

Implantació passarel·la de pagament nou sistema de gestió comercial online

Plec de condicions tècniques

Març 2018

Versió 1.0



Transports
Metropolitans
de Barcelona

TAULA DE CONTINGUTS

Històric de modificacions.....	3
Aprovació	3
Distribució.....	3
1 Introducció	4
Objectius del document i abast	4
Documents de referència	4
Diccionari i acrònims	4
2 Marc del projecte	5
3 Requeriments funcionals d'usuari final.....	8
4 Requeriments normatius.....	10
5 Requeriments tecnològics	11
6 Requeriments de protecció de frau.....	12
7 Requeriments de gestió del frau	14
8 Requeriments de gestió de la informació i informes.....	15
9 Requeriments per la integració de la informació.....	17
10 Requeriments de disponibilitat (SLAs).....	18
11 Penalitzacions per incompliment de SLAs.....	19
12 Requeriments d'operació del servei	21
13 Definició dels requeriments del projecte d'implantació	25
14 Característiques del servei.....	27

Històric de modificacions

Data	Autor	Comentaris	Versió
16/01/2018	Esteve Avilés	Versió inicial	1.0
11/02/2018	Esteve Avilés	Revisió interna components projecte	1.1

Aprovació

Nom	Data	Signatura
Esteve Avilés Aymerich		

Distribució

Intern	Extern

1 Introducció

Objectius del document i abast

L'objectiu d'aquest document és establir el plec de condicions complet per la contractació d'un servei de passarel·la de pagament en entorns digitals online de comerç electrònic per webs i aplicacions mòbils.

Documents de referència

En la següent taula es poden consultar els documents de referència i les versions corresponents:

Nom	Autor	Versió

Taula 1 Documentació de referència

Diccionari i acrònims

En aquest apartat es llistes els termes específics i acrònims empleats al llarg del document:

- RF: Requeriment Funcional
- RT: Requeriment Tècnic
- TdO: Unitat de negoci de Transports de l'Oci dins de TMB
- OciCommerce: Sistema d'Informació Central del Sistema de Ticketing de TdO.
- BBT: Barcelona Bus Turístic
- CBT: Catalunya Bus Turístic
- PCI: Payment Card Industry

2 Marc del projecte

2.1 Context

TMB té la intenció d'habilitar la venda de diferents productes a través dels seus canals online. Per tal de poder dur a terme és necessari la contractació d'un servei de passarel·la de pagament que contempli tots els requeriments funcionals i tècnics especificats en aquest plec de contractació amb la finalitat final de que el client pugui pagar amb diferents mitjans de pagament les seves compres.

El principal mercat al que s'adreça aquest nou servei és el mercat estatal. Per tant, es prioritzarà l'estratègia per donar resposta a aquesta situació.

2.2 Objectiu i abast del projecte

S'estableixen com a objectius bàsics d'aquest projecte el següents:

- Implantació de la passarel·la de pagament: alta, configuració, administració
- **Operació de la passarel·la de pagament**
- Suport a la integració dels productes tecnològics basats en Android i iOS per entorns mòbils i web.
- Parametrització, activació i aplicació de les regles de frau
- Implantació dels processos d'integració d'informació
- Validació del compliment de les normatives de seguretat
- Testeig de tots els processos
- Habilitació dels entorns de test i productius
- Suport al desenvolupament

Per tant, aquest plec fa referència a la contractació d'un **payment gateway** i tots els serveis associats que permetin el compliment dels requeriments expressats en aquest plec.

2.3 Canals actuals i futurs

Els serveis contractats a l'actual licitació podran ser extensibles a altres serveis o canals comercials de la companyia en un futur. És a dir, no caldrà fer una

altre licitació per la connexió d'altres canals de venda que facin ús del servei contractat.

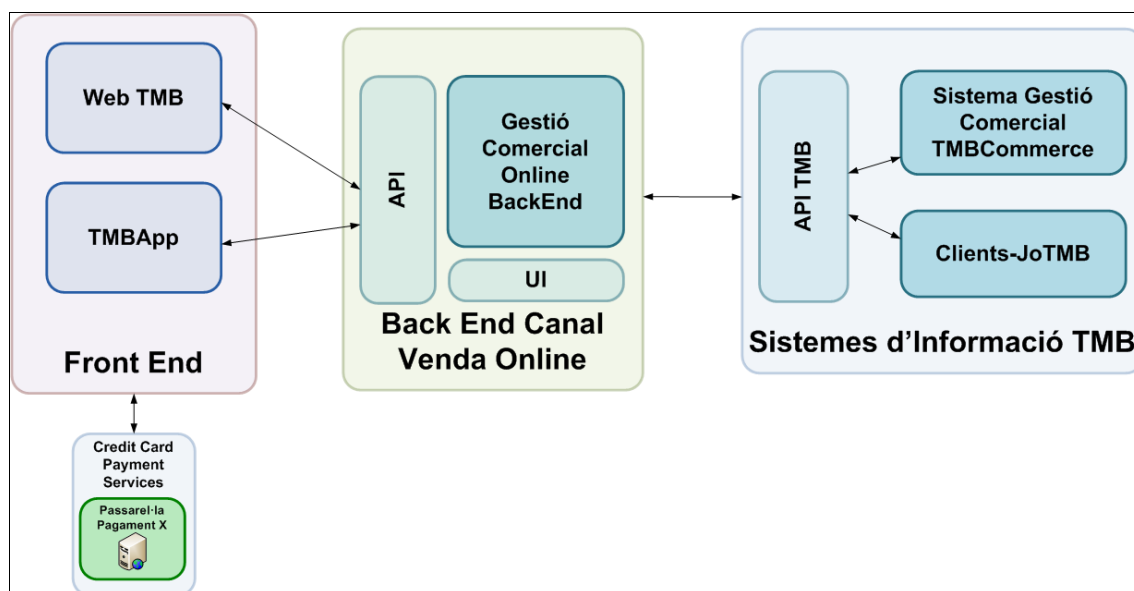
2.4 Fora d'abast

Queda fora de l'abast del projecte els desenvolupaments referents als productes tecnològics que s'han d'integrar amb aquesta plataforma.

Queda fora de l'abast d'aquesta contractació els serveis de banc adquirent que venen fixats en l'apartat corresponent.

2.5 Arquitectura de la solució

En el següent diagrama es mostra l'arquitectura de la solució a mode de referència:



Taula 2. Arquitectura de la solució

Aquest projecte fa referència exclusivament al desenvolupament del component de l'arquitectura *Back End Canal Venda Online*.

Per tal de que s'entengui l'arquitectura de la solució es descriu a continuació, a molt alt nivell, el flux d'informació bàsica d'un procés de venda:

1. A través del Web o la App de TMB, l'usuari consulta els productes disponibles. Aquest productes s'obtenen del BackEnd Canal Venda Online

2. El client a través del Web o la App executa una ordre de compra amb el procés de pagament associat. Aquesta s'envia, es valida i es registre en el BackEnd Canal Venda Online. Aquest retorna tota la informació associada a l'execució de la mateixa: justificants, vouchers, factures, També executa les accions de comunicació com mails de confirmació de compra o notificacions a la APP.
3. El BackEnd Canal Venda Online comunica la informació de la venda al sistema d'informació de Gestió Comercial de forma no transaccional (en diferit)

Per tant, el component BackEnd Canal Venda Online té tota la lògica de negoci referent al procés de compra.

2.6 Servei de banc adquirent

S'estableix que els serveis de banc adquirent els proporcionarà l'entitat **CaixaBank, S.A.**, ja que és un dels proveïdors actuals d'aquest servei en altres línies de negoci del grup.

Per tant, la plataforma gateway, el processador de pagaments amb targeta de crèdit i els altres serveis han de poder treballar amb aquesta entitat bancària en cadascuna de les interaccions que es produeixin per poder prestar els serveis sol·licitats.

3 Requeriments funcionals d'usuari final

TMB necessitarà per a la seva operatòria diària poder executar les següents funcionalitats dels diferents mitjans de pagament.

Els requisits fan referència a nivell mitjans de pagament i a nivell plataforma de pagament. Els mitjans de pagament necessaris s'han de definir d'acord amb les necessitats dels consumidors.

Requeriment	Descripció	Obligatori
RF1	Ha de permetre el pagament amb el següents mitjans de pagament de targeta de crèdit: • Visa • MasterCard • American Express	Sí
RF2	Ha de permetre la integració amb els següents targeters digitals: • PayPal • ApplePay • GoogleWallet • Samsung Pay	
RF3	Ha de permetre la integració amb els següents serveis de transferències digitals: • Sofort • Trustly • Bizzum	
RF4	Cobraments targeta de crèdit: ha de disposar de les dues possibilitats de cobrament en l'entorn de targeta de crèdit: • Captura directe • Autorització més captura	Sí
RF5	Devolucions: Ha de permetre l'execució de devolucions parcials i totals sobre el mitjà de pagament original de la transacció.	Sí
RF6	Possibilitat de realitzar pagaments recurrents i/o subscripcions. I això implica necessàriament la possibilitat de: • En targetes de crèdit, processar transaccions sense el CVV	Sí

	• Disposar d'algun gestor o eina o comunicació per a poder planificar i executar transaccions recurrents.	
RF7	Ha de permetre emmagatzematge de targetes dels clients mitjançant un sistema de 'tokenització' que alliberi a TMB d'haver de capturar i emmagatzemar les dades de targeta de crèdit. Aquest servei ha de oferir la custòdia i emmagatzematge de les dades de targetes de crèdit i dèbit dels nostres clients	Sí
RF8	Les operatives de gestió que permetran realitzar operacions sobre els tokens amb la passarel·la seran com a mínim: • Alta de dades d'un nou registre • Modificació de les dades sobre un registre existent • Modificació automàtica de data de caducitat • Consulta de la validesa del PAN • Baixa de dades En totes les operatives de gestió, la recepció de la confirmació es pot rebre en un client diferent al client des del que s'ha realitzat l'operació.	Sí
RF9	Les operatives de cobrament amb token que cal que implementi el sistema, com a mínim, són les següents: • Transaccions de pre-autorització • Transaccions de pagament • Transaccions de devolució • Anul·lació d'un pagament • Anul·lació d'una devolució • Test de saldo	Sí
RF10	Les operatives de cobrament amb token posteriors a la primera operació es podran realitzar sense haver de executar el pagament segur.	
RF11	Ha de permetre el pagament segur en tots els mitjans de pagament i en tots els entorns.	Sí
RF12	Ha d'estar preparat per l'execució de transferències instantànies en el moment de l'obertura de la llei europea PSD2.	
RF13	La plataforma ha de poder gestionar més d'un	

	comerç i més d'una empresa sota la mateixa compte.	
RF14	Els diferents punts d'interacció amb l'usuari final: pantalles, textos, missatges, ... han de ser multi-idioma. Com a mínim estar en: Català, Castellà, Anglès, Alemany, Italià, Francès.	

Taula 3 Requeriments funcionals d'usuari final

4 Requeriments normatius

A continuació es presenten els requeriments que s'han de complir en matèria de normativa aplicada al processament de transaccions econòmiques en l'àmbit digital.

Requeriment	Descripció	Obligatori
RN1	Compliment normativa processament targeta de crèdit: PCI DSS Nivell 1 Compliant en la última versió 3.2	Sí
RN2	Compliment normativa PSD1	Sí
RN3	Pla de compliment de la normativa o compromís de compliment de nova normativa PSD2	Sí
RN4	Compliment de normatives de lleis de protecció de dades de caràcter personal LOPD i GDPR.	Sí
RN5	Les infraestructures informàtiques han d'estar ubicades en territori estatal.	Sí
RN6	Compliment de qualsevol altre normativa que durant la vigència del contracte pugui sorgir en aquesta matèria i que sigui d'obligat compliment.	Sí

Taula 4 Requeriments funcionals d'usuari final

5 Requeriments tecnològics

A continuació es presenten els requeriments que s'han de complir a nivell tecnològic:

Requeriment	Descripció	Obligatori
RT1	CPD en categoria Tier III segons la classificació de Uptime Institute	
RT2	CPD en arquitectura Multi Availability Zone (Multi AZ)	
RT3	El servei de Payment Gateway i els altres serveis s'han d'oferir en format SaaS (Software as a Service), és a dir, no s'instal·larà cap element hardware de servidors en les instal·lacions de TMB.	Sí
RT4	Disposar de llibreries natives d'integració en les plataformes mòbils (SDKs): • Apple iOS: versió mínima 9 • Google Android: versió mínima 4.4	Sí
RT5	Disposar de llibreries JavaScript per la integració en entorns Web.	
RT6	Disposar de maquetacions Responsive, adaptables segons la mida de la pantalla, per les solucions Web embegudes en els sites de TMB.	
RT7	Disposar d'API d'integració amb tecnologies JSON sobre protocols HTTPS.	Sí
RT8	Backoffice accessible des d'Internet mitjançant tecnologies Web modernes i multi-dispositiu (responsive) i navegador (IE Explorer, Chrome, Firefox i Safari)	
RT9	Possibilitat tècnica de treballar amb múltiples bancs adquirents	

Taula 5 Requeriments tecnològics

6 Requeriments de protecció de frau

A continuació es presenten els requeriments que s'han de complir a nivell funcionalitats per la protecció del frau:

Requeriment	Descripció	Obligatori
RPF1	Pagament segur en tots els canals i per tots els mitjans de pagament amb protocols de seguretat que siguin "liability shift": • 3DSecure per targeta de crèdit per exemple: VISA. Verified by VISA, MASTERCARD. Secure Code, AMEX. SafeKey (si s'escau) • Pels altres mitjans de pagament: Que tinguin protocols de liability shift (la responsabilitat no recau en el comerç). Per exemple: ○ Paypal. En el cas de Paypal, la protecció del comerç ○ ApplePay. No Fraud CBs Policy.	Sí
RPF2	Tractament automatitzat de llistes negres per targeta de crèdit segons els següents criteris mínims: • Nacionalitat IP • Nacionalitat Targeta • Bloquejar transaccions per a usuari a partir de N transaccions en X hores. • Bloquejar transaccions per a targeta a partir de N transaccions en X hores. • Bloquejar transaccions per a IP a partir de N transaccions en X hores.	Sí
RPF3	API d'integració per manteniment automatitzat des de l'exterior de llistes negres.	
RPF4	Possibilitat de bloquejar operativa d'acord amb patrons de comportament fraudulent.	
RPF5	Limitar operacions per: • Import • Número d'operacions en X hores amb la mateixa targeta o client • Per producte	
RPF6	Totes les configuracions de frau han de ser administrables a nivell de comerç i empresa.	
RPF7	Com a conseqüència de l'aplicació de la Segon Directiva Europea de Pagaments, és molt	

	important mencionar que a mitjans de 2019, es llançarà un nou protocol de seguretat obligatori anomenat Strong Customer Authentication. Aquest protocol alliberarà als ecommerces de la responsabilitat del frau i serà d'aplicació per a totes les transaccions en les quals o bé el comerç o bé el mitjà de pagament estiguin a la zona Euro.	
--	--	--

Taula 6 Requeriments protecció de frau

7 Requeriments de gestió del frau

A continuació es presenten els requeriments que s'han de complir a nivell de gestió del frau ja sigui en la part del gateway o en la part de banc adquirent:

Requeriment	Descripció	Obligatori
RGF1	Disposar d'un dashboard de seguiment del frau i les disputes	
RGF2	Poder aplicar devolucions de forma manual, tan parcials com totals.	Sí
RGF3	Poder realitzar la gestió i control de disputes.	
RGF4	Consulta d'operacions individuals.	
RGF5	Recepció i notificació de notificacions d'operativa fraudulenta.	
RGF6	Recepció i notificació de contra-càrrecs.	
RGF7	Possibilitat de poder disputar contra-càrrecs si TMB creu que el titular de la targeta no té raó i /o va en contra de les Condicions de Compra.	
RGF8	Poder accedir a les eines de gestió del frau amb diferents permisos i amb controla d'accés a les diferents funcions.	

Taula 7 Requeriments gestió de frau

8 Requeriments de gestió de la informació i informes

A continuació es presenten els requeriments que s'han de complir a nivell tecnològic:

Requeriment	Descripció	Obligatori
RI1	Accés al llistat de transaccions individuals	Sí
RI2	Accés diferenciat per comerç i global	
RI3	Poder aplicar filtres sobre les transaccions per diferents criteris	
RI4	Poder exportar les dades als formats: MS Excel, CSV, PDF.	
RI5	Els informes han de proveir com a mínim la següent informació: • Import de la transacció • Identificador de la transacció o codi acceptació • Ordre la Venta –del backend de TMB- o número d'identificació del comerç. • ID Mitjà de Pagament • Token del mitjà de pagament (si s'escau) • Identificador del usuari –del backend de TMB- • Identificador del Voucher –del backend de TMB- • Tipus de l'operació (venda o devolució) • Status de la transacció (acceptada / denegada) • Explicació motiu de la denegació (si s'escau) • Data i hora de la transacció –del backend de TMB- • Moneda (sempre Euros) • IP Nacionalitat país • IP Nacionalitat mitjà de pagament (si s'escau)	Sí
RI6	Notificació de les liquidacions per part de la plataforma de pagaments	

Taula 8 Requeriments de gestió de la informació i informes



9 Requeriments per la integració de la informació

A continuació es presenten els requeriments que s'han de complir a nivell tecnològic les APIs d'integració amb sistemes informàtics de TMB:

Requeriment	Descripció	Obligatori
RII1	Descàrrega de la informació de les transaccions detallades	
RII2	Execució de transaccions i tota la operativa comuna de venda	Sí
RII3	Execució de devolucions i tota la operativa de gestió de les devolucions	Sí
RII4	Implementació de tots els processos de gestió i d'operació dels tokens descrits en l'apartat de requeriments funcionals d'usuari final.	Sí
RII5	Obtenció d'informació de l'usuari/client	
RII6	Execució, programació i administració de pagaments recurrents	Sí
RII7	Habilitació de callbacks per la notificació de transaccions i altres esdeveniments.	
RII8	El serveis hauran de ser accessibles tan des de les infraestructures tecnològiques de TMB com les d'altres proveïdors cloud de tecnologia, com pot ser AWS.	
RII9	Caldrà implementar totes les arquitectures d'integració requerides en l'apartat de requeriments d'usuari. Bàsicament, arquitectures Web (aplicació web en servidor i SinglePage App) i arquitectures mòbils.	
RII10	El proveïdor haurà de proporcionar, a part de l'entorn productiu, un entorn de preproducció per poder realitzar proves.	Sí

Taula 9 Requeriments per la integració de la informació

10 Requeriments de disponibilitat (SLAs)

Les incidències es catalogaran en quatre nivells en funció de la afectació al servei del portal web:

- **Crítica:** pèrdua completa o indisponibilitat total del servei .
- **Alta:** pèrdua o indisponibilitat parcial del servei. Per exemple, hi ha dos nodes donant servei i un està fallant i l'altre està donant servei.
- **Mitjana:** pèrdua menor del servei: errors puntuals o problemes de rendiment
- **Baixa:** incidència que no té impacte en el servei.

Categoria incidència	Temps de resposta	Temps de resolució objectiu
Crítica	10 minuts en 24x7	15 minuts en 24x7
Alta	20 minuts en 24x7	30 minuts en 24x7
Mitjana	1 hora en 10x5	90 minuts en 24x7
Baixa	Negociat	Negociat

Taula 10 Taula de temps de resolució d'incidències del servei

S'estableix les següents definicions:

- **Temps de resposta:** es defineix el temps de resposta a al temps en que l'adjudicatari registre la incidència en el sistema de gestió de tickets i aquesta comunica als destinataris, mitjançant el workflow i canals establerts del codi, la definició i la tipificació de gravetat de la mateix. Les fonts mitjançant la qual es poden notificar incidències són:
 - Sistemes de monitorització automatitzats
 - Es realitza una trucada o comunicació per part d'alguna persona de TMB o subcontractada de TMB.
- **Temps de resolució:** és el temps que passa des de l'inici de la incidència (i no des del temps de resposta), fins al restabliment complet del servei, és a dir, fins que les alarmes i els sistemes de monitorització tornen a donar com a bo el servei.

11 Penalitzacions per incompliment de SLAs

En la següent taula es mostren les penalitzacions en percentatge de la facturació mensual en el mes en que s'hagi produït la incidència per l'incompliment dels acords de nivell de servei descrits en aquest document.

11.1.1 Penalitzacions sobre el Temps de Resposta

La penalització s'aplica per cada incidència.

Categoria incidència	Temps de resposta Objectiu	Temps de resposta Real	Penalització
Crítica	10 minuts en 24x7	Major de 30 minuts	1%
		Entre 10 minuts i 30 minuts	0.5%
		Menor de 10 minuts	0%
Alta	20 minuts en 24x7	Major de 60 minuts	1%
		Entre 20 minuts i 60 minuts	0.5%
		Menor de 20 minuts	0%

Taula 11 Taula de penalitzacions per Temps de Resposta

11.1.2 Penalitzacions sobre el Temps de Resolució

La penalització s'aplica per cada incidència.

Categoria incidència	Temps de Resolució Objectiu	Temps de Resolució Real	Penalització
Crítica	15 minuts en 24x7	Major de 30 minuts	3%
		Entre 15 minuts i 30 minuts	2%
		Menor de 15 minuts	0%
Alta	30 minuts en 24x7	Major de 60 minuts	3%
		Entre 30 minuts i	2%

		60 minuts	
		Menor de 30 minuts	0%

Taula 12 Taula de penalitzacions per Temps de Resposta

11.1.3 Penalitzacions sobre còmputos mensuals

La penalització s'aplica sobre el còmput mensual sumant tots els valors de totes les incidències detectades.

Definició	Valor	Penalització
Una disponibilitat del sistema per sota del X % en còmput mensual com a conseqüència directa de la incidència tipus Crítica	99.9% (0.744 hores/mes màxim de no disponibilitat)	5%
X actuacions que impliquin aturada del servei i no s'hagin notificat ni registrat en el sistema de ticketing.	2	5%

Taula 13 Taula de penalitzacions sobre còmputos mensuals

11.2 Penalitzacions sobre la implantació i posta en marxa

El servei de passarel·la de pagament és crític per TMB, qualsevol retard parcial o total en la posta en marxa de la passarel·la implica un cost d'operació que no es pot assumir. Per tant, s'aplicaran les següents penalitzacions en els endarreriments en la posta en marxa i inici del servei, sempre que sigui imputable al proveïdor:

- 5.000€ per a cada setmana d'endarreriment imputable al proveïdor de la posta en marxa, a descomptar de l'import de les primeres factures del proveïdor.

11.3 Condicions de les penalitzacions

Les penalitzacions es facturaran al proveïdor o es descomptaran de la següent factura emesa pel proveïdor.

12 Requeriments d'operació del servei

Desenvoluparà tasques destinades a detectar proactivament incidents amb afectació a la disponibilitat o punts de millora en el funcionament dels serveis de pagament online, realitzarà el tractament, la gestió i resolució de les incidències ja siguin detectades per la monitorització o reportades directament per TMB.

Dins de les tasques a dur a terme s'han identificat de forma inicial les següents:

12.1 Monitorització contínua

Es monitoritzaran en temps real els components externs necessaris pel funcionament del servei de pagament electrònic.

12.2 Escalat i notificació d'incidències detectades

TMB disposa internament del Centre de Suport Tecnològic (CST), que en horari 24x7 realitza tasques de monitorització i operació bàsiques dels sistemes interns de TMB. Aquest centre rep les incidències reportades pels usuaris i pels sistemes de monitorització propis.

Si les incidències detectades tenen afectació a la disponibilitat dels serveis de pagament online caldrà notificar les incidències al CST i als responsables del servei de TMB.

12.3 Gestió d'intervencions programades

En cas que s'hagin de realitzar intervencions programada, ja sigui per aplicar un fix de seguretat, actualitzar els sistemes, ampliar recursos, ... s'haurà de notificar sempre prèviament a TMB mitjançant la creació del ticket corresponent i amb una anticipació de com a mínim 24 hores.

En cas que l'actuació comporti una parada del servei caldrà haver pactat prèviament l'hora i duració exacte de la intervenció.

12.4 Comunicació

Es requereixen els següents canals de comunicació mínims per a la gestió d'incidències:

- Entorn web
- Mail

- Telèfon

Totes les comunicacions TMB – Adjudicatari o Adjudicatari – TMB hauran de fer referència a un ticket de l'eina de gestió central de tickets definida més endavant en aquest document.

12.5 Eina de gestió de tickets

Es sol·licita que el proveïdor posi a disposició de TMB una eina de gestió de tickets que implementi les següents funcionalitats i requeriments bàsics:

- Eina Web accessible a través de navegador des d'Internet
- Accés nominal i amb rols determinats
- Gestió de tickets amb identificador únic
- Visualització de l'estat del ticket: nou, obert, pendent, tancat,...
- Visualització de qui té assignat el ticket
- Notificació via mail dels canvis en els tickets
- Gestió de grups de notificacions
- Possibilitat d'afegir comentaris als tickets

Aquest eina de gestió de tickets servirà com a únic element documental vàlid per a la resolució de discrepàncies a nivell de servei i pel mesurament de la qualitat del mateix.

Qualsevol alarma de monitorització que es consideri important també haurà de registrar automàticament un ticket en aquesta eina.

12.6 Horari del Servei

L'entorn de producció en horari de 24x7 i els entorns que no siguin de producció en horari 10x5.

12.7 Servei de manteniment evolutiu bàsic

Desenvoluparà tasques relacionades amb peticions de canvis sol·licitades des de TMB respecte dels diferents serveis que es puguin afegir durant la duració del contracte.

12.8 Bossa de jornades de suport

El contracte inclourà també una bossa de jornades destinades a la realització de altres tasques no incloses als punts anteriors i al suport postproducció i al desenvolupament de les integracions.

El consum de la bossa es realitzarà a partir d'una petició per part dels tècnics de TMB, el proveïdor haurà de fer una estimació de les hores necessàries i la seva planificació.

Estimem aquesta bossa en 100 hores anuals.

Cal incloure en la oferta les tarifes aplicades a cada perfil ofertat en aquesta bossa d'hores.

12.9 Informes de compliment de ANS

Es sol·licita que de forma mensual (en format documental) o mitjançant una eina online web es pugui fer el seguiment del compliment dels ANS establerts.

12.10 Servei de gestió de seguretat

L'adjudicatari haurà de disposar d'un servei de gestió de la seguretat informàtica que cobreixi principalment les següents accions:

- Servei d'alerta i notificació de vulnerabilitats detectades
- Servei d'aplicació de actualitzacions de seguretat en les diferents capes de software

TMB contractarà de una altra licitació un servei d'auditoria de seguretat que analitzarà i escanejarà els diferents serveis exposats a través d'internet per detectar vulnerabilitats de seguretat. Aquest servei permetrà poder disposar del coneixement de l'estat en que es troba aquest entorn en tot moment per tal d'evitar les següents problemes de seguretat:

- Atacs (D)DOS
- Accedir i modificar el contingut del web
- Assegurar la confidencialitat de les dades de client
- Evitar autenticacions no autoritzades
- Securitització de formularis de consulta
- ...

S'hauran de tenir en compte les CIS Critical Security Controls - Version 6.0 (<http://www.sans.org/critical-security-controls>) que apliquin en aquest projecte.

En aquest servei s'analitzaran les següents capes:

- Anàlisis de la Informació Pública
- Anàlisis de Seguretat a Nivell de Xarxa
- Anàlisis de Seguretat a Nivell de Sistemes
- Anàlisis de Seguretat a Nivell d'Aplicacions
- Anàlisi dels Sistemes de Seguretat

Es faran servir els següents àmbits metodològics o marcs de referència per tal de dur a terme aquest anàlisi:

- OWASP → Obligatòria
- OSSTMM → Opcional
- CobIT → Opcional

13 Definició dels requeriments del projecte d'implantació

El licitador ha de presentar un projecte d'implantació de la passarel·la amb tots els següents punts detallats i ben coberts:

- Estructuració de les etapes, dependència entre elles i fites concretes.
- Planificació temporal de les etapes i fites
- Equip de treball assignat: persones, perfils i estructura
- Metodologia a usar durant el projecte d'implantació
- Detall dels serveis de suport post producció
- Programa d'identificació i gestió del risc
- Pla de formació als usuaris de la plataforma Web en els perfils: tècnic, de finances, administració i gestió del frau.

Per la seva banda, TMB nomenarà un cap de projecte, que serà responsable de supervisar la correcta execució de les aplicacions i serveis inclosos dins l'àmbit de subministrament del present plec, segons la metodologia i els estàndards corporatius.

En aquest mateix sentit, TMB nomenarà els interlocutors i el seu àmbit d'interlocució per a cadascuna de les àrees i serveis afectats per la implantació del sistema.

D'altra banda, l'Adjudicatari haurà d'anomenar un director de projecte que serà l'únic interlocutor vàlid amb TMB i que entre d'altres, haurà de realitzar les següents funcions:

- Vetllar per l'assoliment dels objectius del projecte, segons planificació i pressupost previst.
- Executar i fer el seguiment del projecte i del pla de treball (tasques, terminis, recursos, etc.), generant la corresponent documentació: actes, planificació, informes, plans, etc.
- Gestionar i executar el pla de comunicació del projecte. En particular, periòdicament, haurà de comunicar al cap de projecte de TMB l'estat d'avançament dels projectes, amb la periodicitat que TMB estableixi en

cada moment, incloent un breu informe de seguiment i l'actualització de la planificació prevista.

- Realitzar reunions de seguiment de projecte amb la periodicitat que TMB estableixi en cada moment.
- Gestionar i valorar les peticions de canvi en el projecte, juntament amb TMB.
- Gestionar i supervisar el riscs del projecte.
- Gestionar i valorar els riscos del projecte i executar les actuacions previstes.

TMB també anomenarà un Comitè de direcció de projectes, en el que hi haurà representats de les unitats o divisions afectades pel Servei.

Aquest Comitè de Direcció vetllarà perquè l'enfocament dels serveis i sistemes subministrats es correspongui amb l'abast i els objectius previstos.

Aquest Comitè de Direcció també podrà ser requerit en procediments administratius relacionats amb l'acceptació del projecte o l'aplicació de les sancions previstes dins l'àmbit del present Contracte de subministrament i serveis.

14 Característiques del servei

14.1 Modalitat de contractació

La modalitat de contractació d'aquest projecte és en modalitat de **SERVEI**, és a dir, el proveïdor facturarà el resultat del cost del servei segons oferta presentada.

Qualsevol petició o funcionalitat nova no contemplada en aquest plec caldrà gestionar-la tan bon punt aparegui en un procés de gestió del canvi.

14.2 Lloc de realització dels treballs

Les tasques corresponents al projecte **es realitzaran a les dependències de TMB o a les dependències del proveïdor.**

14.3 Infraestructura i entorn tecnològic

Tots els recursos d'infraestructura tecnològica necessaris per la realització del projecte aniran a càrrec del proveïdor en la infraestructura del proveïdor.

14.4 Metodologia

L'adjudicatari dels serveis es compromet a seguir el marc metodològic de gestió de projectes TIC de TMB, actualment ITIL.

14.4.1 Seguiment i control

L'adjudicatari entregará informes setmanals en format digital on es descriurà el grau d'avenç del projecte. En aquests informes s'hi inclourà, entre altres, els següents aspectes:

- Resum de les tasques realitzades durant la setmana
- Activitats previstes per la següent
- Riscos i desviacions
- Estat actual de la planificació

14.4.2 Estructura y nomenclatura dels lliuraments

L'adjudicatari haurà de seguir i respectar l'estructura i nomenclatura per tots els lliuraments, ja siguin documents o software, que proposi TMB.

14.4.3 Documentació

El nom dels documents seguirà un patró determinat, de manera que pugui identificar-se la següent informació respecte el document:

- Projecte
- Àmbit (Informe, Anàlisi, Disseny,...)
- Proveïdor, en el cas de les ofertes
- Nom descriptiu del contingut del document
- Extensió del fitxer Aquesta informació es compondrà formant un nom del fitxer de la següent manera:
- PXXXXX. NomProjecte-ÀMBIT-PROVEÏDOR-Nom del Fitxer.ext Els valors del camp àmbit poden ser:
 - **INFO**: Informe
 - **ANA**: Anàlisi
 - **DISS**: Disseny
 - **PLEC**: Plec de condicions
 - **OFER**: Oferta,
 - **MAN**: Manual
 - **PRES**: Presentació
 - **PLAN**: Planificació
 - **PLA**: Pla de proves, pla de formació
 - **ACT**: Acta
 - **SEG**: Seguiment

La versió del document **NO** ha de formar part del mateix nom del fitxer ni del document, sinó que aquesta informació s'haurà de gestionar mitjançant l'apartat corresponent dins del document.

14.5 Planificació

Totes les tasques d'implantació hauran de ser completades segons la planificació establerta però mai podran superar la data límit de **31 de Desembre de 2018**. Tant la planificació, en durada i data d'inici, com la prioritització es realitzarà conjuntament entre TMB i l'adjudicatari.

14.6 Garantia de software

N/A.

14.7 Seguretat i confidencialitat

14.7.1 Confidencialitat i publicitat del servei

L'adjudicatari està obligat a guardar secret respecte les dades o la informació prèvia que no essent públics o notoris estiguin relacionats amb l'objecte del contracte.

Qualsevol comunicat de premsa o d'inserció als mitjans de comunicació que el proveïdor realitzi referent al servei que presta a TMB l'haurà d'aprovar prèviament el client.

14.7.2 Propietat intel·lectual

TMB adquirirà en exclusiva la propietat intel·lectual de tot el material que sigui elaborat per l'adjudicatari en execució del contracte i en particular, de tots els drets de propietat intel·lectual patrimonial, industrial i d'imatge que derivin del mateix inclosa l'explotació en qualsevol modalitat i sota qualsevol format, per a tot el món, del treball elaborat per l'adjudicatari o els seus empleats en execució del contracte, reservant-se TMB qualsevol altra facultat annexa al dret de propietat intel·lectual o industrial.

Serà propietat de TMB el resultat dels serveis així quants materials i documents es realitzin en compliment del contracte.

TMB serà titular de tots els drets referits en el paràgraf anterior pel termini màxim legal permès i l'única organització que per tal concepte podrà explotar i comerciar amb el treball desenvolupat en execució del Contracte, abans o després del seu acabament, corresponent als autors materials del mateix únicament els drets morals que els reconeix la legislació vigent en matèria de propietat intel·lectual.

Als efectes previstos en els dos paràgrafs anteriors, l'adjudicatari es compromet al lliurament de tota la documentació funcional i tècnica, així com materials i lliurables generats durant la prestació del servei i en el procés d'anàlisi, disseny, desenvolupament, implantació i proves de les mateixes. Tota la documentació elaborada i els resultats obtinguts per l'adjudicatari en execució del contracte seran propietat de TMB, en el poder del qual quedaran a

l'acabament del contracte, no podent l'adjudicatari utilitzar-la per a altres persones, entitats o empreses.

L'adjudicatari respondrà de l'exercici pacífic de TMB en la utilització del programari i altres drets proporcionats per l'adjudicatari amb motiu del contracte i serà responsable de tota reclamació que pugui presentar un tercer per aquests conceptes contra TMB i haurà d'indemnitzar TMB per tots els danys i perjudicis que aquesta pugui sofrir per aquesta causa. En tot cas les relacions jurídiques derivades del contracte s'establiran entre TMB i l'adjudicatari. TMB no estarà contractualment vinculada amb persones diferents de l'adjudicatari.

14.7.3 Seguretat i protecció de dades

L'adjudicatari dels serveis es compromet a complir els requeriments de seguretat i de continuïtat aplicables a l'objecte del contracte especificats a:

- La legislació vigent en general i, en particular, quan es tractin dades de caràcter personal, el Reglament de Seguretat del Reial Decret 994/1999 de la Llei Orgànica de Protecció de Dades de Caràcter Personal (LOPD).

Adicionalment, l'adjudicatari es compromet a:

- Complir amb les directives tecnològiques, de seguretat i de qualitat que estableixi el client.
- Implementar les mesures, els processos, i els requeriments que el client sol·liciti amb aquesta finalitat i li proposarà els que consideri necessaris per millorar les solucions.
- Facilitat tota aquella informació que el client requereixi per tal que pugui donar compliment a la legislació i normativa referida en aquest apartat.

L'incompliment de les clàusules relacionades en aquest epígraf relatives a la seguretat i la protecció de dades en general constitueix falta greu i motiu suficient per a la resolució unilateral del contracte.

TMB es reserva el dret de realitzar les auditories necessàries per a comprovar el compliment de les mesures de seguretat descrites en aquest plec.

14.8 Compartició de recursos

Per motius de garantir la seguretat, qualsevol compartició de recursos tècnics (infraestructura, de maquinari, etc.) utilitzats en el marc de l'execució del contracte serà prèviament justificada al client amb un informe d'anàlisi de beneficis i de riscos, que aquest haurà d'aprovar.

Els adjudicataris utilitzaran la xarxa, el maquinari i/o el programari propietat de TMB exclusivament per a l'ús o el benefici de TMB.

14.9 Rescissió del contracte

TMB estarà facultat per procedir a la resolució del contracte o acordar la continuïtat de l'execució amb imposició de noves penalitzacions si es compleix una de les dues condicions:

- Les penalitzacions per demora arriben a un múltiple del 5 per 100 del preu del contracte
- L'adjudicatari no proporciona un o més d'un dels serveis sol·licitats en els punts d'operació del servei o de compliment de normatives aplicades en aquest àmbit

La imposició de penalitzacions no exclou la indemnització a què pugui tenir dret la TMB pels danys i perjudicis ocasionats pel retard o actuació imputable al licitador.

14.10 Transició del servei

L'adjudicatari ha de presentar en la oferta un pla de transició del servei perquè en el cas en que en el següent concurs no sigui guanyador, es pugui fer el traspàs del servei a la nova empresa.

Cal que inclogui:

- Llistat de tasques en que es donarà suport
- Estimació temporal en que es donarà suport (hores/persona o temporal)

14.11 Altres condicions

El conjunt d'eines utilitzades per l'adjudicatari per a la realització del projecte no ha d'implicar l'adquisició de llicències complementàries a les eventualment necessàries en manera operativa. TMB requereix una documentació de totes les eines utilitzades per al desenvolupament en format digital. A més, es

requereix la producció i lliura de la documentació tècnica relativa a la implementació.