PLEC DE CLÀUSULES TÈCNIQUES

Contracte relatiu al **Subministrament de llicències SSE-CASB i serveis professionals d'implantació** per **Ferrocarril Metropolità de Barcelona, SA, Transports de Barcelona, SA, Projectes i Serveis a la mobilitat SA, Fundació TMB i Transports Metropolitans de Barcelona, SL**

CPV 48732000-8 - Paquets de programes de seguretat de dades

Expedient número: 15012864
Procediment obert

Aprovat en data 24 de Febrer del 2025

Transports Metropolitans de Barcelona

Ernest Costa Lluch
Responsable de Sistemes de Ciberseguretat

1. Prescripcions tècniques

1.1. Objecte i Abast

Aquest document constitueix el plec de requeriments tècnics que ha de regir el contracte de la Servei de Seguretat d'Accés al Núvol (CASB).

1.2. Situació Actual

L'adopció de serveis Cloud com l'Office 365, ha portat un nou paradigma que aporta diferents beneficis als usuaris, com poden ser la flexibilitat, elasticitat i agilitat. No obstant això, aquests beneficis han vingut acompanyats amb l'aparició de nous riscos. Els serveis Cloud estenen els recursos informàtics més enllà del perímetre corporatiu, la qual cosa resulta en una pèrdua de control sobre els actius d' informació, essent necessària la capacitat de garantir la seguretat en productes, serveis, i aplicacions, independentment del tipus de núvol que adoptem.

El present document de selecció té com a objectiu, la licitació per la implantació d'una eina de tipus SSE amb capacitats CASB i DLP, per aconseguir una protecció a l'usuari, independentment de la seva ubicació i des d'on es connecti. El SSE actua com a punt de control de tràfic dels usuaris cap a internet, entenent per internet SaaS, IaaS i Web.

Es pretén que la Seguretat en el tràfic sigui transparent per l'usuari però que a la vegada, no es deixi d'inspeccionar protegint la informació de TMB, proveint de visibilitat (Monitorització de l'usuari, comportament i forense) i seguretat de les dades (a través de control d'accés, prevenció de fuga d'informació, entre altres opcions).

El producte de CASB ens ha de servir per poder protegir el Servei Cloud d'Office365 que és el SaaS que utilitza TMB com a ús corporatiu, però sense oblidar possibles altres usos de protecció d'altres serveis SaaS o IaaS al Cloud que TMB decideixi protegir, així com aplicacions Web.

2. Prestacions Objecte del Contracte

L'objecte del present Plec de prescripcions Tècniques (PPT) es la definició del Servei de Seguretat d'Accés al Núvol (SSE/CASB).

Els serveis inclosos en aquesta contractació s'indiquen a continuació:

- LOT 1: Subscripció llicencies SSE (que compleixi els requisits de l'Annex 1)
- LOT 2: Serveis Professionals d'implantació

LOT 1: Subscripció llicencies SSE:

Subscripció al servei d'una solució SSE de protecció de l'accés a O365 i altres plataformes SaaS i Web.

Per la cobertura 7.950 usuaris esporàdics + 1.700 usuaris d'ús intensiu, i per una durada de 3 ANYS.
Cal considerar aquesta diferenciació d'usuaris ja que, a la vegada, disposen de llicències de O365 diferents (F3 i E1 respectivament), també per l'ús diferents que en fan del servei.

Ha de complir els requisits de l'Annex 1 del PPT

Entenem per usuaris esporàdics, els usuaris que no disposen d'un equip informàtic en el seu lloc de treball, com per exemple els conductors de bus/metro, etc i per tant l'ús dels serveis SaaS no és de forma intensiva/continuada.

LOT 2: Serveis Professionals d'implantació:

Serveis professionals de posada en marxa.

L'adjudicatari conjuntament amb el suport expert del fabricant:

- Definirà una proposta de política pel SSE que haurà de ser aprovada per TMB.
- Implementació i posada en marxa de la plataforma: desplegament d'Agents i totes les configuracions necessàries (mitjançant les eines disponibles a TMB: Microsoft SCCM, MDM Workspace One i GPOs Active Directory) que es realitzarà amb el suport/supervisió dels tècnics de TMB cap als equips client (Windows 7/10/11, Android, IOs)
- Integració del SSE amb IdP Keycloak (amb el suport del departament de TMB responsable del IdP) per la autenticació SAML i la sincronització d'usauris i grups del directori actiu (AzureID/EntraID).
- Integració amb el SIEM (actualment SPLUNK però en cas de canviar de tecnologia SIEM s'hauria de poder configurar cap a un altre SIEM que TMB disposi en el moment de la execució d'aquesta tasca).
- Aplicació de la proposta inicial de polítiques adaptades a complir els casos d'ús de TMB (Accés SaaS, Shadow IT, Antimalware, DLP) (veure taula adjunta al PPT).
  Inclou la posada en marxa polítiques de les funcionalitats de CASB Inline, CASB API, Antimalware i Secure Web Gateway).
  La part de SWG ha de servir per poder analitzar el Shadow IT que s'esta fent servir i aplicar algun cas d'ús de bloqueig d'accés a algun servei SaaS/aplicacio que podem definir com exemple, i també algun amb no bloqueig directe però si amb notificació concreta pe un servei/app concreta cap a l'usuari (coaching).

La part de DLP, ha de poder aplicar-se la classificació de fitxers que compleixin GDRP i fitxers de tipus SealPath (tecnologia existent a TMB) així com 3 casos d'ús de bloqueig i couching de DLP (per exemple quan es vulgui pujar a servei web/SaaS un fitxer classificat amb DLP).

- Generació de documentació sobre:
    - Configuració inicial acordada i aplicada a la plataforma SSE/CASB (amb els CdUs aplicats i polítiques)
    - Informe sobre el desplegament realitzat (amb una cobertura de mínim el 90%) sobre els equips client amb les funcionalitats implementades en cada cas.

Casos d'ús mínims que TMB vol aplicar:

FUNCIONALITATS	TMB Xarxa Interna	TMB Mobilitat
NAV - O365 corporatiu (Sharepoint,OneDrive,Office) - LLEGIR	SI	SI
NAV - O365 corporatiu (Sharepoint,OneDrive,Office) - EDITAR	SI	SI
NAV - O365 corporatiu (Sharepoint,OneDrive,Office) - DESCARREGAR	SI	NO
NAV - O365 corporatiu (Sharepoint,OneDrive,Office) - GUARDAR USB	NO	NO
NAV - O365 corporatiu (Sharepoint,OneDrive,Office) - IMPRIMIR	SI	NO
APP - O365 corporatiu (Sharepoint,OneDrive,Office) - LLEGIR	SI	SI
APP - O365 corporatiu (Sharepoint,OneDrive,Office) - EDITAR	SI	NO
APP - O365 corporatiu (Sharepoint,OneDrive,Office) - DESCARREGAR	SI	NO
APP - O365 corporatiu (Sharepoint,OneDrive,Office) - GUARDAR USB	NO	NO
APP - O365 corporatiu (Sharepoint,OneDrive,Office) - IMPRIMIR	SI	NO
Sincronizar APP OneDrive	SI	NO
Acceso Buzon Exchange	SI	SI
Subir Contenido Sharepoint	SI	NO
Asistir Reuniones Teams	SI	SI
Convocar Reuniones Teams	SI	SI
Colaborar Canales Teams	SI	SI
Acces SaaS no corporatius (Dropbox, Drive,...)	NO	NO
Subir SaaS no corporatius (Dropbox, Drive,...)	NO	NO
Subir DLP (confidencial) SaaS no corporatius (Dropbox, Drive,...)	NO	NO
Acces Navegació apps Web granular (p.e. WeTransfer,..)	NO	NO
Inventari Shadow IT	SI	SI
Identificació de fitxers segons contingut (DLP) (Machine Learning, GDPR...)	SI	SI
Bloqueig Antimalware (Sharepoint, OneDrive,Teams, Exchange)	SI	SI
AUDIT - Llistar usuaris del servei SaaS	SI	
AUDIT - Exposició publicació Repositoris Public/Privat)	SI	
AUDIT - Exposició publicació Fitxers (Public/Intern/Extern)	SI	

3. Condicions de servei

La 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.

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.

L'horari de les jornades serà de 8h a 14h els dies laborables.

4. Seguretat i 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.

5. 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 en el que fa referència al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE ("RGPD") com per la llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades de Caràcter Personal així com totes les altres normes legals o reglamentàries incideixin, desenvolupin o substitueixin les anteriors en aquest àmbit.

6. Seguiment del contracte

Per facilitar la bona marxa del contracte (LOT2) cal tenir en compte els següents punts:

Es realitzaran reunions periòdiques de treball entre el responsable del servei de l'empresa adjudicatària i el responsable d'aquest a TMB.

La periodicitat es fixarà en funció de la marxa del servei , per analitzar la consecució de les tasques definides de posada en marxa amb els aquests serveis professionals.

Annex 1 (referent al LOT 1)

Condicions que ha de complir la solució SSE:

- **Classificació ENS (Esquema Nacional de Seguretat) nivell ALTA**
- **Consola única per la gestió de totes les funcionalitats de la solució SSE**
- **Agent únic per totes les funcionalitats de la solució SSE**
- **Pels dispositius corporatius, gestió del tràfic a través d'un agent (i transparent a l'ús de qualsevol navegador)**
- **Es sol·licita que la solució disposi de nodes de connexió (PoP) ubicats a España (preferiblement a Barcelona per disposar d'una millor experiència d'usuari), i que aquests nodes tinguin la capacitat de procés local de totes les funcionalitats. I disposi de connexió directe (peering) entre el SSE i els principals proveïdors de servei SaaS: O365, Google,... (en el nostre cas sobretot amb O365) perquè la informació no hagi de passar per tercers i l'experiència d'usuari es vegi impactada.**
- **Ha de ser capaç de proporcionar SLAs de latència per contracte, amb uns llindars mínims acceptables de: 80 milisegons de tràfic xifrat http, i 20 milisegons de tràfic en clar**
- **S'ha de poder monitoritzar, permetre i/o bloquejar la comunicació, amb la possibilitat d' implementar accions de coaching amb l'usuari. De tal manera que es pugui personalitzar la acció el Pop-up de coach per cada regla de la política, inclús recollir una justificació per part de l'usuari.**
- **La solució SSE ha de desxifrar tot el tràfic inclòs el de O365, ja que és la plataforma de col·laboració corporativa.**

Necessitats mínimes que ha de cobrir el SSE (inicialment per al SaaS Office 365):
- Control d'Accés (qui accedeix a la plataforma)
- DLP (identificació de fitxers dins del SaaS que es considerin confidencials)
- DLP (ús de tècniques de prevenció de fuga d'informació) sobre CASB Inline (navegació) i CASB API en repòs, però amb possibilitat d'afegir la funcionalitat d'aplicar a nivell d'Endpoint.
- Control de compartició de documents (què es comparteix com i amb qui)
- Protecció antimalware (en els diferents serveis del SaaS)
- Automatització d'accions en temps real (bloquejar accions que no compleixin la política definida)
- Possibilitat de Couching a l'usuari quan vagi a realitzar una acció no aconsellada i/o permesa.
- Integració amb el nostre SIEM

Característiques destacades que ha de tenir el SSE:
- Identificació d'anomalies automàticament mitjançant funcionalitats d'anàlisi de comportament UEBA basat en algorismes no supervisats i matching learning.
- Correlació d'anomalies mapejat amb el quadre de MITRE ATT&CK que organitza i categoritza els diferents tipus d'atac.
- Identificació de dispositius gestionats/no gestionats per a aplicació de polítiques i ús d'arquitectura diferent.
- Possibilitat d'Arquitectura mixta via Reverse Proxy i via API simultàniament segons dispositius i accés via API per a recollida de dades per a Forensic .
- Govern per a serveis SaaS/Paas/IaaS/Contenidors, control DLP, User and Entity Behavior Analytics i monitoratge.
- Motor DLP amb controls i polítiques sobre la informació Cloud en Data identifiers (predefined data patterns/signatures), Keywords, Regular expressions, Data fingerprints, Dictionaries, File metadata (file name, size, type) i Machine Learning.
- Suport del motor DLP de fingerprinting sobre dades estructurades i no estructurades.

- Identificació de regles DLP en canals de Teams Posting-Chat, permetent distingir dominis interns de dominis externs com a atributs en la definició de polítiques.
- Possibilitat d'aplicar polítiques de control de fuga d'informació independents per canal de MS Teams.
- Possibilitat d'aplicació de polítiques DLP predefinides per vertical (Transport, Salut, Banc), regulació (HIPPA, PCI-DSS, EU).
- Possibilitat d'aplicar polítiques DLP, creades originalment per a Office 365 a entorns IaaS com un Blob Storage d'Azure o un bucket S3 d' AWS.
- Aplicació de polítiques DLP en diferents casos d' ús:
    - o Informació pujada a l'entorn Cloud
    - o Informació compartida des d'aplicacions Cloud
    - o Informació descarregada des de l'entorn Cloud
    - o Informació creada directament a l'entorn Cloud (Exemple Excel online)
- Posició dins del grup de Líders al Magic Quadrant de Gartner
- Creació d'escanejos sota demanda de carpetes Onedrive o llocs Sharepoint específics, amb possibilitat d'exclusions, igual que repositoris AWS, Azure.
- Possibilitat d'enviament d'esdeveniments a un SIEM via Syslog.
- Possibilitat de selecció de l'acció a realitzar davant d'un esdeveniment de DLP:
    - o Block
    - o Couch
    - o Delete
    - o …

- Capacitat d'auto remediació d'incidents de DLP per part de l'usuari. Per exemple: poder enviar una alerta automàtica a l'usuari que ha pujat un arxiu confidencial a OneDrive i si aquest esborra l'arxiu, l'incident quedaria marcat com a resolt sense la necessitat de la seva gestió per part de l'administrador.
- Definició de rols d'usuari amb permisos per a diferents accions:
    - Definir o activar polítiques de compliment o DLP
    - Accedir o remeiar violacions identificades per les polítiques
    - Accedir als documents enviats a quarantena per gestionar la seva possible restauració.
- Identificació de malware mitjançant signatures o serveis Cloud, fitxers pujats coneguts com a sospitosos.

Descripció de les funcionalitats específiques que ha d'oferir la solució sol·licitada:

Funcionalitats de Secure Web Gateway

- Inspecció Inline de tràfic HTTP i HTTPS pels accessos Web, SaaS, IaaS/PaaS.
- Inspecció de traffic TLS incloent nativament v1.3
- Reverse Proxy per serveis Cloud I Apps amb integració amb IdP (Identity Provider) (compatible amb Keycloak que és el que usa actualment TMB)
- Amplia identificació de serveis cloud i apps
- Controls de politiques granulars incloent instància de les app i comportament de les activitats en aquella app (descàrrega, upload, …)
- Base de Dades amb Index de risc de més de 50K apps i serveis Cloud
- Reporting amb mínim de 90 dies de retenció
- Open REST API
- Natiu forward cloud i web proxy amb SSO, MFA i Integració AD

Web Filtering

- URL Filtering per més de 100 categories, més de 150 llenguatges i 99,9% de webs actives.
- Incloent categories de Youtube, serveis de traducció, safesearch i Ad blocking
- Categorització dinàmica de pàgines web per més de 50 categories.
- Possibilitat d'accés a un site per la comprovació de la categoria d'una web amb servei de re-classificació.
- Permetre, bloquejar o avisar amb warning i alertes personalitzades al navegador web.
- Creació de categories personalitzades amb llistes blanques i negres.
- Determinar la inspecció de tràfic per categoria de URL o domini

Protecció d'amenaces

- Motors antimalware, web IPS i anàlisi de fitxers amb identificació del tipus real (per capçalera)
- Fonts d'informació d'amenaces (Threat Intel), a més d'importar IOCs, inclosos URL maliciosos i hash de fitxers
- Aprenentatge automàtic de fitxers executables portàtils (PE) en línia per a la detecció i el bloqueig de programari maliciós Pacient Zero
- Detecció de phishing amb classificador Machine Learning per identificar dominis de Phishing en temps real bloquejant l'accés a aquests llocs
- Sandboxing estàndard per corroborar totes les deteccions AV/ML
- Cloud Threat Exchange (CTE) que permeti la compartició de Threat Intel amb EPP/EDR, SIEM, SOAR, etc. (actualment el SIEM és SPLUNK i la tecnologia EPP/EDR és de Trellix però les dues poden canviar així que la funcionalitat ha de poder existir cap a solucions de tercers).

UEBA (Anàlisi de Comportament de l'Usuari)

- Regles d'anomalies seqüencials per detectar càrregues massives, descàrregues massives, supressions massives, inicis de sessió fallits massius, credencials compartides, esdeveniments rars, anomalies geogràfiques, països de risc i exfiltració de dades entre instàncies personals i de l'empresa.

Data Protection (DLP)

- Anàlisi de dades en moviment per serveis cloud i apps, tràfic web, fitxers i formularis.
- Disponibilitat de Plantilles de compliment normatiu que incloguin: GDPR, PII, PCI, PHI, codi font, etc.
- Identificadors de dades per als tipus de fitxers, a més d'expressions regulars, patrons i diccionaris personalitzats
- Classificadors de documents estàndard AI/ML (currículums, codi font)

Analítica Avançada

- Mínim de 7 dies de base a la plataforma per monitoritzar i investigar els factors de risc en l'activitat al núvol, amb visualitzacions personalitzables.
- Mínim de 7 dies de retenció de dades per a alertes, esdeveniments de pàgina, esdeveniments d'aplicació, esdeveniments d'accés privat i esdeveniments de xarxa de tallafoc al núvol
- Opció per ampliar la retenció de dades a 3, 6 o 13 mesos
- Dashboards preconstruïts sobre l'activitat al núvol, informació sobre riscos, política de compliment.

CASB API per Onedrive, Sharepoint, Microsoft Teams, Exchange

Seguretat habilitada per API per aplicacions SaaS gestionades per monitoritzar, controlar l'ús i protegir les dades.

Protecció mitjançant API, aplicació granular de polítiques, protecció de dades i amenaces, informes estàndard basats en 90 dies de retenció de dades.

- Open REST API disponible per integració amb aplicacions de tercers
- Anàlis DLP de dades en repòs per Serveis Cloud i apps

Suport del fabricant 24x7

- 24x7 telefonic i suport online; 30min de temps de resposta inicial per incidències critiques (P1 urgent)
- 24x7 telefonic i suport online; 2h de temps de resposta inicial per incidències critiques (P2 high)
- 24x7 accés a online knowledge base, manuals d'usuari, FAQs, i release notes

Equips Clients de TMB:

Windows 7/10/11, Android, IOs

Desplegament dels agents de la solució SSE:

Mecanismes de desplegament dels Agents disponibles a TMB:

- **Microsoft SCCM**
- **MDM Workspace One**
- **Polítiques GPOs del Active Directory de Microsoft**

El Tràfic no autenticat no s'ha de contemplar en aquesta licitació, es vol controlar el tràfic autenticat dels usuaris no de sistemes IoT.