PLEC DE PRESCRIPCIONS TÈCNIQUES

Contracte relatiu a "**Subministrament dels equips Gateway FIP a Ethernet per la integració Digital Train en les sèries de trens 2100 (L4) i 500 (L11)"**

Expedient número: **16090417**

Transports Metropolitans de Barcelona

Marc Calzada i Balcells

Tècnic Responsable de Digitalització i Innovació

DIGITALITZACIÓ i INNOVACIÓ METRO

ÍNDEX

1 Objecte

Aquest contracte té per objecte el subministrament de l'equipament de tren necessari per establir una passarel·la entre els protocols de comunicació FIP (Factory Instrumentation Protocol) i Ethernet, amb la finalitat d'integrar els trens de les sèries 2100 (L4) i 500 (L11) de Ferrocarril Metropolità de Barcelona a la plataforma de monitorització DAVANA, aquestes sèries son les úniques actualment no integrades a la dita plataforma i disposen d'un protocol de comunicacions intern FIP (amb distintes versions segons unitat de tren), que difereix de la resta de trens en servei al Ferrocarril Metropolità de Barcelona.

Atesa la tecnologia FIP, actualment en desús, i la disponibilitat limitada d'equipament en el mercat i documentació pel cas d'ús específic, la contractació també inclourà els treballs previs d'enginyeria de configuració, ajust i validació de la lectura de variables de tren, per tal d'assegurar que els equips subministrats s'adeqüin a les necessitats requerides.

2 Propòsit

Dins el marc del procés de digitalització i monitorització remota de la flota de Material Mòbil del Metro de Barcelona (projecte genèric conegut amb el nom de Digital Train), s'inclou la monitorització dels trens de les sèries:

- sèrie 2100, corresponent a L4 i un total de 15 trens
- sèrie 500, corresponent a L11 i un total de 3 trens

essent aquestes les últimes sèries pendents de integrar la seva monitorització dins l'entorn de la plataforma DAVANA.

La monitorització de trens ens ajuda a poder garantir la màxima disponibilitat de la flota de trens en servei que significa minimitzar les incidències crítiques (aquelles disruptives amb el servei), i una bona manera d'aconseguir-ho és disposant d'una monitorització en temps real dels sistemes embarcats sotmesos a més estrès per tal d'intentar anticipar-se a la seva fallada. En cas que això no sigui possible i, finalment, les incidències s'acabin materialitzant, aquesta monitorització ens permetrà diagnosticar més àgil i acuradament quines han estat les causes per, conseqüentment, restablir el normal funcionament del sistema o element afectat.

Addicionalment, aquesta monitorització proporcionarà una gran quantitat d'informació referent a estats i dades dels sistemes embarcats per explotar-les en temps real o en posterior backoffice.

En resum la monitorització de trens ens conduirà a:

- **Reducció de costos de manteniment**: La detecció precoç de problemes permet intervenir de manera oportuna, reduint així els costos de manteniment i minimitzant el risc de incidents.

- **Millora de la disponibilitat del servei**: Un sistema de monitorització contribueix a garantir la disponibilitat del servei, reduint els temps d'interrupció i les molèsties per als usuaris

Actualment ja s'estan monitoritzant tot els trens de la flota del Ferrocarril Metropolità de Barcelona a excepció dels trens corresponents les sèries 2100 i 500, que circulen en les línies L4 i L11 respectivament.

El propòsit d'aquesta contractació és el subministrament del equipament de tren necessari per establir una passarel·la entre els protocols de comunicació FIP (Factory Instrumentation Protocol) i Ethernet, amb la finalitat de poder integrar aquests trens en la dita plataforma DAVANA. Les sèries esmentades disposen d'un protocol de comunicacions intern FIP que difereix de la resta de trens en servei al Ferrocarril Metropolità de Barcelona. Donat que la tecnologia FIP està actualment en desús, la dificultat d'accedir a equipament d'aquesta tecnologia al mercat a causa de la seva obsolescència i la limitada documentació existent pel cas d'ús específic, serà necessària la fabricació a propòsit dels equips per a aquesta contractació. En aquest sentit, es consideren necessaris i s'inclou en aquesta mateixa contractació els treballs previs d'enginyeria de configuració, ajust i validació de la lectura de variables que s'hauran de realitzar en el moment de l'entrega del primer equip i previ a la fabricació de la resta, assegurant així que els equips subministrats s'adeqüin a les necessitats requerides.

Tant mateix, existeixen fins a tres (3) distintes versions del mateix protocol que suposaran particularitats per cada un dels equips subministrats, segons la diferent agrupació d'unitats de tren i versions:

- 5 trens de la sèrie 2100 (UT2401 al 2405) amb protocol de comunicacions FIP versió 6

- 4 trens de la sèrie 2100 (UT2406 al 2409) amb protocol de comunicacions FIP versió 7

- 6 trens de la sèrie 2100 (UT2410 al 2415) i 3 trens de la sèrie 500 (UT 501 al 502) amb protocol de comunicacions FIP versió 8

Serà doncs necessari complementar els treballs d'enginyeria per l'ajust, configuració d'equips i validació de lectura de les variables realitzats amb la versió de protocol del primer equip, amb aquells treballs d'enginyeria que siguin necessaris per validar la solució en cada una de les restants versions i equips del mateix protocol.

3 Detall dels equips subministrar

Els equips a subministrar son els següents:

- Set (7) equips marca Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 6) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC
- Sis (6) equips marca Duagon PC3422 FIP to Ethernet Communications Gateway (Versió FIP 7) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC
- Onze (11) equips marca Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 8) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC

Aquest equips quedaran distribuïts de la següent manera, atenent a les diferents versions de protocol instal·lats en cada dels trens.

Unitats a subministrar pels trens (15) de la serie 2100 que circulen a L4, d'aquestes hauran de correspondre a les diferents versions de protocol FIP de cada una de les unitats amb les següents quantitats:

- Cinc (5) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 6) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC
- Quatre (4) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 7) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC
- Sis (6) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 8) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC

Unitats a subministrar pels trens (3) de la serie 500 que circulen a L11:

- Tres (3) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 8) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC

Unitats subministrades destinades a stock de recanvi:

- Dos (2) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 6) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC

- Dos (2) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 7) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC
- Dos (2) Duagon PC3422 FIP to Ethernet Communications Gateway (versió FIP 8) integrats amb font alimentació Duagon PS3000R Isolated PSU 72-110 VDC to 24 VDC

Característiques dels equips a subministrar:

L'equip a subministra marca Duagon model PC3422 FIP to Ethernet Communications Gateway és una passarel·la de comunicacions FIP a Ethernet conforme a la normativa EN 50155 per a aplicacions en vehicles ferroviaris. Els equips a subministrar, hauran d'haver-se adaptat amb el mòdul d'alimentació marca Duagon model PS300R, aquest és un mòdul d'alimentació de mode commutat per a la gamma de controladors lògics programables de la sèrie PC3 que accepta una entrada de 72-110 VDC i produeix una tensió interna aïllada de 1,4 A 24 VDC per alimentar els mòduls d'E/S de la sèrie PC3 de 24 VDC

El PC3422 ha estat dissenyat utilitzant mòduls de la sèrie PC3 acomplint les exigències requerides per als vehicles ferroviaris, incloent:

1. Sobretensions i transitoris elèctrics segons EN 50155 / EN 50121-3-2.
2. Xocs i vibracions d'acord amb EN 50155 / EN 61373.
3. Rang de temperatura de funcionament de -40 °C a +70 °C i humitat relativa del 5 % al 95 % sense condensació.

4 Abast i fases del Subministrament

El subministrament d'aquest contracte es defineix en un únic lot, el qual estarà compost per les següents fites:

- **Subministrament del primer equip i enginyeria per l'ajust, configuració d'equips i validació de lectura de les variables versió primer equip entregat:** aquí s'inclou la realització de les accions tècniques necessàries, que requereixin intervenció de personal especialitzat, per l'ajust, configuració dels equips i validació de la lectura de variables per tal que els equips a subministrar compleixin els requisits funcionals objecte d'aquesta contractació. Aquesta activitat s'haurà de realitzar prèviament al

subministrament de la totalitat dels equips i coincidint amb l'entrega de la primera unitat.

- **Subministrament primer equip corresponent a la resta de versions de protocol i enginyeria complementaria per l'ajust, configuració d'equips i validació de lectura de les variables (per cada una de les versions de protocol):** aquí s'inclou per cada una de les dos (2) versions de protocol de l'equipament subministrat, diferents a la primera, els treballs d'enginyeria que sigui necessaris per complementar a aquells ja realitzats, amb la primera versió, donades les particularitats de cada una de les versions.
- **Subministrament de la totalitat dels equips de cada una de les sèries:** on es farà l'entrega de la resta d'equipaments corresponents a cada una de les distintes versions de protocol FIP.

L'equipament de reserva (recanvis) que s'inclou en el subministrament serà entregat en les dependències dels Taller de Material Mòbil de Roquetes amb adreça C/ Fenals 9, 08033 Barcelona

La primera fase d'enginyeria per l'ajust, configuració d'equips i validació de lectura de les variables versió primer equip entregat s'executarà amb un termini màxim d'un (1) mes des de la signatura del contracte, essent aquesta primera fase una fita a nivell facturació.

La següents fase s'executaran amb un termini màxim de divuit (18) mesos un cop finalitzada la primera fase. El proveïdor consensuarà amb Ferrocarril Metropolità de Barcelona la planificació al detall de les activitats d'enginyeria complementaria per cada una de les versions, així com l'entrega dels equips, poden ser aquestes fites de facturació independents per cada una de les diferents tipologies d'equips a subministrar segons les versions de protocol FIP.

5 Obligacions de l'Adjudicatari

És responsabilitat del Adjudicatari, la realització de la totalitat dels subministraments i activitats complementàries d'enginyeria d'aquesta licitació aportant els mitjans tècnics i humans necessaris, essent també obligacions de l'Adjudicatari:

- Formació i capacitació del personal assignat a la realització de les activitats descrites.
- Garantir els requisits de seguretat i salut associats al servei de la present licitació per al personal assignat. És necessari que el personal que realitzi les activitats disposi dels coneixements necessaris i experiència en la instal·lació dels equips especificats en l'àmbit de material mòbil i infraestructures, així com coneixement

de tota la normativa referent en l'àmbit de Prevenció de Riscos Laborals, i procedimental general i específiques de Ferrocarril Metropolità de Barcelona.

- Evitar, en el subministrament i realització d'activitats descrites, qualsevol impacte sobre el medi ambient.
- És necessari que els equips s'ajustin als requeriments de model i fabricant estipulats. Altrament podria no ser factible tècnicament ni viable la integració amb els equips i solucions preexistents, comportant desenvolupaments electrònics i en programari addicionals amb sobre costos elevats.

6 Ciberseguretat

6.1 Abreviatures

CCN	Centre Criptogràfic Nacional
DMZ	Zona desmilitaritzada
EDR	Detecció i Resposta de Punts Finals
ENS	Esquema Nacional de Seguretat
IDS	Sistemes de Detecció d'Intrusos
GPDR	Reglament General de Protecció de Dades
IICC	Infraestructures Crítiques
IPS	Sistemes de Prevenció d'Intrusos
IT	Tecnologia de la Informació
IPS	Sistemes de Prevenció d'Intrusos
LOPD	Llei Orgànica de Protecció de Dades Personals i garantia dels drets digitals
NIS	Seguretat de la xarxa i del sistema d'informació
OT	Tecnologia de l'operació
SGSI	Sistema de gestió de seguretat integral
SIEM	Gestió d'esdeveniments i informació de seguretat
SLA	Acord de Nivell de Servei
SL	Nivell de Seguretat
SL-A	Nivell de Seguretat Assolit

SL-T Nivell de Seguretat Objectiu

SOC Centre d'operacions de seguretat

6.2 Objecte dels requeriments de ciberseguretat ferroviària

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

El procés de gestió de la ciberseguretat, per a l'adquisició de l'equip d'auscultació de la geometría de via, haurà de complir amb les normatives i estàndards de seguretat:

- Esquema Nacional de Seguretat (ENS)
- Directiva NIS2
- LOPD
- Els sistemes operacionals hauran de complir amb l'aplicació de les recomanacions recopilades a les Normatives: UNE-EN IEC 62443, EN 50701 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)

Totes les Normes seran considerades a la versió vigent, en la seva darrera publicació a la data d'adjudicació del contracte.

Aquest procés s'aplica a tot el sistema en 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.

A més, cal considerar la ciberseguretat en el context del procés del cicle de vida de la norma EN 50126-1 RAMS.

6.3 Requisits de seguretat per a la fase de disseny i integració

El proveïdor de la solució haurà de nomenar un Responsable de Ciberseguretat (RdC) encarregat de liderar i coordinar totes les activitats relacionades amb la ciberseguretat, incloent-hi la definició d'estratègies, la gestió de riscos i la implementació de polítiques i procediments per protegir tant la infraestructura com el sistema embarcat.

Aquest RdC serà l'interlocutor amb el responsable de Ciberseguretat de FMB, amb qui mantindrà reunions periòdiques per avaluar les propostes de ciberseguretat, la implementació de mecanismes de seguretat i el seguiment de la implementació.

L'adjudicatari haurà de contemplar, com a mínim, els següents requisits de partida, que es poden veure ampliats després de l'anàlisi de risc i la proposta d'arquitectura de seguretat:

1. Compliment de normatives i estàndards de seguretat de FMB.
2. Realitzar una anàlisi de riscos preliminar de ciberseguretat, basant-se en MAGERIT/PILAR i en la norma TS50701, segons la nota tècnica NTOTIC_011_MAPA DE RISCOS OT+IICC.

Identificar escenaris de possibles atacs que puguin involucrar o afectar d'alguna manera els sistemes objecte d'aquest plec.

3. Realitzar una proposta d'arquitectura de seguretat inicial identificant solucions de seguretat que es podrien utilitzar per mitigar els riscos identificats:
    - Identificar les zones de seguretat i els conductes
    - Mecanismes de seguretat a aplicar entre zones
    - Taula de comunicació: identificant flux de dades permès entre zones, i les regles a establir als conductes per restringir l'encaminament de la xarxa
    - El disseny i la implementació de les xarxes haurà de garantir la segregació entre els sistemes operacionals crítics i els de menor criticitat, basant-se en els requisits de la norma ferroviària
    - Cal garantir la segregació entre l'entorn OT i l'entorn IT, per assegurar la seguretat perimetral de la xarxa operacional, mitjançant un filtrat robust del trànsit entrant i sortint entre les diferents zones. La xarxa operativa s'ha de separar de la no operativa mitjançant un díode de dades (quan les dades només surtin de la xarxa operativa) o una zona desmilitaritzada (DMZ) quan calgui comunicació bidireccional.
    - Les màquines per a l'explotació de dades s'allotjaran a una zona específica, fora de la xarxa crítica.
    - En cas de requerir màquines de salt, s'ubicaran en una zona específica. Cal habilitar equips host bastionat com a servidor de salt.
    - La comunicació i les interaccions humanes a les zones d'alta criticitat s'han de supervisar, registrar i emmagatzemar amb fins forenses almenys als límits del subsistema (vegeu també EN IEC 62443-3-3 / SR 2.8)
    - El responsable de la zona de criticitat superior ha de gestionar els dispositius de seguretat entre zones de criticitat diferent que protegeixen la seva zona (vegeu també EN IEC 62443-3-2, ZCR 3.1).
    - La zona de criticitat superior ha de considerar les entrades de la zona de seguretat inferior com a potencialment hostils.
    - L'accés directe (de manteniment) no s'ha de permetre des de les zones de negoci a les zones de control sense control mitjançant un dispositiu de seguretat o similar (per exemple, un servidor intermediari)
    - L'accés de manteniment extern (per exemple, mitjançant Internet) s'ha d'agrupar en una zona separada.

4. Realitzar una anàlisi de riscos detallat per a cada actiu i zona identificat, on es determini per vector els nivells de seguretat objectiu (SL-T) i els nivells de seguretat assolits (SL-A), abans de traspassar els riscos residuals a FMB.
5. Prèviament, sense disposar de l'anàlisi detallada de la solució, el nivell de seguretat mínim per als sistemes operacionals serà el que determini el Comitè de Ciberseguretat SL2.
6. La solució haurà de basar-se en els principis de mínim privilegi, confiança zero i defensa en profunditat.
7. S'haurà de lliurar les guies de "bastionat" de tots els equips, quan s'escaigui.
8. S'haurà de presentar un pla per gestionar la seguretat de la cadena de subministrament.
9. La solució proposada haurà de complir el nivell de seguretat requerit durant tot el cicle de vida del sistema.
10. Gestió de vulnerabilitats i pegats: Especificar la implementació d'un procés formal per a la gestió de vulnerabilitats, que inclogui l'avaluació regular de riscos, el pegat oportú de vulnerabilitats conegudes i la resposta a incidents de seguretat. Indicar quins són els SLAs per publicar pegats i durant quant de temps es comprometen a generar pegats per a les versions lliurades al projecte.
11. Protecció de dades personals: Si escau, caldrà establir mesures per garantir la protecció de dades personals, incloent-hi el xifratge de dades sensibles, la minimització de dades i el compliment de regulacions de privadesa com el GDPR.
12. Autenticació i control d'accés: Si escau, el sistema de control haurà d'integrar-se amb Directori Actiu OT per poder gestionar comptes d'usuaris (afegir, eliminar, modificar o desactivar) establint condicions per pertànyer a un grup i assignar autoritzacions. Així com la capacitat d'admetre la gestió dels identificadors (permetent operar dins un domini o zona de control específic del sistema) per usuari, grup, rol o interfície del sistema de control.
13. Xifratge de comunicacions: Si escau, es requerirà l'ús de xifratge robust per a totes les comunicacions entre els components del sistema, incloent comunicacions internes com a externes. L'adjudicatari haurà d'especificar quins algorismes, mides de clau, etc. utilitzarà en cada cas. (El CCN disposa de la guia CCN-STIC 807 per adequació a l'ENS que pot ser de referència).
14. Monitorització i registre d'esdeveniments: Especificar la implementació d'eines de monitorització de seguretat i registre d'esdeveniments per detectar i enregistrar activitats sospitoses, així com per facilitar la resposta a incidents de seguretat.
15. Si escau, com a part de la solució caldrà incloure una solució de monitorització industrial en temps real que detecti intrusions (IDS).
16. Si escau, per tal de poder cobrir la totalitat dels equips industrials connectats a la xarxa, la gestió d'inventari, intrusions, anomalies i vulnerabilitats s'ha de fer tant, sobre els elements i el trànsit dels equips connectats mitjançant protocols IP, com sobre els equips connectats mitjançant protocols propietaris del sector ferroviari. La supervisió del trànsit s'ha de fer de forma passiva, aprenent del funcionament de la xarxa per alertar-ne els comportaments anòmals. La solució ha de permetre visibilitat, gestió, detecció, identificació i control dels

actius de la xarxa, així com de les anomalies, vulnerabilitats i/o qualsevol esdeveniment present a les xarxes OT del sistema. La monitorització haurà de poder integrar-se amb la plataforma de monitorització OT de FMB basada en tecnologia Guardian de Nozomi Networks. Haurà de tenir capacitat de realitzar tasques de:

- Descobriment i inventariat d'actius
- Identificació de protocols
- Identificació dels fluxos de comunicació i disponibilitat de la xarxa
- Identificació de les vulnerabilitats existents als actius desplegats, així com la situació d'aquestes
- Detecció de trànsit maliciós i anomalies a l'entorn industrial
- Anàlisi de riscos i vectors dentrada
- Detecció d'amenaces avançades que siguin específiques per a xarxes industrials
- Estat de salut i rendiment dels sistemes
- Asset Intelligence: disponibilitat d'enriquir la informació dels Assets descoberts, així com el comportament sense necessitat d'aprendre'l
- Capacitat per extreure els valors de les variables de procés
- Capacitat d'utilitzar els valors de les variables de procés en la generació de la baseline de comportament
- Capacitat de detecció d'anomalies
- Capacitat de detecció d'amenaces, almenys de les següents deteccions davant d'amenaces conegudes:
    - Packet rules
    - YARA rules
    - Indicadors STIX

La solució haurà de ser on-premise, garantint la no sortida de dades de lorganització. La informació obtinguda a través de la plataforma passiva de monitoratge industrial en temps real s'haurà de poder enviar al SIEM de TMB (actualment Splunk).

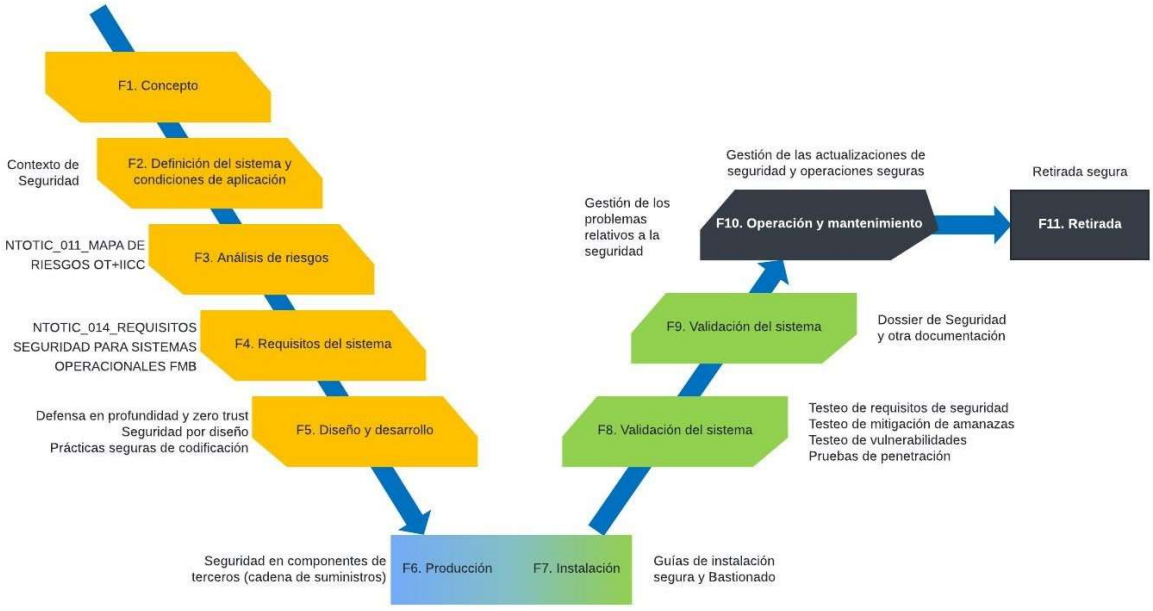
17. Haurà d'assegurar que els equips i aplicacions classificades com a crítiques generin Logs. Aquests hauran de ser custodiats de forma segura per evitar-ne la modificació.
18. El disseny ha d'assegurar la disponibilitat del sistema global (redundància).
19. S'han de fer proves FAT de les solucions de seguretat abans d'implementar-se.

Si escau, FMB es reservarà l'acceptació final de la solució als resultats d'una auditoria de proves de penetració (pentesting) que haurà de presentar l'adjudicatari, podent donar-se el cas de requerir certificar-se a la norma 62443 4.2.

6.4 Requisits de seguretat per a la fase de suport i manteniment

1. Compliment normatiu continu: Assegurar que la solució aportada, el sistema en 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 ha de garantir que la seguretat no es vegi degradada per les activitats.
2. Actualitzacions de seguretat regulars: Cal 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 pegats: Establir un procés per a la gestió eficient i oportuna de pegats de seguretat, que inclogui l'avaluació d'impacte, la programació d'implementació i la verificació de l'efectivitat dels pegats aplicats.
5. Per a la gestió de vulnerabilitats i pegats, l'adjudicatari haurà de donar visibilitat dels seus SLAs per publicar els pegats i comprometre's a generar pegats per a les versions lliurades al projecte.
6. Ús de programari antivirus, antimalware o EDRs. S'haurà de disposar per a tot el programari que s'executa als equips amb antivirus, un inventari explícit dels processos i directoris que s'hagin de posar com a excepcions de l'antivirus, sempre i quan els entorns d'execució siguin vulnerables a aquest tipus d'amenaça.
7. S'haurà d'actualitzar i mantenir plans de continuïtat i recuperació davant de desastres per assegurar la resiliència operativa.
8. 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 al sistema.
9. Auditories de seguretat regulars: Si escau, 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.
10. Suport i recuperació de dades: Establir procediments per fer 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.
11. Monitorització de seguretat contínua: Exigir la implementació de sistemes de monitorització de seguretat contínua, que permetin la detecció primerenca d'activitats sospitoses o anomalies al sistema i facilitin una resposta ràpida a possibles amenaces. Cal establir un monitoratge continu de la xarxa per detectar anomalies. Aquests esdeveniments seran enviats al SIEM Corporatiu de TMB.
12. Si s'escau, en funció de la configuració de xarxa on estiguin connectats els equips, instal·lar Firewalls i implementació de regles basades en privilegis mínims.

13. Gestió d'accessos i privilegis: Si escau, 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 privilegi més baix.
14. Capacitació en seguretat: Continuar proporcionant capacitació 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.
15. Avaluació i millora continuada: 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.
16. Cal disposar d'un entorn de proves que permeti testejar amb garantia les actualitzacions de seguretat.



L'incompliment parcial o total d'aquests punts s'haurà d'acordar amb el CISO de TMB.

6.5 Documentació a lliurar de Cibersefguretat

El proveïdor de la solució haurà de lliurar la següent documentació durant la fase de disseny i integració:

1. Anàlisi de risc preliminar.
2. Inventari d'actius
3. Arquitectura de seguretat
    a. Diagrama de zones i conductes
    b. Anàlisi de risc detallat per a cada zona de seguretat
    c. Propòsit de la comunicació (Funcionalitats, protocols…)
    d. Matriu de comunicacions

e. Flux de dades (origen, destí, nodes…)

f. Regles Firewall (comunicació entre diferents zones)

4. Descripció de contramesures compensatòries.
5. Nivell de seguretat objectiu (SL-T) i nivell de seguretat assolit (SL-A).
6. Guies de "bastionat" dels equips (com Annex s'aporten mesures mínimes de "bastionat" requerit per l'ENS).
7. Pla per gestionar la seguretat de la cadena de subministrament.
8. Gestió de vulnerabilitats i pegats.
9. Així com tota la informació requerida en compliment de la normativa vigent a l'àmbit de la ciberseguretat.
10. Si escau, resultats duna auditoria de proves de penetració.
11. Proposta de pla de manteniment i actualització dels actius inventariats del sistema, amb indicació de les operacions de seguretat i el perfil tècnic requerit per a la seva execució.
12. Plans de recuperació i continuïtat

6.6 Formació de ciberseguretat

El proveïdor de la solució durant la fase de disseny i integració haurà de definir el pla de formació de ciberseguretat que inclogui temari específic en funció del perfil dusuari i/o rol d'interacció amb el sistema i subsistemes.

7 Aspectes/Criteris Mediambientals

En l'execució d'aquest projecte caldrà tenir en compte els següents aspectes mediambientals (d'obligatori compliment):

- Embalatges. Els embalatges no primaris dels productes (embalatge addicional al del propi material per a la distribució final del producte) estaran fabricats a partir de materials reciclats.
- Substàncies perilloses. Els aparells electrònics subministrats no tindran contingut en substàncies classificades com a carcinògenes, perjudicials pel sistema reproductiu, mutagèniques, tòxiques, al·lergèniques, o perilloses pel medi ambient, d'acord amb el Reglament 1272/2008 (CLP) i/o posteriors modificacions.

  El maquinari ofertat haurà de complir amb els requeriments de restricció de substàncies perilloses d'acord amb la Directiva RoHS 2011/65/EU i modificacions posteriors (RoHS compliance), amb els requeriments de la Directiva 2012/19/UE

sobre residus d'aparells elèctrics i electrònics (RAEE) així com amb la resta de normatives de la UE en matèria de Medi Ambient.

- S'oferiran com a mínim 3 anys de garantia comptats a partir de l'entrega del producte.La garantia haurà de cobrir la reparació o substitució, i inclourà un acord de servei amb l'opció de recollida i devolució o de reparació in situ.

8 Obligacions de FMB

FMB realitzarà les activitats operacionals següents relacionades amb el servei:

- Programació de les peticions de treballs i reserva de trens.
- Informació a l'adjudicatari en cas de necessitats de canvis a la programació.
- Avís de les incidències i la seva comunicació a l'equip de manteniment de l'adjudicatari.

9 Comunicacions entre les parts

L'Adjudicatari facilitarà els noms, els telèfons i els correus electrònics de la persona designada com a responsable del subministrament i realització de les activitats del contracte i l'interlocutor en temes administratius.

Per la seva banda, FMB facilitarà a l'adjudicatari una llista d'interlocutors i les seves dades de contacte (telèfon i/o correu electrònic).

10 Garantia

La garantia tindrà una durada de 3 anys i s'iniciarà en la data que es formalitzi el subministrament dels equips.

11 Variants

No se admeten variants.

12 Annexos (datashets)