



Transports Metropolitans
de Barcelona

**Plec de condicions tècniques
per la contractació d'un servei
de consultoria per l'actualització
i aproximació al Esquema
Nacional de Seguretat del PSO
sobre les Infraestructures
Críiques, que estigui actualitzat
a l'estructura actual d'FMB i
harmonitzat amb els PPEs (ja
lliurats a CNPIC) a la seva
metodologia d'anàlisi de riscos.
*Expedient número 16049800***

Versió 1.0
06/2024

ÍNDIX

1. INTRODUCCIÓ.....	2
2. ABAST DEL SERVEI	4
2.1. DE PRODUCTE	¡ERROR! MARCADOR NO DEFINIDO.
2.2. DE SERVEIS PROFESSIONALS.....	¡ERROR! MARCADOR NO DEFINIDO.
3. OBLIGACIONS DE L'ADJUDICATARI.....	6
3.1 INSTAL·LACIÓ I POSADA EN MARXA DE LA SOLUCIÓ I IMPLEMENTACIÓ	¡ERROR! MARCADOR NO DEFINIDO.
3.2 SUPORT TÈCNIC LICÈNCIES NOZOMI	¡ERROR! MARCADOR NO DEFINIDO.
3.3 FORMACIÓ.....	¡ERROR! MARCADOR NO DEFINIDO.
3.4 SERVEI D'ACOMPANYAMENT O MILLORA DE LA PLATAFORMA:	¡ERROR! MARCADOR NO DEFINIDO.
3.4.1 Suport tècnic L2 8x5.....	¡Error! Marcador no definido.
3.4.2 Servei evolutiu de l'aplicació amb actualització de versions .	¡Error! Marcador no definido.
3.4.3 Bossa d'hores per fine tuning de la plataforma.....	¡Error! Marcador no definido.
3.5 ALTRES OBLIGACIONS DE L'ADJUDICATARI.....	¡ERROR! MARCADOR NO DEFINIDO.
3.6 SEGURETAT I CONFIDENCIALITAT	¡ERROR! MARCADOR NO DEFINIDO.
3.7 COMPLIMENT DE LA LLEI ORGÀNICA DE PROTECCIÓ DE DADES DE CARÀCTER PERSONAL...	¡ERROR! MARCADOR NO DEFINIDO.
4. OBLIGACIONS DE TMB	9
5. COMUNICACIONS ENTRE LES PARTS	9
5.1 SEGUIMENT DEL CONTRACTE	9
6. ANNEXE - SISTEMES OPERACIONALS FMB	¡ERROR! MARCADOR NO DEFINIDO.

1. Introducció

L'objecte del present document és definir les condicions per a la presentació d'oferta per un servei de consultoria i assessorament expert en termes d'aproximació a l'ENS del sistema de gestió de la seguretat relacionada amb la Ciberseguretat i amb la protecció de les Infraestructures Críques al mateix temps que s'actualitza (d'acord a l'obligació legal que té FMB) el PSO de les IICC operades per FMB com a Operador Crític i proveïdor d'un Servei Essencial.

Es conclou necessari contractar els serveis professionals experts per un ens acreditat que permetin realitzar: una actualització del contingut dels PSO, una diagnosi de l'estat de l'art sobre gestió integral de la seguretat dins de la companyia, una harmonització de la metodologia sobre la gestió dels riscos (aplicant el mètode MOSLER i el mètode MAGERIT v3.0, combinats), actualitzar l'estat de les amenaces i vulnerabilitats del sistema i establir un pla d'acció per tal de començar l'aproximació de polítiques, normes i procediments interns als requisits indicats per l'ENS, tot amb la finalitat de construir un sistema robust i acreditat de gestió i d'altra banda blindar i enfortir les actuals defenses d'FMB davant possibles atacs dels ciberdelinqüents i terroristes per tal de garantir la seguretat de les persones i la continuïtat del negoci.

Extracte del Marc regulador d'aplicació:

Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

Artículo 14. Instrumentos de planificación del Sistema.

1. La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes planes de actuación:

- a) El Plan Nacional de Protección de las Infraestructuras Críticas.*
- b) Los Planes Estratégicos Sectoriales.*
- c) Los Planes de Seguridad del Operador.**
- d) Los Planes de Protección Específicos.*
- e) Los Planes de Apoyo Operativo.*

4. Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las

permanentes como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

CAPÍTULO III

Los Planes de Seguridad del Operador

Artículo 22. Finalidad, elaboración y contenido.

- 1. Los Planes de Seguridad del Operador son los documentos estratégicos definidores de las políticas generales de los operadores críticos para garantizar la seguridad del conjunto de instalaciones o sistemas de su propiedad o gestión.*
- 2. En el plazo de seis meses a partir de la notificación de la resolución de su designación, cada operador crítico deberá haber elaborado un Plan de Seguridad del Operador y presentarlo al CNPIC, que lo evaluará y lo informará para su aprobación, si procede, por el Secretario de Estado de Seguridad u órgano en el que éste delegue.*
- 3. Los Planes de Seguridad del Operador deberán establecer una metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador y en la que se recojan los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas tanto físicas como lógicas identificadas sobre cada una de las tipologías de sus activos.*

Artículo 23. Aprobación, registro y clasificación.

- 4. Los Planes de Seguridad del Operador estarán clasificados conforme a lo que establece la legislación vigente en materia de secretos oficiales, debiendo constar expresamente en el instrumento de su aprobación. El CNPIC será responsable de garantizar a los agentes del Sistema autorizados el acceso a toda o parte de la información contenida en dichos planes velando por la confidencialidad y la seguridad de la misma. Por su parte, los operadores críticos responsables de la elaboración de los respectivos planes deberán custodiar los mismos implantando las medidas de seguridad de la información exigibles conforme a la Ley.*

Artículo 24. Revisión y actualización.

- 1. Los Planes de Seguridad del Operador deberán ser **revisados cada dos años por los operadores críticos y aprobados por el CNPIC**. Éste podrá requerir en cualquier momento información concreta sobre el estado de implantación del Plan de Seguridad del Operador.*
- 2. La modificación de alguno de los datos incluidos en los Planes de Seguridad del Operador obligará a la automática actualización de éstos, que se llevará a cabo por los operadores críticos responsables y requerirá la aprobación expresa del CNPIC.*

2. Abast del Servei

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

- *De producte (no aplica)*
- **De serveis professionals**

2.1 De serveis professionals

Es planteja un model de servei en tres fases:

2.1.1 Fase inicial

A la posada en marxa del contracte s'establirà una fase inicial per tal d'establir les accions a dur a terme de cara al desenvolupament de la auditoria / consultoria.

Aquesta fase ha de preveure:

- Kick-off del projecte
- Petició de documentació
- Planificar entrevistes
- Planificar visites instal·lacions

Durant aquesta fase es recollirà la informació necessària pel desenvolupament del servei adjudicat.

Aquesta fase no haurà d'estendre's més enllà de 20 dies des de l'assignació del projecte.

2.1.2 Fase desenvolupament

Metodologia de desenvolupament de l'auditoria:

- Identificar els àmbits (tècnics i operatius) i responsables afectats

- Realització de sessions de treball amb els diferents responsables identificats
- Realització de controls mínims basats en el marc regulador: LPIC i ENS i realització de controls mínims basats en les normatives de seguretat: IEC 62443, ISO 27000 (família), NIST-CSF, UNE 50701, per l'acompliment de la Seguretat i Resiliència en Sistemes de Control Industrial i a les Infraestructures Crítiques.
- Actualització del PSO i del registre de pendents, segons nova orientació
- Elaboració d'informes de resultats de l'auditoria: estat de situació de partida, inventari, vulnerabilitats i avaluació de riscos, gestió documental,...
- Definició d'un pla d'accions prioritzat per convergir al model de l'ENS el sistema de gestió de seguretat de FMB i adequar el mateix al compliment del marc regulador i de les normes

Aquesta fase no haurà d'estendre's més enllà de 4 mesos des de la finalització de la fase anterior.

2.1.3 Fase finalització

Fase de presentació de resultats, que ha d'incloure al menys:

- PSO i registre de pendents actualitzats
- Informe executiu
- Roadmap d'implantació del pla d'acció
- Sessió de tancament del servei
- Presentació de conclusions a Direcció
- Aquesta fase no haurà d'estendre's més enllà de 1 mes des de la finalització de la fase anterior.

3. Obligacions de l'Adjudicatari

És responsabilitat del Adjudicatari, la realització de la totalitat de les tasques aportant els mitjans tècnics i humans necessaris.

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

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.

L'Adjudicatari haurà de disposar de les següents certificacions:

- Acreditació vigent a l'ENS
- Experiència demostrable (mínima de 3 treballs en els últims 5 anys) en auditories i consultories en Infraestructures Críiques i entorns industrials (OT)
- Experiència demostrable (mínima de 3 treballs en els últims 5 anys) en treballs relacionats amb l'aplicació (total o parcial) pràctica de: LPIC, ENS, IEC 62443, ISO 27000 (família), NIST-CSF, UNE 50701...
- Experiència demostrable (mínima de 3 treballs en els últims 5 anys) en treballs relacionats amb l'aplicació (total o parcial) pràctica de criteris i recomanacions sobre Seguretat en Sistemes de Control i Automatització Industrial emanats per: INCIBE i CCN
- Experiència en projectes similars, demostrant haver realitzat, durant els últims cinc anys 5 o més, projectes als àmbits demanats.

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

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.

L'adjudicatari haurà de lliurar els següents en un període màxim de 3 setmanes des de la formalització del contracte:

- Planificació dels treballs: s'ha de presentar una proposta de cronograma amb detall de les tasques que implica aquest servei, en particular de les actuacions a realitzar a les dependències de FMB.
- Metodologia: es presentarà el model d'anàlisi i controls que formaren part de l'assessorament i auditoria demanada.

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.

3.1 Seguretat i Confidencialitat

L'Adjudicatari s'obliga a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment de l'actual servei, i a subministrar-la solament al personal autoritzat per TMB.

L'Adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal sota el seu càrrec. Tan mateix, s'obliga a aplicar les mesures necessàries per garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal que participi en el desenvolupament del servei.

Un cop finalitzat el present servei, l'Adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per TMB, així com qualsevol altre producte obtingut com a resultat del present contracte.

L'Adjudicatari ha de complir amb la Política y Cos Normatiu de Seguretat Tecnològica i de la Informació de TMB.

3.2 Compliment de la Llei Orgànica de Protecció de Dades de Caràcter Personal

L'Adjudicatari es compromet a complir quantes obligacions li són exigibles en matèria de protecció de dades personals tant pel Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques en el que fa referència al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE ("RGPD") com per la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades de Caràcter Personal així com totes les altres normes legals o reglamentàries incideixin, desenvolupin o substitueixin les anteriors en aquest àmbit.

4. Obligacions de TMB

TMB realitzarà les activitats operacionals següents relacionades amb el servei:

- Programació de les peticions de treballs (si s'escau)
- Informació a l'Adjudicatari en cas de necessitats de canvis a la programació
- Les peticions i permisos necessaris per a la realització de les activitats

5. Comunicacions entre les parts

L'Adjudicatari facilitarà els noms, els telèfons i correus electrònics de:

1. Gestor del Contracte: és el responsable de la realització de les tasques del contracte i interlocutor en temes administratius
2. Supervisor Coordinador del Contracte: és el responsable del seguiment i supervisió de les activitats descrites al contracte.

Per la seva banda, TMB facilitarà a l'Adjudicatari una llista d'interlocutors i els seus telèfons de contacte.

5.1 Seguiment del contracte

Es mantindran reunions periòdiques, a acordar, per avaluar el funcionament de la plataforma, realitzar propostes de millora, implementacions de millores i seguiment de les implementacions.