Plec de Prescripcions Tècniques

Contractació del Servei d'Oficina Ciberseguretat de TMB

Expedient: 15013625

Octubre de 2025
Versió 1.0

Solucions Corporatives
Àrea de Tecnologia

Marta Gil Aguayo
Responsable Oficina Ciberseguretat TMB

Índex de continguts

1. Introducció

Transportes Metropolitanos de Barcelona (TMB) és la denominació comuna de les empreses Ferrocarril Metropolita de Barcelona, S. A., Transportes de Barcelona, S. A., que gestionen la xarxa de metro i bus de l'Àrea Metropolitana de Barcelona. També inclou les empreses Projectes i Serveis de Mobilitat, S. A., que gestiona el telefèric de Montjuïc; Transports Metropolitans de Barcelona, S. L., que gestiona productes tarifaris i altres serveis de transport, així com la Fundació TMB, que vetlla pel patrimoni històric de TMB i promou els valors del transport públic a través d' activitats socials i culturals.

La missió de TMB és oferir serveis integrals de mobilitat, incloent-hi metro i autobusos, que:

- Contribueixin a la millora de la mobilitat ciutadana i al desenvolupament sostenible.
- Garanteixin la prestació d'un servei excel·lent a la ciutadania.
- Potenciïn les polítiques d'igualtat d'oportunitats i responsabilitat social.
- Utilitzin de forma eficient els recursos públics

TMB depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) i OT (Sistemes Operacionals) per assolir els seus objectius, exercir les seves competències i prestar els serveis que té atribuïts.

La Ciberseguretat s'ha consolidat com un element essencial per garantir la protecció de la informació i la continuïtat operativa dels serveis en entorns digitals. El seu objectiu es assegurar la confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les dades, així com la resiliència dels sistemes TIC i OT d'avant les amenaces.

En aquest context, la prestació de serveis públics ha de realitzar-se amb plenes garanties de seguretat, tant per als ciutadans com per a les infraestructures tecnològiques que els suporten. Això implica disposar de mecanismes d'identificació, prevenció, protecció i resposta davant incidents que puguin comprometre la seguretat dels sistemes d'informació.

Per tal d'abordar aquests reptes, és imprescindible disposar d'un model de govern de la Ciberseguretat que permeti una gestió eficient, coordinada i alineada amb els objectius estratègics de l'organització. Aquest model ha d'integrar-se en un marc de compliment normatiu que inclogui les directrius establertes per les regulacions nacionals i europees, com ara el Real Decret 311/2022, de 3 de maig, que regula l'Esquema Nacional de Seguretat (ENS), el Reglament General de Protecció de Dades (RGPD), la Directiva NIS2 i altres normatives sectorials aplicables.

Així mateix, la Ciberseguretat ha de ser concebuda com una estratègia dinàmica i proactiva, capaç d'adaptar-se als canvis de l'entorn tecnològic i a les noves formes d'amenaça. Aquesta estratègia ha de contemplar la supervisió contínua de l'activitat, la detecció precoç de vulnerabilitats, la resposta ràpida als incidents i la millora contínua dels mecanismes de protecció.

Aquest model es manté a partir d'una Oficina de Ciberseguretat que gestiona les tasques derivades definició del govern de la seguretat fins a la gestió de riscos i supervisió del compliment de les normatives i controls establerts en el model entre d'altres.

2. Objecte de la licitació

L'objecte de la licitació és la contractació de serveis professionals per a la prestació del servei d'Oficina de Ciberseguretat amb l'objectiu de donar resposta les necessitats de TMB en els següents àmbits:

- Govern, Risc i Compliment (GRC)
- Auditories
- Cultura i capacitació
- Suport I Gestió de la demanda
- Portfoli, programes i projectes
- Gestió d'incidents de Ciberseguretat

3. Abast

L'abast d'aquest contracte consisteix en el govern, suport i capacitació en matèria de Ciberseguretat, amb una visió global i transversal a tot TMB. Això inclou:

- Tenir una visió i gestió global del processos de negoci
- Tenir una visió i gestió global del risc en Ciberseguretat associats als processos de negoci
- Identificar els responsables d'informació, responsables de Seguretat dels diferents negocis e sistemes (TIC/OT), promoure revisions de compliment
- Promoure auditories de Seguretat
- Tenir un marc de compliment de la Ciberseguretat transversal
- Assessorar a TMB en matèria de Ciberseguretat
- Tenir coneixement de la gestió de riscos per a entorns TIC i OT
- Tenir coneixements ens la gestió de projectes i requeriments de Seguretat en els mateixos.

4. Descripció del servei

4.1. Govern Risc i Compliment

El grau de complexitat i nombre d'aspectes a tenir en compte par tal de definir i garantir un nivell de seguretat acceptable per l'organització, fa necessaris l'establir un model i una estructura transversal a totes les empreses que formen part de TMB en l'àmbit de la Ciberseguretat amb capacitat per controlar i donar visió conjunta del nivell de seguretat actual i ajudar a prendre totes les decisions que així ho requereixin.

Per tal de portar-ho a terme s'han de dotar de certes accions com un marc de referència normatiu coherent amb els diferents negocis que maqui normes, criteris, polítiques per assegurar i controlar el nivell de seguretat de la informació.

Dins d'aquest bloc de Govern risc i compliment l'adjudicatari prestarà els següents serveis

4.1.1. Govern

Aquest servei compren les següent tasques.

- **Definició i creació d'indicadors e informes**: La definició i creació d'indicadors és clau per poder monitoritzar l'estat de la Ciberseguretat. L'adjudicatari definirà de manera conjunta amb l'àrea de Ciberseguretat els indicadors clau de rendiment (KPI). S'espera que el licitador aporti idees d'indicadors. També es definiran els diferents informes a presentar, contingut i periodicitat. Aquest KPIs e informes estaran presents en cadascuna de les activitats que es sol·liciten durant la licitació. Aquests informes i KPIs permetran a la direcció i altres col·lectius disposar d'una visió clara i actualitzada sobre l'estat de Ciberseguretat, nivell de compliment, riscos, evolució etc.

  .
- **Creació del quadre de comandament de Ciberseguretat**: Es desenvoluparà un quadre de comandament integral que consolidi els indicadors definits, facilitant la presa de decisions estratègiques i operatives. Aquest quadre haurà de ser accessible, dinàmic i capaç d'integrar dades procedents de diferents sistemes i eines corporatives

  .
- **Revisió i definició del model de relació de govern de la Ciberseguretat:** Es revisarà el model actual de governança i es definiran les relacions entre els diferents actors implicats (unitats de negoci, departaments tècnics, òrgans de direcció), establint rols, responsabilitats i fluxos de comunicació clars.

- **Redacció dels diferent models de relació:** Es redactaran els documents que formalitzin els models de relació i governança, incloent protocols de coordinació, comitès, i mecanismes de supervisió i control.

- **Revisió periòdica i actualització dels procediments i tasques del govern de la Ciberseguretat:** Es garantirà la revisió i actualització periòdica dels procediments associats al govern de la Ciberseguretat, assegurant la seva adequació a l'evolució normativa, tecnològica i organitzativa.

4.1.2. Risc

Aquest servei respon a l'objectiu de governar el risc de Ciberseguretat corporatiu (tant IT com OT) per donar una visió complerta de la gestió de riscos. Els riscos de Ciberseguretat tot i que es gestionaran i controlaran des de l'Oficina de Ciberseguretat s'integraran amb l'àrea de riscos globals de TMB.

Aquesta gestió s'allunya de la visió de risc únicament com controls no complerts. Aquesta gestió ha de tindre una relació estreta amb la resta d'àrees operatives i de projecte de TMB per tal de poder valorar millor i amb més amplitud aquest riscos.

Aquest servei inclou les següents activitats:

- **Definició del catàleg d'amenaces IT/OT:** Elaboració d'un catàleg complert d'amenaces que afectin a entorns IT i OT tenint en compte les particularitats del sistemes corporatius e industrials. Aquests catàleg haurà d'estar contrastat i validat amb les diferents departaments de Seguretat i tècnic de les diferents unitats de negoci (Bus, Metro i aTec)

- **Definició de metodologies:** Establiment de metodologies per l'anàlisi i gestió de riscos basades en estàndards reconeguts i adaptades a les necessitats de l'organització. Tant per IT com a OT. L'adjudicatari proposarà una o dos metodologies i serà TMB qui aprovarà la metodologia a aplicar. La metodologia ha de permetre gestionar els riscos dins el marc de requeriments de l'ENS.

- **Execució d'anàlisis de riscos:** Es realitzaran avaluacions periòdiques de riscos sobre sistemes, processos i actius (mínim crítics) identificant vulnerabilitat, impactes, probabilitats i assignant responsables de la seva mitigació. A més es donarà suport a les diferents àrees e unitats corporatives quan no s'hagi pogut realitzar un anàlisis de riscos executant la tasca específica.

- **Seguiment de riscos:** Implantació d'un procés continu de monitorització i seguiment dels riscos identificats, incloent la seva evolució i estat de mitigació.

- **Reporting:** Generació d'informes periòdics que reflecteixin la situació dels riscos, les accions de mitigació i les tendències, per facilitar la presa de decisions estratègiques així com la definició e implantació de indicadors de l'estat del risc que haurà d'estar tant en la eina de GRC com en el QdC Global de Ciberseguretat

- **Identificació i centralització de riscos de Ciberseguretat (nous o existents)**: Consolidació en un repositori únic dels riscos detectats, tant nous com existents, assegurant la seva traçabilitat i gestió coordinada. Els inputs interns per poder identificar els riscos són: auditories, projectes, seguiment de proveïdors, àrea de qualitat I

compliment, àrees de Bon Govern, incidents de Seguretat, indicadors del QdC, excepcions, etc.

4.1.3. Compliment

Aquest servei inclou les següents tasques necessàries per assegurar el compliment de la normativa aplicable i la correcta gestió dels requisits legals i reguladors en matèria de Ciberseguretat en cadascun dels negocis i diferents entitats que conformen TMB.

- **Realització del mapa de traçabilitat Normativa:** Elaboració d'una mapa que identifiqui totes les normatives aplicables a TMB amb els processos, sistemes i controls existents garantint la traçabilitat i el seguiment del compliment. S'ha de tindre en compte tota la normativa aplicable TMB de manera genèrica però també s'ha de tindre en compte les Normatives específiques de cada negoci segons els sector que apliqui (p.exe: Bus, Metro) tant per la part IT com la part OT. Es partirà de ENS, NIS2 com a empresa de sector públic però s'ha de tindre en compte

  Aquest mapa de traçabilitat també ha de tindre un creuament de controls de cadascuna de les normes per tal d'identificar requisits comuns a les normes i simplificar el control i la gestió de les evidències de cadascun.

- **Servei continu de revisió de la Normativa aplicable**: L'adjudicatari haurà de vetllar per la monitorització i actualització periòdica de la normativa vigent, incloent canvis legislatius, reguladors i estàndards sectorials, noves normes, lleis derogades, actualitzades, etc. Per tal d'assegurar l'adaptació constant de l'organització.

  Quan es detecti qualsevol modificació l'adjudicatari serà l'encarregat d'actualitzar el mapa de traçabilitat normativa amb l'anàlisi i els canvis aplicables.

- **Declaració d'aplicabilitat:** Redacció i manteniment de la declaració d'aplicabilitat que defineixi els controls implementats i justificació dels no aplicables, d'acord amb les normatives i marcs de referència.

- **Anàlisis d'impacte:** Realització d'anàlisis d'impacte derivat dels canvis normatius, tecnològics o organitzatius, per determinar les implicacions en processos i controls

- **Disseny pla de compliment ENS:** Definició del pla estratègic per a compliment de l'Esquema Nacional de Seguretat (ENS), analitzant el model actual i definint el model cap el nivell adient segons la naturalesa de l'organització, incloent objectius, accions, terminis, responsables, estimacions, kpis, etc.

- **Execució del pla de compliment**: Implementació de les mesures definides en el pla, coordinant les accions amb les àrees implicades i assegurant el seguiment i control de l'execució.

- **Definició del model de relació i col·laboració per mesures derivades del pla de compliment:** Establir els rols, responsabilitats i canals de comunicació entre les diferents àrees per la correcta implementació de les mesures. Tot aquest model quedarà reflectit en un document

- **Suport i col·laboració amb el Delegat de protecció de dades (DPD):** L'adjudicatari col·laborarà amb el DPD donant suport tècnic als requeriments imposats per RGPD i la LOPDGDD i altres nomes aplicables.

- **Suport a diferents àrees de negoci i departaments:** Assessorament sobre procediments, protocols i accions derivades de la normativa aplicable, adaptant-los a les necessitats específiques de cada unitat. Suport en la redacció dels procediments, protocols i accions derivades així com supervisió de que s'inclouen tots els aspectes requerits a nivell de compliment.

- **Gestió d'excepcions:** Des de l'oficina de Ciberseguretat es tindrà control, seguiment i aprovació sobre les excepcions de Ciberseguretat aplicades i noves que van en contra d'una Norma. Es definirà i s'implementarà un procediment per tal d'identificar, documentar i aprovar les excepcions al compliment normatiu amb un anàlisis de riscos associats. En aquest procediment podran estar involucrats altres persones d'altres departaments o unitats de negoci. Es responsabilitat de l'Oficina de Ciberseguretat (i per tant del licitador) definir el mecanisme de sol·licituds (tenint en compte les eines de TMB actuals) i tant la sol·licitud com el seguiment de les mesures compensatòries per la temporalitat de les excepcions aprovades. El procediment també haurà d'incloure el seguiment de l'excepció, notificacions al peticionari avisant de la caducitat de la mateixa i les accions derivades

una vegada s'hagi caducat i no renovat o no aprovat la renovació a més de les dependències i comunicacions amb altres serveis (per exemple: gestió de riscos) Aquesta tasca no preveu la compra d'una nova eina.

- **Identificació i classificació d'actius globals**: Des de l'Oficina de Ciberseguretat es treballarà amb altres departaments i/o àrees de negoci per tal de tindre un inventari global e unificat d'actius (tant IT com OT) amb la seva classificació pel compliment normatiu, assegurant la seva protecció i gestió adequada.

- **Suport i consultoria:** A partir de qualsevol tasca derivada de compliment, donar suport i consultoria especialitzada per atendre necessitats puntuals relacionades amb les tasques de l'Oficina de Ciberseguretat

- **Millora continua de metodologia, cos normatiu:** Revisió i evolució constant de la metodologia de compliment, actualitzacions e integracions. S'espera per part del adjudicatari pro activitat en la evolució del servei aportant idees, millores, automatitzacions, etc de les tasques que es desenvoluparan en tota l'Oficina de Ciberseguretat

4.1.4. Eina de Govern risc i compliment

Actualment TMB no disposa de cap eina de GRC. L'adjudicatari serà l'encarregat de proporcionar una per tal de portar el servei. Serà l'encarregat de tot el cicle de vida de la mateixa (disseny, implantació, explotació i manteniment de la mateixa). Una vegada implantada serà l'eina principal del servei per fer seguiment i control.

L'adjudicatari haurà de dur terme el manteniment de la mateixa per tant haurà de:

- Establir mecanismes necessaris per automatitzar la interoperabilitat d'aquesta eina amb altres sistemes corporatius dels quals s'alimenta i amb aquells als quals servirà de font d'actualització de la informació
- Avaluació constant de l'estat de l'eina
- Proposar evolucions i millores
- Vetllar per l'estat de vulnerabilitats de la mateixa i actualitzacions
- La gestió dels usuaris haurà d'integrar-se amb l'eina de gestió d'accessos e identitat de TMB.

L'adjudicatari documentarà tota la metodologia, implantació, procediments, guies i altres documents necessaris relacionats amb la posada en marxa de l'eina, la configuració, interconnexió de l'eina amb altres sistemes d'informació amb els quals s'hagi d'intercanviar informació.

4.2. Auditories

Aquest servei té com a objectiu verificar el nivell de compliment, eficàcia i adequació dels controls de Ciberseguretat implantats, així com identificar oportunitats de millora per reforçar la postura de Ciberseguretat de l'organització. Aquestes activitats ajudaran a l'Organització a prioritzar les resolucions dels incompliments que es detectin. Tot i que aquest servei es realitzarà des de l'Oficina de Ciberseguretat haurà d'estar alineat i coordinat amb l'àrea de Qualitat de TMB. Les activitats incloses són:

- **Disseny d'un pla anual d'auditories:** Elaboració d'un pla estratègic que defineixi el calendari, abast i objectius de les auditories a realitzar durant l'any, prioritzant àrees crítiques i sistemes crítics

- **Execució del pla d'auditories:** Realització de les auditories programades segons el pla anual, aplicant metodologies reconegudes i assegurant la cobertura dels requisits normatius i de seguretat.

- **Auditories puntuals:** Execució d'auditories específiques resposta a incidents, canvis significatius, requeriments interns o necessitat detectada. El tipus d'auditoria pot ser tant de compliment Normatiu, com de vulnerabilitats, etc.)

- **Auditories parcials:** Revisió focalitzada en processos, sistemes o controls determinats, per validar la seva correcta implementació i eficàcia.

- **Suport a auditories externes cap a TMB:** Coordinació i assistència en auditories realitzades per tercers, facilitant la informació necessària i assegurant la correcta gestió de les evidències.

- **Seguiment i control sobre les millores identificades en les revisions** Centralització i seguiment de les accions correctives derivades de les auditories, assegurant la seva implantació i verificació en els terminis establerts.

Totes les activitats seran mesurades i algunes generaran informes a pactar amb l'adjudicatari, tal i com indica el punt 4.1.1 de la licitació.

4.3. Cultura i capacitació

Les persones són la primera línia de defensa davant les amenaces digitals, més enllà de la tecnologia i són el principal vector d'atac.

En una organització tan gran i amb perfils operatius tan diferents és essencial establir una cultura de Ciberseguretat sòlida i transversal.

La capacitació i la conscienciació permet reduir aquest risc, assegurant que cada persona entengui el seu paper en la protecció dels actius corporatius i disposi de les competències necessàries per actuar de manera segura.

Aquest servei inclou les següents tasques:

- **Anàlisis dels perfils actuals de la companyia:** Identificació i classificació dels perfils professionals existents, tenint el compte el paper que desenvolupen a la companyia, la seva interacció amb sistemes IT i OT responsabilitats, coneixement, etc. per tal de tindre diferents perfils als quals poder desenvolupar contingut a mida de les seves necessitats.

- **Definició d'un pla de formació:** Disseny d'un pla formatiu específic per a cada perfil detectat, assegurant que les competències adquirides responguin a les necessitats operatives i estratègiques de l'organització

- **Disseny d'un pla de conscienciació transversal:** Creació d'un programa global de conscienciació orientat a tota l'organització, amb campanyes, materials divulgatius, accions periòdiques per reforçar la cultura de la seguretat. Aquest pla ha de ser original i dinàmic.

- **Ciber exercicis:** Planificació i execució de Cibersimulacres (exemple: exercici de resposta a incidents, proves de phising, crisis simulades, etc) per tal d'avaluar la

preparació i capacitat de la reacció dels equips. Per a cada ciber exercici es farà una avaluació i es mesurarà si la resposta ha estat adient, si s'han detectats gaps als procediments, etc. (el contingut de l'informe es definirà amb l'adjudicatari durant la prestació del servei)

Totes les activitats seran mesurades i algunes generaran informes a pactar amb l'adjudicatari, tal i com indica el punt 4.1.1 de la licitació.

4.4. Suport i gestió de la demanda

En una organització com TMB la gestió eficient de la demanda i el control dels proveïdors són elements importants per garantir la seguretat i compliment normatiu. Directives com NIS2 i l'Esquema Nacional de Seguretat (ENS) que són d'aplicació a TMB estableixen obligacions específiques per a entitats del sector públic, incloent la necessitat de supervisar els proveïdors i tercers que accedeixen a sistemes o dades de TMB. Aquest control és essencial per reduir riscos derivats de la cadena de subministrament i assegurar que les mesures de Ciberseguretat s'apliquen de manera homogènia.

El servei de Suport i Gestió de la demanda té com objectiu centralitzar, prioritzar i donar resposta a les necessitats relacionades amb la Ciberseguretat. Les activitats incloses són:

- **Ciberseguretat a les licitacions:** Aquesta activitat inclou l'anàlisi de les mesures actuals que s'inclouen tant de caire tècnic com requisits de compliment als proveïdors referent a ENS. L'adjudicatari farà aquest anàlisis actual i proposarà millores sobre aquesta documentació. L'adjudicatari participarà en cadascuna de les licitacions actuals prescrivint els requeriments necessaris en base a l'objecte licitat i validant en fases posteriors a la definició de requeriments que la documentació aportada per guanyador de la licitació és la correcta. A més interactuarà amb altres àrees internes per tal de d'automatitzar aquest procés.

- **Seguretat en els proveïdors:** Verificació i seguiment del compliment de requisits de seguretat per part dels proveïdors durant tot el cicle de vida de la contractació. Aquesta activitat por incloure tant auditories al proveïdor com validacions que els certificats de compliment segueixen vigents.

- **Atenció a la bústia de correu genèrica:** Existeix una compte de correu genèrica de Ciberseguretat. L'adjudicatari farà la gestió i resposta de les consultes, comunicacions,

peticions sol·licitades a través de la bústia. Aquesta bústia no és l'entrada d'incidents de Ciberseguretat o peticions de seguretat dels usuaris, ja que hi ha altres mecanismes i òrgans per aquestes gestions més tècniques.

- **Registre i classificació de noves peticions:** Registre de les noves sol·licituds, peticions, consultes amb la seva classificació per tipologia, priorització, i altres camps.

- **Resolució de consultes:** Atenció i resolució dels diferents dubtes plantejats per les diferents àrees de l'organització.

- **Suport a l'evolució de la gestió de la demanda i peticions de suport:** S'espera que l'adjudicatari realitzi millora contínua sobre els processos actuals de la gestió de la demanada, adaptant-los a noves necessitats i requisits normatius. A més de participar de qualsevol evolutiu i automatització de les mateixes.

4.5. Portfoli, programes i projectes

La gestió de programes i projectes és un pilar fonamental per garantir que les iniciatives de Ciberseguretat s'executin de manera ordenada, eficient i alineada amb els objectius estratègics de l'organització. En una organització com TMB amb alta complexitat operativa, és essencial disposar d'un marc que asseguri la integració de la seguretat en totes les fases del cicle de vida dels projectes, des del disseny fins al tancament. Aquest servei permet coordinar esforços, prioritzar accions i assegurar que els projectes compleixin amb els requisits normatius i les millors pràctiques.

Les activitats incloses són:

- **Tindre un programa de projectes de Seguretat:** Crear i actualitzar un programa global que agrupi tots els projectes de Seguretat en curs i planificats.

- **Suport a l'edició del procediment de gestió de projectes:** Assistència en la definició i millora dels procediments corporatius per la gestió de projectes, incorporant requisits de Seguretat.

- **Realització de formularis o checklist de control en les diferents fases:** Creació d'eines de control tant a l'inici del projecte com una part de seguiment i al tancament del

mateix per tal verificar que els requisits de Seguretat queden ben definits com validats la seva execució i abans d'entrar en servei.

- **Suport a la realització dels procediments interns de l'Oficina de Ciberseguretat dins els cicle de vida dels projectes:** Revisió de la documentació actual i redacció dels procediments i protocols interns de l'Oficina de Ciberseguretat per l'execució d'aquestes tasques

- **Registre de nous projectes:** Alta i classificació de projectes, assegurant la traçabilitat i el seguiment

- **Participació en els diferents programes i projectes:** Presència a en els diferents projectes i programes en comitès, reunions, grups de treball per tal de garantir la incorporació de la seguretat en el cicle de vida dels projectes.

- **Seguiment de cada projecte:** Monitorització periòdica de l'estat, riscos i desviacions dels projectes

- **Gestió de projectes PM:** Participació activa com a responsable de projecte (PM) en aquelles iniciatives de Ciberseguretat que, per la seva **estratègia, complexitat, criticitat o impacte directe en l'organització**, requereixin una gestió dedicada i coordinada. L'Oficina de Ciberseguretat assumirà la direcció operativa del projecte, incloent la **planificació, seguiment, coordinació d'equips, gestió de riscos i reporting**, assegurant l'alineació amb els objectius estratègics de TMB i la correcta integració de la seguretat en totes les fases del cicle de vida del projecte

- **Definició i redacció del model de relació amb riscos i excepcions:** Establir els protocols de comunicació i gestió entre els diferents projectes, i la gestió de riscos de Ciberseguretat i excepcions de Ciberseguretat per garantir el correcte avís i registre de detecció arrel de l'execució d'un projecte

- **Suport en la definició del Pla Director de Seguretat (PDS):** Suport en l'elaboració del PDS, alineat amb els objectius estratègics de seguretat.

- **Seguretat en el disseny (arquitecte):** Incorporació de criteris de Ciberseguretat en la fase de disseny e implantació actuant com a consultor. Proposant solucions adients, valorant solucions plantejades, etc. Aquesta figura tindrà relació amb altres arquitectes de la companyia. S'espera que aquest arquitecte faci revisions fora de projectes i detecti arquitectures millorables, arquitectures que van en contra de la normativa i es plantegin solucions i suport a la implantació

4.6. Gestió incidents de seguretat

La gestió dels incidents de seguretat es gestionen des del SOC (que no depèn funcionalment de l'Oficina de Ciberseguretat).

La normativa aplicable tant nacional com europea, obliga a notificar incidents de seguretat relatius a la Ciberseguretat. Des del servei es realitzaran les següents tasques:

- **Revisió protocols i procediments**: Es revisarà el model actual de notificació i de coordinació amb el SOC per tal de validar e implementar els mecanismes i processos per tal de realitzar les notificacions d'incidents de Seguretat
- **Suport a l'orquestració dels incidents de Seguretat greus**: Coordinació interna i externa en casos de Ciber incidents de seguretat que queden fora de l'abast del SOC
- **Training ciber incidents**: Sessions sobre ciber incidents, per tal d'explicar a les persones involucrades els seu rol i responsabilitat I accions davant un incident de seguretat

A més es realitzaran revisions periòdiques e informes sobre els incidents. El detall dels informes i els KPIs es definiran amb l'adjudicatari a l'inici del contracte.

5. Model de prestació del servei

El model de prestació descriu com s'organitzarà i s'executarà el servei de l'Oficina de Ciberseguretat. Es defineixen els mecanismes operatius, la disponibilitat, els perfils professionals implicats i la coordinació amb l'equip intern de TMB, amb l'objectiu de garantir una prestació eficient, segura i alineada amb les necessitats de l'organització

5.1. Tipologia de servei

El servei objecte d'aquesta licitació es prestarà de manera **continuada**, amb l'objectiu de donar suport especialitzat en matèria de Ciberseguretat a l'organització. L'oficina externa actuarà com a extensió de l'equip intern de TMB, contribuint a la gestió proactiva de totes les tasques descrites en la descripció del servei

5.2. Modalitat de prestació

La prestació del servei es durà a terme en **modalitat híbrida**, combinant la presència física i el treball remot segons les necessitats operatives.

Es preveu la figura d'un/a **responsable del servei**, que estarà presencialment a les instal·lacions de TMB **tres dies per setmana**, i la resta en modalitat remota. Aquesta figura actuarà com a interlocutor/a principal amb l'organització i facilitarà la coordinació entre l'equip extern i intern. Per defecte el responsable del servei estarà ubicat a l'oficina Corporativa de Zona Franca

L'equip tècnic treballarà principalment en remot.

Tant el responsable del servei com l'equip tècnic haurien de tindre **la possibilitat de desplaçar-se a altres instal·lacions de TMB** per a la realització de tasques específiques que requereixin presència física. Aquests desplaçaments seran **planificats prèviament** i no generaran **cap cost addicional** per a TMB.

L'adreça de l'oficina Corporativa és:

TMB Oficines Corporatives – Edifici Zona Franca II
Direcció: Carrer 60, 21-23 Sector A 08040 Barcelona

5.3. Disponibilitat del servei

L'adjudicatari haurà de cobrir el servei de dilluns a divendres de 08:00 AM a 16:00 PM, inclòs el període vacacional on es mantindrà operatiu el servei. Si es tindran en compte el calendari de festes de Catalunya i municipi.

Sense perjudici de l'horari ordinari del servei, en cas d'incident greu de ciberseguretat, emergència operativa o situació excepcional que pugui afectar la continuïtat del servei, la seguretat de la informació o els sistemes corporatius, l'adjudicatari haurà d'estar disponible per prestar suport fora de l'horari establert, de manera puntual i extraordinària, a requeriment de TMB

5.4. Equip de treball

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis.

Cal que els licitadors detallin en les seves propostes quina és l'organització que proposen per al servei, tenint en compte que hauran de dotar el personal necessari per assegurar les funcions que són objecte d'aquest contacte descrites a l'apartat 4 de la licitació.

L'empresa adjudicatària haurà de proposar un **equip de treball adequat** per a la prestació del servei, **assegurant-ne la continuïtat i estabilitat** durant tota la vigència del contracte. En la seva proposta, haurà de detallar els **recursos assignats**, incloent-hi els **perfils professionals**, les **funcions associades** i les **certificacions tècniques corresponents**. No obstant això, TMB estableix com a mínims obligatoris els perfils que es descriuen a continuació, considerant-los **imprescindibles** per al correcte desenvolupament del servei.

A continuació es detallen els diferents rols necessaris per tal de portar a terme les funcions descrites anteriorment. El llistat de responsabilitats és una aproximació de mínims però no estan especificades totes les tasques prèviament descrites. S'espera que en les ofertes presentades es plantegin una proposta amb el detall dels perfils i tasques que s'han d'escometre dins de l'Oficina de Ciberseguretat on inclogui totes les tasques a realitzar repartides en els diferents perfils. Les tasques aquí mencionades són les que principalment seran objecte de revisió en el seguiment del contracte.

S'espera un equip dedicat per a cada perfil. TMB controlarà que així sigui i qualsevol canvi passarà pels requeriments de notificació detallats més abaix:

PERFIL	DESCRPIPCIÓ
Responsable del servei	**RESPONSABILITAT MINIMES**
	Interlocutor únic davant de TMB. Responsable de garantir que la prestació del servei és correcte. Coordinador global que ha de realitzar principalment les següents funcions: • Garantir l'execució del servei tal i com s'especifica en el plec • Coordinar i supervisar l'equip al seu càrrec i comunicar a TMB possibles canvis amb els motius, garantint els requeriments esmentats sobre el canvi de personal • Gestió de la planificació de les tasques • Gestió dels riscos detectats durant el servei així com el pla de mitigació dels mateixos

	• Seguiment de la qualitat del servei • Detectar oportunitats de millora • Elaboració del informes de servei i justificació de compliment de ANS • Garantir la implementació del Quadre de Comandament del servei • Proposar e implementar millores en la gestió del servei (prèviament acceptades per TMB) • Participació en els comitès del servei • Elaboració d'informes i kpis
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els 5 darrers anys gestió de serveis de Ciberseguretat Acreditar 3 anys d'experiència en gestió d'oficines de Ciberseguretat (dels últims 5 anys) Acreditar experiència en entorns públics o grans organitzacions que combinin sector IT i OT Acreditar coneixement i experiència en governança de la Ciberseguretat Acreditar coneixement i experiència en normatives (ENS, ISO 27001) Acreditar coneixements en gestió de projectes
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	Dedicació complerta amb presencialitat en oficines de TMB 3 dies per setmana – 1 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Consultor GRC	**RESPONSABILITAT MINIMES**
	Especialista en estàndard i normatives de seguretat, elaboració de cossos normatius de seguretat , gestió de riscos de seguretat de la informació i eines GRC així com compliment tècnic de la legalitat • Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment del marc normatiu corporatiu • Suport, anàlisis, elaboració d'informes i assessorament del compliment tècnic de lleis aplicables a TMB

	• Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment de gestió de riscos (metodologies, anàlisis i seguiment) • Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment de gestió d'excepcions (metodologies, anàlisis i seguiment) • Control i seguiment, suport, assessorament dels nivells de compliment de proveïdors de TMB • Elaboració quadres de comandament • Elaboració d'informes i kpis
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els darrers 5 anys , 3 anys d'experiència en serveis de consultoria de GRC Acreditar participació (preferentment lideratge) en més d'un projecte de l'àmbit d'elaboració de normatives i mapes de traçabilitat normativa Acreditar participació en elaboració d'anàlisis de riscos en els sectors IT i OT Acreditar coneixement en normatives de sector IT i OT Acreditar coneixement en metodologies de gestió de riscos Acreditar el coneixement de l'ús i explotació d'eines de GRC, ja sigui en projectes on ha implantat l'eina en un client o com a servei fent ús de les mateixes.
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	Dedicació 2 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Auditor	**RESPONSABILITAT MINIMES**
	Especialistes en realitzar auditories de diferents àmbits. • Compliment: Protecció de dades, Esquema Nacional de Ciberseguretat (ENS), sistemes de gestió de seguretat de la informació (SGSI), NIS2, auditories sector OT

	• Tècniques: Pentent, anàlisis de vulnerabilitats, anàlisis d'aplicacions, anàlisis d'aplicacions mòbils, anàlisis de codi (estàtic i dinàmic) Principals tasques a realitzar: • Definició i aprovació del Pla Anual d'auditories • Execució d'auditories internes de compliment • Execució d'auditories tècniques • Donar suport en l'execució d'auditories externes de compliment • Suport a les diferents àrees de negoci, departaments sobre les millores sorgides • Gestió del seguiment de les correccions • Elaboració d'informes i kpis • Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment d'auditories de ENS • Auditories i control de proveïdors
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els 5 darrers anys, 3 anys d'experiència en auditories de compliment (ISO27001, ENS) Acreditar durant els 3 darrers anys la participació en més d'un projecte d'auditories tècniques Acreditar durant els 3 darrers anys la participació en més d'un projecte d'anàlisis de riscos IT i OT
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	1.5 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Gestor de projectes programes i portfoli	**RESPONSABILITAT MINIMES**
	Especialista en la gestió de projectes realitzant com a mínim les següents tasques: • Creació i coordinació de portfolis, programes i projectes de Ciberseguretat

	• Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment de procediment de gestió de projectes i altres metodologies i models de relació • Suport, desenvolupament, elaboració, control, manteniment, modificació d'eines de control de projectes • Gestió de projectes (PM) d'alguns projectes estratègics • Suport en la definició del Pla Director de Seguretat (PDS) • Elaboració d'informes i kpis
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els 5 darrers anys, 3 anys d'experiència en gestió de projectes de seguretat Experiència en gestió de projectes complexes Experiència en gestió de projectes en entorns mixtos (IT i OT) Acreditar coneixement en metodologies de gestió de projectes, programes i portfoli Experiència en participació la definició de Pla Director de Seguretat en els darrers 3 anys
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	1,5 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Tècnic sènior especialista en seguretat	**RESPONSABILITAT MINIMES**
	Suport tècnic en la seguretat i gestió de la demanda • Revisió de requeriments tècnics de validació de mesures de Seguretat • Suport a les licitacions i validacions proveïdors • Persona d'enllaç amb diferents àrees de la companyia i diferents àrees de negoci de caire tècnic • Suport en la gestió d'incidents de seguretat
	CONEIXEMENTS I EXPERIÈNCIA
	Experiència en gestió d'incidents en infraestructures crítiques Experiència en coordinació IT/OT Acreditar coneixement ISA/IEC 62443 Habilitat per actuar com a enllaç entre les àrees tècniques i de negoci, facilitant la traducció bidireccional de requisits i solucions, especialment en entorns híbrids IT/OT i en organitzacions del sector públic.
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	0,5 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Arquitecte de seguretat	**RESPONSABILITAT MINIMES**
	Especialista en la integració de la seguretat en el dissenys dels projectes. Principals tasques: • Participació en els projectes per tal de analitzar, donar suport, dissenyar, solucions segures alineades amb la normatives vigents i bones pràctiques • Anàlisis de les arquitectures actuals per tal de detectar millores. Dissenyant propostes de solució més segura • Suport i coordinació amb l'àrea d'arquitectura de sistemes oberts e industrials per tal d'analitzar, definir solucions • Elaboració d'informes, metodologies, estàndards i kpis • Suport elaboració de plans de millora de riscos
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els 5 darrers anys, 3 anys d'experiència en anàlisis i definició d'arquitectures segures IT Acreditar durant els 5 darrers anys, 3 anys d'experiència en anàlisis i definició d'arquitectures segures OT Acreditar participació en projectes de seguretat de cloud Acreditar coneixement ISA/IEC 62443 Acreditar coneixement en normatives i bones pràctiques
	TITULACIONS
	Titulació universitària en enginyeria informàtica, telecomunicacions o similar
	DEDICACIÓ
	0,5 FTE (Full Time Equivalent)

PERFIL	DESCRPIPCIÓ
Formació i capacitació	**RESPONSABILITAT MINIMES**
	Especialista en formació i capacitació de grans organitzacions: • Anàlisis i definició dels perfils de la companyia • Definició de plans de formació i conscienciació adaptada a cada perfil • Disseny d'un pla de formació i conscienciació transversal • Planificació i execució de Cibersimulacres • Realització d'informes amb els resultats i anàlisis dels cibersimulacres • Propostes de millores respecte els gaps detectats • Elaboració d'informes i KPIs
	CONEIXEMENTS I EXPERIÈNCIA
	Acreditar durant els 5 darrers anys, 3 anys d'experiència en anàlisis i definició de plans de formació i capacitació Acreditar coneixement en formació i cultura de Ciberseguretat per a grans empreses Acreditar coneixement en formació i cultura de Ciberseguretat en entorns OT i IT Haver participat en definició i coordinació d'exercicis de Cibersimulacres per empreses amb més de 5000 empleats Haver participat en definició i coordinació d'exercicis de Cibersimulacres en empreses amb actius OT Acreditar coneixements en awareness & training
	TITULACIONS
	Grau o titulació universitària en Pedagogia, Psicologia, comunicació, formació de persones adultes o enginyeria informàtica, telecomunicacions o similar amb especialització en formació
	DEDICACIÓ
	0,5 FTE (Full Time Equivalent)

Addicionalment l'adjudicatari designarà un únic **responsable del compte** que serà el darrer responsable del de la licitació. Aquesta figura es mantindrà durant tota la vida del contracte en la gestió comercial, durant l'execució del servei i fins la devolució d'aquest i serà l'interlocutor i responsable en cas de que es produeixin canvis en l'abast o cost del serveis que impliquin una modificació contractual.

TMB podrà demanar en qualsevol moment a l'adjudicatari el llistat de persones que formen part de l'equip del projecte

TMB es reserva el dret de verificar les capacitats del personal assignat o que participa puntualment en l'Oficina de Ciberseguretat i rebutjar-lo en cas de que no compleixi amb les requisits exigits o amb el rendiment esperat. Les despeses que es derivin com a conseqüència del canvis en l'equip aniran a càrrec de l'adjudicatari.

L'empresa adjudicatària haurà de mantenir l'equip de treball adscrit al contracte durant tota la vigència d'aquest. En cas que s'hagi de produir la substitució d'algun membre de l'equip, que no sigui per causes de força major, l'adjudicatari ho comunicarà a TMB i la substitució s'haurà de fer per un perfil que com a mínim tingui les mateixes característiques professionals i tècniques que les exigides en aquest apartat.; en cas contrari aquest fet serà susceptible de penalització.

A més, en cas de substituir algun membre de l'equip de treball, s'exigirà que:

- En cas de substitució d'un membre de l'equip, s'exigeix un període de coexistència mínim de 15 dies entre la persona que causa baixa i la persona que s'incorpora, amb l'objectiu de garantir la transferència de coneixement. Aquesta condició no serà exigible quan la baixa es produeixi sense preavís per causes de força major, acomiadament immediat, malaltia sobtada o altres circumstàncies que facin impossible la coexistència
- Una formació de TMB i del servei a desenvolupar (a càrrec de l'adjudicatari)

5.5. Mecanismes de comunicació i coordinació

Per garantir una gestió eficient i alineada amb les necessitats de TMB, l'adjudicatari haurà de designar un/a **interlocutor/a únic/a** com a responsable de la coordinació general del servei. Aquesta figura actuarà com a punt de contacte principal amb TMB, gestionant la planificació, el seguiment i la resolució de les actuacions derivades del servei.

No obstant això, TMB podrà contactar directament amb altres membres de l'equip de l'oficina externa de Ciberseguretat per a la gestió operativa de tasques específiques, amb l'objectiu de facilitar una resposta més àgil i eficient. En tot cas, el/la responsable designat/da per l'adjudicatari **serà informat/da de totes les interaccions** per garantir la traçabilitat i la coherència en la prestació del servei.

Durant la fase inicial del servei, es definirà **la periodicitat de les reunions de seguiment**, així com **la constitució de diversos comitès**, amb funcions diferenciades:

- Un comitè estratègic, orientat a la revisió global del servei, alineació amb els objectius de TMB i propostes de millora.
- Un o més comitès operatius, centrats en el seguiment de les activitats tècniques, gestió d'incidències i coordinació funcional.

Aquests comitès estaran formats per representants de TMB i l'adjudicatari, i la seva composició i dinàmica de treball es formalitzaran a l'inici de la prestació.

La responsabilitat de generar les actes resultants d'aquests comitès serà de l'adjudicatari

5.6. Metodologia del contracte

L'adjudicatari definirà un Pla de Contracte que descrigui com portarà a terme els serveis contractats. El servei es desplegarà en les següents fases:

5.6.1. Fase d'implatació:

Objectiu: Posar en marxa el servei de manera ordenada, segura i coordinada

Tasques mínimes principals:

- Reunió inicial Kick-off amb TMB
- Validació del pla de qualitat
- Definició del pla de contracte
- Definició del pla de treball/servei
- Revisió i definició de la gestió de la demanda
- Definició dels diferents comitès amb la periodicitat
- Assignació de l'equip i validació de TMB
- Configuracions d'accés als sistemes i eines
- Transferència de coneixement inicial
- Establir canals de comunicació i protocols d'escalament

Duració: Aquesta fase no pot durar més de 3 mesos del kick-off

Resultat esperat: Servei operatiu amb tots els mecanismes de gestió I seguiment activats

En els casos que no hi hagi documentació prèvia necessària per a prestar el servei, l'adjudicatari haurà de planificar i executar la seva elaboració, d'acord amb els responsables de TMB i sense cap cost addicional per TMB.

5.6.2. Fase execució del servei

Objectiu: Desenvolupar el servei segons els requeriments tècnics i operatius establerts

Tasques mínimes principals:

- Prestació continuada del servei de l'Oficina de Ciberseguretat acord el pla de treball i les tasques definides al plec
- Participació en comitès
- Creació de Quadre de Comandament
- Elaboració d'informes periòdics

- Avaluació dels KPIs, ANS i propostes de millora
- Revisió post-implantació (entre els tres i sis mesos) per ajustar el servei

Duració: Durant la vigència del contracte (amb pròrrogues si aplica)

Resultat esperat: Servei estable, traçable i alienat amb els objectius de TMB

En els casos que no hi hagi documentació prèvia necessària per a prestar el servei, l'adjudicatari haurà de planificar i executar la seva elaboració, d'acord amb els responsables de TMB i sense cap cost addicional per TMB.

S'espera que l'adjudicatari realitzi propostes de millora en el servei i la seva implantació dependrà de l'aprovació per part de TMB

5.6.3. Fase devolució del servei

Objectiu: Finalitzar el contracte garantint la continuïtat operativa i la conservació del coneixement.

Tasques mínimes principals:

- Elaboració del pla de devolució del servei, consensuat amb TMB
- Transferència de coneixement acumulat a TMB i al nou adjudicatari, si escau
- Lliurament de documentació final
- Tancament d'accés als sistemes i revocació de credencials
- Suport actiu en el procés de transició cap el nou adjudicatari, facilitant la comprensió dels serveis prestats, els sistemes utilitzats i les casuístiques operatives
- Participació, si es cau, en reunions de traspàs amb TMB i el nou adjudicatari
- Revisió conjunta del servei prestat
- Clausura dels comitès i valoració final

Duració: Durant la vigència del contracte. Es definirà conjuntament amb TMB si s'inicia 2 mesos abans de la data de venciment en funció de les necessitats operatives, garantint la transferència completa de coneixement. Aqueta fase es realitzarà en paral·lel a la fase d'execució del servei sense cost addicional.

Resultat esperat: Tancament ordenat del servei amb tota la informació transferida i sistemes protegits

Pla de devolució:

L'adjudicatari serà el responsable d'elaborar el Pla de devolució del contracte sobre el coneixement del conjunt d'iniciatives, tasques que s'han executat dins els servei a més de les que estan en curs o properament a iniciar-se.

El Pla ha d'incloure totes les activitats, traspàs de documentació, procediments, customitzacions realitzades, etc que formen part del coneixement de TMB i que s'hauran de traslladar a TMB i al nou adjudicatari.

El pla ha de complir com a mínim els següents principis i continguts:

- Transferència de coneixement a TMB i al nou proveïdor incloent procediments, , configuracions, casuístiques operatives, metodologies per cadascuna de les activitats amb les particularitats de cada tasca/servei i lliçons apreses
- Lliurables generats i documentació generada durant la vigència del contracte en les últimes versions. Inclouen informes tècnics, manuals d'ús, inventaris, històrics d'actuacions, etc.
- Ha de contemplar les tasques mínimes descrites en la fase de devolució de servei
- Suport en la validació del traspàs amb disponibilitat per a consultes durant el període de transició
- Informe de tancament de servei

Aquest pla haurà de ser validat per TMB abans de la seva execució i formarà part dels lliurables finals del contracte.

5.7. Gestió de la demanda

Actualment TMB disposa d'una bústia de correu genèrica per tal d'atendre les peticions tal i com es detalla a l'apartat 4.4 Suport i gestió de la demanda del present document. Durant la fase d'implantació es revisarà el procediment actual i es definirà la seva evolució de manera junta entre TMB i l'adjudicatari. L'adjudicatari haurà de proposar un procediment flexible i escalable per a la recepció, classificació, priorització i seguiment de les peticions de servei incloent:

- Tipologia de demandes (consultes, incidències, actuacions planificades).
- Canal de comunicació (ticketing, correu, etc.).
- Temps de resposta orientatius segons cripticitat.

- Protocols d'escalament.

Aquest procediment haurà de ser validat per TMB i revisat periòdicament.

5.8. Governança del servei

La governança del servei es basarà en mecanismes de seguiment i control corresponents al Pla de qualitat que es validadarà a l'inici de la prestació. El proveïdor haurà de participar en comitès de seguiment amb TMB, amb una composició i periodicitat que es determinaran durant la fase d'implantació.

Els comitès podran ser:

- Estratègics: per revisar l'evolució global del servei i propostes de millora.
- Operatius: per fer seguiment de les actuacions tècniques i indicadors de servei.

S'establiran també indicadors de qualitat (KPI) i mecanismes de revisió des SLA /ANS que seran part del sistema de control de servei i que es revisaran en el moment d'implantació del servei

5.9. Integració amb l'equip intern

El servei haurà de prestar-se de manera coordinada amb la Responsable de l'Oficina de Ciberseguretat de TMB i el CISO facilitant la col·laboració i la transferència de coneixement.

Tot i que la relació principal serà entre la responsable de l'Oficina de Ciberseguretat de TMB amb el responsable del servei durant la vigència del contracte i donada la naturalesa de la mateixa s'haurà de participar en reunions internes, grups de treball amb altres unitats de negoci, àrees, etc.

Aquest model podria requerir desplaçament a reunions en altres ubicacions de TMB fora de l'oficina de corporativa tal i com es detalla en l'apartat 5.2 Modalitat de prestació.

Aquest models de relació es formalitzarà durant la fase d'implantació.

6. Requeriments del servei

6.1. Requeriments tècnics

TMB no proporcionarà els equips informàtics (PCs, portàtils o altres dispositius) necessaris per a la prestació del servei. Per tant, el licitador haurà de disposar dels **mitjans tècnics propis** adequats per garantir el correcte desenvolupament de les tasques assignades, incloent-hi la connexió segura als sistemes de TMB quan sigui necessari.

La connexió amb TMB es detallarà amb l'adjudicatari

L'adjudicatari ha de tindre coneixement i experiència demostrable en l'ús d'eines de GRC.

L'adjudicatari ha de tindre capacitat per treballar en entorns híbrids (cloud i on-premise)

6.2. Acords Nivell servei (ANS)

Els nivells de servei i terminis exigibles per a atendre la demanda de les noves peticions de l'Oficina de Ciberseguretat (ja sigui a través de la bústia genèrica o dels mecanismes que s'implantin durant la vigència del contracte són els següents:

- **Temps de registre de noves sol·licituds**: És el temps transcorregut entre que entra la petició per qualsevols dels canals i es registra, classifica i prioritza. **8h laborables**
- **Temps de resolució:** És el temps transcorregut des de que la petició es registra fins que es dona per tancada o correctament derivada a l'afectat o responsable: **32h laborables**
    - Totes aquelles peticions que es classifiquin com **urgents** s'haurà de donar resposta en **8h laborable**

Serà la responsable de l'Oficina de Ciberseguretat qui determinarà si la petició és urgent

Penalitzacions aplicables

Àmbit	Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment
Informes	Entrega d'informes periòdics dins del termini pactat (5 primers dies del mes)	% d'informes entregats fora de termini	Mensual	Crítica: <95% Alta: 95–97% Mitjana: 97–99% Baixa: ≥99%
Peticions urgents	Temps de resposta a peticions urgents	% de peticions urgents resoltes en ≤8h laborables	Mensual	Crítica: <90% Alta: 90–95% Mitjana: 95–98% Baixa: ≥98%
Presencialitat	Presència del responsable 3 dies/setmana	Dies de presència efectiva vs. dies requerits	Mensual	Crítica: <80% Alta: 80–90% Mitjana: 90–95% Baixa: ≥95%
Substitució de personal	Substitució sense preavís ni perfil equivalent	Casos detectats vs. total canvis	Per cas	Crítica: Qualsevol substitució sense validació
Incorrecta dedicació del personal	Detecció de rotació del personal assignat a cada perfil sense preavís o autorització pel tipus de tasca	Casos detectats vs persones assignades	Per cas	Crítica: Qualsevol substitució sense validació
Quadre de comandament	Actualització mensual del QdC	% de mesos amb actualització completa	Trimestral	Crítica: <90% Alta: 90–95% Mitjana: 95–98% Baixa: ≥98%

Gestió de la demanda	Temps de registre i resolució de peticions	% de peticions registrades en ≤8h i resoltes en ≤32h	Mensual	Crítica: <85% Alta: 85–90% Mitjana: 90–95% Baixa: ≥95%
Comitès	Redacció i entrega d'actes dels comitès en el termini acordat	% d'actes entregades dins del termini	Mensual	Crítica: <90% Alta: 90–95% Mitjana: 95–98% Baixa: ≥98%
Escalat de temes crítics	Escalat de temes urgents/crítics a TMB en temps adequat	% de casos escalats en ≤4h (laborables o temes critics fora d'hores)	Mensual	Crítica: <90% Alta: 90–95% Mitjana: 95–98% Baixa: ≥98%
Auditories	Resultats d'auditories externes o internes sobre el compliment del contracte	Nombre d'incidències crítiques o altes detectades	Per auditoria	Crítica: ≥1 incidència crítica Alta: ≥2 incidències altes
Dedicació de recursos	Verificació que la dedicació dels recursos és la pactada	Hores reals dedicades vs. hores compromeses	Mensual	Crítica: <85% Alta: 85–90% Mitjana: 90–95% Baixa: ≥95%

6.3. Requeriments organitzatius

Tota la documentació, comunicacions i informes derivats del servei s'hauran de redactar en català, i si escau, també en castellà, segons les indicacions de TMB.

L'empresa adjudicatària haurà de presentar un **pla de qualitat** que defineixi els mecanismes de control, seguiment i millora contínua aplicables a la prestació del servei. Aquest pla haurà d'incloure com es garanteix el compliment dels requeriments tècnics i organitzatius, la gestió de les incidències, la traçabilitat de les actuacions, i els procediments d'auditoria interna.

Així mateix, s'hauran d'establir indicadors de qualitat (KPI) que permetin a TMB avaluar el rendiment del servei, així com propostes de revisió periòdica per assegurar l'adaptació a les necessitats canviants de l'organització.

El pla de qualitat formarà part de la documentació a lliurar en la proposta tècnica i serà revisat i validat per TMB durant la fase d'implantació del servei

TMB es reserva el dret d'auditar a l'adjudicatari per tal de garantir que s'està complint amb les condicions de la licitació

7. Requeriments mediambientals

Criteri	Descripció
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. | • 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	En el cas que la licitació inclogui el lliurament de productes o materials, i aquests se subministrin amb embalatges no primaris, aquests hauran d'estar fabricats íntegrament amb materials reciclats. (1) embalatge addicional al del propi material per a la distribució final del producte)
Vessament I abocament de líquid	En el cas d'utilització de líquids 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."