de d'incidència inclourà la següent informació:

- Número d'incidència
- Data de realització
- Materials utilitzats
- Descripció dels treballs realitzats

5.5 MANTENIMENT PREVENTIU

S'entén com Manteniment Preventiu el manteniment realitzat de forma sistemàtica amb revisions periòdiques i planificades, realitzades per personal especialitzat amb l'objectiu d'assegurar el correcte funcionament del sistema anticipant-se a possibles problemes o avaries que puguin sorgir i que afectin al seu funcionament.

El manteniment preventiu es basarà en l'estat de l'equip a través de mesures periòdiques dels seus paràmetres més significatius, tenint en compte les condicions de funcionament de l'equip. Per això, a l'hora d'efectuar el manteniment preventiu es tindrà en compte:

- Estadística d'incidències o avaries
- Dades històriques del manteniment
- Grau d'envelliment dels equips
- Condicions ambientals de funcionament

Les actuacions de manteniment preventiu es realitzaran en aquell horari que afecti mínimament al servei d'explotació de FMB.

La planificació del manteniment preventiu es realitzarà amb una antelació mínima d'un (1) mes.

5.5.1 Actuacions de Manteniment Preventiu

De forma genèrica les actuacions de manteniment preventiu a realitzar sobre l'equipament son les definides a continuació:

<u>General</u>

Conjuntament amb FMB, es coordinaran les actuacions de preventiu de qualsevol sistema en explotació que pugui afectar al desenvolupament de l'activitat comercial i seran, preferentment, en dies laborables i horari nocturn, fora de l'horari d'explotació. Per la resta de l'equipament, els preventius podran realitzar-se durant l'horari d'explotació.

Servidors CCIF

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Obtenció i anàlisis de la informació de l'estat de l'equip, revisió de logs.	ANUAL
Realització de Ghost i imatge en un disc de backup.	ANUAL
Actualització, depuració i emmagatzematge de la informació de la BBDD SQL Server (esborrat de log's) i projectes Scada.	ANUAL

Servidor WEB

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Obtenció i anàlisis de la informació de l'estat de l'equip, revisió de logs.	ANUAL
Realització de Ghost i imatge en un disc de backup.	ANUAL
Actualització, depuració i emmagatzematge de la informació de la BBDD SQL Server (esborrat de log's).	ANUAL

PONT CCIF

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Verificació d'errors, revisió i neteja de logs	ANUAL
Realització de Ghost (sempre que la còpia no estigui actualitzada) i una imatge en un disc de backup	ANUAL

SQLSERVER

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Obtenció i anàlisis de la informació de l'estat de l'equip, revisió de logs.	ANUAL
Realització de Ghost i imatge en un disc de backup.	ANUAL
Actualització, depuració i emmagatzematge de la informació de la BBDD SQL Server (esborrat de log's) i projectes Scada.	ANUAL

PAE BACKUP

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Obtenció i anàlisis de la informació de l'estat de l'equip, revisió de logs.	ANUAL
Realització de Ghost i imatge en un disc de backup.	ANUAL
Actualització, depuració i emmagatzematge de la informació de la BBDD SQL Server (esborrat de log's) i projectes Scada.	ANUAL

Client CCIF BACKUP

OPERACIONS DE MANTENIMENT	
Descripció	Periodicitat
Verificació d'errors, revisió i neteja de logs	ANUAL
Realització de Ghost (sempre que la còpia no estigui actualitzada) i una imatge en un disc de backup	ANUAL
Actualització de l'aplicatiu del CCIF disponible en el STM1, armari O-Recanvis, i verificació funcional d'aquest client.	ANUAL

Base de dades històriques

Exportar les dades històriques de la bases de dades "històric" amb una antiguitat superior a 1 (UN) any en format text i treure-ho fora del sistema emmagatzemant en un suport electrònic extern.

Cal tenir en compte les següents tasques:

Prova de restabliment des de zero: Verificació obligatòria de la capacitat de restaurar el sistema totalment sobre maquinari proporcionat per FMB.

Actualització: Execució d'una actualització anual de versions de programari per garantir la vigència tecnològica. L'execució de l'actualització estarà condicionada al anàlisis de riscos i s'haurà d'acordar prèviament.

L'adjudicatari lliurarà un informe detallat post-inspecció que inclogui un checklist d'elements revisats i una proposta d'accions correctores de millora.

5.6 MANTENIMENT CORRECTIU

S'entén com Manteniment Correctiu les tasques realitzades, per personal tècnic qualificat, per reparar una avaria o superar el deteriorament d'algun element que hagi deixat de funcionar correctament. El seu objectiu serà atendre les avaries que provoquen un funcionament incorrecte de l'equip en qüestió aplicant els serveis que es detallen en aquest mateix plec.

S'actuarà sempre sota petició expressa de FMB. El Manteniment Correctiu inclou la disponibilitat dels tècnics per desplaçar-se a les instal·lacions segons la modalitat 24x7.

Les possibles intervencions que es puguin dur a terme seran objecte d'una facturació addicional segons els imports de preu hora/tècnic definides en el pressupost d'aquest document.

Per a cadascuna de les intervencions de correctiu es realitzarà el corresponent informe tècnic amb les actuacions realitzades. Cada intervenció de software tindrà un període de garantia de 24 mesos durant els quals no es podran imputar o facturar més hores pel mateix concepte.

5.7.1 Temps de resolució funcional

A fi d'establir una mètrica que permeti avaluar i analitzar la qualitat del manteniment realitzat, s'estableixen els següents indicadors, que es calcularan sobre les instal·lacions actives.

És el temps que triga L'ADJUDICATARI en resoldre la incidència de manera funcional, es a dir, es possible que la situació en que quedi el sistema no sigui la resolució definitiva, però s'hauran portat a terme mesures que puguin garantir la seva funcionalitat de manera temporal.

Existeixen situacions on la incidència queda fora de l'abast d'aquest manteniment. En aquests casos els temps definits en aquest apartat no seran temps de resolució sinó que serà el temps màxim en fer el diagnosis de la incidència.

L'ADJUDICATARI haurà de garantir els següents temps mitjos en la resolució dels avisos d'incidències. Aquests temps són els transcorreguts des de que és notifica la incidència via telefònica a l'ADJUDICATARI per part de FMB fins que la incidència és resolta per l'ADJUDICATARI i és comunicada a FMB.

El temps de resolució d'una incidència es calcularà:

TR_I = data i hora final d'incidència – data i hora inicial d'incidència

A partir de les dades de les avaries del mes, i per a cada nivell de prioritat, es calcula el temps mitjà de resolució de les avaries, MTR_i:

$$MTRi = \frac{1}{n}\sum_{i=1}^{n} TR\,i$$

On n és la suma de les avaries resoltes en el mes.

Es defineixen els següents temps de resolució funcional contractual:

Prioritat	Horari	Definició d'incidència	Temps mig de resolució
1	0:00 a 5:30h (nocturn)	Pèrdua de servei al departament d'Operació en un número d'estacions >= al 10% de la totalitat d'estacions	4h
2	0:00 a 5:30h (nocturn)	Pèrdua de servei al departament d'Operació en un número d'estacions < al 10% de la totalitat d'estacions	6h
3	5:30h a 0:00h (diürn)	Pèrdua de servei al departament d'Operació en un número d'estacions >= al 10% de la totalitat d'estacions	7h
4	5:30h a 0:00h (diürn)	Pèrdua de servei al departament d'Operació en un número d'estacions < al 10% de la totalitat d'estacions	8h
5		Incidències amb afectació al departament de Operació	8h
6		Error en l'execució de les seqüències GPS	8h
7		Resta de incidències sense afectació a departament de Operació	48h

La situació de prioritat 1 és la situació crítica la qual caldrà respondre de la manera més ràpida possible per tal de garantir la funcionalitat del telecomandament a l'obertura del servei (horari d'obertura entre 4:30 i 5:00h). Caldrà donar prioritat a la realització d'algunes de les implementacions recollides en aquest plec per tal de minimitzar la situació de risc al no tenir possibilitat d'obrir les estacions.

5.7.2 Temps de resposta telefònica

És el temps comprés entre que FMB realitza la trucada telefònica i un tècnic coneixedor del sistema realitza una primera avaluació.

Aquest temps tal i com ja s'ha indicat a de ser inferior a **(1) hora**.

El temps de resposta telefònica es calcularà:

TR_T = data i hora resposta telefònica tècnic – data i hora trucada de FMB

5.8 MANTENIMENT EVOLUTIU

Es disposarà d'una borsa de 300 hores anuals per a millores, noves funcionalitats, adaptacions normatives o per obsolescència.

Procediment: Cada intervenció serà valorada en hores i termini per l'adjudicatari i requerirà l'acceptació expressa de TMB.

Intervencions Crítiques: En cas de sol·licituds que afectin la disponibilitat del sistema, el termini màxim d'implementació serà de 15 dies laborables.

Entre les tasques principals es trobaran aspectes relacionats amb la Ciberseguretat:

- Anàlisis de tràfic de dades existents
- Actualització de "pegats"
- Anàlisis de vulnerabilitats i la seva correcció

Es valorarà la integració de nous dispositius dins del telecomandament d'instal·lacions fixes definint un preu en els següents casos:

- Actuació telecomandament. Preu per una integració d'un dispositiu ja existent dins dels models de base de dades, tant si el dispositiu es de nova implantació com si el dispositiu és un renove, inclou:
  1 intervenció diürna per la implantació i configuració del telecomandament.
  1 intervenció nocturna per reiniciar projecte i fer efectiu els canvis.
  1 jornada de proves del dispositiu.
  Actualització, si cal, de totes les aplicacions externes SQLSERVER, alarmes CCIF, GPS.
  No Inclou: desenvolupament de noves pantalles, nou model de base de dades, desenvolupament de noves funcionalitats.

- Actuació Concentrador Local de Xarxa. Preu per la càrrega del software del CXL versió 204 o superior. Incloent la configuració individualitzada de cada estació.
- Actuació PLC de dispositiu. Preu per la càrrega del software del dispositiu ASC,ESC,POU,QBT,TAP,VNT,PAE, inclou verificació i suport per la connectivitat IP amb el CXL.

5.7 LÍMITS DEL SISTEMA

Els límits dels sistema són les fronteres dels equips objectes de manteniment per part de l'ADJUDICATARI amb altres instal·lacions i/o sistemes.

Es considerarà frontera tots els elements aliens al sistema de telecomandament, es considerà element aliè tot allò no inclòs en aquest contracte de manteniment (com poden ser les instal·lacions elèctriques, la configuració de xarxa MPLS que dona connectivitat als elements de camp).

El límit d'intervenció (inclòs) de l'Adjudicatari pel que fa a la instal·lació del Telecomandament a les sales tècniques de FMB és la boca de connexió al mòdul del Sistema de Transmissió assignat a aquest servei. (Xarxa IP MPLS corporativa).

Aquest Plec no contempla el manteniment de la xarxa física sobre la qual es troba instal·lat el sistema. Després de cada incidència, l'Adjudicatari realitzarà les proves pertinents a fi d'esbrinar i concretar l'origen de qualsevol problema de comunicacions i proporcionarà un informe que inclourà les proves realitzades.

L'ADJUDICATARI atendrà totes les incidències que es manifestin en el sistema independentment de l'origen de la mateixa.

La responsabilitat de l' ADJUDICATARI serà determinar i diagnosticar l'avaria, si aquesta avaria és produïda per un element frontera, l'ADJUDICATARI ho comunicarà a FMB i aquest escalarà l'avaria al mantenidor corresponent.

Es considera Telecomandament d'Estacions tots els serveis i equips que proporcionen el servei de supervisió i operació d'aquest sistema en la xarxa convencional. Es consideren els servidors, serveis, llocs d'operació, aplicatius, etc. que formen part d'aquest entorn.

Si es determina que l'avaria és produïda per un sistema frontera, l'Adjudicatari ho comunicarà a FMB per tal d'escalar l'avaria al mantenidor corresponent.

Les incidències provocades per causes externes no comptabilitzen a efectes de càlcul de fiabilitat ni disponibilitat, ni índexs de qualitat del manteniment.

5.8 COMUNICACIONS ENTRE LES PARTS

L'ADJUDICATARI comunicarà a FMB una llista d'interlocutors i els seus telèfons mòbils de contacte, de manera que es pugui contactar amb ells per a la realització de les tasques incloses en aquest contracte.

També s'ha de tenir constància dels telèfons dels diferents perfils de l'organigrama de manteniment que intervenen en la gestió del contracte. Hi haurà una persona de l'ADJUDICATARI responsable de la gestió global del contracte.

Per la seva banda, FMB també facilitarà a L'ADJUDICATARI una llista d'interlocutors i els seus telèfons de contacte.

Sempre que li sigui requerit, L'ADJUDICATARI informarà de la localització del seu personal en servei en les instal·lacions de la Xarxa de FMB.

En general L'ADJUDICATARI entrarà la informació tècnica i d'activitat del manteniment correctiu i preventiu mitjançant informes i albarans de intervencions, per tal de poder emetre les corresponents certificacions.

5.8.1 Comunicació de les incidències

Alta d'incidències

FMB comunicarà a l'ADJUDICATARI les incidències en el moment que les detecti. Es facilitarà la següent informació:

- Data i hora.
- Servei o Equip afectat.
- Descripció en Text de la incidència.
- Estació.

Aquesta comunicació es realitzarà normalment via telefònica o mitjançant correu electrònic als contactes que l'ADJUDICATARI faciliti a FMB, essent obligat disposar de dispositiu mòbil amb atenció 24h dins de l'horari establert.

Tancament d'incidències L' ADJUDICATARI comunicarà a FMB la finalització de la incidència una vegada s'hagi efectuat la reparació i verificació del restabliment de la funció afectada.

Aquesta comunicació es realitzarà a través del telèfon als números i a les persones que FMB facilitarà a l'ADJUDICATARI.

Per a cada incidència atesa, l'ADJUDICATARI emplenarà un document de treball que caldrà que sigui signat per l'interlocutor assignat de FMB.

- Data i Hora final de la incidència
- Nom complert del personal que han realitzat la reparació.
- Text ampliat de la descripció de la incidència
- Equip afectat i la seva identificació
- Element que causa l'avaria (Part Objecte codificat)
- Símptoma (codificat i text lliure si és necessari)
- Causa de l'avaria (codificat i text lliure si és necessari)
- Accions o treballs realitzats (en text lliure ampliat de descripció de la incidència)
- Origen de l'avaria si és aliena al sistema i altres observacions (en text lliure ampliat de descripció de la incidència)

5.8.2 Comunicació del manteniment preventiu efectuat

L'ADJUDICATARI proposarà dates per la realització del manteniment preventiu anual. Si es detecta alguna situació de degradació d'equips FMB pot invocar la realització d'aquest manteniment preventiu per tal de solucionar la situació. L'ADJUDICATARI, realitzarà un informe de manteniment amb la següent informació:

- Notificació d'Empleat/s que han fet el manteniment
- Denominació de la revisió
- Equip
- Ubicació dels equips

- Operacions realitzades
- Mesures efectuades
- Accions posteriors que es deriven del manteniment
- Observacions

L'ADJUDICATARI reportarà aquesta informació mitjançant un correu electrònic, no més tard de l'endemà del dia en que s'ha finalitzat el manteniment preventiu.

5.8.3 Comunicació de d'inici i final dels treballs

L'ADJUDICATARI haurà de comunicar l'inici i fi dels treballs al Centre de Control de FMB (Supervisor i Enginyers de manteniment ext. 88225 o 67590) o personal en estació.

5.8.4 Comunicació de Situacions de Risc

Si l'ADJUDICATARI detectés qualsevol situació de possible risc o deficiències en equips, instal·lacions, dependències, equips de treball i equips de protecció, col·lectiva o individual, que al seu judici comporti un risc, ha de comunicar-lo immediatament a FMB, a fi de que puguin adoptar-se les mesures adients.

5.8.5 Seguiment del Manteniment

Trimestralment es realitzarà una reunió de seguiment on L'ADJUDICATARI portarà un informe amb:

- Document resum de totes les incidències del període.
- Documentació d'anàlisi de les incidències del període classificades per causes, símptomes, element, estació, etc. Revisió del temps de resposta i de resolució en aquests casos.
- Revisions realitzades fora de l'àmbit del manteniment correctiu.

L'ADJUDICARI proposarà un model de gestió del conjunt de les dades que faciliten el seguiment i anàlisis del manteniment. Un cop aprovat per FMB, L'ADJUDICATARI facilitarà aquesta informació trimestralment o quan sigui requerit.

De la posada en comú d'aquesta informació es determinaran respecte el període de temps analitzat:

- Si apliquen penalitzacions per no assolir els paràmetres de qualitat i nivell de servei, en el cas d'aplicar el seu percentatge i import.
- Si apliquen penalitzacions per desatenció del servei i faltes i en el cas d'aplicar el seu percentatge i import.
- Si s'ha realitzat la totalitat del manteniment preventiu. A part que pugui ser causa de resolució del contracte les revisions no realitzades no es facturen i és descompte el seu import de la factura trimestral.

Aquests punts determinaran l'import trimestral. El detall i l'import del període es consignarà en l'acta de la reunió i es signarà per FMB i l'ADJUDICATARI.

Periòdicament s'aniran realitzant reunions entre representants de L'ADJUDICATARI i FMB amb la intenció de millorar la documentació del manteniment i els procediments que es realitzin.

5.9 RESPONSABILITATS OBLIGACIONS TRANSVERSALS I GESTIÓ DEL RISC

Tot i que de manera inicial es faran servir els procediments interns de FMB, serà responsabilitat de l'ADJUDICATARI definir l'estratègia de manteniment i la realització de la totalitat de les tasques definides a l'activitat, aportant els mitjans tècnics i humans necessaris per la consecució dels següents objectius durant la vigència del contracte.

Legals:

- L'assumpció de responsabilitats legals derivades i inherents a l'activitat del manteniment.
- El compliment de les normatives i reglamentacions que apliquin a les instal·lacions objecte del contracte.

Manteniment:

- La realització de totes les tasques i operacions necessàries per a la consecució dels objectius proposats, a més de les que siguin exigibles i establertes específicament per a aquest tipus d'instal·lacions d'acord amb la legislació vigent a la signatura del contracte.
- Garantir el correcte funcionament dels sistemes dins dels límits de nivell de servei i objectius de qualitat especificats en aquest document.
- El manteniment correctiu s'ha de realitzar amb els temps de resposta indicats en aquest document. El desviament d'aquest paràmetres donarà lloc a les penalitzacions o resolució de contracte detallat al plec de prescripcions administratives de la licitació. Addicionalment, en el cas en que l'ADJUDICATARI no resolgui una incidència, per complexa que aquesta sigui, FMB es reservarà el dret de sol·licitar la resolució a un tercer. L'import de les despeses generades es podrà aplicar en concepte de penalització a l'ADJUDICATARI.
- Formació i capacitació del personal de manteniment.

Medi ambient:

- Estricte compliment de la legislació mediambiental vigent, així com els procediments interns de FMB.
- Evitar en la realització de les tasques de manteniment qualsevol impacte sobre el medi ambient (gestió dels residus).
- Avaluació mediambiental amb indicadors reconeguts a la UE de les tasques de manteniment per garantir el mínim impacte al medi ambient, amb emissió d'informes previs d'avaluació i

posteriors certificats de destrucció, en el cas que sigui necessari, a un centre homologat de reciclatge.

Vigilància de l'Obsolescència:

- Comunicar anticipadament qualsevol risc de falta de subministrament de components.
- Lliurar un Informe Anual d'Obsolescència amb informació actualitzada de productes i serveis. A l'informe caldrà informa dels riscos i possibles actuacions de millora per tal de resoldre les problemàtiques d'obsolescència.

5.10 OBLICACIONS DE TMB

TMB realitzarà les activitats operacionals següents relacionades amb el manteniment correctiu:

- Avís de la incidència i la seva comunicació al equip de manteniment de l'Adjudicatari
- Les activitats operacionals necessàries per poder efectuar les activitats de manteniment i prova

TMB realitzarà les activitats operacionals següents relacionades amb el manteniment preventiu:

- Programació de les peticions de treballs
- Informació a l'Adjudicatari en cas de necessitats de canvis a la programació
- Les peticions i permisos necessaris per a la realització del manteniment

TMB haurà de valorar la possibilitat de implementar una connexió remota al sistema, ja sigui al telecomandament o als elements que es considerin requerits per a la seva revisió.

5.11 ACCÉS A LES INSTAL·LACIONS

El personal de L'ADJUDICATARI disposarà del nivell de formació requerit i les homologacions necessàries per accedir per sí sol a les instal·lacions on ha de realitzar activitats de manteniment. Aquestes homologacions estaran sempre d'acord amb la normativa vigent tant per l'administració com FMB.

FMB facilitarà l'accés a les seves instal·lacions al personal de l'ADJUDICATARI assignat a les tasques objecte d'aquest contracte a la XARXA DE FMB. Per a això FMB lliurarà una autorització nominal a cada agent de l'ADJUDICATARI. El personal haurà de presentar-lo cada vegada que li sigui requerit per un empleat de FMB. Aquesta autorització no serveix per a viatjar per la XARXA DE FMB.

El tècnic o tècnics de l'ADJUDICATARI seran responsables en tot moment de les accions de manteniment portades a terme i de l'adequada senyalització i protecció de les zones de treballs.

5.10.1 Dipòsit i utilització de les claus i codis d'accés a les instal·lacions

FMB lliurarà a L'ADJUDICATARI claus, targetes CAT i qualsevol mitjans vigents en cada moment per accedir a les diferents instal·lacions de la Xarxa a les que tingui autorització.

És responsabilitat de l' ADJUDICATARI definir i supervisar el circuits de dipòsit, custòdia i condicions d'utilització d'aquestes claus.

En cas de produir-se alguna circumstància com pèrdua, trencament, robatori, etc, l'ADJUDICATARI informarà a FMB de forma immediata. Els costos que se'n derivin de la reposició seran a càrrec de l' ADJUDICATARI.

5.11 PREUS I CONDICIONS

S'establirà uns costos fixes i uns costos variables:

COST FIX

- Cost fix anual → Dins d'aquest cost està inclosa la disponibilitat 24 x 7 del tècnic corresponent.
- Cost fix dels manteniments preventius (1 vegades/any)

COST VARIABLE

- Atenció d'incidències (manteniment correctiu) es facturarà segons el preu/hora tècnic definit. Es preveu una estimació anual d'hores per al servei, però la facturació atendrà a les hores realment dedicades.
- Preciari. Cost variable en funció de l'item executat segons relació de tasques valorades.

El cost fix es facturarà de manera trimestral.

El cost variable, quan existeixi, es facturarà de manera mensual.

6. DISPOSICIONS GENERALS

6.1 PERSONAL DESTINAT AL SERVEI

El Contractista ha d'ésser representat ja sigui per una o varies persones amb el coneixement suficient per resoldre/diagnosticar la incidència o tasca a realitzar.

Els responsables dels sistemes als quals fa referencia aquest plec es reserven el dret de treure del servei esmentat els treballadors del Contractista que siguin perjudicials per la execució dels treballs, segons el seu criteri.

El Contractista està obligat a substituir ràpidament aquest personal al rebre la notificació corresponent.

6.2 CONFRONTACIÓ DE LA DOCUMENTACIÓ/PLÀNOLS

El Contractista ha de confrontar tots els plànols després de rebre'ls i informar, tot seguit, de qualsevol contradicció que hi vegi.

6.3 PROTECCIÓ I NETEJA

El Contractista ha conservar perfectament nets tots els espais interiors i exteriors de les instal·lacions on estigui actuant.

6.4 DURACIÓ DEL SERVEI

La duració del servei es la que indica el Quadre de característiques associat a aquest Plec.

6.5 RESCISSIÓ DEL CONTRACTE

Els motius de rescissió del contracte, son els descrits per la Legislació Vigent, segons la qual es farà la liquidació corresponent al servei. Els casos en que queden definides les causes de rescissió de contracte queden reflexades en l'apartat AG del Quadre de característiques associat a aquest Plec.

6.6 RECEPCIÓ PROVISIONAL

Respecte de les modificacions que es puguin originar en el telecomandament, la recepció provisional es farà al finalitzar de forma satisfactòria el servei i les proves sobre la correcta instal·lació i funcionament de l'equipament i software implantant, d'acord amb els protocols de proves a definir i aprovar per part de FMB. Es realitzarà un acta de recepció provisional on constin les modificacions realitzades i la data.

6.7 GARANTÍA

El termini de la garantia s'inicia després de la recepció provisional del servei esmentat i serà de dos anys. Al finalitzar aquest temps es realitzarà la recepció definitiva.

Mentre duri el termini de garantia, són a càrrec de l'Adjudicatari les despeses de reparació del sistema i instal·lacions annexes, incloses les substitucions i modificacions necessàries del material sempre i quan la substitució o reparació vingui derivada d'un defecte del material o de la instal·lació realitzada.

Per la comunicació de les incidències i consultes relacionades amb la garantia de les modificacions l'adjudicatari facilitarà els següents telèfons:

Un número de fax o telèfon fix per comunicar les incidències.

L'avís inclourà la següent informació:

Nom de la persona de FMB que avisa.
Estació a que correspon l'avís.
Equip amb incidència.
Problema que es presenta i símptomes.

Un número de telèfon de contacte els dies feiners per assessorament tècnic en el cas de sorgir dubtes sobre la realització de treballs de conservació.

Es garantirà la reparació o substitució, transport, reinstal·lació i proves d'elements avariats sense cost algun per a FMB durant un any a partir de la data de recepció provisional de la instal·lació.

L'abast inclourà tant els materials com la mà d'obra necessària i els desplaçaments de personal, sempre que els problemes o avaries sorgides s'hagin originat amb l'ús normal de les instal·lacions i equips, exceptuant el normal desgast dels mateixos. Només es consideren causes invalidades de la garantia aquelles en les quals els elements hagin estats exposats a circumstàncies alienes al seu ús adequat, com són operacions fora dels límits de disseny, mal tractaments, etc. així com les causes de força major.

Aquest concepte és independent del manteniment que es realitzi per FMB durant el mateix temps per garantir la correcta conservació de l'equipament.

L'Adjudicatari garantirà que tots els materials emprats en la construcció de les escales estaran disponibles i en catàleg per a FMB en els propers anys.

6.8 RECEPCIÓ DEFINITIVA

En finalitzar el termini de garantia es fa la recepció definitiva del servei de la forma i condicions establertes per la legislació vigent.

6.9 PROVES I POSADA EN SERVEI

L'acceptació del subministrament sol·licitat per FMB estarà supeditada a la comprovació dels requisits funcionals dels responsables dels sistemes afectats.

Per a la comprovació d'aquests requisits es realitzaran proves exhaustives sobre el seu funcionament.

L'adjudicatari vindrà obligat a presentar una proposta de protocols de proves generals per a tots els sistemes.

Les proves seran a càrrec de l'adjudicatari i es tindran que fer prèviament a notificar a FMB que la modificació es troba finalitzada.

El protocol de proves haurà de ser presentat per l'adjudicatari del contracte i validat per FMB. FMB lliurarà un protocol de proves de referència per a fer les proves, que caldrà completar per part de l'adjudicatari.

Si verificades les proves, alguna part de l'equipament no aconseguís els resultats garantits, el subministrador es comprometrà a reposar o modificar la part defectuosa fins a aconseguir els resultats sol·licitats.

L'existència de proves per part de la propietat o el personal per aquest delegat, no eximeix al servei de les responsabilitats que poguessin derivar-se del mal funcionament del material subministrat.

Aquestes proves no exclouran al subministrador de les obligacions que contrau respecte a les garanties donades al material.

Qualsevol prova o assaig no especificat i que sigui necessari per a l'acceptació d'equips o instal·lacions haurà de ser indicada i executada per l'adjudicatari.

6.10 DOCUMENTACIÓ

El cost de tota la documentació descrita als subapartats següents s'entendrà inclosa en l'import total del servei.

6.11 PENALITZACIONS

Queden recollides en el Quadre de característiques associat a aquest Plec.

6.12 CONTRACTES, ACCIDENTS DE TREBALL I PROTECCIÓ A LA INDÚSTRIA

El Contractista està obligat al compliment del que s'ha establert en la Llei sobre Contractes i reglamentacions de treball, disposicions reguladores dels subsidis i assegurances socials en vigor, Llei d'Assegurança Social en tot allò que sigui vigent.

6.13 MESURES D'ORDRE I SEGURETAT

El Contractista està obligat a adoptar totes les mesures d'ordre i seguretat necessàries per la bona i segura marxa de treballs.

En tot cas, el Contractista es únicament i exclusivament el responsable, durant l'execució del servei, de tots els accidents o perjudicis que li pugui passar al personal o causar aquest u altra persona, o entitat, assumint en conseqüència el Contractista totes les responsabilitats alienes al compliment de la Llei.

6.14 DESPESES A CÀRREC DEL CONTRACTISTA

Són obligacions del Contractista pagar totes les despeses d'anuncis, escriptures, permisos i la formalització del Contracte, els Impostos Vigents Aplicables.

7. CRITERIS AMBIENTALS

Tipus de Criteri	Nom del Criteri	Descripció del Criteri
Obligatori	Impressió d'informes i documents	Acordar amb TMB la impressió, prioritzant la reducció d'impressions, l'ús de paper 100% reciclat i la impressió a doble cara en blanc i negre.
Obligatori	EMBALATGES - material reciclat	Els embalatges no primaris han d'estar fabricats íntegrament amb materials reciclats.
Obligatori	Etiqueta ambiental dels vehicles	Els vehicles (turismes o furgonetes) han de tenir adjudicada l'etiqueta ambiental tipus C com a mínim.
Obligatori	Vessament i abocament de líquids	Prendre mesures per evitar qualsevol abocament al medi ambient i disposar de mitjans de contenció per a productes perillosos.
Obligatori	RESIDUS - Productor de residu	El contractista actua com a productor del residu, complint la legislació vigent i sense deixar residus a les dependències de TMB.
Obligatori	RESIDUS - Codificació i separació	Caracteritzar, codificar, separar i classificar els residus segons el Catàleg de residus de Catalunya (CRC).
Obligatori	RESIDUS - Emmagatzematge	Realitzar l'emmagatzematge en condicions adequades, sense superar els 6 mesos per a residus perillosos.
Obligatori	RESIDUS - Etiquetatge	Etiquetar els residus de manera clara, visible i llegible seguint la normativa d'aplicació.
Obligatori	RESIDUS - Documentació de gestió	Formalitzar la documentació de control (notificacions, contractes, fitxes d'acceptació i fulls de seguiment).
Obligatori	RESIDUS - Transport i Gestió	Utilitzar empreses transportistes i gestors autoritzats per al transport i tractament dels residus.
Obligatori	Direcció d'obra - Supervisió i Informes	Supervisar les mesures ambientals, validar els materials segons criteris ecològics i elaborar informes mensuals i finals.

8. REQUERIMENTS DE CIBERSEGURETAT

Per la necessitat d'abordar la gestió de riscos de seguretat de la informació en el sector ferroviari per al sistema licitat, FMB requereix establir les condicions mínimes a satisfer pel sistema objecte d'aquest plec, en matèria de Ciberseguretat. Per complir els requisits establerts en l'SGSI de FMB i garantir la prestació d'un servei essencial, l'Adjudicatari complirà les exigències especificades en el document següent. El procés de gestió de la Ciberseguretat haurà de complir les normatives i estàndards de seguretat:

- Esquema Nacional de Seguretat (ENS)
- Directiva NIS2
- LOPD
- Els sistemes operacionals hauran de complir l'aplicació de les recomanacions recopilades en les Normatives: UNE-EN IEC 62443, EN 50701 en particular per al sector ferroviari —o la seva futura transposició a IEC63452 que ja està en curs— i l'Esquema Nacional de Seguretat (ENS – CCN), segons la nota tècnica NTOTIC_014 REQUISITS SEGURETAT PER A SISTEMES OPERACIONALS FMB.

Totes les Normes es consideraran en la versió vigent, en la seva última publicació a la data d'adjudicació del contracte.

Aquest procés s'aplica a tot el sistema en el seu conjunt (tots els subsistemes que integren el sistema, les interfícies entre els diferents subsistemes, etc.) i les interfícies que resultin aplicables entre el sistema licitat i el Sistema Ferroviari de FMB.

S'haurà de considerar, a més, la ciberseguretat en el context del procés del cicle de vida de la norma EN 50126-1 RAMS.

Requisits de seguretat per a suport i manteniment:

1. Compliment normatiu continu: Assegurar que la solució aportada, el sistema en el seu conjunt i les operacions de suport i manteniment continuïn complint totes les normatives i estàndards de seguretat rellevants durant tot el cicle de vida del producte. El mantenidor del sistema haurà de garantir que la seguretat no es vegi degradada per les seves activitats.

2. Actualitzacions de seguretat regulars: S'haurà d'establir un procés per regular l'actualització de programari i maquinari, i les actualitzacions de seguretat periòdiques per abordar noves vulnerabilitats i amenaces de seguretat que puguin sorgir durant el cicle de vida del sistema.

3. Actualització i manteniment de programari i sistemes operatius.

4. Gestió de pedaços: Establir un procés per a la gestió eficient i oportuna de pedaços de seguretat, que inclogui l'avaluació d'impacte, la programació d'implementació i la verificació de l'efectivitat dels pedaços aplicats.

Per a la gestió de vulnerabilitats i pedaços, l'Adjudicatari haurà de donar visibilitat dels seus SLA per publicar els pedaços i comprometre's a generar pedaços per a les versions lliurades en el projecte.

5. Ús de programari antivirus, antimalware o EDR.

S'haurà de disposar, per a tot el programari que s'executa en els equips amb antivirus, d'un inventari explícit dels processos i directoris que s'hagin de posar com a excepcions de l'antivirus.

6. Haurà d'actualitzar i mantenir plans de continuïtat i recuperació davant de desastres per assegurar la resiliència operativa.

7. Resposta a incidents de seguretat: Especificar la disponibilitat d'un equip de resposta a incidents de seguretat dedicat, que pugui proporcionar assistència immediata en cas que es detecti una vulnerabilitat o incident de seguretat en el sistema.

8. Auditories de seguretat regulars: Requerir la realització d'auditories de seguretat periòdiques per part d'un tercer independent, per avaluar el compliment dels requisits de seguretat, identificar possibles deficiències i recomanar millores.

9. Còpia de seguretat i recuperació de dades: Establir procediments per realitzar còpies de seguretat periòdiques de les dades crítiques del sistema i garantir la disponibilitat de mecanismes de recuperació de dades en cas de pèrdua o corrupció d'informació. Realització de proves de restauració periòdiques.

10. Monitoratge de seguretat continu: Exigir la implementació de sistemes de monitoratge de seguretat continu, que permetin la detecció primerenca d'activitats sospitoses o anomalies en el sistema i facilitin una resposta ràpida a possibles amenaces. S'haurà d'establir un monitoratge continu de la xarxa per a la detecció d'anomalies. Aquests esdeveniments seran enviats al SIEM Corporatiu de TMB.

11. Instal·lació de tallafocs i implementació de regles basades en privilegis mínims.

12. Gestió d'accessos i privilegis: Si aplica, establir polítiques i procediments per a la gestió segura d'accessos i privilegis, incloent-hi la revisió regular dels drets d'accés i l'aplicació de principis de menor privilegi.

13. Formació en seguretat: Continuar proporcionant formació en conscienciació sobre seguretat al personal involucrat en el suport i manteniment del sistema, per mantenir la seva sensibilització sobre les amenaces de seguretat i les millors pràctiques de seguretat.

14. Avaluació i millora contínua: Establir un procés d'avaluació i millora contínua de la seguretat, que permeti identificar àrees de millora, implementar mesures correctives i adaptar les pràctiques de seguretat a mesura que evolucionin les amenaces i els requisits.

15. S'haurà de disposar d'un entorn de proves que permeti testejar amb garantia les actualitzacions de seguretat.

8.1 REQUISITS DE SEGURETAT DEL SISTEMA SL3

El sistema està classificat amb un nivell de seguretat SL3, per tant, implica que el sistema ha d'estar protegit davant atacs intencionats realitzats amb mitjans sofisticats, recursos moderats i coneixements específics de sistemes industrials (SCADA).

A continuació s'enumeren de forma exhaustiva els security requeriments que són d'aplicació. Molts dels quals no són d'aplicació i caldrà realitzar una renovació de la plataforma per tal de dur-los a terme.

Requisitos de seguridad del sistema

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
SR 1.1	BR	Todos los usuarios que accedan al sistema han de ser identificados y autenticados tanto a nivel de sistemas como de aplicación puede ser a través de contraseñas, dispositivos de acceso o multifactor (combinación de las anteriores).
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios humanos.
	RE2	El sistema de control debe proporcionar la capacidad de emplear la autenticación multifactor para permitir el acceso de usuarios humanos al sistema de control a través de una red que no es de confianza.
SR 1.2	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar todos los procesos de software y dispositivos. Esta capacidad debe hacer cumplir dicha identificación y autenticación en todas las interfaces que proporcionen acceso al sistema de control para permitir los privilegios mínimos, de conformidad con las políticas y procedimientos de seguridad aplicables.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única todos los procesos de software y dispositivos.
SR 1.3	BR	El sistema de control debe tener la capacidad de gestionar cuentas de usuarios (agregar, eliminar, modificar o desactivar) estableciendo condiciones para pertenecer a un grupo y la asignación de autorizaciones. Sólo se admitirán cuentas compartidas, cuando por condiciones del sistema se establezca en el análisis de riesgo, aunque deberán de establecerse contramedidas y documentarlas.
	RE1	El sistema de control debe proporcionar la capacidad de admitir la gestión de cuentas unificada.
SR 1.4	BR	El sistema de control debe proporcionar la capacidad de admitir la gestión de los identificadores (permite operar dentro de un dominio o zona de control específico del sistema) por usuario, grupo, rol o interfaz del sistema de control.
SR 1.5	BR	El sistema de control debe proporcionar la capacidad de: 1) iniciar el contenido del autenticador; 2) cambiar todos los autenticadores predeterminados; 3) cambiar/actualizar los autenticadores; 4) protegerlos contra la divulgación y modificación no autorizada. Ejemplos de autenticadores son claves físicas, tarjetas de acceso, claves privadas, entre otras.

	RE1	Para los usuarios de procesos de software y dispositivos, el sistema de control debe proporcionar la capacidad de proteger los autenticadores pertinentes a través de mecanismos de hardware.
SR 1.6	BR	El sistema de control debe proporcionar la capacidad de identificar y autenticar a todos los usuarios que participen en una comunicación inalámbrica. Ejemplos de tecnologías inalámbricas son Bluetooth, infrarrojos, enrutadores móviles, etc.
	RE1	El sistema de control debe proporcionar la capacidad de identificar y autenticar de manera única a todos los usuarios (personas, procesos de software o dispositivos) que participen en la comunicación inalámbrica.
SR 1.7	BR	En los sistemas de control que utilicen la contraseña como medio de autenticación debe aplicar una fortaleza configurable en base a la longitud mínima y la variedad de caracteres. Se aplicará vigencia máxima para las contraseñas y se notificará cuando esta expire. Esta protección se puede mejorar limitando la reutilización de las contraseñas.
	RE1	El sistema de control debe proporcionar la capacidad de evitar que una cuenta de un usuario humano determinada reutilice una contraseña para un número configurable de generaciones. Además, el sistema de control debe proporcionar la capacidad de aplicar restricciones de vigencia mínimas y máximas de las contraseñas a los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad.
SR 1.8	BR	En los casos en los que se utilice una PKI, el sistema de control debe proporcionar la capacidad de que una PKI funcione con arreglo a las mejores prácticas comúnmente aceptadas u obtener certificados de clave pública de una PKI existente. El registro de esta debe incluir la autorización de un supervisor que verifique la identidad del titular del certificado y que garantice que se emite al usuario previsto.
SR 1.9	BR	En el caso de los sistemas de control que utilicen autenticación de clave pública (PKI), el sistema de control debe proporcionar la capacidad de: l)validar los certificados comprobando la validez de la firma de un certificado determinado; m)validar los certificados a través de una ruta de certificación a una CA aceptada o, en el caso de los certificados autofirmados, desplegando certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; n)validar los certificados comprobando el estado de revocación de un certificado determinado; o)establecer el control del usuario sobre la clave privada correspondiente; y p)asignar la identidad autenticada a un usuario.
	RE1	El sistema de control debe proporcionar la capacidad de proteger las claves privadas pertinentes a través de mecanismos de hardware con arreglo a las prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad.
SR 1.10	BR	El sistema de control debe proporcionar la capacidad de ocultar la retroalimentación de la información de autenticación durante el proceso. No debe dar pistas sobre los fallos de autenticación como, por ejemplo, "nombre de usuario desconocido"
SR 1.11	BR	El sistema de control debe proporcionar la capacidad de aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por cualquier usuario dentro de un periodo configurable de tiempo.
SR 1.12	BR	El sistema de control debe proporcionar la capacidad de mostrar un mensaje de aviso del sistema antes de la autenticación. El personal autorizado debe poder configurar el mensaje de aviso de uso del sistema.

SR 1.13	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza. Debe permitir el acceso sólo cuando se esté autorizado y restringir el acceso desde conexiones telefónicas o no autorizadas. Es posible que los procedimientos requieran la autenticación multifactor para permitir el acceso remoto.
	RE1	El sistema de control debe proporcionar la capacidad de supervisar y controlar todos los métodos de acceso al sistema de control a través de redes que no son de confianza.
FR2. Control de uso		
SR 2.1	BR	El sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios humanos para controlar el uso del sistema de control a fin de admitir el reparto de tareas y el privilegio mínimo. Verificar que las acciones del usuario están permitidas según el rol asignado y permitir que solo las personas cualificadas y autorizadas realicen cambios en los componentes del sistema.
	RE1	En todas las interfaces, el sistema de control debe proporcionar la capacidad de aplicar las autorizaciones asignadas a todos los usuarios (personas, procesos de software y dispositivos) para controlar el uso del sistema de control con el fin de admitir el reparto de tareas y el privilegio mínimo.
	RE2	El sistema de control debe proporcionar la capacidad de que un usuario o rol autorizado defina y modifique la asignación de permisos a roles para todos los usuarios humanos.
	RE3	El sistema de control debe admitir el permiso manual del supervisor de las autorizaciones actuales de los usuarios humanos para un tiempo o secuencia de eventos configurables.
SR 2.2	BR	El sistema de control debe proporcionar la capacidad de autorizar, supervisar y aplicar las restricciones de uso para las conexiones inalámbricas al sistema de control con arreglo a las prácticas comúnmente aceptadas en el sector de la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de identificar e informar de la presencia de dispositivos inalámbricos no autorizados que transmitan dentro del entorno físico del sistema de control.
SR 2.3	BR	El sistema de control debe proporcionar la capacidad de aplicar automáticamente las restricciones de uso configurables, que incluyen: a) prevenir el uso de dispositivos portátiles y móviles; b) requerir autorización basada en un contexto específico; y c) restringir la transferencia de códigos y datos a/de dispositivos portátiles y móviles.
	RE1	El sistema de control debe proporcionar la capacidad de verificar que los dispositivos portátiles y móviles que están intentando conectarse a la zona cumplan con los requisitos de seguridad de la misma.
SR 2.4	BR	El sistema de control debe proporcionar la capacidad de aplicar restricciones de uso para las tecnologías de código móvil basadas en la posibilidad de que causen daños al sistema de control, incluyendo: a) prevenir la ejecución del código móvil; b) requerir procesos de autenticación y autorización adecuados para el origen del código; c) restringir la transferencia del código móvil a/del sistema de control; y d) supervisar el uso del código móvil.

	RE1	El sistema de control debe proporcionar la capacidad de verificar la integridad del código móvil antes de autorizar que se ejecute el código.
SR 2.5	BR	El sistema de control debe proporcionar la capacidad de evitar un acceso posterior iniciando un bloqueo de la sesión tras un período de tiempo configurable de inactividad o mediante iniciación manual. La sesión debe continuar bloqueada hasta que el usuario autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados. En los casos en los que el sistema de control no pueda admitir el bloqueo de la sesión, la entidad responsable debería emplear las contramedidas compensatorias que se consideren adecuadas como mayores medidas de seguridad física y auditorias.
SR 2.6	BR	El sistema de control debe proporcionar la capacidad de terminar una sesión remota, ya sea automáticamente después de un período de inactividad configurable o manualmente por parte del usuario que inició la sesión.
SR 2.7	BR	El sistema de control debe proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado a un número configurable de sesiones.
SR 2.8	BR	El sistema de control debe proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: control de acceso, errores de solicitud, eventos del sistema operativo, eventos del sistema de control, eventos de copias de seguridad y restauración, cambios en la configuración, actividad potencial de reconocimiento y eventos del registro de auditoría. Los registros individuales de auditoría deben incluir la marca de tiempo, fuente (dispositivo, proceso de software o cuenta de usuario humano de origen), categoría, tipo, identificador del evento y resultado del evento.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar de manera centralizada los eventos de auditoría y de elaborar registros de auditoría de múltiples componentes a través del sistema de control en una pista de auditoría para todo el sistema (lógica o física) con correlación de tiempo. El sistema de control debe proporcionar la capacidad de exportar dichos registros de auditorías en formatos habituales para la industria para que se analicen con las herramientas comerciales habituales de análisis de registros, como por ejemplo la administración de eventos e información de seguridad (SIEM).
SR 2.9	BR	El sistema de control debe asignar una capacidad suficiente de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros y la configuración del sistema. el sistema de control debe proporcionar mecanismos de auditoría para reducir la posibilidad de que se exceda dicha capacidad.
	RE1	El sistema de control debe proporcionar la capacidad de emitir un aviso cuando el volumen de almacenamiento de registros de auditoría asignado alcance un porcentaje configurable de capacidad máxima de almacenamiento de registros de auditoría.
SR 2.10	BR	El sistema de control debe proporcionar la capacidad de alertar al personal y evitar la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de auditorías. El sistema de control debe proporcionar la capacidad de admitir las acciones apropiadas en respuesta a un fallo en el procesamiento de auditorías de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.

SR 2.11	BR	El sistema de control debe proporcionar marcas de tiempo (fecha y hora) para la generación de registros de auditoría. Evitar que las fuentes horarias sufran alteraciones no autorizadas.
	RE1	El sistema de control debe proporcionar la capacidad de sincronizar los relojes internos del sistema a una frecuencia configurable.
SR 2.12	BR	El sistema de control debe proporcionar la capacidad de determinar si un usuario humano ha realizado una acción concreta.
FR3. Integridad del sistema		
SR 3.1	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el sistema para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos criptográficos para reconocer cambios de información durante la comunicación.
SR 3.2	BR	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección para prevenir, detectar, mitigar e informar de los efectos de un código malicioso o de software no autorizado. El sistema de control debe proporcionar la capacidad de actualizar los mecanismos de protección.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos de protección contra códigos maliciosos en todos los puntos de entrada y salida.
	RE2	El sistema de control debe proporcionar la capacidad de gestionar los mecanismos de protección contra códigos maliciosos.
SR 3.3	BR	El sistema de control debe proporcionar la capacidad de admitir la verificación del funcionamiento previsto de las funciones de seguridad (medidas de antivirus, identificación, detección de intrusos y auditorias) e informar de las anomalías que se produzcan durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado. Las funciones de seguridad deben incluir todas las funciones que sean necesarias para cumplir con los requisitos de seguridad especificados n esta norma.
	RE1	El sistema de control debe proporcionar la capacidad de emplear mecanismos automáticos para facilitar la gestión de la verificación de la seguridad durante los ensayos de aceptación en fábrica y en emplazamiento y durante el mantenimiento programado.
SR 3.4	BR	El sistema de control debe proporcionar la capacidad de detectar, registrar, informar y proteger contra cambios no autorizados en el software y en la información en reposo.
	RE1	El sistema de control debe proporcionar la capacidad de emplear herramientas automatizadas que notifiquen a un conjunto configurable de receptores cuando se produzcan discrepancias durante la verificación de la integridad.

SR 3.5	BR	El sistema de control debe validar la sintaxis y el contenido de cualquier entrada que se utilice como entrada de control de procesos industriales o entrada que tengan un impacto directo en la acción del sistema de control. Las directrices a tener en cuenta deberían incluir la Code Review Guide del Open Web Application Security Project (OWASP).
SR 3.6	BR	El sistema de control debe proporcionar la capacidad de establecer el valor de salida a un estado predeterminado si no se puede mantener el funcionamiento normal como resultado de un ataque.
SR 3.7	BR	El sistema de control debe identificar y tratar las condiciones de error de manera tal que se pueda aplicar un remedio efectivo. Esto se debe hacer sin proporcionar información que pueda ser aprovechada por adversarios para atacar el sistema de control, a no ser que sea necesario para resolver los problemas de manera oportuna.
SR 3.8	BR	El sistema de control debe proporcionar la capacidad de proteger la integridad de las sesiones. El sistema de control debe rechazar cualquier uso por parte de identificadores de sesión no válidos.
	RE1	El sistema de control debe proporcionar la capacidad de anular los identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación).
	RE2	El sistema de control debe proporcionar la capacidad de generar un identificador de sesión único para cada sesión y considerar no válidos todos los identificadores de sesión imprevistos.
SR 3.9	BR	El sistema de control debe proteger la información y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
SR 4.1	BR	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información (especialmente en dispositivos portátiles) para la que se admite la autorización explícita de lectura, ya esté en reposo o en tránsito. La técnica elegida tenga en cuenta las posibles ramificaciones en el rendimiento del sistema de control y la capacidad de recuperarse tras un fallo del sistema o un ataque.
	RE1	El sistema de control debe proporcionar la capacidad de proteger la confidencialidad de la información en reposo y en sesiones con acceso remoto a través de una red que no es de confianza.
SR 4.2	BR	El sistema de control debe proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura de los componentes que vayan a ser liberados del servicio activo y/o puestos fuera de servicio.
	RE1	El sistema de control debe proporcionar la capacidad de evitar la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles (no retienen la información después de ser liberados para la gestión de la memoria).
SR 4.3	BR	Si se requiere el uso de criptografía, el sistema de control debe usar algoritmos criptográficos, tamaños de clave y mecanismos para el establecimiento y gestión de claves con arreglo a las prácticas y recomendaciones de seguridad comúnmente aceptadas en el sector que se encuentran en documentos como la Publicación Especial NIST SP800-57

FR5. Flujo de datos restringidos		
SR 5.1	BR	El sistema de control debe proporcionar la capacidad de segmentar de manera lógica las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de otras redes del sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de segmentar físicamente las redes del sistema de control de redes no pertenecientes al sistema de control, así como redes críticas del sistema de control de las redes no críticas del sistema de control.
	RE2	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
SR 5.2	BR	El sistema de control debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas y conductos de riesgo. Como parte de una estrategia de protección de defensa total, se deberían dividir los sistemas de control de mayor impacto en zonas separadas utilizando conductos para restringir o prohibir el acceso a la red con arreglo a las políticas y procedimientos de seguridad y a una evaluación de riesgos.
	RE1	El sistema de control debe proporcionar servicios de red a redes el sistema de control, ya sean críticas o no, sin que se establezca una conexión con redes no pertenecientes al sistema de control.
	RE2	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
	RE3	El sistema de control debe proporcionar la capacidad de evitar cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo). Esta función de "cierre en caso de fallo" debe designarse de tal forma que no interfiera en el funcionamiento de un sistema instrumentado de seguridad (SIS) o en otras funciones relacionadas con la seguridad.
SR 5.3	BR	Un sistema de control debe proporcionar la capacidad de evitar la recepción de mensajes de propósito general (correo electrónico, redes sociales o cualquier otro sistema de mensajería) entre personas recibidos de usuarios o sistemas externos al sistema de control.
	RE1	El sistema de control debe proporcionar la capacidad de evitar tanto la transmisión como la recepción de mensajes entre personas de propósito general.
SR 5.4	BR	El sistema de control debe proporcionar la capacidad de admitir la partición de datos (por medios físicos o lógicos), aplicaciones y servicios en base a su criticidad para facilitar la implementación de un modelo de zonificación.
FR6. Respuesta oportuna a los incidentes		
SR 6.1	BR	El sistema de control debe proporcionar la capacidad de que las personas y/o las herramientas autorizadas accedan a los registros de auditoría en modo de lectura.

	RE1	El sistema de control debe permitir el acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API).
SR 6.2	BR	El sistema de control debe proporcionar la capacidad de supervisar continuamente el rendimiento del mecanismo de seguridad utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
SR 7.1	BR	El sistema de control debe proporcionar la capacidad de funcionar en modo degradado durante un evento de denegación de servicio. Un evento de denegación de servicio en el sistema de control no debería afectar negativamente a ningún sistema relacionado con la seguridad.
	RE1	El sistema de control debe proporcionar la capacidad de gestionar las cargas de comunicación (por ejemplo, limitando la tasa) para mitigar los efectos de los tipos de desbordamiento de información de los eventos de denegación de servicio.
	RE2	El sistema de control debe proporcionar la capacidad de restringir la posibilidad de que cualquier usuario provoque eventos de denegación de servicio que puedan afectar a otros sistemas de control o redes.
SR 7.2	BR	El sistema de control debe proporcionar la capacidad de limitar el uso de recursos por parte de las funciones de seguridad para evitar el agotamiento de los recursos.
SR 7.3	BR	El sistema de control debe facilitar la identidad y ubicación de los archivos críticos y la capacidad de llevar a cabo copias de seguridad de la información a nivel del usuario y del sistema (incluyendo información sobre el estado del sistema) sin que esto afecte a las operaciones habituales.
	RE1	El sistema de control debe proporcionar la capacidad de verificar la fiabilidad de los mecanismos de copias de seguridad.
	RE2	El sistema de control debe proporcionar la capacidad de automatizar la función de copia de seguridad en base a una frecuencia configurable.
SR 7.4	BR	El sistema de control debe proporcionar la capacidad de recuperarse y reconstituirse hasta un estado seguro conocido después de una interrupción o fallo. Un estado seguro conocido significa que se atribuyen a todos los parámetros del sistema (ya sean predeterminados o configurables) valores seguros, se reinstalan los parches críticos para la seguridad, se restablecen los ajustes de configuración relacionados con la seguridad, se dispone de la documentación y los procedimientos operativos del sistema, se reinstala y configura la aplicación y el software del sistema con ajustes seguros, se carga la información de las copias de seguridad más recientes y conocidas y se somete a ensayo y se comprueba el funcionamiento del sistema en su totalidad.
SR 7.5	BR	El sistema de control debe proporcionar la capacidad de cambiar de y a una fuente de alimentación de emergencia sin que esto afecte el estado de seguridad existente o un modo degradado documentado.

SR 7.6	BR	El sistema de control debe proporcionar la capacidad de ser configurado de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El sistema de control debe proporcionar una interfaz a los ajustes de configuración de red y seguridad desplegados actualmente.
	RE1	El sistema de control debe proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad desplegados actualmente en un formato legible por una máquina.
SR 7.7	BR	El sistema de control debe proporcionar la capacidad de prohibir y/o restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
SR 7.8	BR	El sistema de control debe proporcionar la capacidad de informar de la lista actual de componentes instalados y de sus propiedades asociadas.

Requisitos de seguridad del componente generales

ID req	BR/RE	Explicación
FR1. Control de identificación y autenticación		
CR 1.1	BR	Los componentes deben proporcionar la capacidad de identificar y autenticar a todos los usuarios en todas las interfaces que permita el reparto de tareas y los privilegios mínimos. Se puede proporcionar a nivel componente o a nivel sistema.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios humanos.
	RE2	Los componentes deben proporcionar la capacidad de emplear la autenticación multifactor para todo el acceso de usuarios humanos al componente.
CR 1.2	BR	Los componentes deben proporcionar la capacidad de identificarse a sí mismos y autenticar a cualquier otro componente de acuerdo con el requisito del sistema SR 1.2 de la NormaIEC62443-3-3.Si el componente, como en el caso de una aplicación, se ejecuta en el contexto de un usuario humano, además, la identificación y autenticación del usuario humano de acuerdo con el requisito del sistema SR1.1 de la Norma IEC62443-3-3 puede formar parte del proceso de identificación y autenticación del componente hacia los demás componentes.
	RE1	Los componentes deben proporcionar la capacidad de identificar y autenticar de forma única a cualquier otro componente.
CR 1.3	BR	Los componentes deben proporcionar la capacidad de permitir la gestión de todas las cuentas de forma directa o integrándose en un sistema que gestione las cuentas.
CR 1.4	BR	Los componentes deben proporcionar la capacidad de integrarse en un sistema que soporte la gestión de identificadores y/o la capacidad de permitir la gestión de identificadores.

CR 1.5	BR	Los componentes deben proporcionar la capacidad de: a) permitir el uso del contenido inicial del autenticador; b) permitir el reconocimiento de los cambios en los autenticadores predeterminados realizados en el momento de la instalación; c) funcionar correctamente con operaciones periódicas de modificación/actualización de los autenticadores; y d) proteger a los autenticadores de la divulgación y modificación no autorizada cuando se almacenan, utilizan y transmiten.
	RE1	Los autenticadores en los que se apoya el componente deben estar protegidos mediante mecanismos de hardware (Memoria protegida por contraseña, memoria OTP, comprobaciones de integridad hardware de datos y mecanismo de arranque de seguridad de dispositivos.).
CR 1.7	BR	Los componentes que utilicen autenticación basada en contraseña, deben proporcionar o integrarse en un sistema que proporcione la capacidad de aplicar la fortaleza de las contraseñas configurables de acuerdo con directrices de contraseñas reconocidas y probadas internacionalmente.
	RE1	Los componentes deben proporcionar, o integrarse en un sistema que proporcione la capacidad de proteger una cuenta de usuario humano determinada contra la reutilización de una contraseña para un número configurable de generaciones. Además, el componente debe proporcionar la capacidad de aplicar las restricciones de vigencia mínimas y máximas de la contraseña para los usuarios humanos. Estas capacidades se deben ajustar a las prácticas comúnmente aceptadas en el sector de la seguridad. El componente debería proporcionar la capacidad de solicitar al usuario que cambie su contraseña en un tiempo configurable antes de su caducidad.
CR 1.8	BR	Cuando se utilice una infraestructura de clave pública (PKI), el componente debe proporcionar o integrarse en un sistema que ofrezca la capacidad de interactuar y funcionar de conformidad con el requisito del sistema SR 1.8 de la Norma IEC62443-3-3.
CR 1.9	BR	Los componentes que utilicen autenticación basada en clave pública deben suministrarse directamente o integrarse en un sistema que ofrezca la capacidad en el mismo entorno del sistema de control para: a)validar los certificados comprobando la validez de la firma de un certificado determinado; b)validar la cadena de certificados o, en el caso de los certificados autofirmados, desplegar certificados de hoja a todos los hosts que se comunican con el sujeto al que se emite el certificado; c)validar los certificados comprobando el estado de revocación de un certificado determinado; d)establecer el control del usuario sobre la clave privada correspondiente; e)asignar la identidad autenticada a un usuario y f)garantizar que los algoritmos y claves utilizados para la autenticación de clave pública cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger las claves privadas críticas de larga duración mediante mecanismos de hardware.
CR 1.10	BR	Cuando un componente ofrezca la capacidad de autenticación, el componente debe ofrecer la capacidad de ocultar la retroalimentación de la información del autenticador durante el proceso de autenticación.
CR 1.11	BR	Cuando un componente ofrezca una capacidad de autenticación, el componente debe proporcionar la capacidad de: a) aplicar un límite de un número configurable de intentos de acceso no válidos consecutivos por parte de cualquier usuario durante un período de tiempo configurable; b) denegar el acceso durante un período de tiempo específico o hasta que un administrador lo desbloquee

		cuando se haya alcanzado este límite. Un administrador puede desbloquear una cuenta antes de la caducidad del período de tiempo de espera.
CR 1.12	BR	Cuando un componente proporcione un acceso de usuario humano local/IHM, debe proporcionar la capacidad de mostrar un mensaje de notificación de uso del sistema antes de la autenticación. Personal autorizado debe poder configurar el mensaje de notificación de uso del sistema.
CR 1.14	BR	Para los componentes que utilicen claves simétricas, el componente debe proporcionar la capacidad de: a) establecer la confianza mutua utilizando la clave simétrica; b) almacenar de forma segura el secreto compartido; c) restringir el acceso al secreto compartido; y d) garantizar que los algoritmos y claves utilizados para la autenticación de clave simétrica cumplen con los requisitos establecidos.
	RE1	Los componentes deben proporcionar la capacidad de proteger claves simétricas críticas y de larga duración mediante mecanismos de hardware.
FR2. Control de uso		
CR 2.1	BR	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios identificados y autenticados en función de las responsabilidades que se les hayan asignado.
	RE1	Los componentes deben proporcionar un mecanismo de aplicación de la autorización para todos los usuarios en función de las responsabilidades que se les asignen y del privilegio mínimo.
	RE2	Los componentes, directamente o a través de un mecanismo de compensación de seguridad, deben proporcionar un rol autorizado para definir y modificar la asignación de permisos a roles para todos los usuarios humanos. Los roles no deberían limitarse a jerarquías fijas anidadas en las que un rol de nivel superior sea un superconjunto de un rol menos privilegiado. Por ejemplo, un administrador de sistema no debería incluir necesariamente privilegios de operador.
	RE3	Los componentes deben proporcionar el permiso manual del supervisor durante un tiempo o secuencia de eventos configurables. La implementación de un permiso manual, controlado y auditado de mecanismos automatizados en caso de emergencia u otros eventos graves permite a un supervisor autorizar a un operador para que reaccione rápidamente ante condiciones inusuales sin cerrar la sesión actual y establecer una nueva sesión como un usuario humano con mayores privilegios.
CR 2.2	BR	Si un componente soporta el uso a través de interfaces inalámbricas, debe proporcionar la capacidad de integrarse en el sistema que soporta la autorización de uso, la supervisión y las restricciones de acuerdo con las prácticas industriales comúnmente aceptadas.
CR 2.5	BR	Si un componente proporciona una interfaz para un usuario humano, tanto si se accede localmente como a través de una red, el componente debe proporcionar la capacidad de: a)protegerse contra el acceso posterior iniciando un bloqueo de sesión después de un período de tiempo configurable de inactividad o mediante la iniciación manual por parte del usuario y b)mantener el bloqueo de la sesión hasta que el usuario propietario de la sesión, u otro usuario humano autorizado, restablezca el acceso utilizando los procedimientos de identificación y autenticación adecuados.

CR 2.6	BR	Si un componente soporta sesiones remotas, el componente debe proporcionar la capacidad de terminar una sesión remota automáticamente después de un período de inactividad configurable, manualmente por parte de una autoridad local, o manualmente por parte del usuario que inició la sesión.
CR 2.7	BR	Los componentes deben proporcionar la capacidad de limitar el número de sesiones simultáneas por interfaz para cualquier usuario determinado (persona, proceso de software o dispositivo).
CR 2.8	BR	Los componentes deben proporcionar la capacidad de generar registros de auditoría pertinentes para la seguridad de las siguientes categorías: a) control de acceso; b) errores de solicitud; c) eventos del sistema de control; d) evento de copia de seguridad y restauración; e) cambios de configuración; y f) eventos de registro de auditoría. Los registros de auditoría individuales deben incluir: a) marca de tiempo; b) fuente (dispositivo de origen, proceso de software o cuenta de usuario humano); c) categoría; d) tipo; e) ID del evento; y f) resultado del evento.
CR 2.9	BR	Los componentes deben: a) proporcionar la capacidad de asignar una capacidad de almacenamiento de registros de auditoría de acuerdo con las recomendaciones comúnmente reconocidas para la gestión de registros; y b) proporcionar mecanismos para proteger contra un fallo del componente cuando alcance o supere la capacidad de almacenamiento de datos de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de emitir un aviso cuando el almacenamiento de registros de auditoría asignado alcance un umbral de capacidad configurable.
CR 2.10	BR	Los componentes deben: a) proporcionar la capacidad de proteger contra la pérdida de servicios y funciones esenciales en caso de que falle el procesamiento de una auditoría; y b) proporcionar la capacidad para permitir las acciones apropiadas en respuesta a un fallo en el procesamiento de una auditoría de acuerdo con las prácticas y recomendaciones comúnmente aceptadas del sector.
CR 2.11	BR	Los componentes deben proporcionar la capacidad de crear marcas de tiempo (incluyendo fecha y hora) para su uso en los registros de auditoría.
	RE1	Los componentes deben proporcionar la capacidad de crear marcas de tiempo que estén sincronizadas con una fuente de tiempo de todo el sistema.
CR 2.12	BR	Si un componente proporciona una interfaz para un usuario humano, el componente debe proporcionar la capacidad de determinar si un determinado usuario humano ha realizado una determinada acción. Los elementos de control que no puedan permitir tal capacidad se deben enumerar en los documentos de los componentes.
FR3. Integridad del sistema		
CR 3.1	BR	Los componentes deben proporcionar la capacidad de proteger la integridad de la información transmitida. Configurando el componente para la mejora de la seguridad tanto cibernética, utilizando protocolos seguros, como física utilizando hardwares adecuados para el contexto en el que se encuentran.
	RE1	Los componentes deben proporcionar la capacidad de verificar la autenticidad de la información recibida durante la comunicación.

CR 3.3	BR	Los componentes deben proporcionar la capacidad de permitir la verificación de la operación prevista de las funciones de seguridad de acuerdo con el requisito del sistema.
CR 3.4	BR	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de integridad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de integridad.
	RE1	Los componentes deben proporcionar la capacidad de realizar o permitir verificaciones de autenticidad del software, la configuración y otra información, así como el registro y la notificación de los resultados de dichos controles, o bien integrarse en un sistema que pueda realizar o permitir las verificaciones de autenticidad.
	RE2	Si el componente está realizando la verificación de la integridad, debe poder notificar automáticamente a una entidad configurable cuando descubra que se ha intentado realizar un cambio no autorizado.
CR 3.5	BR	Los componentes deben validar la sintaxis, la longitud y el contenido de cualquier dato de entrada que se utilice como entrada de control de procesos industriales o entrada a través de interfaces externas que tengan un impacto directo en la acción del componente.
CR 3.6	BR	Los componentes que se conectan física o lógicamente a un proceso de automatización deben proporcionar la capacidad de establecer salidas a un estado predeterminado si no se puede mantener el funcionamiento normal definido por el proveedor de componentes.
CR 3.7	BR	Los componentes deben identificar y tratar las condiciones de error de manera que no proporcionen información que pueda ser aprovechada por adversarios para atacar el sistema de control.
CR 3.8	BR	Los componentes deben proporcionar mecanismos para proteger la integridad de las sesiones de comunicación, incluyendo: a) la capacidad de invalidar identificadores de sesión al cerrar la sesión el usuario o después de cualquier otro tipo de cierre de sesión (incluidas las sesiones de navegación); b) la capacidad de generar un identificador de sesión único para cada sesión y reconocer solo los identificadores de sesión generados por el sistema; y c) la capacidad de generar identificadores de sesión únicos con fuentes de aleatoriedad comúnmente aceptadas.
CR 3.9	BR	Los componentes deben proteger la información de auditoría, los registros de auditoría y las herramientas de auditoría (si existen) contra el acceso, la modificación y la eliminación no autorizados.
FR4. Confidencialidad de los datos		
CR 4.1	BR	Los componentes deben: a) proporcionar la capacidad de proteger la confidencialidad de la información en reposo para la que se admite la autorización explícita de lectura; y b) permitir la protección de la confidencialidad de la información en tránsito, como se define en el requisito del sistema SR 4.1 de la Norma IEC62443-3-3.
CR 4.2	BR	Los componentes deben proporcionar la capacidad de eliminar toda la información con autorización explícita de lectura, de los componentes que vayan a ser liberados del servicio activo y/o poner fuera de servicio.

	RE1	Los componentes deben proporcionar la capacidad de proteger contra la transferencia de información no autorizada y no intencionada a través de recursos de memoria compartida volátiles.
	RE2	Los componentes deben proporcionar la capacidad de verificar que se ha producido el borrado de la información.
CR 4.3	BR	Si se requiere el uso de criptografía, el componente debe utilizar mecanismos de seguridad criptográfica de acuerdo con prácticas y recomendaciones de seguridad internacionalmente reconocidas y probadas.
FR5. Flujo de datos restringidos		
CR 5.1	BR	Los componentes deben permitir una red segmentada que admitan zonas y conductos, según sea necesario, para permitir una arquitectura de red más amplia basada en la segmentación lógica y la criticidad.
FR6. Respuesta oportuna a los incidentes		
CR 6.1	BR	Los componentes deben proporcionar la capacidad para que las personas y/o las herramientas autorizadas puedan acceder a los registros de auditoría de solo lectura.
	RE1	Los componentes deben proporcionar acceso mediante programación a los registros de auditoría utilizando una interfaz de programación de aplicaciones (API) o enviando los registros de auditoría a un sistema centralizado.
CR 6.2	BR	Los componentes deben proporcionar la capacidad de ser continuamente supervisados utilizando prácticas y recomendaciones comúnmente aceptadas en el sector de la seguridad para detectar, caracterizar y reportar infracciones de seguridad de manera oportuna.
FR7. Disponibilidad de los recursos		
CR 7.1	BR	Los componentes deben proporcionar la capacidad de mantener las funciones esenciales cuando operen en modo degradado como resultado de un evento de denegación de servicio.
	RE1	Los componentes deben proporcionar la capacidad de mitigar los efectos de los tipos de eventos de denegación de servicio de desbordamiento de información y/o mensajes.
CR 7.2	BR	Los componentes deben proporcionar la capacidad de limitar el uso de recursos en las funciones de seguridad para proteger contra el agotamiento de los recursos.
CR 7.3	BR	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.
	RE1	Los componentes deben proporcionar la capacidad de participar en operaciones de copia de seguridad a nivel de sistema con el fin de salvaguardar el estado de los componentes (información a nivel de usuario y de sistema). El proceso de copia de seguridad no debe afectar a las operaciones normales de los componentes.

CR 7.4	BR	Los componentes deben proporcionar la capacidad de poder ser recuperados y reconstituidos hasta un estado de seguridad conocido después de una interrupción o fallo.
CR 7.6	BR	Los componentes deben proporcionar la capacidad de poder ser configurados de acuerdo con las configuraciones de red y seguridad recomendadas, tal y como se describe en las directrices proporcionadas por el proveedor del sistema de control. El componente debe proporcionar una interfaz con los ajustes de configuración de red y seguridad actualmente desplegados.
	RE1	Los componentes deben proporcionar la capacidad de generar un informe que enumere los ajustes de seguridad actualmente desplegados en un formato legible por una máquina.
CR 7.7	BR	Los componentes deben proporcionar la capacidad de restringir específicamente el uso de funciones, puertos, protocolos y/o servicios innecesarios.
CR 7.8	BR	Los componentes deben proporcionar la capacidad de permitir un inventario de componentes del sistema de control de acuerdo con el requisito del sistema SR 7.8 de la Norma IEC62443-3-3.

Requisitos de seguridad del componente a nivel de software

ID req	BR/RE	Explicación
SAR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	La aplicación debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
SAR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.

Requisitos de seguridad para los dispositivos integrados (PLCs, IED)

ID req	BR/RE	Explicación
EDR 2.4	BR	En caso de que una aplicación de software utilice tecnologías de código móvil, dicha aplicación debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en la aplicación de software: a) controlar la ejecución del

		código móvil; b) controlar qué usuarios están autorizados a transferir código móvil desde/hacia la aplicación; c) controlar la ejecución de código móvil basándose en los resultados de una verificación de la integridad previa a la ejecución del código.
	RE1	El dispositivo integrado debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
EDR 2.13	BR	Los dispositivos integrados deben proteger contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, depuración JTAG).
	RE1	Los dispositivos integrados deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
EDR 3.2	BR	El proveedor del producto de aplicación debe calificar y documentar qué protección contra los mecanismos de código malicioso son compatibles con la aplicación y debe considerar cualquier requisito especial de configuración.
EDR 3.10	BR	El dispositivo integrado debe admitir la capacidad de ser actualizado y someterse a una subida de nivel.
	RE1	El dispositivo integrado debe validar la autenticidad e integridad de cualquier actualización o subida de nivel del software antes de la instalación.
EDR 3.11	BR	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	El dispositivo integrado debe ofrecer mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
EDR 3.12	BR	Los dispositivos integrados deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
EDR 3.13	BR	Los dispositivos integrados deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
EDR 3.14	BR	Los dispositivos integrados deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el arranque del componente y los procesos en tiempo de ejecución antes de su uso.
	RE1	Los dispositivos integrados deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

ID req	BR/RE	Explicación
HDR 2.4	BR	En caso de que un dispositivo host utilice tecnologías de código móvil, dicho dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo host: a) controlar la ejecución del código móvil; b) controlar qué usuarios están autorizados a cargar código móvil en el dispositivo host; y c) controlar la ejecución del código basándose en comprobaciones de integridad en el código móvil y antes de que el código se ejecute.
	RE1	El dispositivo host debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
HDR 2.13	BR	Los dispositivos host deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos host deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.
HDR 3.2	BR	Los dispositivos host deben contar con mecanismos homologados por el proveedor de productos del sistema de control que garanticen la protección contra códigos maliciosos. El proveedor del producto del sistema de control debe documentar cualquier requisito especial de configuración relacionado con la protección contra el código malicioso.
	RE1	El dispositivo host debe informar automáticamente de las versiones del software y de los archivos de protección contra el código malicioso en uso (como parte de la función de registro general).
HDR 3.10	BR	Los dispositivos host deben contar con la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos host deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
HDR 3.11	BR	Los dispositivos host deben ofrecer la capacidad de admitir mecanismos de resistencia a la manipulación y de detección para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos host deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
HDR 3.12	BR	Los dispositivos host deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.

HDR 3.13	BR	Los dispositivos host deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
HDR 3.14	BR	Los dispositivos host deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos host deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.

Requisitos de seguridad para los dispositivos de red

ID req	BR/RE	Explicación
NDR 1.6	BR	Un dispositivo de red que permita la gestión de acceso inalámbrico debe proporcionar la capacidad de identificar y autenticar a todos los usuarios (personas, procesos de software o dispositivos) que participan en la comunicación inalámbrica.
	RE1	El dispositivo de red debe proporcionar la capacidad de identificar y autenticar de forma única a todos los usuarios (personas, procesos o dispositivos de software) que participen en la comunicación inalámbrica.
NDR 1.13	BR	El dispositivo de red que permita el acceso de dispositivos a una red debe poder supervisar y controlar todos los métodos de acceso al dispositivo de red a través de redes que no son de confianza.
	RE1	El dispositivo de red debe proporcionar la capacidad de denegar las solicitudes de acceso a través de redes que no sean de confianza a menos que se apruebe explícitamente mediante un rol asignado.
NDR 2.4	BR	En caso de que un dispositivo de red utilice tecnologías de código móvil, el dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad para el uso de tecnologías de código móvil. La política de seguridad debe permitir, como mínimo, las siguientes acciones para cada tecnología de código móvil utilizada en el dispositivo de red: a) controlar la ejecución del código móvil; b) controlar qué usuarios (persona, proceso de software o dispositivo) están autorizados a transferir código móvil hacia/desde el dispositivo de red; y c) controlar la ejecución del código basándose en verificaciones de integridad antes de que el código se ejecute
	RE1	El dispositivo de red debe proporcionar la capacidad de aplicar una política de seguridad que permita al dispositivo controlar la ejecución del código móvil basándose en los resultados de una comprobación de autenticidad antes de que se ejecute el código.
NDR 2.13	BR	Los dispositivos de red deben protegerse contra el uso no autorizado de la(s) interfaz(ces) física(s) de diagnóstico y ensayo de fábrica (por ejemplo, la depuración JTAG).
	RE1	Los dispositivos de red deben proporcionar una supervisión activa de las interfaces de diagnóstico y ensayo del dispositivo y generar una entrada de registro de auditoría cuando se detecten intentos de acceso a estas interfaces.

NDR 3.2	BR	El dispositivo de red debe proporcionar protección contra códigos maliciosos.
NDR 3.10	BR	Los dispositivos de red deben admitir la capacidad de ser actualizados y someterse a una subida de nivel.
	RE1	Los dispositivos de red deben validar la autenticidad e integridad de cualquier actualización o subida de nivel de software antes de la instalación.
NDR 3.11	BR	Los dispositivos de red deben ofrecer mecanismos de detección y resistencia a la manipulación para proteger contra el acceso físico no autorizado al dispositivo.
	RE1	Los dispositivos de red deben poder notificar automáticamente a un conjunto configurable de destinatarios si descubren que se ha intentado realizar un acceso físico no autorizado. Todas las notificaciones de manipulación se deben registrar como parte de la función general de registro de auditoría.
NDR 3.12	BR	Los dispositivos de red deben proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del proveedor del producto que se utilizarán como una o más "raíces de confianza" en el momento de la fabricación del dispositivo.
NDR 3.13	BR	Los dispositivos de red deben: a) proporcionar la capacidad de proporcionar y proteger la confidencialidad, integridad y autenticidad de las claves y datos del propietario del activo que se han de utilizar como "raíces de confianza"; y b) permitir la capacidad de aprovisionamiento sin depender de componentes que puedan estar fuera de la zona de seguridad del dispositivo.
NDR 3.14	BR	Los dispositivos de red deben verificar la integridad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de utilizarlo en dicho proceso de arranque.
	RE1	Los dispositivos de red deben utilizar las raíces de confianza del proveedor del producto del componente para verificar la autenticidad del firmware, el software y los datos de configuración necesarios para el proceso de arranque del componente antes de que se utilice en dicho proceso de arranque.
NDR 5.2	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de supervisar y controlar las comunicaciones en los límites de la zona para aplicar la compartimentación definida en el modelo de zonas de riesgo y conductos.
	RE1	El componente de red debe proporcionar la capacidad de denegar tráfico de red por defecto y permitir tráfico de red por excepción (también denominado "denegar todo, permiso por excepción").
	RE2	El componente de red debe ofrecer la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control (también denominado modo isla).
NDR 5.3	RE3	El componente de red debe proporcionar la capacidad de proteger contra cualquier comunicación a través del límite del sistema de control cuando se produzca un fallo operativo de los mecanismos de protección de límites (también denominado cierre en caso de fallo).

	BR	Un dispositivo de red en un límite de zona debe proporcionar la capacidad de proteger contra la recepción de mensajes de propósito general entre personas recibidos de usuarios o sistemas externos al sistema de control.

9. SEGURETAT I SALUT LABORAL

9.1. ASPECTES GENERALS

L'adjudicatari assumeix a títol exclusiu el caràcter de patró o empresari respecte del personal que realitzi els serveis comentats en aquest contracte, sense que existeixi cap vinculació jurídica d'aquests treballadors amb FMB.

Conseqüentment, l'adjudicatari es compromet i obliga a complir de manera exacta i fidel totes les obligacions laborals que es derivin de la seva condició empresarial o de patró; com són, per exemple, la inclusió de la seva empresa i els treballadors en el Règim General de la Seguretat Social, tenir actualitzat el llibre de matrícula del personal, la filiació i la cotització a la Seguretat Social, observar amb la diligència deguda les mesures de prevenció, seguretat i higiene en el treball previstes per la legislació vigent o que fossin establertes per la futura, en general respectar i complir escrupolosament totes i cadascuna de les obligacions imposades per les lleis laborals vigents.

FMB lliurarà a l'adjudicatari les normatives específiques per a l'execució dels treballs en la xarxa de FMB. L'adjudicatari garantirà la difusió i el compliment d'aquestes normes per part de tot el seu personal que treballi en les instal·lacions de FMB.

L'adjudicatari haurà de disposar d'una avaluació de riscos laborals de l'exercici de les diferents tasques a les que fa referència aquest contracte segons la llei 31/1995 de Prevenció de Riscos Laborals. Totes les eines i les maquines que es facin servir en la realització d'aquestes tasques hauran de complir aquesta normativa o la que estigui vigent en cada moment.

9.2. COORDINACIÓ D'ACTIVITATS EMPRESARIALS (CAE)

Segons la Llei de Prevenció de Riscos Laborals i el RD 171/2004 es facilitarà el següent intercanvi de documentació:

Documentació a facilitar per part de FMB:

- Procediment P055 "Rilabex" ,A plicació de la normativa de prevenció de riscos laborals en la realització de treballs per empreses externes dins de les instal·lacions del FMB.
- Procediments i instruccions a aplicar.
- Plans d'autoprotecció dels centres de treball i consignes d'actuació en cas d'emergència.

Documentació de l'empresa adjudicatària que estarà disponible en el centre de treball on es realitza les activitats i que s'actualitzarà permanentment. Aquesta documentació pot ser sol·licitada per un interlocutor assignat per FMB.

- Concert amb Servei de Prevenció aliè (o justificació Serveis de prevenció propis).
- Avaluació de riscos, planificació activitat preventiva dels treballs, i Pla de Seguretat i Salut al inici del contracte. Adequació dels equips de treball a la normativa vigent.
- Fitxes de seguretat dels productes químics que es pugin utilitzar.
- Llistat dels treballadors assignats en el centre de treball (Nom, cognoms i DNI).
- TC's del mes en curs.
- Registre de formació del treballador en matèria de PRL.

- Formació específica de cada treballador: Recurs preventiu (si correspon), Pilot
- Homologat de Seguretat, formació tècnica, en eines i utillatges....).
- Justificant de lliurament de EPI's.
- Resultats de la vigilància de la Salut de cada treballador.
- Procediments a seguir en cas d'accident.
- Relació d'accidents de treball i les seves investigacions.

De forma prèvia a l'inici de les activitats, es mantindrà una reunió de coordinació entre FMB i els representants de l'adjudicatari. En aquesta reunió l'empresa contractada aportarà la informació sobre els riscos que es puguin derivar de la seva activitat.

Durant la reunió es determinaran:

- Mesures de control per als riscos a tercers derivats de les activitats.
- Persona de contacte per a tractar temes relatius a PRL.
- Interlocutors per a qüestions de PRL del centre de treball.

Tanmateix, s'haurà de facilitar la documentació necessària i concreta especificada als procediments de FMB.

9.3. VIGILÀNCIA I CONTROL PER PART DE L'ADJUDICATARI

Pel present plec l'adjudicatari es compromet a:

- Vigilar que el seu personal, o en el cas de que sigui autoritzat a subcontractar algun servei objecte del plec el de les empreses subcontractades i els treballadors autònoms, depenent del mateix o de les empreses subcontractades, compleixin la legislació vigent en matèria de prevenció de riscos laborals així com els procediments de FMB que siguin aplicables, i l'efectiva adopció de les mesures preventives que s'hagin acordat.
- Si ho considera necessari acordarà noves mesures preventives a aplicar havent de comunicar la seva adopció a FMB. Si estimés oportú no executar alguna de les ja establertes, haurà de comunicar-ho prèviament a FMB, que podrà aprovar o denegar la proposta.
- En el cas que hagués de realitzar modificacions en l'execució dels treballs no especificades en l'avaluació de riscos inicialment presentada, comunicarà a l'agent en matèria de coordinació d'activitats assignat per FMB, les citades modificacions i les mesures preventives corresponents, el que haurà de realitzar mitjançant la confecció d'un annex a l' esmentada Avaluació, que presentarà per a la seva anàlisi i aprovació, si escau.
- L'adjudicatari mantindrà actualitzat el llistat de treballadors, tant propis com de les empreses subcontractades i autònoms, així com la documentació necessària (Llibre Registre de Subcontractacions).

FMB podrà realitzar seguiment del compliment de la normativa vigent en matèria de Prevenció de Riscos Laborals i de les mesures preventives establertes per al compliment de contracte. FMB podrà assignar aquesta inspecció a un agent extern.

9.4. CENTRE DE TREBALL

Segons l'art. 2a del RD 171/2004, és qualsevol àrea, edificada o no, en la qual els treballadors hagin de romandre o a la que hagin d'accedir per raó del seu treball.

Per tant, abans de començar els treballs, l'adjudicatari haurà de realitzar una comunicació d'obertura d'un centre de treball o represa d'activitats al departament competent.

9.5. PLA DE SEGURETAT I SALUT I LLIBRE DE REGISTRE DE SUBCONTRACTES

L'adjudicatari ha d'elaborar un pla de seguretat i salut (PSS), en el qual s'analitzin, estudiïn, desenvolupin i complementin les previsions de l'estudi o estudi bàsic. En aquest pla s'han d'incloure, si cal, les propostes de mesures alternatives de prevenció que el contractista proposi, amb la corresponent justificació tècnica, que no poden implicar disminució dels nivells de protecció previstos en l'estudi o estudi bàsic.

El pla de seguretat i salut ha de ser aprovat abans de l'inici del servei pel coordinador en matèria de seguretat i salut.

També s'ha de comptar amb un llibre de subcontractació d'acord a la llei 32/2006 actualitzat on s'hi inscriuen les circumstàncies relatives als subcontractistes que hi intervenen.

En data 10 de juny de 2026 es signa l'especificació tècnica:

PPTE_MANTENIMENT INST. FIXES LC- Servei de manteniment pel sistema de control centralitzat d'instal·lacions fixes de línies convencionals del Ferrocarril Metropolità de Barcelona

*T*ècnic Responsable de Projectes de
Telecontrol i Xarxes

Juan Carlos López Mañas
UEE

PRESSUPOST

CAPÍTOL	DESCRIPCIÓ	Amidament	Ud	Preu	Cost servei total [€]
MANTENIMENT DEL CONTROL CENTRALITZAT D'INSTAL·LACIONS FIXES DE LÍNIES CONVENCIONALS					
MANTENIMENT CORRECTIU I SERVEI D'ASSISTÈNCIA TELEFÒNICA D'INCIDÈNCIES					
A	**Servei d'assistència telefònica d'incidències (anual) amb disponibilitat 24x7x365d.** El servei compren el suport via telefònica d'un tècnic en un termini màxim de (1) hora. En cas de que no sigui possible solucionar la incidència mitjançant l'assistència, el tècnic assignat es desplaçarà físicament a les instal·lacions de FMB per solucionar-ho en un termini fitxat segons tipus de incidència.	5	any	22321,39	111.606,93
MANTENIMENT PREVENTIU					
B	**Servei de manteniment preventiu (una intervenció anual).** Inclou totes les actuacions amb l'abast i periodicitat indicada el plec tècnic sobre els servidors i clients del sistema	5	any	7657,56	38.287,82
HORES MANTENIMENT EVOLUTIU					
C	**Servei de manteniment evolutiu (bossa d'hores / any).** Partida de preu fixe no modificable. Les actuacions evolutives i correctives seran facturades per hores dedicades, cada any disposarà d'un import fixe i es facturaran les hores realment consumides segons la tarifa de tècnic sènior i junior del preciari que s'adjunta.	5	any	20646,05	103230,25
PREU HORA TÈCNICS					
	Hora de tècnic sènior dedicada en manteniment correctiu o evolutiu	1	hora	77,5	
	Hora de tècnic junior dedicada en manteniment correctiu o evolutiu	1	hora	65	
MODIFICACIONS CONTRACTUALS PREVISTES EN TASQUES DE MANTENIMENT DESPRÉS DE LA RENOVACIÓ DEL TELECOMANDAMENT					
D	**Actualització de certificats** Renovació dels certificats en el conjunt de màquines que composen el sistema (20 servidors + 160 clients + 130 PLC's concentradors)	0	Certificat	40	
E	**Actualització de pegats dels sistemes Operatius i bases de dades.** Instal·lació dels pegats en el conjunt de màquines que composen el sistema (20 servidors + 160 clients)	0	Pegat	35	
F	**Actualització de firmware en els PLC's** Instal·lació de noves versions de firmware en els PLC's que composen el sistema (130 PLC's concentradors)	0	Firmware	35	

G	**Redundància de clústers** Verificació de la correcta redundància del sistema. Realitzant les tasques necessàries per el centre de dades principal i verificar que tots els serveis funcionen correctament en el centre secundari o backup	0	Intervenció	1240	
H	**Anàlisis tràfic sondes NDS** Revisió del tràfic de xarxa del sistema amb l'objectiu de identificar possibles amenaces de seguretat	0	Intervenció	775	
J	**Actualització del directori actiu** El sistema pot encabir més de 3000 usuaris nominatius i més de 300 màquines a gestionar mitjançant un directori actiu, les tasques principals incloses serà la inclusió o eliminació de nous actius dins d'aquest directori	0	Intervenció	100	
PEM					253.125
Despeses Generals					32.906,25
Benefici Industrial					15.187,5

TOTAL DEL CONTRACTE	**301.218,75 €**

Els imports indicats son Pressupost Execució Contracte, PEC. És a dir son preus Pressupost Execució Material (PEM) incloent el benefici industrial (BI) i despeses indirectes (DI). PEC=PEM+BI+DI.