



Plec de Prescripcions Tècniques

Adquisició Firewall DMZ i Servidor de Logs.

Expedient: 16107966
Juny 2025

Signatura

Nom: Jose Molina López
Tècnic de xarxes

Xarxes i infraestructures de Telecomunicacions
Solucions de Negoci
Àrea de Tecnologia

Índex de continguts

1. Presentació.....	3
2. Àmbit de la contractació.....	4
2.1. Adquisició de l'equipament, llicències i suport del fabricant Checkpoint.	4
2.2. Serveis de desplegament dels nous equips Checkpoint a TMB.	5
2.3. Garantia i manteniment.....	6
2.4. Serveis de manteniment correctiu.....	6
2.5. Actualització de versions de Software.	7
2.6. Help Desk (assistència telefònica, correu electrònic, videoconferència).....	7
2.7. Reporting de incidències i/o actuacions.....	7
3. Criteris ambientals al subministrament d'aparells electrònics.....	8
3.1. Substàncies perilloses.	8
4. Procediment d'instal·lació.....	8
4.1. Instal·lació d'equips.	8
4.2. Planificació de la instal·lació.	9
4.3. Control de qualitat de la instal·lació.	9
4.4. Planificació de les proves amb serveis.	9
5. Documentació a entregar.	9
5.1. Informes de seguiment.	10
6. Clàusula Electronics Watch.	10

1. Presentació.

Actualment la xarxa de la DMZ de TMB disposa de dos equips Checkpoint a Sagrera funcionant en mode actiu-actiu integrats a Checkpoint Maestro i d'un equip Checkpoint a Triangle també integrat a Checkpoint Maestro funcionant en mode passiu com a contingència en cas de que es produeixi una caiguda dels equips de Sagrera. Aquest equip de Triangle és petit en cas de caiguda dels dos de Sagrera i cal substituir-lo per un model amb més capacitat.

Per altra banda la configuració i gestió de l'equipament Checkpoint es fa des de un únic equip virtual que té instal·lat el software Security Management Server (SMS) que realitza les següents funcions: Management Server, Log Server i SmartEvent Server. Actualment s'està generant un volum de logs diari molt gran que s'han d'escriure al disc del servidor SMS. Aquest servidor és un equip virtual desplegat a la infraestructura de Vmware de TMB i durant l'últim any hem tingut diverses incidències repetides pel fet que es produeix lentitud en la escriptura i posterior indexació dels logs. Com a conseqüència d'aquest problema no es poden consultar els logs de forma actualitzada.

Per evitar aquest problema el fabricant Checkpoint recomana la separació de les diferents funcions de l'equip SMS en servidor diferents. A més donat el volum de logs que tenim a TMB la recomanació es que l'equip que fa les funcions de Log Server sigui físic i no virtual.

A més per implementar les funcionalitats de Identity Awareness seguint les recomanacions del fabricant Checkpoint es necessari l'adquisició de llicències per desplegar un gateway virtual a la infraestructura de Vmware.

2. Àmbit de la contractació.

Els objectius d'aquest plec són els següents:

- Adquisició, instal·lació, configuració i posada en servei d'un nou equip Checkpoint 9400 per la substitució del equip Checkpoint 6700 actual de Triangle.
- Trasl·lat a Sagrera, reconfiguració i posta en producció del equip Checkpoint 6700 actual de Triangle per ampliar els equips actuals de Firewalls a Sagrera.
- Adquisició, instal·lació, configuració i posada en servei d'un nou appliance físic de Checkpoint per fer les funcions de Smartevent i Log Server de l'equipament Checkpoint de TMB.
- Adquisició de les llicències per desplegar un Gateway de Checkpoint a la infraestructura de Vmware per implementar el rol de PDP. En aquest cas només cal subministrar les llicències.

A continuació es detallen els diferents elements i serveis objectes d'aquesta contractació.

Els equips que formen aquesta contractació no són per muntar una nova infraestructura sinó per ampliar la infraestructura existent de tallafocs d'Internet i de CPD que tenim instal·lada i en producció a TMB. Per tant, aquests equips s'han d'integrar amb els equips actuals i s'han de gestionar de manera conjunta amb una plataforma única. Tot això implica que han de ser equips del mateix fabricant Checkpoint, ja que en aquests entorns de seguretat no es poden barrejar equips de diferents fabricants.

2.1. Adquisició de l'equipament, llicències i suport del fabricant Checkpoint.

Adquisició dels següents elements del fabricant Checkpoint.

Descripció	Product Number	Observacions	Unitats
9400 Quantum Force SandBlast Appliance for Maestro	CPAP-SG9400-PLUS-MHS-SNBT		1
Next Generation Threat Prevention and Sandblast for additional 2 years for 9400 PLUS Appliance	CPSB-SNBT-9400-PLUS-2Y		1
Collaborative Premium For 3Y	CPCES-CO-PREMIUM-ADD	Covered Product: CPAP-SG9400-PLUS-MHS-SNBT	1
Smart-1 7000-L Base SmartEvent appliance for 75 gateways (perpetual)	CPAP-NGSM7000L-BASE-EVNT		1

Collaborative Premium For 3Y	CPCES-CO-PREMIUM-ADD	Covered Product: CPAP-NGSM7000L-BASE-EVNT	1
1 CloudGuard Network virtual core for VMware ESXi, Hyper-V, KVM Gateway. Annual subscription for 3 years	CPSG-VSEC-VEN-BUN-NGTX-3Y		4
Collaborative Premium For 3Y	CPCES-CO-PREMIUM	Covered Product: CPSG-VSEC-VEN-BUN-NGTX-3Y	1

2.2. Serveis de desplegament dels nous equips Checkpoint a TMB.

Es demana els següents serveis:

- Desplegament, configuració i posta en producció dels nou equip Checkpoint 9400 a la infraestructura de Checkpoint Maestro de TMB al CPD de Triangle.

El nou equip s'haurà de configurar i integrar en el Security Groups actual de la DMZ a on està configurat el Checkpoint 6700. La idea es aprofitar les capacitats que proporciona Checkpoint Maestro per tenir hardware de diferents models en el mateix Security Group. És important destacar que la convivència de hardware diferent en el Security Group només serà durant el procés de substitució i no es pretén que es mantingui en el temps.

- Trasllat a Sagrera, reconfiguració i posta en producció del equip Checkpoint 6700 actual de Triangle a la infraestructura de Checkpoint Maestro de TMB a Sagrera. Aquest equip s'haurà d'integrar al Security Group actual de la DMZ a Sagrera.
- Desplegament, configuració i posta en producció d'un appliance Checkpoint Smart-1 6000-L amb les funcionalitats de Smartevent i Log Server al CPD de Sagrera per a tots els equips Checkpoint de TMB.

Aquests serveis hauran d'incloure com a mínim el següent:

- El disseny i enginyeria global (projecte detall i configuració) del desplegament dels equips segons requeriments funcionals de TMB.
- Instal·lació i configuració dels equips als CPDs de Sagrera i Triangle. Queda fora de l'abast d'aquesta licitació la instal·lació de cablejat nou entre armaris del CPD.

- Integració i configuració dels nous equips a la infraestructura de Checkpoint Maestro actual que es troba en producció.
- És molt important tenir en compte que els tallafocs actuals de TMB estan en producció i que es treballarà amb l'objectiu de minimitzar el possible tall de servei que es pugui produir. Això implicarà que una part dels treballs d'aquest projecte s'hauran de realitzar en horari nocturn segons indicacions de TMB.
- Documentació d'acord amb els requeriments de TMB de la instal·lació realitzada i dels procediments bàsics d'operació.
- Formació als tècnics del departament de Xarxes de TMB.
- Formació als tècnics TLC del departament d'Operacions de TMB.

2.3. Garantia i manteniment.

Garantia de 3 anys de tots els equips amb un temps de resposta de 24x7x4 amb la empresa adjudicatària, a partir de la data de posada en servei de l'equipament. Durant aquests anys, el suport del fabricant haurà d'estar inclòs.

2.4. Serveis de manteniment correctiu.

Serveis de manteniment correctiu durant la duració del contracte amb l'objectiu de restablir el funcionament del servei de qualsevol element inclòs en aquest contracte en cas de fallada. L'empresa adjudicatària haurà de disposar dels recursos necessaris per garantir aquest servei.

El manteniment correctiu serà efectuat en la seva totalitat pel personal de la empresa adjudicatària. La cessió parcial o total del servei sense autorització de TMB podrà suposar la cancel·lació del contracte de manteniment.

L'empresa adjudicatària haurà de disposar d'un servei de manteniment amb capacitat de intervenció a les instal·lacions de TMB amb la modalitat de manteniment 24x7 amb un temps de resposta màxim de 4h.

Per realitzar el manteniment correctiu es podrà realitzar un diagnòstic remot. Per fer-ho TMB habilitarà una connexió VPN per intercanviar informació i tenir accés restringit a l'equipament objecte del contracte. En el cas del manteniment correctiu es pretén que mitjançant l'accés remot es pugui diagnosticar amb més precisió la possible causa de la incidència. En cap cas, aquest servei eximirà de realitzar el manteniment correctiu in situ. Aquest servei només pretén facilitar i agilitzar les tasques de diagnòstic del manteniment correctiu.

L'empresa adjudicatària haurà d'establir amb els fabricants dels equips els contractes de suport adients per assegurar el suport tècnic de l'equipament objecte del manteniment.

2.5. Actualització de versions de Software.

Aquest manteniment ha de permetre a TMB l'actualització, sense cost, de totes les versions de software dels equips inclosos en aquest contracte durant la seva duració.

2.6. Help Desk (assistència telefònica, correu electrònic, videoconferència).

L'empresa adjudicatària disposarà d'un servei de help-desk propi amb modalitat 24x7 accessible telefònicament i amb correu electrònic com a mínim.

Aquest help-desk es podrà fer servir per les següents tasques:

- Notificació d'incidències i avaries.
- Suport a les funcionalitats existents o millores d'aquestes.
- Dubtes de la operativa diària dels equips inclosos a aquest contracte.

La notificació d'una incidència d'un sistema serà notificada generalment a través del departament d'operacions de TMB (OTS, TLCs), aquest proporcionarà un número d'incidència que es el que ha d'utilitzar l'empresa mantenidora per la notificació de les actuacions. Les intervencions realitzades per solucionar els problemes es documentaran d'acord amb el format proposat per l'adjudicatari i acceptat per TMB.

Personal de TMB establirà la severitat del problema i col·laborarà, juntament amb el personal de l'empresa adjudicatària, en la identificació i aïllament del problema i en les seves accions correctives. S'haurà d'incloure una descripció de l'evolució de la incidència així com tot l'intercanvi d'informació (fitxers d'error, logs..) que es produeixin durant la resolució de la mateixa.

L'empresa adjudicatària serà la responsable del registre, manteniment i actualització del diari d'incidències durant el període de manteniment.

TMB podrà consultar en tot moment l'estat de la incidència, pel que l'empresa adjudicatària haurà de proposar un sistema de consulta "on line" de la informació.

2.7. Reporting de incidències i/o actuacions.

L'empresa adjudicatària haurà de portar a terme un seguiment de la qualitat del servei i presentarà a TMB un informe de forma periòdica del seguiment de les incidències i la resta d'actuacions realitzades.

En el cas d'una incidència s'haurà de proporcionar, com a mínim, la següent informació:

- Codi. Identificador proporcionat pel departament d'operació de la incidència.
- Prioritat (greu, principal, secundaria).
- Dia i hora d'apertura.
- Dia i hora de tancament.
- Descripció de la incidència.

- Persona que comunica la incidència per part de TMB.
- Persona que atén la incidència per part de l'empresa adjudicatària.
- Elements substituïts i/o accions realitzades.

Es generarà un informe que haurà d'incloure:

- N° total d'incidències ateses
- N° incidències corresponents a cada sistema
- Temps de resolució empleat per incidència
- Altres activitats realitzades

3. Criteris ambientals al subministrament d'aparells electrònics.

3.1. Substàncies perilloses.

L'aparell no tindrà contingut en substàncies classificades com a carcinògenes, perjudicials pel sistema reproductiu, mutagèniques, tòxiques, al·lèrgèniques, o perilloses pel medi ambient, d'acord amb el Reglament 1272/2008 (CLP) i/o posteriors modificacions.

Les màquines que s'ofertin hauran 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.

4. Procediment d'instal·lació.

4.1. Instal·lació d'equips.

Els equips s'instal·laran en armaris de comunicacions situats en CPDs. No es pot fer cap instal·lació ni entrada de material sense la prèvia autorització de TMB.

TMB indicarà la ubicació exacta dels equips i s'hauran d'enracar i connectar correctament. Els equips hauran d'estar perfectament identificats mitjançant etiquetes.

Els tirantets de fibra i cables de coure també hauran d'estar correctament identificats amb la nomenclatura que definirà TMB.

L'adjudicatari haurà de portar tot material que sigui necessari per la instal·lació: material necessari per enracar els equips, tirantets de fibra entubats, tirantets de coure, espirals de protecció de cables, etc.. L'adjudicatari també haurà de realitzar les modificacions que siguin necessaris en els armaris de comunicacions, com talls de rejibands, redistribució d'equips, retirada de safates, etc...

Tots aquests materials i tasques es concretaran en la fase de replanteig. S'hauran de fer els replantejos necessaris per a que les condicions d'instal·lacions quedin ben definides.

L'adjudicatari haurà de complir tota la normativa d'instal·lació, etiquetatge i documentació definida en l'annex de normativa d'instal·lacions d'aquest plec.

4.2. Planificació de la instal·lació.

Abans de la instal·lació s'haurà de fer una planificació completa indicant l'afectació, la durada de la instal·lació i les proves que es realitzaran. Sense aquesta planificació no es podrà autoritzar cap canvi.

4.3. Control de qualitat de la instal·lació.

TMB revisarà totes les instal·lacions físiques per assegurar-se que la qualitat de la instal·lació és correcta.

4.4. Planificació de les proves amb serveis.

Un cop feta la instal·lació i configuració s'hauran de fer proves de funcionament. Les proves de hauran de ser exhaustives.

Abans de realitzar les proves serà necessari planificar-les i proporcionar un document amb el protocol de proves.

TMB no autoritzarà la realització d'aquestes proves sense aprovar prèviament el protocol.

Les proves i la posada en servei serà efectuada per l'adjudicatari amb la supervisió de TMB i l'adjudicatari haurà de garantir el bon funcionament de la xarxa i resoldre incidències en cas que es produeixin.

5. Documentació a entregar.

A la finalització de la instal·lació de l'equipament de xarxa s'haurà de lliurar la següent documentació:

- Documentació "AS BUILT". Ha d'incloure descripció de la ubicació i configuració de tots els equips així com un mapa global de tota la xarxa. També inclourà la definició dels serveis de la xarxa i l'adreçament IP definit.
- Diagrames de xarxa. Per tal de tenir la xarxa ben documentada serà necessari entregar, a més del mapa global de la xarxa, els següents diagrames:
 - Diagrama Físic: mostra tots els switches, routers, connexió MPLS, etc. (ha d'incloure enllaços, grups, velocitats, ports, slots, tipus de xassís, software, MACAddress, ports bloquejats, enllaços principals, enllaços de backup...).

- Diagrama Lògic: mostra les funcionalitats a nivell 3 (routers, VLANs i segments Ethernet). Adreces IP, subxarxes, capes d'accés, distribució i nucli i tota la informació de routing.
- La documentació es complementarà amb catàlegs de tot l'equipament instal·lat amb les seves característiques tècniques incloent codis i referències.
- Inventari detallat per introduir a la CMDB de TMB tot el material instal·lat amb la següent informació: equipament (nom, model, versió HW), número de sèrie, adreça IP, versió software.
- Procediments bàsics d'operació.

Seràn propietat de TMB tots els documents elaborats para la instal·lació del present contracte.

Tota la documentació estarà escrita en català o en castellà.

5.1. Informes de seguiment.

Per tal de tenir un control exhaustiu de tota la instal·lació que s'està realitzant serà necessari la següent informació:

- Abans de començar la instal·lació serà necessari una planificació detallada de tota la instal·lació.
- Actes de seguiment periòdiques amb tot el que s'ha instal·lat durant aquest període. En aquestes actes s'ha de contemplar evolució de la instal·lació, incidències possibles que hi hagi pogut haver, fotos dels punts crítics d'instal·lació, així com tota aquella informació que el Contractista consideri oportuna. La periodicitat pot variar si TMB ho creu necessari i segons l'avanç del projecte.
- A part d'aquesta documentació seran necessàries reunions periòdiques per fer el seguiment de l'avanç del projecte i analitzar problemes o futures actuacions. Aquestes reunions podran ser quinzenals o mensuals segons cregui TMB. En aquestes reunions s'haurà de lliurar tota documentació de les setmanes anteriors i la planificació al dia de la instal·lació indicant punts crítics per possibles de retards si s'escau.

6. Clàusula Electronics Watch.

El Cap Responsable de Contracte de l'empresa contractada haurà de complir els drets laborals i normes de seguretat en les cadenes de producció de les fàbriques on es produeixen els béns, els productes específics o els components produïts.

Ferrocarril Metropolità de Barcelona, SA en data de 04 de desembre de 2019, es va adherir al projecte Electronics Watch als efectes de garantir el compliment dels drets laborals i les normes de seguretat dels treballadors i les treballadores de les fàbriques on es produeixen els béns, productes específics o components adquirits de tipus electrònic. Amb aquest objectiu, Ferrocarril Metropolità de Barcelona, SA demana al contractista que dugui a terme la diligència deguda

perquè, en les fàbriques esmentades, es compleixi el Codi de Normes Laborals elaborat per Electronics Watch (Annex 14 A PCP)

Obligacions adquirides pel contractista:

Dur a terme la diligència deguda per tal que a les fàbriques de producció dels béns electrònics es compleixi l'establert al Codi de Normes Laborals elaborat per Electronics Watch, de manera que s'aconsegueixin els béns esmentats per mitjà de condicions de comercialització justa.

Lliurar al Responsable del Contracte, en el termini de 25 dies des de la formalització del contracte, el Pla de Compliment del Contractista (Annex 14 –B del PCP) i cada 6 mesos el contractista haurà d'entregar un informe detallat sobre la seva implementació i actualitzacions del Pla. Aquest Pla ha de prendre en consideració quines pràctiques dels seus proveïdors poden contribuir a provocar l'incompliment del Codi Normes Laborals en la producció dels béns electrònics i ha d'informar sobre com el contractista exercirà la seva influència per gestionar aquestes pràctiques.

Lliurar al Responsable del Contracte, en el termini de 25 dies des de la formalització del contracte, el Formulari de divulgació (Annex 14 –C del PCP) i cada 6 mesos el contractista haurà de confirmar si s'han dut a terme informes d'auditoria industrial de qualsevol de les fàbriques on es produeixen els béns electrònics.

Exercir tota la influència possible per aconseguir que l'equip de monitoratge independent d'Electronics Watch pugui accedir a les fàbriques de producció dels béns electrònics per mitjà de visites no anunciades als llocs de treball que incloguin: visites a totes les plantes de treball, residències i hostals pertinents; entrevistes amb eles / les treballadors/es sense la presència de supervisors/es o gerents; i anàlisi de registres importants de la fàbrica (convenis de col·lecció col·lectiva, registres de personal, registres d'hores de feina i sous, etc.). En ocasions, aquestes visites es podran dur a terme després d'haver enviat una notificació a la fàbrica de producció dels béns electrònics tot informant que es realitzarà durant un període específic de quatre setmanes.

Annex A: Taula Amidaments Firewall DMZ i Log Server.

AnnexB: Plec normativa instal·lacions.

En aquest annex s'inclouen els plecs de normatives d'instal·lacions a les cambres de comunicacions de TMB.