Plec de Prescripcions Tècniques

SERVEI GESTIONAT D'OPERACIÓ DE CIBERSEGURETAT DE TMB

Expedient: ***15012999***

Març de 2024

Versió 1.0

Solucions Corporatives
Àrea de Tecnologia

Ernest Costa Lluch
Responsable de Sistemes de Ciberseguretat

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.

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. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

L'objectiu de la Ciberseguretat és garantir la confidencialitat, integritat, autenticitat, disponibilitat i traçabilitat de la informació, així com la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC i OT han d' estar protegits contra amenaces de ràpida evolució. Per garantir la prestació contínua dels serveis i defensar-se d' aquestes amenaces, es requereix una estratègia que s' adapti als canvis de l' entorn. Això suposa que, en funció de les competències de cada àmbit, els departaments hagin d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS, operat per Reial Decret 311/2022, de 3 de maig), fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents.

2. Objecte

El present contracte té per objecte la contractació d'un Servei de Ciberseguretat Gestionada què doni resposta a les necessitats del grup Transports Metropolitans de Barcelona (TMB), d'acord amb les prescripcions tècniques que es descriuen en el present plec.

2.1. Abast

El servei cobreix els àmbits de ciberseguretat en general (IT i OT), de la totalitat dels serveis TIC de TMB. Tanmateix s'inclouen tant aquelles infraestructures TIC que estiguin ubicades en les instal·lacions de TMB com aquelles que puguin estar en serveis externs subcontractats basats en Cloud.

Amb aquest objectiu s'utilitzaran tant les eines pròpies de TMB descrites al plec com eines que pugi aportar l'adjudicatari.

Inclou una Oficina tècnica que gestionarà la totalitat del contracte, que es desglossarà en els següents serveis:

a) Oficina Tècnica d'Operació de Ciberseguretat
b) Servei d'Operació de Ciberseguretat (SOC)
c) Vigilància Digital
d) Equip de Resposta davant d'Incidències de Seguretat i anàlisis forense (CSIRT)
e) Administració tècnica de plataformes de seguretat

Volumetries

A efectes d'ajudar a dimensionar els recursos necessaris per donar cobertura als serveis del contracte s'ha de tenir en compte que l'ordre de magnitud dels actius que s'han de gestionar son:

- Servidors: 1.000 (Linux/Windows)
- Clients: 5.000
- Empleats: 9.000

3. Fases de la prestació del servei

Tot seguit es descriuen les fases de la prestació del servei:

● Fase de Recepció del servei:
S'entén per fase de Recepció del servei el període que va entre l'entrada en vigor del contracte adjudicat al nou contractista i la transició d'inici de l'assumpció del servei, amb l'acompanyament de l'adjudicatari sortint (si encara hi té contracte i per TMB).

● Fase de Devolució del servei:
S'entén per devolució del servei totes aquelles accions precises per tal de traspassar en condicions òptimes tot el servei sense cap merma ni pèrdua de funcionalitats al nou adjudicatari a la finalització o extinció prematura d'aquest contracte.

3.1. Recepció del servei

Actualment TMB ja disposa d'un servei de SOC així com una sèrie de projectes en marxa relacionats amb ciberseguretat i per tant el contracte ha de preveure un temps inicial de presa del servei on desenvolupar les tasques preparatòries necessàries per garantint una transició ordenada i sense interrupcions del servei i iniciatives en procés.

Important recalcar que actualment hi ha una sèrie de Casos d'Ús (CdU) implementats que s'haurien de revisar a l'etapa de recepció del projecte, per adaptar/millorar/evolucionar, perquè les alertes s'enviïn al servei de Monitorització 24x7 corresponent, així com incorporar tots els CdU que poguessin faltar per a les Best Practice que recomani el proveïdor (basat en la seva experiència amb altres clients).

Aspectes mínims a tenir en compte en la pressa del servei:

- Revisió dels processo i documentació existent
- Integració dels processos de notificació de Service Desk
- Anàlisi/adaptació de casos d'ús: biblioteca playbooks, alertes, falsos positius,…
- Configuració d'accessos i provisió d' usuaris als entorns requerits.
- Identificació de contactes.
- Definició del model de governança
- Definició del model d' informes
- Matriu d'escalats
- Definició del model de seguiment de SLA's
- Quadres de comandament inicials

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

La dedicació i els recursos usats pel nou contractista dedicats al traspàs de coneixements i assimilació del nou entorn i característiques del servei seran sense cap cost addicional per TMB.

L'adjudicatari podrà fer propostes de nous elements per a la gestió i seguiment del servei o proposar millores en el servei, i la seva implantació dependrà de l'aprovació per part de TMB.

3.2. Servei Regular

La fase regular s'inicia un cop acabades totes les tasques de la fase anterior i s'estén fins l'extinció del contracte i abans de la fase de devolució del servei.

Totes les activitats que, com a mínim, haurà de realitzar es descriuen a l'apartat 4 de descripció del servei.

Addicionalment l'adjudicatari haurà de presentar propostes que permetin assegurar l'evolució del servei tant des del punt de vista tecnològic, com de governança o incorporació de noves funcionalitats i tasques al servei.

Els mecanismes d'evolució han d'incloure informació detallada sobre les pautes d'activació, els instruments de seguiment, integració de tasques i procediments de forma tant reactiva com proactiva per part de l'adjudicatari.

A banda dels criteris generals, els mecanismes d'evolució han de tenir en compte la incorporació de noves funcionalitats que no s'hagin previst inicialment o que l'evolució del mercat i de la demanda facin que TMB decideixi incorporar-les (nous serveis al núvol, noves

aplicacions, nous serveis de ciber-intel·ligència, etc ...).

3.3. Devolució del servei

El proveïdor haurà de tenir en compte que al final del contracte, serà necessari fer un traspàs de coneixement, documentació, procediments, playbooks aplicats, etc, que formen part del know-how de TMB, i que s'haurà de traslladar (i facilitar aquest trasllat) al següent contracte, en el cas que fos un altre proveïdor.

El procés d' offboarding ha de contemplar:

- Formalitzar data de finalització
- Programació del darrer report de servei
- Desactivació de les integracions TMB-Proveïdor
- Desactivació dels accessos als sistemes de TMB
- Desactivació de notificacions

4. Descripció del servei regular

4.1. Oficina Tècnica

L'objectiu d'aquest servei és col·laborar amb els equips interns de TMB en supervisar, gestionar i optimitzar les operacions relacionades amb la seguretat de la organització, garantint la protecció de les seves infraestructures, actius i dades. Aquesta oficina s'encarregarà d'implementar i mantenir sistemes i procediments de seguretat operativa, assegurant una resposta efectiva davant d'incidents de seguretat i minimitzant els riscos associats amb les amenaces tant internes com externes.

Amb aquest objectiu en ment, el servei es dimensionarà perquè cobreixi els aspectes següents:

- Coordinació, seguiment i millora continua del servei
- Manteniment del SIEM
- Thread Hunting
- Gestió de vulnerabilitats
- Auditories i pentesting
- Consultoria i Projectes

4.1.1. Coordinació, seguiment i millora continua del servei

Aquest procés encarregarà de liderar, gestionar i controlar l'evolució dels diferents serveis per a ser més eficients i eficaços en l'execució de les tasques responsabilitat de cada àmbit, sempre amb visió a l'alineament d'aquestes accions amb els objectius de seguretat de TMB.

El servei haurà de mantenir constantment una coordinació de tots els serveis d'aquesta contractació i ha de poder treballar de forma integrada amb client.

L'objectiu del servei és ser l'interlocutor principal del Servei de Ciberseguretat Gestionada aportant una visió global de tots els serveis de seguretat contractats per TMB. Gestió d'escalats i seguiment d'indicadors/SLAs, lliurament d'informes setmanals i executius mensuals, etc. controlant la qualitat extrem a extrem d'acord amb els compromisos adquirits i en general, d'impulsar l'evolució dels serveis de Seguretat del Client al llarg de la vida del projecte.

El servei inclourà un procés de millora continua amb propostes escrites de recomanacions sobre les solucions i serveis actuals, amb canvis i d'altres millores correctives que potenciïn l'evolució positiva del servei. Així com possibles ampliacions que serien recomanables disposar de cara a una evolució futura.

L'aplicació de les millores serà a decisió i criteri dels responsables de TMB. Una vegada hagin esta aprovades, la OT s'encarregarà de coordinar la seva execució.

Es demana pro activitat en el servei, treballant de manera cooperativa amb el client, i no limitant-se a la comunicació amb les verticals del propi servei sinó, també amb altres proveïdors per poder mantenir una coordinació amb ells, i informant quan es detecti alguna mancança per part del servei d'algun proveïdor que en conseqüència pugui influir negativament amb la seguretat de TMB.

La coordinació inclourà la gestió de la bossa d'hores contractades amb el proveïdor, proposant a client, de manera proactiva, la millor manera de fer-les servir. S'encarregarà de fer tots els passos per articular l'activació d'aquestes consultories i projectes als serveis definits a l'apartat de "Consultoria i Projectes sota demanda".

Es detallen a continuació altres tasques que seran cobertes pel servei de la OT:

- Responsabilitat davant del Client de la provisió i explotació dels serveis de seguretat que tingui contractats. Intervenir en tots els projectes de seguretat nous que es contractin i responsabilitat en la planificació i el seguiment global de la seva implantació.
- Gestió externa i interna, d'escalats d'avaries per a tots els serveis de seguretat. Coordinació interna amb els responsables d'altres serveis del proveïdor des d'un punt de vista tècnic.
- Interlocució principal, tant davant TMB com internament al proveïdor per a la gestió d'escalats i coordinacions d'incidències d'alt impacte relacionades amb les infraestructures de seguretat.
- Implantació del model de govern i atenció amb TMB, així com l'aplicació de les metodologies actualitzades que condueixin a la pràctica d'una cultura de seguretat informàtica.
- Gestió de canvis i gestió de la configuració en el model/abast de prestació del Servei.
- Visió extrem a extrem de la qualitat del servei de seguretat prestat al Client, seguiment i control dels indicadors/SLA, reporting al Client i a l'organització interna.
- Definició i execució de procediments d'actuació per garantir la provisió i l'explotació correcta dels serveis, recolzant-se en la resta de figures/unitats dedicades a l'atenció del Client.

- Definició i lideratge de Plans de Millora Contínua de la prestació del servei i de totes les plataformes gestionades pel servei. Identificació de problemes tant de seguretat com dins del servei, i n'és responsable de la gestió.
- Assessorament sobre la constant evolució tecnològica i com aquesta pot beneficiar o augmentar els nivells de seguretat existents a TMB.
- Compartir els coneixements sobre les millors pràctiques seguides per garantir la continuïtat del negoci, la confidencialitat de la informació i la seva integritat.
- Disponibilitat Proveïdor les 24 hores del dia i els 365 dies de l'any per poder atendre qualsevol situació crítica o greu sobre algun dels serveis de seguretat prestats pel proveïdor que el client consideri que en requereixi l'atenció o el coneixement. En cas de substitució per vacances/baixes, etc. de les persones assignades a la OT, es comunicarà a TMB i es farà el traspàs amb la antelació que ho requereixi el canvi.
- Seguiment dels incidents rellevants amb afectació al servei i creació del corresponent informe d'incident post mortem.

4.1.2. Manteniment del SIEM

El servei que se sol·licita inclou el desenvolupament, la posada a punt i millora contínua dels panells del SIEM de TMB, actualment implementats sobre una plataforma Splunk onpremise, mitjançant la incorporació de les fonts de dades i procediments d'actuació (playbooks) que es considerin necessaris per millorar la detecció i gestió de les alertes.

El SIEM de TMB que actualment està basat en una plataforma SPLUNK onpremise on s'ingesten diàriament uns 200Gb de diverses fonts: Firewalls, Antispam, Backup, Events de directori actiu, IRM (SealPath), Antimaware (antivirus i application control), eina de gestió de vulnerabilitats, O365, CASB,.... i on hi han configurades més de 80 alertes amb el seu playbook associat.

El proveïdor haurà d'operar la solució del SIEM de Splunk, propietat de TMB. No obstant si durant la duració del contracte, TMB decidís migrar a un altre, l'Oficina Tècnica s'hauria d'adaptar a aquesta nova tecnologia i col·laborar a migrar els Casos d'Us (CdU) existents a l'actual plataforma i evolucionar-la.

El proveïdor haurà de contemplar que al llarg del contracte, la volumetria d'ingesta, la quantitat de fonts o inclús els productes, poden variar. A títol de exemple, s'està treballant en canviar les fonts d'Antivirus/EDR i CASB.

Requeriments sol·licitats:

La gestió de la solució ha de contemplar:

- **Capa de Recol·lecció de Dades**, amb capacitat de recol·lecció de fonts de dades multi-entorn (On-premise, cloud o híbrid), sota diferents formats i vies de recol·lecció. El servei ha de contemplar la incorporació de totes les fonts de dades, ya siguin de IT com d'OT, que siguin susceptibles d'aportar informació de qualitat al SIEM, per a un bon govern de seguretat.

- **Gestió d'alertes del SIEM**, creació i manteniment de casos d'ús (IT i OT) que es considerin necessaris, tant per part del proveïdor i la seva experiència en el servei (adaptant el seu catàleg estàndard de casos d'ús) com per part de TMB que vulgui implementar casos d'ús concrets per necessitats. Aplicant els ajustos necessaris d'excepcions.
- **Definició de procediments**, de manera que cada alerta disposi del corresponent procediment operatiu documentat que estigui acordat amb TMB, que contingui el Playbook amb l'arbre de decisió fins a la resolució final. Han de quedar clars els passos concrets fins a la resolució de cada CdU independentment de si ho realitzarà el SOC o si s'abordarà amb recursos propis de TMB. TMB proveirà un repositori sharepoint on deixar de forma ordenada tota la documentació generada en el decurs del servei.
- **Capa d'Orquestració i Automatització** que permet aplicar automatitzacions. Sempre que sigui possible i amb els serveis disponibles del client (amb SOAR o altres solucions complementàries, p.e. Ansible), es tractaran d'automatitzar tots els CdU que sigui possible per millorar la velocitat de resposta i la dependència de treballs manuals.
- **Capa d'Intel·ligència d'Amenaces** (IOC) amb fonts obertes, pròpies i de tercers que permeten millorar la ràtio de detecció i disposar de capacitats addicionals d'enriquiment i automatització mitjançant un TIP (Threat Intelligence Platfom) del proveïdor.
- El proveïdor haurà de proporcionar un **ampli catàleg de casos d'ús propis** en contínua evolució amb una base de coneixement elaborada sobre la base de més. Aquest catàleg haurà d'estar mapejat i alineat amb el framework de MITRE.

4.1.3. Threat Hunting

El Servei de Threat Hunting realitzarà cerques iteratives i proactives als sistemes i xarxes de TMB, amb l'objectiu d'identificar amenaces avançades que poden haver evadit els controls de seguretat ja establerts. És una mesura de seguretat preventiva i proactiva, capaç de proporcionar detecció d'amenaces abans que tinguin un impacte al negoci, i no gira al voltant d'eines específiques.

El Servei de Cerca d'Amenaces segueix un enfocament d'hipòtesis. L´objectiu d´aquestes hipòtesis és detectar possibles atacants que operin entre les fases de reconeixement i exfiltració del marc MITRE ATT&CK. Una hipòtesi es defineix com "una suposició de comportament maliciós capaç d'evadir els controls de seguretat existents en un entorn concret d'una manera específica".

L'equip de Threat hunting generarà diferents consultes per a cada hipòtesi, que s'executaran sobre la infraestructura de TMB seguint els procediments aprovats pel Servei de Theat Hunting. Els resultats d'aquestes consultes seran analitzats per l'equip i, si hi ha prou proves, es notificaran com a alertes. Les alertes es defineixen com "l´evidència d´activitat maliciosa que no ha estat detectada prèviament per altres eines o equips".

TMB serà informat de les hipòtesi que s'analitzaran i dels resultats d'aquests anàlisis.

Lliurables

El servei de cerca d'amenaces proporciona els mecanismes de seguiment i generació d'informes següents:

- Informe de cerca d'amenaces: informe mensual estàndard basat en l'execució del servei i que conté investigació d'amenaces, alertes i recomanacions.
- Notificacions d'alerta: troballes rellevants que s'han de notificar com més aviat millor, sense esperar a l'informe mensual.

4.1.4. Gestió de vulnerabilitats

El servei ha de cobrir el seguiment de la publicació de vulnerabilitats aplicables a les tecnologies que utilitza TMB. Gestionant els riscos detectats, i realitzant un seguiment de les accions necessàries fins aconseguir mitigar-los o minimitzar-los.

Com a fonts d'informació disposarà de la eina pròpia de TMB de Gestió de Vulnerabilitats, així com newsletters públiques i/o fonts internes del proveïdor.

Com a fonts d'informació es contemplaran comunicacions externes (CERTS, alertes primerenques, fabricants, zero days, etc …), comunicacions internes de la operació de seguretat de TMB (incidents de seguretat reportats, notificacions del personal TMB, detectades pel propi servei de ciberseguretat, derivades de les auditories de seguretat o dels propis escanejos de vulnerabilitats, etc …) i d'altres vulnerabilitats detectades per organismes externs a TMB.

La resolució si cal fer-la a través de recursos externs al proveïdor (ja sigui amb recursos de TMB o contractes a empreses de tercers), en farà el seguiment i realitzarà les sol·licituds que calgui realitzar amb la plataforma de ticketing oportuna en cada cas.

També supervisarà l'estat de la operació de la eina de Gestió de Vulnerabilitats que serà operada per tercers, però haurà de portar la vigilància/control de la correcta execució, donant a conèixer a TMB si es detecta algun mal funcionament/execució de la gestió de vulnerabilitats.

4.1.5. Auditories i Pentesting

L'objectiu d'aquest servei és facilitar una visió clara de la vulnerabilitat de TMB i els riscos potencials als quals es troben exposats els seus sistemes d'informació, a partir d'aquí proveir d'una sèrie de mesures correctives i preventives, així com recomanacions addicionals de seguretat proactiva, que permetin garantir un nivell de seguretat adequat.

El resultat final ha d'ajudar a TMB en el seu esforç per millorar la postura de seguretat i conèixer els riscos reals que afecten l'exposició de l'empresa, presentant informes amb els riscos que necessiten ser remeiats i una orientació per fer-ho.

Els informes han de identificar clarament les millores que s'han d'abordar, amb priorització, i proporcionar l'acompanyament per realitzar tots els ajustos necessaris, que s'han de gestionar des de la Oficina tècnica que serà qui coordinarà l'aplicació de les accions correctives a realitzar.

El servei contemplarà l'execució d'almenys 4 simulacres per quadrimestre (12 execucions a l'any) així com la possibilitat de realitzar execucions a petició de TMB (que es gestionaran amb la bossa d'hores de l'oficina tècnica).

El proveïdor haurà de proporcionar les eines **Simulació d'Infraccions i Atac (BAS)** necessàries per poder realitzar les autories/pentesting de TMB. Aquestes eines haurien de estar basades i presentar el resultats segons el marc MITRE ATT&CK.

Tots els mòduls de l'eina escollida pel proveïdor, seran administrats en **modalitat servei** (TMB no disposarà de llicenciament ni suport de la solució que proporcioni el proveïdor) i per tant inclourà serveis professionals tant per a la implantació i manteniment com per l'explotació de l'eina.

El servei ha d'incloure les capacitats per actuar de manera homogènia i coordinada per:

- Provar totes les fases d'un atac, des de la preexplotació fins a la postexplotació, la persistència i el manteniment de l'accés.
- Realitzar proves de forma contínua, periòdica i sota demanda.
- Realitzar proves segures sense interferir en l'operativa de TMB.
- Provar controls de seguretat tant perimetrals com interns.
- Actualització contínua per oferir simulacions que també incloguin amenaces detectades "in-the-wild".
- Proporcionar informes exhaustius i concloents que incloguin recomanacions de mitigació.

4.1.6. Funcionament del servei

El servei disposarà d'un perfil Analista de Seguretat dedicat al servei BAS (Breach and Attack Simulation) que, coordinat amb l'oficina tècnica i comptant si es necessari amb el suport d'altres experts del proveïdor:

- Recomanarà les simulacions que millor s'adaptin a la postura i la maduresa de seguretat del TMB.
- Definirà clarament l'abast dels simulacres en relació amb l'actiu (xarxa, aplicació, etc.) i els objectius.
- Planificarà les proves amb un enfocament estructurat amb una metodologia organitzada en diverses etapes: prèvia a la intervenció (abast, planificació), intervenció (execució de les proves) i posterior a la intervenció (suport a la remediació, presentació d'informes, re-testing).
- L'analista de seguretat haurà de tenir relació directa i suport pel fabricant de l'eina.

Cicle de Vida

S'estructurarà cada simulacre en quatre fases principals que es desenvoluparà i es repetiran de manera cíclica i en les quals interactuen un conjunt definit de persones, tecnologia i processos:

1. **Planificació**, En una fase inicial s'acordarà i planificarà amb TMB l'abast, les franges horàries i les possibles restriccions. En base a aquesta informació, es provisionarà el servei perquè estigui llest i el equip tècnic pugui executar les proves de seguretat.
2. **Execució de les proves,** Les proves de seguretat són executades en base a la planificació acordada. Després de realitzar l'avaluació, es genera una puntuació que reflecteix la magnitud de les amenaces potencials per als sistemes o recursos objectiu, amb una avaluació comparativa específica del sector.
3. **Comunicació de resultats,** En aquesta fase es generaran els informes i entregables del resultat dels simulacres, on s' indicaran les mesures de mitigació per a cadascuna de les bretxes de seguretat trobades. També en aquesta fase, l'analista de seguretat assignat realitzarà reunions amb l'equip de seguretat de TMB per poder explicar els findings i els informes lliurats.
4. **Re-Test, e**s realitzarà una repetició de les proves per validar si els passos de remediació proposats pels experts han estat executats i han sigut efectius.

Lliurables

Els informes de les proves presentaran l'acompliment dut a terme pel servei inclòs en aquesta proposta.

Després de cada simulacre, es lliuraran un informe tècnic i un altre executiu el contingut del qual pot variar depenent del tipus de simulacre o vector d'atac utilitzat, però que bàsicament inclouran la següent informació:

- Descripció: Inclou la motivació de TMB per dur a terme la prova.
- Abast: Conté els actius objectiu dins l'abast i el calendari de proves.
- Conclusions: Informació general que transmet les troballes detallades en una valoració resumida.
- Recomanacions generals: Sobre la base dels resultats de les proves, ofereix recomanacions generals que resumeixen les mesures a adoptar.
- Llista prioritzades de totes les bretxes de seguretat i riscos trobats sobre els actius testats, ordenats per grau de severitat i impacte.

4.1.7. Mòduls de la Eina (BAS)

A continuació es mencionen diferents mòduls que haurà de poder cobrir la eina amb la realització de simulacions que proporcionin la postura de seguretat en diferents àmbits:

Desafiament dels Controls de DLP

Les filtracions de dades creen un enorme impacte financer en la reputació de les empreses víctima. Les solucions de DLP estan dissenyades per protegir contra la filtració de dades. Les organitzacions depenen gairebé per complet de la implantació, metodologia i configuració de la DLP per protegir les seves valuoses dades.

El mòdul d'exfiltració de dades està dissenyat per avaluar en quina mesura les solucions i controls de DLP impedeixen l'extracció d'informació crítica des de l'exterior de l'organització. La

plataforma posa a prova els fluxos de sortida de dades (com informació d'identificació personal, mèdica, financera i confidencial empresarial) per validar que aquests actius d'informació romanen a l'interior.

El vector empaqueta les dades en diferents tipus d'arxius, incloent imatges i arxius, i intenta exfiltrar-les utilitzant múltiples mètodes d'exfiltració.

Proves d'Endpoint Security

El mòdul d'avaluació Endpoint Security permet provar i optimitzar l'eficàcia de la seguretat dels endpoints. Aquest vector desafia les mesures de seguretat dels endpoints contra un conjunt complet d'atacs que simulen el comportament maliciós de ransomware, cucs, troians i altres tipus de malware.

Les proves permeten crear escenaris d'atac personalitzats utilitzant cents de comandaments en tota la Kill-Chain dels ciberatacs, mapejats al marc MITRE ATT&CK.

Moviment lateral (Hopper)

El mòdul de protecció de la xarxa interna o vector de moviment lateral desafia les polítiques de segmentació i configuració de la xarxa interna contra diferents tècniques i mètodes utilitzats pels atacants per propagar-se dins de la xarxa i controlar sistemes addicionals.

El vector simula un adversari que té el control d'un sol equip de treball i intenta moure' s lateralment dins de l'organització. El resultat de l'avaluació és una visualització de tots els endpoints als quals l'avaluació ha pogut arribar amb una descripció detallada dels mètodes utilitzats per a cada salt.

L'avaluació identifica els punts febles de la infraestructura, els errors de configuració de la xarxa i les contrasenyes no segures, i proporciona orientació per a la seva correcció.

Protecció de Web Gateway

Aquest mòdul desafia els controls que protegeixen els empleats tant de l'accés com de la descàrrega de malware allotjat en llocs web maliciosos i compromesos.

El vector prova la protecció d'entrada contra milers de diferents arxius maliciosos i exploits simulats, i la protecció de sortida contra informació composta per milers d'URL que s'actualitzen diàriament.

Seguretat del correu electrònic

Permet provar i optimitzar la postura de ciberseguretat del correu electrònic de la companyia. Aquest vector desafia les mesures de seguretat del correu electrònic contra un ampli conjunt d'atacs mitjançant l'enviament de correus electrònics amb arxius adjunts que contenen ransomware, cucs, troians o enllaços a llocs web maliciosos.

La simulació revela els correus electrònics maliciosos, tipus d'arxius i arxius incrustats que podrien arribar a la safata d'entrada dels empleats.

Seguretat del WAF

Permet provar i optimitzar les mesures de seguretat web. Aquest vector identifica en primer lloc tots els formularis i altres mitjans d'importació de dades disponibles en el domini de seguretat d'infraestructura tècnica i, a continuació, desafia el WAF contra milers d'atacs, incloent-hi els principals payloads d'OWASP, injecció de comandaments i atacs d'injecció d'arxius per avaluar la integritat de la configuració del WAF i les seves capacitats de bloqueig.

4.1.8. Consultoria i Projectes sota demanda

Aquest servei es consumirà en format de bossa d'hores, i d'aquesta manera permetrà abordar ràpidament les necessitats emergents i proporcionar solucions immediates dins el procés de millora contínua de la ciberseguretat.

Aquestes podran provenir de TMB o bé de propostes que vinguin de la Oficina Tècnica.

Per dur a terme aquest servei es comptarà amb recursos de perfils tècnics de l'àmbit de la seguretat com son: Consultors, Projectistes, Compliance, Vigilancia digital, Auditors/pentesting, conscienciació, etc

Metodologia de treball

- Presentació de la proposta de servei de consultoria/projecte
- Valoració de l'esforç en hores
- Definició de la documentació de la proposta i d'entregables
- Aprovació de TMB
- Execució
- Entrega d'entregables i tancament

A mode d'exemple, a continuació es mostra una relació de possibles activitats:

1. Anàlisi de riscos
2. Avaluació de la maduresa de seguretat de proveïdors.
3. Procediments de desenvolupament segur de software.
4. Revisió sobre el compliment normatiu de la Directiva NIS2.
5. Revisió sobre el compliment de la Llei de Protecció d'Infraestructures Crítiques (LPIC).
6. Pla de formació i conscienciació en Ciberseguretat.
7. Acompanyament a la certificació ISO 27001.
8. Estat de salut del Directori Actiu
9. Elaboració del pla d'adequació al ENS i la seva implementació.
10. Consultes en l'àmbit de Compliance (p.e. protecció de dades personals).
11. Model de govern de la Ciberseguretat segons ISA/IEC 62443.
12. Revisió sobre el Pla de Continuïtat de Negoci.
13. Procediment de Gestió d'Incidents.
14. Anàlisi d'Impacte (BIA)
15. Simulació de phishing

4.2. Monitorització/Operació 24x7

La missió principal del Centre d'Operacions de Seguretat (SOC) serà protegir la informació i els sistemes de TMB contra les amenaces cibernètiques en modalitat 24x7x365. Per a això el servei tindrà com a principal comesa la monitorització i anàlisi continua de l'activitat de la xarxa, els sistemes i les aplicacions de TMB a la recerca d'activitats sospitoses o anomalies per tal de detectar i donar resposta als possibles incidents de seguretat.

Les funcions clau del SOC inclouen:

- **Investigació de possibles incidents:** Analitzar les alertes per determinar si són atacs reals o falsos positius.
- **Triatge i priorització d'incidents:** Avaluar i prioritzar els incidents per optimitzar recursos i minimitzar riscs.
- **Coordinació de resposta i resolució d'incidents:** Comptant amb recursos tècnics propis del SOC o orquestrant els diversos actors involucrats i eines disponibles.

El centre d'operacions de seguretat (SOC) serà coordinat per la oficina tècnica i comptarà com a mínim amb els següents recursos:

- Servei d'operació: **Equip 24x7** responsable del 1er. Nivell encarregat de la recepció diagnòstic i coordinació de la resposta i resolució de les alertes.
- Tècnics 2on i 3er. Nivell **(8x5 + guàrdies)** especialistes en les plataformes de seguretat de TMB (punt 3.5 d'aquest document).

Requeriments sol·licitats:

La llista mínima de tasques que cal oferir és:

- El contractista disposarà d'un centre operatiu (SOC) en mode 24x7x365 que pertanyi a la "Red nacional de SOC" on es rebran, notificaran, gestionaran i escalaran les alertes i incidents de ciberseguretat. Aquest centre haurà d'estar redundat amb un centre de contingència que permeti la continuïtat del servei en cas d'incidència greu al seu centre d'operacions.
- Monitorització 24x7x365 de les alertes i events generats i rebuts dins la plataforma SIEM de TMB. El contractista assumirà la integració de les alertes amb els seus sistemes.
- Monitorització 24x7x365 de les alertes i events generats per l'EDR de TMB, utilitzant les capacitats EDR per fer investigacions sobre les alertes accedint a la consola EDR (és a dir, la interfície d'usuari dins de la plataforma corresponent).
- Monitorització 24x7x365 de les alertes i events generats per altres canals que no són el SIEM i que es considerin necessaris: CASB,...
- TMB podrà també obrir un tiquet mitjançant correu a una adreça de correu electrònic o trucada telefònica a l'equip de Nivell 1.
- El Servei només durà a terme les accions de resposta, sempre que hagin estat prèviament aprovades per TMB i estiguin documentades als playbooks del Servei.

- Les alertes seran registrades en una plataforma de tiqueting que permeti fer el seu seguiment.
- Gestió de les alertes en 24x7: procediments de registre, diagnosis, classificació, resolució/mitigació per part de Nivell 1 i en cas necessari escalat a Nivell 2.
- L'adjudicatari s'integrarà amb els diferents organismes oficials en què TMB estigui subjecte per llei (RGPD) o amb el que es considerin oportuns per la cooperació a la gestió i detecció d'incidents (fòrum CSIRT.es, Xarxa Nacional de SOC's, Agència de Ciberseguretat de Catalunya, CCN-CNI). I si el servei ho requereix, es durà a terme la ingesta dels sistemes de registre i notificació d'incidents corporatius.

4.2.1. Quadre de comandaments del servei d'operació

El proveïdor generarà un quadre de comandament dins de la plataforma Splunk de TMB, que faciliti el seguiment de les operacions de seguretat i l'Estat de la Ciberseguretat a TMB.

Haurà de proporcionar una visió mensual de la prestació del servei, amb les activitats executades, accions planificades, punts bloquejants o que requereixin atenció, així com un resum de les incidències gestionades, volumetries associades al serveis i propers passos i propostes de millora de servei.

S'acordarà el contingut dels quadres de comandament facilitant la llista següent com a exemple:

- **Estat general de la Ciberseguretat**
  - Filtres per temps, estat, tipus de tiquet i prioritat
  - Mapa interactiu de geolocalització d'IPs públiques corresponents a atacs
  - Categoria de tiquets, subcategoria de tiquets, prioritat de tiquets
  - Tipus d'atac detectat i Taula detallada de tots els tiquets.
- **SLAs**
  - Temps mitjà de vida de notificació d'un incident de Seguretat
  - Nombre de tiquets mesurats per al càlcul del SLA
  - Percentatge de compliment
  - Evolució del compliment de SLA dels tiquets en el temps
  - Nombre de tiquets que incompleixen de criticitat baixa i % del total
- **Volum**
  - Filtres per temps, estat, tipus de tiquets i prioritat
  - Distribució de tipus de tiquets en el període
  - Nombre d'incidents gestionats
  - Dia de màxim nombre d'incidents gestionats i quantitat
  - Nombre de peticions gestionades
  - Mapa de calor d'atenció de tiquets
- **Productivitat**
  - Filtres per temps, estat, tipus de tiquet i prioritat
  - Distribució de tots els tiquets gestionats en el temps segons la tipologia

  - Nombre d'incidents de seguretat gestionats
  - Nombre d'incidents de seguretat amb impacte gestionats
  - Tipologia de tots els tiquets gestionats
- **Mètriques i KPI avançats** detall de les d'operacions i seguretat per al seguiment del servei, així com de l'estat de la seguretat corporativa. Aquestes mètriques s'han de poder revisar en qualsevol moment en temps real amb Dashboards personalitzats, així com un quadre de comandament de l'estat de la postura de seguretat per a la visió d'un CISO. Així com poder generar un informe a qualsevol moment de la postura de seguretat actual.

4.3. Administració tècnica de les plataformes

S'inclouen en aquest mòdul els serveis d'administració tècnica per a les plataformes de seguretat de TMB: Antivirus/EDR, Antispam i CASb de TMB.

Aquests serveis inclouran de forma genèrica les següents tasques:

Manteniment Correctiu

- Resolució d'incidències i fallades tècniques.
- Intervenció urgent en cas de problemes crítics que afectin l'operativitat de la plataforma.
- Registre i seguiment de totes les incidències fins a la seva resolució.

Manteniment Preventiu

- Revisió periòdica de l'estat de la plataforma.
- Aplicació d'actualitzacions de seguretat i pegats.
- Realització de proves de rendiment i ajustaments necessaris per garantir l'estabilitat del sistema.
- Anàlisi i prevenció de possibles fallades futures.

Manteniment Evolutiu

- Implementació de millores i noves funcionalitats.
- Configuració de la plataforma conforme a les noves necessitats de TMB.
- Gestió d'accessos: usuaris i rols
- Integració amb altres sistemes i plataformes segons es requereixi.
- Formació i capacitació al personal intern sobre noves funcionalitats.

Altres

- Generació d'Informes: Crear informes regulars d'activitat, incloent estadístiques, tendències i anàlisis de seguretat.
- Reunions de Revisió: Realitzar reunions periòdiques per revisar els informes i platejar possibles millores en el sistema.
- Capacitació del Personal: Formar el personal sobre l'ús de les diferents plataformes i les millors pràctiques pel seu ús.

- Assistència Tècnica: Proporcionar suport tècnic continu per resoldre problemes i respondre a preguntes.
- Documentació: Mantenir una documentació detallada i actualitzada del sistema i les seves configuracions.
- Assegurar el Compliment: Garantir que les diferents plataformes compleixin amb les normatives i lleis vigents sobre protecció de dades i privadesa.
- Escalabilitat: Assegurar que el sistema pugui escalar segons el creixement i les necessitats de TMB.
- Resiliència i Redundància: Implementar mesures per assegurar l'alta disponibilitat i la continuïtat del servei en cas de fallades.

4.3.1. Administració EDR

El proveïdor haurà de gestionar la solució EDR de TMB, que actualment es basa en la solució que es Trellix (amb Endpoint Security, EDR i Application Control).

Si en algun moment, TMB canvia de producte EDR (per a la totalitat o part del parc gestionat per Trellix, haurà de fer l'administració de la/les plataforma/es que cobreixin tot aquest parc d'equips.

En el cas particular d'equips Legacy que es cobreixen amb Application Control, en cas de no poder gestionar-se amb una nova eina EDR, s'hauran de continuar cobrint amb aquest producte (que tindrà llicenciat TMB) fins que desapareguin aquests equips Legacy. Aquest parc d'equips Legacy és actualment de menys de 1.000 clients.

A més de les tasques d'administració tècnica que s'han establert com a genèriques, la plataforma EDR inclourà tasques especifiques d'operació de l'eina, com son:

- L'administració de les polítiques pròpies de l'EDR respecte a la detecció i contenció d'alertes i incidències.
- L'administració de les polítiques pròpies de l'antivirus i la configuració de polítiques adhoc per perfils que li puguin ser sol·licitades.
- La gestió dels IOCs relacionats amb l'EDR, tant en llista blanca com en llista negra.
- Gestionar les vulnerabilitats dels dispositius sota control de l'EDR i farà els informes de vulnerabilitats relacionats, tal i com es descriu a l'apartat 4.1.1 d'aquest document.
- Suport a la integració de l'agent EDR en els nous equips en què hagin de ser instal·lats.
- Comprovar i testejar aleatòriament, amb periodicitat setmanal, que les sondes i agents de l'EDR funcionen correctament i generen alertes que acaben ingestades en el SIEM.

4.3.2. Administració Antispam

El servei de gestió i administració tècnica de la plataforma antispam ha d'incloure diverses tasques essencials per garantir que el sistema funcioni de manera òptima, protegint eficaçment contra correus electrònics no desitjats i potencialment perillosos.

A més de les tasques d'administració tècnica que s'han establert com a genèriques, la plataforma antispam inclourà tasques especifiques més importants que s'han de considerar:

- Alertes i Notificacions: Configurar alertes automàtiques per a incidents de spam i activitats sospitoses.
- Actualització de Filtres i Regles: Actualitzar regularment els filtres i regles de detecció de spam basats en les últimes amenaces i patrons de spam.
- Ajustos de Configuració: Ajustar la configuració del sistema per optimitzar la detecció i filtratge de spam sense afectar la lliurament de correus legítims.
- Integracions: Integrar la plataforma antispam amb els altres sistemes i eines de TMB.
- Llistes Blanques i Negres: Gestionar llistes blanques (whitelists) i llistes negres (blacklists) de remitent.
- Revisions Periòdiques: Revisar i actualitzar periòdicament aquestes llistes per mantenir la seva efectivitat.

4.3.3. Administració CASB/SSE

El servei de gestió i administració tècnica de la plataforma CASB (Cloud Access Security Broker) te com objectiu que la plataforma CASB funcioni de manera efectiva, protegint l'empresa contra amenaces i garantint la seguretat i compliment normatiu en l'ús de serveis al núvol.

A més de les tasques d'administració tècnica que s'han establert com a genèriques, la plataforma CASB inclourà tasques especifiques, les més importants que s'han de considerar:

- Monitoratge en temps real: Supervisar l'activitat dels usuaris i els dispositius en aplicacions al núvol per detectar comportaments anòmals i possibles amenaces.
- Alertes i Notificacions: Configurar alertes automàtiques per a incidents de seguretat, accessos no autoritzats i activitats sospitoses.
- Configuració: Configurar la plataforma CASB per a la integració amb les aplicacions i serveis al núvol utilitzats per l'empresa.
- Definició de Polítiques: Establir i mantenir polítiques de seguretat per a l'accés i ús de les aplicacions al núvol.
- Ajustos de Polítiques: Ajustar les polítiques basades en els resultats del monitoratge i noves necessitats.
- Revisions Periòdiques: Realitzar revisions periòdiques del sistema per assegurar-se que funciona correctament i detectar possibles vulnerabilitats.
- Millores i Noves Funcionalitats: Implementar millores i noves funcionalitats en la plataforma CASB.
- Integracions: Integrar la plataforma CASB amb altres sistemes de seguretat i eines de gestió de l'empresa.
- Control d'Accessos: Gestionar i controlar els accessos dels usuaris a les aplicacions i serveis al núvol segons les polítiques establertes.

- Auditoria d'Accessos: Realitzar auditories periòdiques dels accessos per assegurar-se que només els usuaris autoritzats tinguin accés a la informació sensible.

El proveïdor té com a missió proporcionar una solució integral i prospectiva de seguretat que protegeixi, garanteixi, possibiliti i millori el negoci actual i futur del client. El Servei Security Edge del proveïdor ha de comptar i aprofitar-se de les sinergies del Security Operation Center (SOC) del proveïdor.

El Servei Security Edge gestionat pel proveïdor ha d'estar destinat a proporcionar seguretat al perímetre del negoci, on el núvol i el treball des de qualsevol lloc i dispositiu han suposat una transformació radical, permetent al client tant delegar la gestió de la protecció de la navegació web i l'accés a les seves aplicacions corporatives, així com la gestió d'incidents de seguretat en un equip expert (SOC), permetent fer focus en aquelles tasques de més valor per al nucli del seu negoci.

S'ha de fer un acompanyament en l'evolució quant a l'aplicació de polítiques (DLP, Navegació, etc) i de Conscienciació/educació de l'usuari perquè hi hagi una maduració quant a l'ús que fan els usuaris de les plataformes SaaS. Mitjançant les Best Practices i l'experiència del proveïdor amb altres clients, es proposarà la millor manera per anar evolucionant cap al millor control de la seguretat dels clients mitjançant les diferents funcionalitats de CASB inline, CASB API, Security Gateway, etc.

Es farà un seguiment periòdic de l'estat de salut i de reporti del comportament dels usuaris, i una estratègia de millora contínua.

4.3.4. Administració eina gestió vulnerabilitats

L'objectiu de la Gestió de vulnerabilitats és identificar vulnerabilitats o debilitats de seguretat conegudes o potencials a les xarxes i sistemes d'informació de TMB davant d'atacs externs i interns i aplicar els ajustaments o configuracions que permetin corregir-les.

Dins aquest àmbit, allò que se sol·licita concretament a l'adjudicatari d'aquest servei és l'administració tècnica de la plataforma amb responsabilitat sobre les tasques genèriques que s'han establert per a globalment aquest capítol.

Hi haurà altres proveïdors que seran usuaris de la plataforma i que la utilitzaran per realitzar l'anàlisi i la remediació de les vulnerabilitats detectades.

En tot cas, si serà responsable d'aquest servei donar resposta a consultes tècniques o peticions de suport o de configuració que aquests altres actors li sol·licitin.

4.3.5. Administració Eines CCN-CERT

Se sol·licita la gestió de les eines de CCN-CERT, així com la conveniència de fer-les servir o substituir-les per altres serveis que disposi el client.

Actualment es disposa de microCLAUDIA i CLARA, que són d'ús gratuït proporcionats pel CCN-CERT, però que requereixen un servei de gestió que haurà de proporcionar el proveïdor de la licitació i si cal, l'escalat d'incidències/bugs amb CCN- CERT i potser fabricants de tercers.

També és possible la necessitat de gestió d'un altre tipus de serveis que CCN-CERT pugui recomanar com a LUCIA, que és una eina per a la gestió d'incidents de seguretat (Llistat Unificat de Coordinació d'Incidents i Amenaces).

Està desenvolupada pel CCN-CERT per a la Gestió de Ciberincidents a les entitats de l'àmbit d'aplicació de l'Esquema Nacional de Seguretat. Amb ella es pretén millorar la coordinació entre el CERT Governamental Nacional i els diferents organismes i organitzacions amb què col·labora.

4.4. Equip de Resposta davant d'Incidències de Seguretat i anàlisis forense (CSIRT)

L'equip que oferirà el servei en base als següents recursos:

- 20 jornades anuals (8x5) + 5 jornades anuals (fora 8x5), d'especialistes per a gestió d'incidents d'impacte, investigació, anàlisis forense o altres tasques especialitzades a petició de TMB.

La metodologia requerida haurà de ser aprovada pel CCN-CERT, d'acord amb l'Esquema Nacional de Seguretat (ENS) i que està referenciada a les guies CCN-STIC-403 i CCN-STIC-817.

Aquest servei ha de cobrir com a mínim:

- Possible activació des del servei de Monitorització del SIEM i/o de l'operació EDR, així com a petició de TMB o de la Oficina Tècnica.
- Capacitats de recerca i anàlisi forense:
  - Avaluació inicial i d'evidències preliminars.
  - Extracció i recol·lecció d'evidències sobre sistemes compromesos
  - Contextualitzar l'amenaça, avaluar el nivell de compromís, possibles moviments laterals, escalada de privilegis, etc.
- Resposta i remediació
  - Coordinació durant l'incident amb l'equip de Seguretat TIC de TMB.
  - Suport sobre l'execució de la contenció per minimitzar l'impacte.
  - Suport a l'erradicació, recuperació del servei
  - Monitorització i control post incident
- Anàlisi de codi maliciós
  - Identificar el comportament dels artefactes
  - Identificar els IOC aplicables a la infraestructura de seguretat de TMB per a detecció i bloqueig posteriors
  - Identificar els seus mecanismes de propagació
- Informes tècnics de l'incident

- Informe de detall de tota la investigació de gestió de l'incident i de la possible anàlisi del codi maliciós (malware)

- Lliçons apreses i propostes de millora

4.5. Vigilància Digital

Es demana el servei de Vigilància Digital per tal de protegir el negoci, marca i reputació contra els riscos que sorgeixen de la transformació digital.

El servei ha de presentar un enfocament holístic que cobreixi tant la web oberta com la deep i la dark web, proporcionant informació accionable sobre amenaces que permeti reduir els atacs exitosos disminuint la superfície d'atac i ajudar a detectar possibles bretxes de seguretat i accelerar la recuperació.

TMB haurà de disposar d'accés al MISP (Plataforma d'Intel·ligència d'Amenaces) dins del servei de Threat Intelligence per accedir als IOC. Així que es podran consumir aquests indicadors automàticament sense cost addicional per a TMB.

Aquesta plataforma haurà de poder ser accedida per serveis d'automatització, per exemple si és via Web, a través d'una API que permeti consultar les deteccions, a fi de poder automatitzar les accions a realitzar. Per tant, que no exclusivament es pugui accedir als continguts de la plataforma a través de l'accés manual. La idea és poder automatitzar un procediment en quant a la plataforma aparegui un contingut detectat per la Intel·ligència d'Amenaces.

El servei de Vigilancia Digital, inclourà la subscripció a una newsletter de seguretat del propi servei (que inclogui informació sobre Vulnerabilitats, Malware, organitzacions criminals actives,...) sense cost addicional per TMB.

El servei de Vigilància digital es prestarà sobre els següents àmbits:

- Reputació i marca
  - Ús no autoritzat de marca
  - Dominis sospitosos
  - Counterfeit
- Frau en línia
  - Apps mòbils sospitoses
- Disrupció del negoci
  - Robatori de credencials

Reputació i marca

Ús no autoritzat de marca

S' identificaran aquells llocs web i continguts en xarxes socials o altres plataformes, que pretenguin suplantar o aprofitar-se de la imatge i reputació del client per confondre l' usuari final mitjançant l' ús de la seva marca, logo o imatge.

Per a això es monitoritzaran xarxes socials, canals relacionats amb el sector del client i blogs a la recerca d'usos no autoritzats de les seves marques.

Dominis sospitosos

Es detectaran aquells nous registres de dominis que continguin en el seu nom paraules clau directament relacionades amb el client. Aquest mòdul es complementa a més amb capacitats de typosquatting basades en algoritmes de similitud i proximitat:

- Similitud: reemplaçant certs caràcters per altres similars o deformant les paraules perquè siguin visualment iguals.
- Proximitat: eliminant o reemplaçant només certs caràcters.

A més, es proporcionarà sempre que estigui disponible, la informació de registre (WHOIS) associada als dominis sospitosos identificats. Per a això es consultaran les bases de dades dels dominis d'alt nivell (TLDs, incloent ccTLD i gTLD), prenent com a referència els dominis registrats pel client.

Counterfeit

S'identificaran canals de comercialització no autoritzats en els quals es trobin disponibles productes del client, falsificacions d'aquests, rèpliques, productes de segona mà o que simulin ser un canal oficial de distribució.

Per a això es monitoritzaran xarxes socials, plataformes de venda/compravenda online, canals relacionats amb el sector del client, canals de distribució no oficials, publicitat, blogs i fòrums relacionats amb el seu sector.

Frau en línia

Apps mòbils sospitoses

Es detectarà la publicació d' aplicacions mòbils sospitoses relacionades amb el client o la suplantació de les aplicacions oficials facilitades per ell, amb el possible objectiu de confondre els seus usuaris per obtenir credencials, dades personals o infectar-les amb algun tipus de malware.

Per a això es monitoritzaran els mercats mòbils oficials (Apple Store, Google Play), així com mercats mòbils alternatius, identificant aquelles aplicacions mòbils amb referències al nom del client o a la seva marca.

Disrupció de negoci

Robatori de credencials

S' identificaran credencials que s' hagin vist compromeses, ja sigui en una fuita o en un robatori, i corresponguin amb permisos d' accés a sistemes, instal·lacions i processos relacionats amb el client.

Per a això es monitoritzaran fonts públiques, com plataformes de compartició d'informació (pastes), i informació recollida per botnets (crime servers). Així com llocs de la Deep i Dark Web, en cas d'haver contractat aquest àmbit de monitoratge.

Per als robatoris, es proporcionarà a més la informació de context disponible: nom d'usuari, contrasenya (en cas de ser de serveis de tercers o de pertànyer a col·laboradors o clients es

mostrarà ofuscada), url del servei afectat, tipus d'usuari afectat, ubicació del servei afectat, organització del servei afectat, data de compromís, domini de l'usuari compromès, host del servei afectat, port del servei afectat, tipus de botnet associada, evidència.

El servei no inclou la verificació de la validesa o vigència de les credencials.

Consum de les accions de Takedown per la resposta a amenaces

L'objectiu prioritari en la resolució d'amenaces, i al qual estan enfocades totes les capacitats de resposta del Servei, és la gestió del tancament del lloc que allotja l'amenaça (i/o els llocs intermedis que donen accés al frau, com proxy, dns, etc.), mentre es mitiga paral·lelament el seu potencial impacte. Per a això s'analitzarà el tipus d'informació publicada i la naturalesa del dany (drets d'autor, propietat intel·lectual...), i, en base al mitjà de difusió i a la legislació aplicable, es procedirà a realitzar les gestions pertinents en nom del client. En aquest punt cal tenir en compte que les capacitats de resposta s'apliquen únicament sobre aquelles fonts del servei que són públiques.

Per gestionar aquestes accions, el proveïdor necessitarà comptar amb els documents que acreditin el registre de les marques del client als països en els quals estigui disponible, dades de contacte de la persona o departament en client per a la gestió de casos que requereixin firma de Digital Millennium Copyright Act (DMCA) i una autorització expressa que autoritzi el servei Digital Risk Protection del proveïdor a actuar en el seu nom. No comptar amb aquests documents podrà demorar o fins i tot impossibilitar la correcta resolució del cas.

En alguns casos és possible que sigui necessari que el client gestioni directament certes accions, fonamentalment qüestions d'índole legal. En aquest cas, la tasca del proveïdor es limitaria a aportar les evidències o informació disponible. Les tasques d' assessorament legal al client es troben fora de l' abast del servei.

Sempre que el servei iniciï les gestions de tancament d' un cas, aquest cas es descomptarà de la bossa contractada. En determinades circumstàncies, és possible que el proveïdor realitzi totes les accions al seu abast i no s' arribi a un nivell de resolució adequat. Quan es doni aquesta situació, o passats un màxim de 60 dies des de l' inici de les gestions, el proveïdor tancarà el cas. Per a aquesta sèrie de casos, el proveïdor proporcionarà al client les evidències recol·lectades durant el procés de gestió del cas en qüestió.

El tancament d'una amenaça ve definit mitjançant l'agrupació dels diferents recursos maliciosos (URLs, adreces IPs, comptes de correu, etc.) en unitats denominades casos, segons els següents criteris:

Per a les amenaces de Phishing i pharming i Malware, aquesta agrupació es duu a terme mitjançant l' aplicació d' una sèrie de regles o criteris:

- Per a un mateix instant de temps, tots els recursos online d'un mateix domini o adreça IP s'agrupen dins d'un únic cas (ex. http://fraude1.dominioX.com; http://fraude2.dominioX.com; etc.).
- De la mateixa manera, dins d'un mateix cas només poden existir URLs d'un mateix domini (ex. fraude.com) o adreça IP (ex. http://123.123.123.123/fraude).

- Si el frau està allotjat en un sol lloc, però és accessible des de múltiples noms de domini o adreces IP, tots aquests recursos seran tractat com un únic cas.
- Si una amenaça inclou recursos maliciosos en diferents dominis allotjats en llocs diferents (diferents ISPs, empreses de hosting, etc.) es tractaran com a casos separats dins de la mateixa amenaça.
- En el cas que, posterior a la resolució d'un cas, reapareguin URLs (les mateixes o altres de noves) pertanyents al mateix domini o adreça IP ja tractada, es reobrirà de nou el cas (sense cost associat), sempre que no s'hagi complert el període de garantia (48 hores). Per contra, en el cas que el període de garantia hagués expirat, s'obrirà un nou cas (cas fill), el qual serà relacionat al Portal amb el cas anterior (cas pare) i es comptabilitzarà com un nou cas.
- Els elements associats a un cas que no formin part intrínseca del recurs maliciós principal (i per tant el seu tancament no condueixi a la resolució final del frau en qüestió) seran gestionats com a relacions del cas, i no seran comptabilitzats com a cas. En aquest sentit, el criteri que definirà cada resolució dependrà directament de la naturalesa del frau. A tall d' exemple, podríem esmentar els següents escenaris:
  - Una web redirectora a una pàgina de phishing serà generalment tractada com a relació d'un cas (web de phishing)
  - Un compte de correu podrà ser gestionat com a relació (ex. correu electrònic contenint la URL de la web de phishing) o com a cas en si mateix (ex. estafa de carta nigeriana).

  Per a la resta de les amenaces, cada recurs maliciós (perfil social, aplicació mòbil, pastís, etc.) es correspondrà amb un cas.

Peticions sota demanda

El proveïdor ha de disposar de tots els mòduls, encara que TMB, inicialment partirà dels mòduls indicats, podent utilitzar-se els indicats, de la bossa d'hores dedicades per a projectes de l'Oficina Tècnica:

- Reputació i marca
  - Contingut ofensiu (A demanda)
  - Seguiment d'identitat digital (A demanda)
- Frau en línia
  - Phishing y Pharming (A demanda)
  - Programari maliciós (A demanda)
  - Carding (A demanda)
- Disrupció del negoci
  - Exposició d'informació (A demanda)
  - Hacktivisme (A demanda)
  - Activisme (A demanda)

    Vulneració de mecanismes de seguretat (A demanda)

4.5.1. Abast

- 8 Marques
- 17 dominis externs
- 4 dominis interns
- 4 dominis de correu
- 14 IPs de serveis públic
- 300 IPs públiques
- 2 Productes Web (venda i Att client)
- 15 Perfils de Xarxes Socials
- 4 Aplicacions mòbils
- 50 Accions de takedown
- 10 jornades d'analista de Seguretat per a cerques a Dark Web o altres peticions relacionades a l'àmbit de Vigilància digital a petició de TMB.

5. Acords de nivell de servei (SLA)

Monitorització/Operació 24x7

En la següent taula es mostren els SLA pel servei:

TEMPS DE RESPOSTA

Prioritat	Període de Notificació	Nivell de suport
Crítica	30 minuts (*)	24/7
Alt	1h (*)	24/7
Mitja	4h (*)	24/7
Baixa	NBD (*)	24/7

(*) la mètrica objectiu fa referencia a la **primera acció de resposta**, no a que l'incident s'hagi gestionat per complet dins d'aquest període de temps.

Classificació de les prioritats:

Prioritat	Descripció

Crítica	TMB ha confirmat que la xarxa està essent atacada de forma sostinguda, i/o que s'ha produït un brot de virus a gran escala (o que afecti a actius crítics), i/o ha identificat una bretxa a gran escala, que afectarà de forma imminent la reputació o el negoci del Client (inclosa una violació del treball confidencial, Registres de Salut o altres dades controlades).
Alta	La infraestructura de TMB està sota un atac sostingut i/o diversos sistemes es veuen afectats per un virus, i/o s'ha identificat una violació a gran escala que no inclou un impacte immediat en la reputació comercial del client (treball no confidencial, informació personal identificativa comuna com correu electrònic i nom d'usuari), i/o s'informa d'un atac immediat contra el client en els mitjans de comunicació.
Mitja	Un sol servidor (no crític) es veu compromès per malware o les credencials d'un sol usuari estan exposades a través de malware o pirateria.
Baixa	El sistema d'un sol usuari està compromès per malware, No és un atac d'impacte.

Resposta d'avant d'incidències de Seguretat i anàlisi forense (CSIRT)

En la següent taula es mostren els SLA pel servei:

TEMPS DE RESPOSTA

Prioritat	Període de Resposta	Nivell de suport
Crítica	1h	24/7
Mitja	4h	24/7
Baixa	8h	24/7

Classificació de les prioritats:

Prioritat	Descripció
Crítica	Incidents que tenen un impacte considerable (afectació a la confidencialitat, disponibilitat i la integritat) a informació considerada crítica per a l'activitat de TMB i/o sistemes TIC crítics. L'incident amb capacitat d'afectació a gran quantitat d'informació valuosa i causar la degradació de serveis vitals de TMB. Aquests incidents poden ser típicament, malware destructiu, denegació de serveis, compromís de sistemes, incidents de hacking i violacions de polítiques que afectin sistemes crítics o informació crítica per TMB.
Mitja	Un sol servidor (no crític) es veu compromès per malware o les credencials d'un sol usuari estan exposades a través de malware o pirateria.
Baixa	Incidents de seguretat en sistemes no crítics per a TMB.

Penalitzacions aplicables al servei regular (TAULA 5.1)

Àmbit	Descripció ANS	Càlcul	Periodicitat del càlcul	Llindar de compliment	Tipus
Monitorització	Temps màxim de resposta per incidències Crítiques i Altes	Temps objectiu transcorregut entre que es detecta/notifica fins que es genera una resposta del servei.	S'avaluarà el càlcul mensualment.	**Crítiques** >60 minuts (previst 30m) **Altes** >2h (previst 1h) **Mitja** >8h (previst 4h)	Molt greu Greu Lleu
Resposta d'avant d'incidències de Seguretat i anàlisi forense (CSIRT)	Temps màxim de resposta per incidències Crítiques i Altes	Temps objectiu transcorregut entre que es notifica al CSIRT fins que es genera una resposta del servei.	S'avaluarà el càlcul mensualment.	**Crítica** >2h (previst 1h) **Mitja** >8h (previst 4h) **Baixa** >NBD (24h) (previst 8h)	Molt greu Greu Lleu
Oficina Tècnica	Activitats del servei de Pentesting executades.	Diferència entre el nombre d'escanejos previstos i el nombre d'escanejos realitzats.	S'avaluarà el càlcul mensualment.	Inferior l'establert (4 simulacres x quadrimestre)	Lleu
Oficina Tècnica	Notificació immediata de deteccions amb risc crític, molt alt i alt cap al responsable del	Diferència entre vulnerabilitats presents als informes i notificacions efectuades.	S'avaluarà el càlcul mensualment.	Immediat en tenir confirmació de la detecció.	Lleu

	servei segons procediment.				
Monitorització	Temps màxim de lliurament d'informes de tancament en cas d'incidències crítiques.	Dies transcorreguts des de la data fixada pel seu lliurament	S'avaluarà el càlcul mensualment.	2 dies laborables.	Molt lleu
Oficina Tècnica	Temps de resposta a la petició sota demanda.	Dies transcorreguts entre la demanda i la resposta rebuda del contractista.	S'avaluarà el càlcul mensualment.	5 dies laborables.	Molt lleu
Oficina Tècnica	Informe resum del Comitè Estratègic de seguiment del servei.	Presentació de l'informe 2 dies laborables posteriors a la reunió	S'avaluarà el càlcul mensualment.	10 dies laborables posteriors a la data establerta d'entrega (2 dies després de la reunió)	Molt lleu
Oficina Tècnica	Informe resum del Comitè Tàctic mensual de seguiment del servei.	Presentació de l'informe 2 dies laborables posteriors a la reunió	S'avaluarà el càlcul mensualment.	10 dies laborables posteriors a la data establerta d'entrega (2 dies després de la reunió)	Molt lleu
Oficina Tècnica	Revisió del correcte funcionament de les plataformes de seguretat (si no s'inclou al comitè tàctic)	Presentació de l'informe 2 dies laborables posteriors a la reunió	S'avaluarà el càlcul mensualment.	10 dies laborables posteriors a la data establerta d'entrega (2 dies després de la reunió)	Molt lleu

6. Confidencialitat

L'empresa col·laboradora ha d'acceptar la Política de Seguretat Tecnològica i de la Informació de TMB. L'adjudicatari es compromet a no difondre i guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del servei actual i a la qual només el personal autoritzat per TMB. L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir pel personal sota el seu càrrec.

Se l'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.

Una vegada finalitzat el present servei 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'empresa col·laboradora ha d'acceptar el compromís de confidencialitat respecte a les dades a les quals tindrà accés i que són propietat de TMB.

Els permisos d'accés als sistemes i aplicació, en cas de ser necessari, tindran el nivell necessari per al treball a realitzar i assignats a usuaris personals. En cas de precisar de l'accés amb un usuari amb privilegis elevats en el sistema es durà a terme a través de l'eina que disposa TMB per a aquest fi, de manera que quedin traçades les accions que es realitzin.

Compliment de la llei Orgànica de Protecció de Dades de Caràcter Personal

L'adjudicatària 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 pel que fa 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.

7. Model de relació

Estarà basat en la figura de l'interlocutor/coordinador únic entre l'adjudicatari i TMB.

Aquest interlocutor és fonamental per a acompanyar i donar suport en l'establiment de les polítiques, bones pràctiques i controls de seguretat en l'àmbit del servei.

7.1. Governança i reporting

El govern del servei de ciberseguretat gestionada ha de complir:

- Gestió centralitzada a nivell transversal i de tots els sub-serveis.
- Generació la capa de reporting a diferents nivells, tàctic i operatiu.
- Garantia de la implementació d'un Quadre de comandament (Dashboard) integral amb tots els indicadors identificats dels diferents subserveis.

7.2. Model organitzatiu de l'equip de treball

El present servei objecte de licitació ha de permetre certa autosuficiència a l'hora de contactar, gestionar i resoldre qualsevol tipus d'incidències o tasques de projectes que impliquin proveïdors externs, sense que la interlocució depengui exclusivament del responsables de TMB.
Per donar resposta a les necessitats plantejades per TMB, es demana tenir un model de relació basat en 3 nivells, amb l'objectiu de:

- Garantir el seguiment i bon govern del servei.
- Maximitzar el seu alineament a les necessitats estratègiques i operatives de TMB mentre duri la prestació del servei.

Així doncs, aquest model organitzatiu es basa en l'establiment d'una relació entre l'adjudicatari i TMB a tres nivells i comitès:

- Nivell estratègic / Comitè estratègic.
- Nivell tàctic / Comité tàctic.
- Nivell operatiu / Comité operatiu.

7.2.1. Nivell estratègic

Es defineix a nivell estratègic un comitè executiu que es reunirà de manera ordinària dues vegades l'any amb la finalitat de mantenir un punt de contacte a alt nivell per assegurar el bon funcionament del servei contractat. A aquest nivell, es proposa que per part de l'adjudicatari hi assisteixi com a mínim la persona responsable de compte, el/la coordinadora del servei, i per part de TMB la persona responsable de la Direcció d'Operacions de TMB, així com el CISO i persones responsables de seguretat IT i OT, així com la persona/es responsable/es de la gestió del servei a TMB.
Els/les assistents a aquest comitè tindran capacitat decisòria sobre els compromisos del mateix i en aquells aspectes que puguin originar la modificació del servei.

7.2.2. Nivell tàctic

Es proposen reunions mensuals per poder dur a terme un seguiment del servei i poder posar en comú els punts que es considerin necessaris exposar. Per part de l' adjudicatari, hi assistirà el coordinador del servei i, si fos necessari, un o més especialistes de servei que puguin aportar informació rellevant del servei.

Per part de TMB hi assistirà, el responsable del servei i, si fos necessari, els tècnics especialistes.
La finalitat d'aquestes reunions mensuals serà exposar:

- L'estat del servei.
- Les principals incidències que hagin sorgit o estiguin en actiu.
- La situació dels projectes i tasques en curs.
- Revisió del calendari previst.

7.2.3. Nivell operatiu

Es proposa una reunió setmanal de revisió tècnica tipus "clínic" per poder resoldre els temes més urgents que hi pugui haver i fer seguiment tècnic dels projectes i tasques. Per part del proveïdor adjudicatari hi assistirà el coordinador o els especialistes involucrats si ho vol delegar i per part de TMB hi assistiran el responsable del servei i els tècnics especialistes de seguretat necessaris.
L'objectiu bàsic serà tractar les problemàtiques específiques que afectin al servei prestat.

7.2.4. Funcions i activitats dels nivells del model organitzatiu

Nivell estratègic / Comitè estratègic:

- Seguiment i control de l'execució del contracte.
- Seguiment i avaluació del servei prestat. Analitzarà les necessitats del servei i podrà decidir ampliacions o reduccions del mateix. Validar l'abast general, objectius i resultats esperats.
- Validació de la planificació de les tasques previstes a realitzar.
- Verificació del compliment de les especificacions sol·licitades.
- Propostes de modificacions/ampliacions d'Acords de Nivell de Servei (ANS).
- Seguiment econòmic del contracte.
- Resolució de conflictes.
- Lliurables mínims esperats:
    - Abans de la convocatòria:
        - Assistents convocats.
        - Ordre del dia.
        - Documentació auxiliar.
        - Informes necessaris dels temes a tractar.
    - Després de la reunió:
        - Acta amb els acord assolits i la presa de decisions.
        - Convocatòria per la següent reunió: data, hora i lloc.

Nivell tàctic / Comitè tàctic:

- Validació de les tasques de control de l'explotació i implantació dels serveis.
- Revisió d'informes mensuals dels diferents serveis.
- Verificació de l'acompliment dels acords de servei establerts.

- Aprovació de projectes de millores.
- Seguiment de la realització de millores i evolució del servei regular.
- Verificació de l'acompliment dels ANS.
- Resolució de conflictes.
- Anàlisi i priorització de tasques.
- Validació dels procediments de millora per part dels Responsables de Seguretat.
- Anàlisi i control de l'ocupació dels perfils assignats per la consecució del servei (informe setmanal i acumulat mensual).
- Lliurables mínims esperats:
    - Abans de la convocatòria:
        - Assistents convocats.
        - Ordre del dia.
        - Ordre del dia.
        - Informe seguiment del servei
        - Documentació auxiliar.
        - Informes necessaris dels temes a tractar.
    - Després de la reunió:
        - Acta amb els acord assolits i la presa de decisions.
        - Convocatòria per la següent reunió: data, hora i lloc.

Nivell operatiu / Comitè operatiu:

- Seguiment rutinari.
- Propostes de millora i canvis.
- En cas d'identificar-se riscos o canvis significatius en l'evolució del servei es convoquen les reunions operatives per tractar el tema en qüestió.
- En cas d'evidenciar un risc elevat, es procedirà a convocar el Comitè Estratègic o al Comitè Tàctic segons es consideri.
- Anàlisi d'incidències detectades dels operadors que impliquen sol·licitar una reunió operativa.
- Anàlisi de peticions que impliquin un control detallat degut a un impacte tècnic, econòmic, d'execució, etc.
- El comitè podrà ser convocat per iniciativa tant de TMB com de l' adjudicatari. El comitè es constituirà en un màxim de 24h des del moment de la convocatòria.
- Lliurables mínims esperats:
    - Abans de la convocatòria:
        - Assistents convocats
        - Ordre del dia
        - Ordre del dia
        - Documentació auxiliar
        - Informes necessaris dels temes a tractar
    - Després de la reunió:
        - Acta amb els acord assolits i la presa de decisions.
        - Convocatòria per la següent reunió: data, hora i lloc

8. Prestació del servei

8.1. Horari

L'adjudicatari haurà de cobrir els horaris de dilluns a divendres entre les 08:00 AM i les 14:00 PM, inclòs el període vacacional on es mantindrà operatiu el servei.
L'adjudicatari cobrirà fora de l'horari laboral definit la recepció i resolució d'incidents de nivell crític alt.
Aquest horari no aplicarà pels serveis requerits 24x7x365 especificats als serveis regulars.

8.2. Localització física

La prestació del servei objecte d'aquesta contractació ha de complir amb els ítems següents:

Tret de la presència del Service Manager (que serà d'almenys 3 dies en presencial), l'execució de les tasques es durà a terme principalment de forma remota.

No obstant això, si TMB ho considera, per la naturalesa de la invenció o incidència, pot demanar realitzar les tasques de forma presencial. En aquet cas, de no indicar una altra cosa, es faran a l'oficina de TMB situada a la següent adreça:

Centre de Suport Tecnològic
C/Josep Estivill, 47
08027, Barcelona

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

La sol·licitud dels serveis es realitzarà, en els casos que no es tracti d'incidència, amb un període d'antelació, a convenir entre les parts, mai superior a una setmana natural.

El servei disposarà d'un referent que serà l'interlocutor amb el responsable del servei de TMB i es disposaran dels recursos necessaris per finalitzar les tasques en les dates acordades.

Es presentarà una planificació dels treballs a realitzar per acordar amb TMB la durada del treball en cas que es tracti de tasques que permetin aquesta planificació.

TMB facilitarà que l'adjudicatari realitzi les tasques i les reunions de forma virtual utilitzant eines de videoconferència, eines col·laboratives o de connectivitat segura.

A petició de TMB, algunes reunions o actuacions seran de presencialitat obligada, entre altres poden ser:

- Les reunions de nivell estratègic, tàctic i operacional.

- Les incidències de seguretat de nivell alt.
- Les tasques que requereixin la realització d'entrevistes o recollida d'evidències físiques.
- I totes aquelles tasques en que no sigui possible l'ús de la virtualitat per la realització de les mateixes.

9. Recursos del contracte

Els recursos necessaris per cobrir els serveis que es demanen serien quantificats en dedicació:

Oficina tècnica d'Operació de Seguretat

- Service Manager 1 FTE 8x5 dedicació exclusiva a TMB amb una presencialitat mínima de 3 dies a la setmana en TMB
- Equip d'analistes de seguretat 2 FTE
- Consultoria i projectes: bossa d'hores: 80 Jornades anuals

Servei d'Operació de Seguretat

- Servei Nivell 1,2,3: 24X7X365

Administració Técnica de plataformes de seguretat

- Equip d'analistes de Seguretat Tècnics especialistes: 1 FTE 8x5

Equip de Resposta davant d'Incidències de Seguretat i anàlisis forense (CSIRT)

- 20 jornades anuals (8x5) + 5 jornades anuals (fora 8x5), d'especialistes per a gestió d'incidents d'impacte, investigació, anàlisis forense o altres tasques especialitzades a petició de TMB.

Vigilància Digital

- Serveis de vigilància segon abast definit al plec
- Serveis de remediació: 50 Accions de takedown anuals

NOTA: sempre que s'indica horari 8x5 es en horari d'oficina de TMB.

Recordar que a l'abast de la licitació inclou que el proveïdor haurà de proporcionar una eina **Simulació d'Infraccions i Atac (BAS)** per poder realitzar les autories/pentesting de TMB (a tall d'exemple, Cymulate, Pentera, etc). Incloent els possibles mòduls addicionals d'escenaris avançats que siguin necessaris per prestar el servei d'una manera adequada i completa.

A continuació es detallen els tipus de perfils que l'adjudicatari haurà d'assignar al servei, amb les seves responsabilitats:

- Responsable de compte.
- Service Manager (Coordinador del servei de seguretat).
- Analistes de Seguretat / Especialistes.

- Consultors de seguretat de la informació.

9.1. Responsable de Compte

L'adjudicatari designarà un únic responsable de compte que serà el referent per tots els contractes que tingui amb TMB, i serà el darrer responsable dels de la prestació dels serveis.

Aquesta figura es mantindrà durant tota la vida del contracte en la gestió comercial, durant l'execució del servei i fins a la devolució d'aquest, i serà l'interlocutor i responsable en cas que es produeixin canvis en l'abast o cost dels serveis que impliquin una modificació contractual.

9.2. Service Manager

Serà l'interlocutor únic davant de TMB i serà el responsable de garantir que la prestació del servei és correcta. És a dir, garantirà el servei assegurant l'optimització del mateix i, per tant, minimitzant els possibles riscos.

Haurà de realitzar principalment les següents funcions:

- Garantir l'execució del servei, tal i com s'especifica en aquest plec, assegurant tots i cadascun dels temps de resposta demanats i que TMB pugui requerir.
- Coordinar i supervisar de forma periòdica l'equip al seu càrrec, comunicant si s'escau els possibles canvis en aquest, així com les seves causes.
- Gestió dels riscos detectats així com la presentació del pla de mitigació dels mateixos.
- Detectar oportunitats de millora.
- Elaboració dels informes de servei i justificació del compliment dels ANS.
- Garantir la implementació del quadre de comandament del servei .
- Proposar i incorporar, si són acceptades, millores en la gestió global del servei.

En quant al recurs assignat, TMB tindrà la potestat de demanar canvi sempre i quan, i de manera justificada, aquest no presti el servei de forma satisfactòria per TMB.

L'adjudicatari es compromet a mantenir el coordinador durant la vigència del contracte, podent-lo substituir només per causes justificades. En aquest cas, la persona que el substitueixi haurà de complir amb la solvència requerida, sent TMB qui validarà que el perfil s'ajusti a la solvència.
Per altra banda, l'adjudicatari haurà de sol·licitar per escrit qualsevol canvi en el perfil i amb una antelació suficient que garanteixi un correcte traspàs de coneixements per tal d'evitar afectacions en el servei. El canvi només podrà fer-se si prèviament s'ha validat per TMB el compliment dels requisits de solvència anteriorment mencionats.

9.3. Analistes de Seguretat / Especialistes

Els especialistes seran els tècnics assignats al servei per l'adjudicatari que duran a terme les tasques i actuacions que requereixin una especialització tècnica per poder garantir un resultat satisfactori.
L'equip de l'adjudicatari que prestarà el servei a TMB comptarà amb treballadors que tinguin perfils d'especialistes al menys en els següents àmbits:

- Tècnic especialista en hacking ètic i pentesting.
- Analista de seguretat.
- Auditor en seguretat de la informació i continuïtat de negoci.
- Tècnic especialista en seguretat de la resposta a incidents de seguretat de la Informació.
- Professional certificat en seguretat de la informació en entorns cloud.
- Tècnic administrador de plataformes tecnològiques (SIEM).
- Tècnic especialista en informàtica forense i investigació interna

Tant el coordinador del servei com els perfils especialistes assignats al servei hauran de complir els requeriments expressats a l'apartat de solvència tècnica del PCP.

9.4. Consultors en seguretat de la informació

El perfil de consultors en seguretat de la informació o consultors en ciberseguretat son qui prestaran el servei basat en bossa d'hores/Jornades.

Aquests perfils han de complir les següents capacitats o competències:

- Coneixement profund en les millors pràctiques de seguretat de la informació i les tendències actuals en ciberseguretat.
- Capacitat per avaluar riscos i definir estratègies de mitigació.
- Coneixement de les regulacions de seguretat de la informació rellevants com RGPD.
- Capacitat per traduir problemes tècnics en termes de comprensibles per les persones no tècniques.
- Habilitat per analitzar situacions complexes de seguretat i trobar solucions efectives.
- Capacitat per crear informes de executius clars i concisos que resumeixin troballes o recomanacions de seguretat de manera comprensible per l'alta direcció o altres stakeholders.
- Habilitat per presentar dades tècniques i mètriques de seguretat de manera visualment atractiva mitjançant gràfics i taules.
- Experiència en la redacció d'informes d'avaluació de riscos i documentació tècnica que recolzi la presa de decisions informades en seguretat de la informació.
- Capacitat per gestionar una crisi en cas d'incident greu de seguretat.
- Compromís amb l'aprenentatge constant i l'actualització de coneixements, donat que la ciberseguretat és un camp en constant evolució.