Transports Metropolitans de Barcelona

Plec de condicions tècniques per l'adquisició, instal·lació, implementació i manteniment de la plataforma de còpies de seguretat per sistemes operacionals de FMB

Expedient número 16110297

Versió 1.0

10/2025

Índex

1. Introducció:

L'objecte del present document és definir les condicions per a la presentació d'oferta d'una plataforma de còpies de seguretat centralitzada per sistemes operacionals de FMB.

Un sistema centralitzat de còpies i la protecció de la informació resulta fonamental per garantir la continuïtat del negoci en cas d'un incident de ciberseguretat.

2. Abast del Servei

L'abast dels serveis tècnics objecte de la present licitació són:

- De producte
- De serveis professionals

a. De producte

Una solució de plataforma de còpies que permeti:

- **Centralització de les còpies seguretat**
- **Eficiència**: Tenir una ràtio òptima de reducció de dades, de manera que el creixement de les dades de producció provoqui el mínim creixement de l'espai del repositori, i que permeti tenir major retenció de còpies locals al menor cost.
- **Capacitat protecció contra atacs ransomware**: Serà indispensable que davant d'un atac cibernètic (Ransomware) es garanteixi la recuperació de les dades de backup que poguessin haver estat esborrades o xifrades.
- **Arquitectura escalable horitzontalment**: L'arquitectura permetrà el creixement lineal del sistema, de manera que en augmentar la seva capacitat augmenti també el rendiment i la connectivitat (arquitectura scale-out), amb l'objectiu de no incrementar el temps dedicat a les còpies de seguretat i mantenir la finestra de backup sota control. Els mòduls que s'afegeixin al sistema podran ser de diferents capacitats i generacions, segons es requereixi en cada moment, i compartiran un únic catàleg de de-duplicació, per la qual cosa l'eficiència aconseguida serà òptima.
- **Rèplica Eficient**: El repositori de còpies de seguretat disposarà de la capacitat de replicar la informació sobre un altre sistema situat en un altre centre de dades d'una forma eficient i xifrada, per optimitzar l'ús dels recursos.

Amb els requeriments d'aplicatiu de còpies de seguretat següents:

1. **Funcionalitats de la solució:**
    - **De-duplicació global i nativa** per programari d'algoritme propietari, agnòstica al maquinari, evitant la utilització de maquinari especialitzat que realitzi aquesta funció de forma independent i suportat en entorns locals, núvol o híbrids. La solució proposada ha de tenir capacitats d'administració d'emmagatzematge eficients mitjançant la de-duplicació per programari per a: de-duplicació en client (en origen), de-duplicació en el servidor (en destí), i amb possibilitat d'utilitzar algoritmes de longitud fixa (FLD) i variable (VLD).
    - **Compressió de la dada** en línia en origen amb independència del maquinari i appliances en entorns on-premise, cloud o híbrids. Actualment, els sistemes operacionals de FMB son on-premise.
    - **Suport de múltiples mètodes de protecció**, backup, arxivat, orquestració de snapshots, replicació i indexació de contingut des d'un únic producte i interfície d'administració.
    - **Consola Multi-tenant**. Des de la mateixa consola ha de ser possible la definició de diferents "tenants" que puguin també identificar-se com a organitzacions, tenint en compte que els recursos i dades associats a un tenant no han de ser visibles pels altres tenants.
    - L'administració del tenant estarà basada en capacitats de control d'accés mitjançant la definició de rols (**Role Based Access Control - RBAC**).
    - Possibilitat d'establir diversos **nivells d'autorització** per a tasques específiques, com eliminar dades i configuracions, canviar períodes de retenció dels backups i restaurar còpies de seguretat.
    - S'han d'admetre autenticació single sign-on SAML i els mecanismes de Doble Factor d'Autenticació (MFA).
    - Capacitat per organitzar les còpies de seguretat i realitzar cerques basades en diferents filtres (per exemple, dates de referència) i mantenir diverses còpies de seguretat simultàniament.
    - Possibilitat de poder seleccionar carpetes i arxius per fer-ne còpia de seguretat i possibilitat d'excloure tipus d'arxius per nom, extensió i mida per a còpies de seguretat de tipus sistema de fitxers (amb instal·lació d'un agent als servidors per fer-ne còpia de seguretat).
    - Possibilitat de modificar les polítiques de retenció aplicades a les còpies de seguretat.
    - Possibilitat de restaurar dades triant la versió de les dades a restaurar en funció de la retenció que se'ls apliqui.
    - Recuperació granular de les dades (únic fitxer, correu, taula, etc.) en mode "in-place" o "out-of-place".
    - Suport per a usuaris i rols de gestors d'autenticació de tercers, així com xifrat de dades i accessos de control de dades.

- Possibilitat de realitzar Backup Full, Incremental, Diferencial i Backup Full Sintètic.
- Servei d'autogestió per a l'usuari final: accés mitjançant aplicació web i mòbil.
- Ha d'admetre la replicació segura de dades a un entorn aïllat amb capacitats d'Air Gap natives via programari, independentment del maquinari utilitzat i sense la necessitat d'afegir maquinari o solucions de tercers per a tal fi.
- Les dades han de signar-se digitalment durant la còpia de seguretat i verificar-se automàticament la seva integritat (suma de comprovació CRC) en les operacions d'escriptura, còpia, lectura o validació. Això s'aplica a tots els tipus d'emmagatzematge (disc, núvol, cinta).
- S'inclourà l'arxivat en la mateixa consola.
- La solució proposada ha de detectar la presència d'aplicacions/base de dades en VMs (**Application-Aware**) i protegir-les consistentment sense necessitat de la instal·lació d'un agent manualment previ al primer backup.
- Compatibilitat amb la funció **WORM** a nivell de matriu d'emmagatzematge
- Possibilitat d'activar **WORM a nivell de programari** de còpia de seguretat per evitar tasques d'eliminació de treballs de còpia de seguretat, canvi de retenció o elements lògics associats a la dada emmagatzemada.
- Còpia de seguretat de dades **immutable** mitjançant un sistema de protecció natiu a nivell de pila d'E/S que bloquegi qualsevol procés/servei aliè a la solució de backup que intenti manipular o modificar les dades de còpia de seguretat fora dels processos administratius de còpia de seguretat autenticats. Això ha de ser independent del maquinari destí de backup utilitzat.

2. **Seguretat:**
   - **Capacitats natives de seguretat** integrades per a la detecció primerenca d'anomalies en la dada productiva (viva) i en la dada de còpia de seguretat (backup), monitorització en temps real i constant mitjançant l'ús d'**Intel·ligència Artificial (IA)** i **aprenentatge automàtic (ML)** per identificar canvis massius en el sistema (creació, modificació i eliminació de fitxers), incloent anàlisi d'integritat de la dada o indicador de compromís que indiqui la presència de malware en les dades, comprovació de les extensions dels arxius protegits (mime), assegurant que la seva extensió i tipus de dada coincideix amb el seu contingut. Aquests mecanismes han de ser independents de l'ús de programari de tercers, permetent també l'enviament d'alertes associades a aquestes anomalies amb destí al **SIEM corporatiu (SPLUNK)** per al tractament de les alertes.

- Un **panell integrat** dins de la interfície d'administració que permeti monitoritzar la notificació de fallades, alertes de seguretat amb capacitat de notificar possibles indicadors de compromís, sistema de seguiment i registre de l'activitat del sistema de còpies de seguretat. Recomanacions per millorar la postura de seguretat de l'entorn a través de l'ús d'aprenentatge automàtic (ML) i Intel·ligència Artificial (IA).
- Possibilitat de configurar les comunicacions de xarxa entre el lloc primari i l'emmagatzematge de còpies de seguretat a través de **túnels TLS 1.3** que suporten connexions unidireccionals o bidireccionals tant en mode directe com a través de proxies. Les comunicacions poden interrompre's deshabilitant ports, deshabilitant VLAN, activant controls de tallafocs, etc., de forma totalment orquestrada i automàtica mitjançant un motor de flux de treball (workflows) natiu de programari.
- **Xifrat de comunicacions** entre tots els components de la infraestructura, a través de l'ús de certificats únics d'autenticació evitant la suplantació d'identitat
- Capacitat de detectar amenaces i riscos com hashes d'arxius i patrons d'arxius, que permeti posar en **quarantena de forma automatitzada** les fonts de ransomware o codis de malware de les còpies de seguretat afectades abans de ser restaurades amb la finalitat d'evitar la reinfecció dels sistemes.
- Capacitat de posar en quarantena automàticament els malware trobats en la verificació, fins i tot amb propòsits d'anàlisi forense, sense la necessitat de scripts manuals.
- **Selecció automàtica d'un punt de recuperació** anterior a l'anomalia amb la possibilitat de sobreescriure la versió anterior dels arxius i descarregar o restaurar en una ubicació diferent per a la seva posterior anàlisi.

3. **Capacitats de governança, gestió i supervisió:**
   - En cas que es produeixi l'emmagatzematge de dades personals, la capacitat d'identificar les **dades sensibles** tant en dades en viu com en les còpies de seguretat. A més, haurà de tenir la possibilitat de crear i gestionar workflows per a la recopilació d'aquestes dades personals dels usuaris.
   - Proveeix les següents funcionalitats:
     - Notificació de fallades, avaries i atacs a la seguretat. Possible integració amb SIEM mitjançant syslog i webhooks.
     - Seguiment i registre de l'activitat del sistema de còpies de seguretat.
     - Monitorització i optimització de l'ús dels recursos d'emmagatzematge.

        - Automatització d'informes i auditoria de compliment (KPI, SLA).
        - Quadres de comandament (dashboards) i informes personalitzables i predefinits en el mateix programari de backup.
    - La solució proposada ha de proporcionar **detecció d'anomalies** en els arxius dels equips client per monitoritzar i alertar als administradors en temps real d'aquestes anomalies.

4. **Capacitats d'integració:**
    - **Integració nativa** amb solucions SIEM/SOAR com ServiceNow, NetSkope, DarkTrace, Splunk (SIEM/SOAR), Microsoft/Azure Sentinel, PaloAlto, Acante, Dasera i CrowdStrike.
    - **Compatibilitat nativa amb llibreries de cintes** sense necessitat de programari o dispositius addicionals.
    - **Compatibilitat nativa** per realitzar còpies de seguretat primàries i secundàries en l'emmagatzematge d'objectes sense utilitzar appliances especialitzats.
    - **Suport de les següents versions de Sistema Operatiu** (sempre que estigui suportada pel seu fabricant) com AIX v6.1-7.6, HP-UX v11, Debian v5 a v12, Fedora v8 a v35, Oracle Linux v5 a v9, CentOS v5 a v9, Red Hat v5 a v9, Rocky Linux v8 a v9, Ubuntu v8 a v24, Amazon Linux 2023 i Amazon Linux 2 i Solaris v10 a v11 en arquitectures x86 i SPARC. També s'haurà de suportar la família de sistemes operatius de Microsoft (Windows), ja siguin llocs d'operació o servidors, tenint present que caldria suportar versions legacy del mateix. S'han de suportar versions dels sistemes operatius ja sigui en servidor físic o màquina virtual.
    - **Suport dels següents hipervisors** sense necessitat de desplegar agents: VMware i VMware Cloud Director, Oracle Linux Virtualization Manager (OLVM), Hyper-V, Oracle VM, RHEV, Nutanix, Oracle Cloud Infrastructure (OCI), OpenStack, Huawei FusionCompute, XenServer (Citrix), Alibaba Cloud, Proxmox VE, AWS, Azure, Google i equivalents, amb possibilitat de realitzar restauracions, rèplica/migració en hipervisor de diferent infraestructura.
    - La solució proposada ha de ser compatible amb la tecnologia Snapshot amb la finalitat d'integrar-se amb els principals arrays d'emmagatzematge de la indústria com Cisco, DataCore, Dell EMC, Fujitsu, Isilon/PowerScale, Infinidat, Nutanix, Hitachi, Huawei, HPE, NetApp, IBM, Pure Storage, Trinti i proveïdors cloud com Azure, Google Cloud i AWS, per automatitzar la creació de Snapshots de maquinari indexats i amb reconeixement d'aplicacions (consistència a nivell aplicació), permetent la protecció de càrregues com VMware, Hyper-V, Nutanix, Oracle i Oracle RAC, SQL Server, MongoDB, NAS (CIFS/NFS), SAP

HANA, SAP for Oracle, Sybase, NDMP, DB2, MySQL, PostgreSQL, etc.

- Ha de permetre realitzar la còpia de seguretat de màquines virtuals a través de l'hipervisor per còpia de snapshot o mitjançant la còpia realitzada per agents instal·lats en les màquines virtuals.
- La solució ha d'oferir la possibilitat de suportar nativament les **aplicacions comunes de mercat**: Active Directory, Azure Entra ID, MSExchange, Oracle, MS SQL Server, MS SharePoint, MySQL, PostgreSQL, MongoDB, Informix, Sybase, Cassandra, CrockroachDB, Hadoop, YugabyteDB, i M365, inclosa la protecció de càrregues tipus PaaS en hyperscalers com Azure, Alibaba Cloud, AWS i Google Cloud Platform.
- Per a tots els emmagatzematges d'objectes compatibles, la **de-duplicació i compressió en origen**, i el xifrat han de ser suportats de forma nativa.
- **Integració de gestió d'accés a identitats**: Plugin certificat per a sistema Delinea.

Amb el requeriments de repositori següents:

- La solució ha de dimensionar-se per satisfer les necessitats actuals expressades més avall i el manteniment dels sistemes durant 3 anys.
- L'emmagatzematge mínim requerit és de 100TB, entenent-se com a tal emmagatzematge total net utilitzable real.
- El sistema ofert tindrà una escalabilitat mínima de 2.000TB de capacitat neta utilitzable real addicional a la presentada en aquesta oferta.
- Per calcular l'emmagatzematge net no es poden considerar els estalvis en l'eficiència obtinguda per de-duplicació; es tracta de la capacitat neta en disc un cop realitzades tasques com el format de discos, definició del RAID, etc.
- La solució serà un únic sistema de maquinari, amb de-duplicació global basat en tecnologia de disc d'extrem a extrem, però contemplarà dues zones (tiers) diferenciades:
    - Una zona de rendiment o zona d'aterratge de les dades (Landing Zone)
        - La informació en aquesta zona no patirà cap alteració i s'emmagatzemarà a velocitat de disc en el format original de l'aplicatiu de còpies de seguretat, per facilitar el rendiment en temps de Backup.
    - Una segona zona orientada a la retenció a mitjà i llarg termini.
        - La informació residirà comprimida i de-duplicada en aquesta zona, amb l'objectiu d'obtenir eficiència i controlar el creixement a llarg termini.
- Els mecanismes de de-duplicació han de tenir lloc íntegrament en el sistema ofert, i no requeriran l'ús de cicles de CPU per part dels servidors de producció, servidors de còpies de seguretat, o servidors de mitjana.

- S'evitaran els processos de de-duplicació inline a mesura que s'ingereixen les dades, a fi d'optimitzar la durada de la finestra de còpia de seguretat.
- Existirà un air-gap entre ambdues zones, que permeti aïllar l'entorn de retenció a llarg termini de possibles atacs realitzats des de la xarxa (dades no exposades a la xarxa).
- Les dades emmagatzemades en la zona de retenció de mitjà i llarg termini hauran de garantir la seva integritat.
- El sistema disposarà de la funcionalitat (Retention Time Lock) necessària per retenir les dades i posposar l'esborrat accidental o malintencionat de les mateixes per part del programari de còpies de seguretat o qualsevol altra aplicació o comandament durant un període de temps parametritzable.
- El sistema ofert disposarà d'alarmes que permetin detectar un comportament anòmal fruit d'un possible atac de ransomware, com ara l'esborrat massiu d'informació o el canvi de patró de dades que poguessin indicar una possible encriptació de la informació.
- Protecció contra ciberatacs. Les capacitats descrites en els 4 punts anteriors, d'air-gap natural entre zones, immutabilitat, retenció dels esborrats i alertes de comportaments sospitosos hauran de permetre la recuperació de la informació davant d'un esborrat massiu o atac criptogràfic de la producció (ransomware).
- La solució oferta presentarà capacitat de creixement lineal (Scale-Out) que permeti mantenir o millorar la ingesta i el rendiment del sistema quan s'incrementi la seva capacitat.
- El creixement de la capacitat en disc s'acompanyarà del corresponent increment en els recursos de CPU, memòria, connectivitat i ample de banda.
- La capacitat addicional implica afegir nodes o elements i no requereix reemplaçar l'equip existent.
- Es garantirà l'escalabilitat del sistema com a mínim fins a una capacitat 30 vegades els requeriments actuals de TMB, millorant el seu rendiment de forma percentual a l'increment de capacitat, de manera que la finestra de còpia de seguretat no creixi i es mantingui sota control.
- La solució serà compatible amb l'aplicatiu de còpies de seguretat d'aquest mateix plec tècnic.
- La connectivitat es realitzarà a través de la xarxa i serà accessible mitjançant protocols de xarxa estàndard, almenys NFS, CIFS, proporcionant un rendiment del còpia de seguretat similar al d'un disc de xarxa (NAS) sense processament afegit.
- El sistema ofert respectarà la de-duplicació nativa pròpia de l'aplicatiu de còpies de seguretat, proporcionant eficiències i de-duplicació addicional.
- La parametrització de les operacions de còpies de seguretat i restauració de la còpia ha de ser gestionable a través de la consola de de l'aplicatiu de còpies de seguretat, sense passos addicionals.
- La solució ofertada ha de ser completament gestionable dins d'una GUI única i fàcil d'usar.

- Es podran definir diferents rols o tipus d'usuaris acords al nivell de les tasques a realitzar, com ara operador, administrador o responsable de seguretat.
- La solució disposarà de doble factor d'autenticació per als usuaris, com a mesura per prevenir el robatori de contrasenyes.
- Aquelles tasques que puguin considerar-se destructives requeriran l'autorització de, almenys, dos usuaris, cadascun amb el seu doble factor d'autenticació.
- La solució ha de tenir la capacitat d'enviar alertes de servei per correu electrònic al personal de suport extern per a suport proactiu i integrar-se amb les principals consoles SNMP.
- La solució ha de ser altament fiable, i els seus discos i fonts d'alimentació intercanviables en calent.
- La protecció dels discos serà RAID 6, per suportar la caiguda simultània d'un mínim de dos discos sense pèrdua de dades, i haurà de disposar de disc de spare.

L'equipament haurà de ser on-premise, garantint la no sortida de dades de la organització, derivat de que els sistemes operacionals actualment estan aïllats del exterior.

TMB disposa d'un entorn de virtualització. Es requisit que l'aplicatiu funcioni sobre aquest entorn. Actualment, és una solució VmWare.

A incloure:

S'inclourà tot el material hardware i cablejat necessari per a la instal·lació i el correcte funcionament del sistema de còpies de seguretat, segons requeriments de l'aplicatiu i repositori. Pel dimensionament tant de les llicències de l'aplicatiu, com del hardware que realitzarà les funcions de repositori, es faciliten les següents dades inicials de volumetria:

- 20 TB de front-end o dades de producció
- 30 màquines virtuals d'entorn VmWare
- Creixement anual del 10%.
- Cicle de còpies de seguretat Full setmanal i diari incremental
- Pel que fa a les polítiques de retenció de Retenció GFS objectiu:
  - 4 setmanes els Backups diaris i full setmanals
  - 12 mesos els backups full mensuals
  - 3 anys els Backups full anuals

Es requisit de la solució, que aquesta ha de garantir la seva escalabilitat, en previsió d'incloure tasques de còpies de seguretat de més sistemes operacionals en següents fases. Aquesta ampliació de sistemes pot implicar integrar nous

sistemes i una ampliació de volumetria no inclosa a les dades inicials de dimensionament.

• Subministrament de llicències Commvault, incloent tres anys de subscripció i suport tècnic del fabricant.

• Subministrament de llicències Exagrid, tres anys de subscripció i suport tècnic del fabricant.

• Subministrament de totes les llicències necessàries per a la correcta activació de totes les funcionalitats descrites en el plec, independentment de la capacitat o nombre de discos, incloent la de-duplicació, protecció davant del ransomware, replicació remota, gestió, integració amb l'aplicatiu de còpies de seguretat, etc.

Per efectuar el llicenciament, s'haurà de tenir en compte que el sistema no disposa de connexió a internet.

b. De serveis professionals

- Instal·lació de l'equipament a la ubicació indicada per FMB (dos CPDs)
- Posada en marxa de la solució i integració amb els sistemes OT
- Suport tècnic del fabricant
- Formació bàsica de manteniment i operació del sistema
- Servei d'acompanyament o millora de la plataforma:
    - Suport tècnic L2 8x5
    - Servei evolutiu de l'aplicació amb actualització de versions
    - Bossa d'hores per un fine tuning de la plataforma

3. Obligacions de l'Adjudicatari

És responsabilitat del Adjudicatari, la realització de la totalitat de les tasques aportant els mitjans tècnics i humans necessaris per mantenir la plataforma de monitorització industrial operativa per acomplir la seva funció i proporcionar els

serveis descrits al capítol Abast del Servei, durant la vigència del contracte, amb els nivells descrits a continuació:

a. Instal·lació i posada en marxa de la solució i implementació

- Anàlisi, disseny i configuració del producte per la volumetria indicada al punt anterior.
- Implementació/desplegament de la solució en TMB (requereix part de l'activitat en mode presencial):
  - Configuració inicial de l'equipament hardware, incloent la instal·lació / actualització del firmware, configuració de la xarxa, etc.
  - Instal·lació dels equips als CPDs
  - Configuració inicial de l'equipament d'emmagazematge
  - Desplegament de l'aplicatiu de sistema de còpies (centralització del sistema), en una plataforma de virtualització VmWare ja existent
  - Configuració de l'aplicatiu segons les especificacions indicades per FMB
- Integració del repositori i aplicatiu de còpies de forma que es puguin integrar amb els sistemes operacionals de FMB.

b. Suport tècnic

Es proporcionarà suport tècnic per al repositori i aplicatiu de còpies de seguretat durant 3 anys per tal de:

- Suport tècnic per resolució de dubtes i consultes
- Accés base de dades de coneixement, manuals d'usuari i documentació tècnica
- Manteniment software: Descàrrega de darreres versions de software amb millores, correcció d'errors i pegats de seguretat
- Manteniment hardware: Substitució d'equips defectuosos

El suport tècnic, que inclou manteniment de l'aplicatiu i el hardware, es considerarà actiu en el moment en què la plataforma estigui disponible per a

realitzar còpies independentment de les integracions amb sistemes que estiguin ja implementades.

c. Formació

- Curs de conceptes fonamentals per operar la plataforma de còpies de seguretat
- Curs de manteniment de la plataforma de còpies de seguretat, atenció d'incidències bàsiques del sistema
- Formació d'integració de la plataforma amb els sistemes operacionals

Les persones que realitzaran el curs realitzen torns rotatius, es demana que els curs estigui orientat per tal que puguin consumir el mateix, ja sigui al torn o de forma online. Es proposa una sessió presencial en torn de matí, que pugui ser enregistrada per tal que la resta de torns pugui fer el curs. Es requerirà una sessió de dubtes per les persones que no puguin atendre presencialment al curs.

d. Servei d'acompanyament o millora de la plataforma:

- Suport tècnic L2 8x5
- Servei evolutiu de l'aplicació amb actualització de versions
- Bossa d'hores per la realització d'un fine tuning de la plataforma

e. Suport tècnic L2 8x5

El servei per 3 anys des de la formalització de la implementació de la plataforma.

Inclou:

- Suport tècnic de nivell 2 (Integrador / Adjudicatari) de la plataforma de còpies de seguretat:
    - En horari d'atenció 8x5
    - Idioma castellà / català

- Escalat a suport tècnic de nivell 3 (fabricant) en cas necessari
- Punt de contacte, qui gestionarà i resoldrà les peticions de TMB, contactant amb fabricants en cas necessari
- Revisió periòdica per assegurar el funcionament òptim de la plataforma
- Resolució d'incidències i apertura de casos a fabricant, incloent manteniment hardware RMA i software
- Execució d'accions programades sobre els equips per a la instal·lació de noves versions de firmware o actualitzacions

f. Servei evolutiu de l'aplicació amb actualització de versions

Aquest servei compren l'actualització de la versió de la plataforma amb les recomanacions del fabricant Commvault i Exagrid.

g. Bossa d'hores per fine tuning de la plataforma

Aquest servei compren una bossa de **125 hores** a consumir durant un període de 2 anys per tal de realitzar integracions de la plataforma de còpies de seguretat amb els sistemes operacionals.

També Inclou:

- Creació d'usuaris amb control d'accés basat en rols (perfil seguretat, perfil mantenidor, perfil tècnic sistema operacional, etc.)
- Revisió proactiva de la configuració per adaptar-la a les necessitats de FMB
- Personalització de la plataforma. Generació de Built-in reports i dashboards sobre la plataforma, segons capacitat de la mateixa
- Resolució de dubtes sobre el funcionament de la plataforma
- Revisió de les alertes: assessorament, suport en la interpretació
- Integració amb altres eines de seguretat amb l'objectiu d'establir mètriques de detecció i resposta a possibles incidents de seguretat que siguin detectats

- Suport del fabricant per resolució de tasques complexes
- Anàlisi de registres per detectar i corregir problemes de funcionament o generar propostes de millora en funció del tràfic detectat

h. Altres Obligacions de l'Adjudicatari

A part de la realització de les tasques necessàries descrites en els punts anteriors també són obligacions de l'Adjudicatari:

- Formació i capacitació del personal assignat a la realització d' aquestes tasques.

  El personal haurà de disposar de la formació tècnica adequada per les tasques específiques del lloc de treball.

  El personal assignat al projecte haurà de disposar de les acreditacions professionals adients per demostrar la seva experiència.

  Tota la formació tècnica necessària serà impartida per l'Adjudicatari.

  L'Adjudicatari facilitarà a tot el seu personal la formació necessària en els riscos laborals propis per a la execució de les diferents tasques en la xarxa de Metro.

- Vigilància de l'Obsolescència dels equips i components dels sistemes que conformen la plataforma, comunicant a TMB anticipadament qualsevol amenaça per disponibilitat de components del sistema que pugui esdevenir.

- Vigilància de la ciberseguretat: Acompliment de la política de Seguretat de sistemes tecnològics de TMB i el cos normatiu derivat d'aquestes. Suport i execució de les tasques de ciberseguretat necessàries per vetllar per la seguretat.

- El desenvolupament dels treballs ha de garantir que no sigui intrusiu, per tal de no comprometre la continuïtat del negoci, tractant-se de sistemes crítics.

- Evitar en la realització d'aquestes tasques qualsevol impacte sobre la seguretat i salut de les persones i del medi ambient.

No s'admetran càrrecs que no estiguin inclosos en el preu de la oferta referents a desplaçaments, dietes, ni allotjament, en el cas de requerir tasques presencials.

4. Accés a les instal·lacions

L'Adjudicatari es compromet a disposar del nivell de formació requerit i les homologacions necessàries per accedir a les instal·lacions on s'han de realitzar les corresponents activitats.

5. Criteris mediambientals

L'Adjudicatari haurà de complir amb els següents criteris mediambientals:

Nom criteri	Descripció criteri
Impressió d'informes - documents de treball i/o documents finals	En cas que sigui necessària la impressió de qualsevol document de treball, s'haurà de: -Acordar amb TMB la impressió o no del mateix. I prioritzar:- -Reduir el màxim possible el número de impressions, ajustant-les a les necessitats. -Utilitzar paper 100% reciclat (excepte per plànols no imprimibles en DINA4 o DINA3). - Imprimir els documents a doble cara i en blanc i negre (el color només s'utilitzarà en casos en els que no es pugui interpretar en blanc i negre)
EMBALATGES -no primaris material reciclat	Els embalatges no primaris (*) dels productes estaran fabricats al 100 % a partir de materials reciclats. (*) embalatge addicional al del propi material per a la distribució final del producte)
Etiqueta ambiental dels vehicles	Els vehicles (turismes o furgonetes) que donin el servei en aquest contracte hauran de tenir adjudicada l'etiqueta ambiental tipus C com a mínim.

Vessament i abocament de líquid	S'hauran de prendre les mesures que calgui durant la realització del servei per què en cap cas hi hagi cap tipus d'abocament o vessament de líquid directe al medi ambient. Alhora si el servei implica l'ús i/o manipulació de productes líquids perillosos s'haurà de disposar de mitjans de contenció i absorció davant de possibles vessaments."
RESIDUS Productor de residu	A tots els efectes, el contractista actuarà com a productor del residu generat derivat de l'activitat objecte d'aquest contracte, donant compliment als requeriments legals d'aplicació derivats de la legislació ambiental aplicable, especialment la Llei 7/2022 de residus i sòls contaminats per a una economia circular, el Decret Legislatiu 1/2009 pel qual s'aprova el Text refós de la Llei reguladora dels residus, el Reial Decret 553/2020 pel que es regula el trasllat de residus a l'interior del territori de l'Estat i el Decret 152/2017 sobre la classificació, la codificació i les vies de gestió dels residus a Catalunya, i altres normes concordants.
RESIDUS Codificació, separació i classificació de residus	El contractista haurà de caracteritzar, codificar, separar i classificar els residus que produeixi o posseeixi de conformitat amb les determinacions del Catàleg de residus de Catalunya (CRC).
RESIDUS Emmagatzematge de residus	El contractista haurà de realitzar l'emmagatzematge de residus abans de la seva cessió a transportista autoritzat, en condicions adequades d'higiene i salut, i sempre utilitzant envasos adequats i en zones d'emmagatzematge acords amb la legislació. El període d'emmagatzematge mai podrà superar els 6 mesos per als residus perillosos (a excepció de disposar d'una autorització especial per a superar aquest temps) o en el cas dels residus no perillosos aquest període serà inferior a 2 anys en cas que es destinin a valorització, i un any quan es destinin a eliminació

RESIDUS Etiquetatge de residus	El contractista haurà d'etiquetar els residus abans de la seva cessió a transportista autoritzat de manera clara i visible, llegible i indeleble, seguint la normativa d'aplicació i, en el cas dels residus perillosos, haurà d'identificar la natura dels riscos mitjançant els pictogrames d'aplicació segons les normatives vigents.
RESIDUS Documentació de gestió de residus	El contractista haurà de formalitzar la documentació de control de la gestió de residus (notificacions prèvies, contractes particulars, fitxes d'acceptació, fitxes de destinació, fulls de seguiment).
RESIDUS Transport de residus	El contractista haurà d'utilitzar per al transport dels residus empreses transportistes autoritzades. En cap cas realitzarà cap trasllat del residu amb un transportista no autoritzat. Els residus generats a les instal·lacions de TMB hauran de ser transportats directament a gestor autoritzat mitjançant un transportista autoritzat.
RESIDUS Gestió de residus	El contractista haurà de gestionar el residu mitjançant gestor autoritzat, i sempre mitjançant una via de gestió autoritzada, pels residus que es produeixen o gestionen a Catalunya.
RESIDUS Registre propi de residus	El contractista haurà de portar al dia un registre propi de residus (arxiu cronològic) amb la informació de les retirades de residus efectuades i, on haurà de constar, com a mínim, les dades especificades per la normativa vigent.
RESIDUS Procediments de gestió de residus	El contractista haurà de disposar de procediments i pautes de treball per a la correcta gestió del residu a les seves instal·lacions i el personal que hi treballa n'haurà de ser coneixedor.
RESIDUS Inspecció aleatòria	El contractista haurà d'accedir a que TMB pugui en tot moment inspeccionar i vigilar de manera mostral i aleatòria els seus treballs com a adjudicatari del contracte, així com el compliment de les seves obligacions. Restarà obligat a facilitar tota la col·laboració

	necessària per a la realització d'aquestes tasques d'inspecció (facilitarà documentació, donarà lliure accés a les instal·lacions, etc.).
RESIDUS subcontractacions	En el cas que el contractista subcontracti part de la seva activitat a un tercer que inclogui la generació de residus, és responsabilitat del contractista principal indicar en el contracte qui actuarà com a productor del residu generat (contractista o sub-contractista). En cas de no indicar-hi res, el contractista principal assumirà aquesta funció així com les responsabilitats que se'n deriven.
RESIDUS Contenidors TMB	El residus es gestionaran respectant la normativa d'aplicació i els procediments interns de gestió de residus i sistemes de recollida selectiva establerts per TMB. En cap cas, els residus poden ser abandonats o dipositats en llocs que no siguin habilitats per a tal funció. Els residus sempre es dipositaran en els llocs especialment habilitats per a la seva recollida i posterior gestió. Referència: Procediment 502 de TMB.
Direcció d'obra- Supervisió ambiental per Direcció d'obra	La Direcció d'obra haurà d'incorporar en el seu Pla de Treball la supervisió de les mesures ambientals recollides al Pla d'Ambientalització i assegurar-ne el compliment durant l'execució.
Direcció d'obra- Informe ambiental en modificacions d'obra	En cas de modificacions al projecte, la Direcció d'obra haurà d'emetre un informe ambiental específic sobre l'impacte d'aquestes modificacions abans de la seva aprovació.
Direcció d'obra- Control ambiental de materials	La Direcció d'obra haurà de revisar i validar que els materials emprats compleixin els criteris ambientals establerts (ecoetiquetes, reciclats, fusta certificada...).
Direcció d'obra- Informe final ambiental de	La Direcció d'obra elaborarà un informe final que indiqui el grau de compliment dels criteris ambientals establerts, amb evidències

l’obra	documentals i conclusions.

Annex. Requeriments ciberseguretat addicionals

Es sol·licita que el proveïdor del servei compleixi amb els requeriments de ciberseguretat de FMB.

Es sol·licita que el proveïdor estigui certificat a l'ENS (Esquema Nacional de Seguridad).

Es sol·licita que es compleixin els següents requeriments de ciberseguretat:

1. Compliment normatiu continu: Assegurar que la solució aportada, el sistema en el seu conjunt i les operacions de suport i manteniment continuïn complint amb totes les normatives i estàndards de seguretat rellevants durant tot el cicle de vida del producte. El proveïdor i integrador 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 a regular l'actualització de programari i maquinari, i les actualitzacions de seguretat periòdiques per a 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. Per a la gestió de vulnerabilitats i pegats, l'Adjudicatari haurà de donar visibilitat de les seves SLAs per a publicar els pegats i comprometre's a generar pegats per a les versions lliurades en el projecte.

5. En cas d'ús de programari antivirus, antimalware o EDRs. S'haurà de disposar, per a tot el programari que s'executa en els equips amb antivirus, un inventari explícit dels processos i directoris que hagin de posar-se com a excepcions de l'antivirus.

6. Haurà d'actualitzar i mantenir plans de continuïtat i recuperació davant desastres per a 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: Es podrà requerir la realització d'auditories de seguretat periòdiques per part d'un tercer independent, per

a avaluar el compliment dels requisits de seguretat, identificar possibles deficiències i recomanar millores.

9. Suport i recuperació de dades: Establir procediments per a 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 contínua: Exigir la implementació de sistemes de monitoratge de seguretat continu, que permetin la detecció precoç 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 Firewalls i implementació de regles basades en privilegis mínims. El sistema hauria de funcionar dins de DMZ OT, on ja s'estan aplicant FW que restringeixen els accessos entre xarxes.

12. Gestió d'accessos i privilegis: 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. Es proporcionaran guies de bastionat de tots els equips.

14. Es presentarà un pla per a la gestió de la seguretat de la cadena de subministrament.

o

Francisco Ramiro Martín

Tècnic Unitat Monitorització i Suport tècnic CCM