PLEC DE PRESCRIPCIONS TÈCNIQUES (PPT) DE LA LICITACIÓ DEL CONTRACTE DE PLATAFORMA DE SEGURETAT I OPTIMITZACIÓ D'APLICACIONS WEB (CDN, WAF I PROTECCIÓ DDOS) PER A BARCELONA ACTIVA

1. Objecte i abast

1.1. Objecte del contracte

L'objecte d'aquest contracte és la contractació d'un **servei gestionat de seguretat i optimització d'aplicacions web al núvol** que comprèn capacitats de xarxa de distribució de continguts (CDN), tallafoc d'aplicacions web (WAF), protecció contra atacs de denegació de servei distribuïda (DDoS) i serveis professionals associats, per a la protecció, optimització i disponibilitat de les aplicacions web públiques de Barcelona Activa.

Les prescripcions tècniques d'aquest plec es formulen en termes de rendiment i exigències funcionals, d'acord amb l'article 126.5.a de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (LCSP).

Qualsevol solució que acrediti el compliment equivalent dels requisits funcionals establerts serà admesa, independentment del fabricant o proveïdor tecnològic.

1.2. Abast del servei

L'abast del contracte comprèn:

- **1 domini principal** de Barcelona Activa.
- **Fins a 27 subdominis** associats a aplicacions web d'accés públic. El nombre de subdominis pot variar durant la vigència del contracte per altes, baixes o modificacions derivades de l'evolució del catàleg de serveis digitals de Barcelona Activa. El licitador haurà de preveure en la seva oferta un model de gestió àgil d'aquesta variabilitat.
- **Servei de posada en marxa**: configuració inicial, ajust fi i coordinació amb l'empresa de manteniment d'aplicacions.
- **Borsa de 30 hores anuals** de suport tècnic especialitzat.

2. Requisits funcionals de la plataforma

2.1. Funcionalitats mínimes exigides

La solució ofertada haurà d'incloure, com a mínim, les prestacions funcionals següents:

Funcionalitat	Especificació mínima
Regles de seguretat personalitzades (WAF)	Mínim 250 regles personalitzades actives simultàniament
Gestió de redireccions massives	Mínim 10.000 entrades de redirecció
Autenticació federada (SSO)	Integració amb proveïdors d'identitat estàndard (SAML 2.0, OAuth 2.0 / OpenID Connect)
Gestió de trànsit automatitzat (bots)	Protecció avançada amb analítica i classificació de bots
Ample de banda	Il·limitat, sense cost addicional per volum de trànsit
Disponibilitat de la xarxa de distribució	SLA igual o superior al 99,99% mensual

2.2. Tallafoc d'aplicacions web (WAF)

El servei haurà d'incloure un WAF gestionat amb les característiques següents:

- Conjunts de regles gestionades i actualitzades de forma contínua pel proveïdor.
- Capacitat de creació de regles personalitzades per a les necessitats específiques de Barcelona Activa.
- Mode de registre (*log mode*) per a la detecció de falsos positius abans de l'activació del mode bloqueig.
- Visibilitat en temps real dels esdeveniments de seguretat mitjançant consola d'administració.

Capacitats de definició de polítiques de seguretat

La plataforma haurà d'incorporar capacitats de definició de polítiques de seguretat per a, com a mínim, les funcions següents:

- **Virtual patching de vulnerabilitats**: aplicació de regles de mitigació temporal per a vulnerabilitats identificades, sense necessitat de modificar el codi font de l'aplicació, amb capacitat d'activació immediata.
- **Protecció OWASP Top 10**: regles de protecció alineades amb les categories de riscos de la guia OWASP Top 10 en la seva versió vigent, incloent-hi injeccions SQL, XSS, CSRF i configuracions incorrectes de seguretat.
- **Control d'accés geogràfic**: definició de polítiques d'accés basades en la geolocalització de les adreces IP d'origen, amb granularitat mínima a nivell de país.
- **Control d'accés per adreces IP**: gestió de llistes d'adreces IP o rangs CIDR (*allowlist* i *blocklist*), amb capacitat d'aplicació immediata sense intervenció del proveïdor.
- **Rate limiting**: limitació de taxa de peticions per URL, endpoint o grup de recursos, amb definició granular de llindars, finestres temporals i accions de resposta (bloqueig, repte, registre).
- **Protecció d'APIs**: capacitats específiques per a APIs, incloent-hi validació d'esquemes (JSON/XML), detecció d'abusos i cobertura dels riscos de l'OWASP API Security Top 10 en la seva versió vigent.
- **Protecció contra bots**: sistema de gestió i mitigació de trànsit automatitzat no legítim, amb capacitat de distingir entre bots legítims i maliciosos i d'aplicar polítiques diferenciades. Ha de suportar mecanismes de repte actiu (CAPTCHA o equivalent) i passiu (anàlisi de comportament).
- **Protecció contra vulnerabilitats conegudes (CVE)**: mecanisme d'actualització contínua de signatures associades a vulnerabilitats publicades al catàleg CVE, amb cobertura de vulnerabilitats crítiques en un termini màxim definit al contracte des de la seva publicació oficial.
- **Protecció davant tècniques d'evasió**: detecció i bloqueig de tècniques d'evasió habituals, com ara codificació de peticions malicioses, fragmentació de paquets, ofuscació de càrregues útils (*payload obfuscation*) o ús de protocols alternatius.
- **Detecció de patrons d'atac de capa 7**: anàlisi i detecció de patrons d'atac a la capa d'aplicació (capa 7 del model OSI), incloent-hi atacs de tipus *slow HTTP*, abús de lògica de negoci i altres vectors que no generin necessàriament un volum elevat de trànsit.

2.3. Protecció DDoS

El servei haurà d'incloure protecció contra atacs de denegació de servei distribuïda (DDoS) de capa 3, 4 i 7, sense límit de volum d'atac i sense cost addicional.

2.4. Rendiment i CDN

- Xarxa de distribució de continguts (CDN) global amb presència a Europa.
- Optimització automàtica d'imatges i recursos estàtics.
- Suport per a HTTP/3 i QUIC.
- Certificats SSL/TLS gestionats i inclosos en el servei.

2.5. SLA de la plataforma

El proveïdor haurà de garantir una disponibilitat igual o superior al 99,99**% mensual** de la xarxa de distribució i seguretat. En cas d'incompliment del SLA, el proveïdor haurà de gestionar activament la reclamació davant el fabricant de la solució i traslladar els crèdits de servei corresponents a Barcelona Activa.

3. Servei de posada en marxa

3.1. Abast i termini

El proveïdor haurà de realitzar la configuració inicial i la posada en marxa del servei en un termini màxim de **4 setmanes** des de la formalització del contracte. Aquest servei inclou:

- Configuració de zones DNS per al domini principal i tots els subdominis inicials.
- Configuració inicial de les regles WAF, polítiques de seguretat i redireccions.
- Activació i configuració del SSO.
- Configuració de la protecció DDoS i de la gestió de bots.
- Configuració dels certificats SSL/TLS.

3.2. Període de log mode

Durant els **primers 15 dies naturals** des de l'activació del servei, el WAF operarà en **mode registre (*log mode*)**, de manera que les regles registraran els esdeveniments però no bloquejaran el trànsit. Durant aquest període:

- El proveïdor haurà de monitorar activament els registres i identificar falsos positius.
- Es realitzaran els ajustos necessaris a les regles per minimitzar l'impacte sobre el trànsit legítim.
- Al final del període, el proveïdor lliurarà un informe de falsos positius detectats i les accions correctores aplicades.
- L'activació del mode bloqueig requerirà la validació expressa de Barcelona Activa.

3.3. Coordinació amb l'empresa de manteniment d'aplicacions

Atès que Barcelona Activa disposa d'una empresa de manteniment de les seves aplicacions web, el proveïdor haurà de:

- Establir un canal de comunicació directe amb l'equip tècnic de l'empresa de manteniment.
- Coordinar les tasques de configuració per evitar interrupcions del servei durant la posada en marxa.
- Documentar els canvis que puguin afectar a les aplicacions i notificar-los amb antelació suficient (mínim **48 hores**) a l'empresa de manteniment.
- Participar en almenys **una reunió de coordinació** prèvia a l'inici de la posada en marxa amb els equips tècnics de Barcelona Activa i de l'empresa de manteniment.

3.4. Ajust fi (*fine-tuning*)

Un cop finalitzat el període de *log mode* i activat el mode bloqueig, el proveïdor haurà de realitzar un procés d'ajust fi durant les **2 setmanes** següents, que inclourà:

- Revisió i optimització de les regles WAF en funció del trànsit real.
- Ajust dels paràmetres de rendiment (caché, optimització d'imatges, etc.).
- Configuració de les alertes de monitoratge.
- Lliurament del document de configuració final (*as-built*).

4. Borsa d'hores de suport tècnic

4.1. Dotació i model de gestió

El contracte inclou una **borsa de 30 hores anuals** de suport tècnic especialitzat, gestionada sota el model següent:

- **Reserva pressupostària**: l'import equivalent a les 30 hores es reserva pressupostàriament en el moment de la formalització del contracte per a cada anualitat.
- **Facturació per consum real**: la facturació es realitzarà únicament per les hores efectivament consumides, amb periodicitat trimestral.
- **Sense acumulació**: les hores no consumides en una anualitat no s'acumulen per a l'anualitat següent.
- **Alerta de consum**: el proveïdor haurà de notificar a Barcelona Activa quan s'hagi consumit el **75%** de la borsa d'hores, per tal de permetre la planificació de possibles necessitats addicionals.

4.2. Tipologia de tasques imputables

Són imputables a la borsa d'hores totes les tasques de suport tècnic especialitzat relacionades amb la plataforma contractada, incloent-hi, a títol enunciatiu i no limitatiu:

- Configuració i modificació de regles WAF i polítiques de seguretat.
- Alta, baixa i modificació de subdominis.
- Diagnòstic i resolució d'incidències tècniques.
- Optimització de la configuració de rendiment i seguretat.
- Assessorament tècnic sobre funcionalitats de la plataforma.
- Revisió i actualització de la configuració davant noves amenaces o vulnerabilitats.
- Suport en la coordinació amb l'empresa de manteniment d'aplicacions.

4.3. Imputació i registre d'hores

- Tota imputació d'hores a la borsa requerirà la **validació prèvia** de Barcelona Activa mitjançant ordre de treball (*work order*).
- El proveïdor haurà de mantenir un registre detallat de les hores consumides, amb indicació de la data, la tasca realitzada, el tècnic assignat i la durada.
- El registre haurà d'estar accessible per a Barcelona Activa en tot moment, preferentment mitjançant una eina de *ticketing* o gestió de projectes.
- Les fraccions mínimes d'imputació seran de **30 minuts**.

4.4. Nivells de servei (SLA) de la borsa d'hores

Les sol·licituds d'ús de la borsa d'hores es classificaran en tres nivells de prioritat, amb els temps de resposta i resolució següents:

Nivell	Descripció	Temps de resposta	Temps de resolució
Crític (P1)	Incidència que afecta la disponibilitat o seguretat de les aplicacions en producció	4 hores (24/7)	8 hores
Normal (P2)	Incidència o tasca que afecta el funcionament però no la disponibilitat	8 hores (horari hàbil)	2 dies hàbils
Baix (P3)	Consulta, millora o tasca planificable	2 dies hàbils	5 dies hàbils

L'horari hàbil s'entén de dilluns a divendres, de 8:00 a 18:00 h, exclosos festius oficials de Catalunya i de la ciutat de Barcelona.

En els casos en què la resolució depengui d'una actuació del fabricant de la solució com a tercera part, els temps de resolució quedaran suspesos durant el temps d'espera de la seva resposta, sempre que el proveïdor acrediti haver obert el tiquet corresponent i estar fent-ne el seguiment actiu.

5. Nivells de servei (SLA) i penalitzacions

5.1. SLA de disponibilitat de la plataforma

Indicador	Valor exigit
Disponibilitat de la xarxa de distribució i seguretat	99,99 % mensual o superior
Temps de recuperació davant incidències de la plataforma (RTO)	Segons SLA del fabricant de la solució adjudicada

5.2. SLA de temps de resposta del proveïdor

Nivell	Temps de resposta	Temps de resolució
Crític (P1)	4 hores (24/7)	8 hores
Normal (P2)	8 hores (horari hàbil)	2 dies hàbils
Baix (P3)	2 dies hàbils	5 dies hàbils

5.3. Règim de penalitzacions

Les penalitzacions s'aplicaran sobre el **preu mensual del contracte** (llicència + servei de suport), IVA exclòs, d'acord amb l'article 192 LCSP. La penalització màxima per falta no podrà superar el **10% del preu del contracte**, ni el total de penalitzacions el **50% del preu del contracte**.

Incompliment	Penalització
Incompliment del temps de resposta P1	3% del preu mensual per incidència
Incompliment del temps de resolució P1	2% del preu mensual per cada 4 hores addicionals
Incompliment del temps de resposta P2	1% del preu mensual per incidència
Incompliment del temps de resolució P2	1% del preu mensual per dia hàbil addicional
No lliurament d'informe mensual en termini	0,5% del preu mensual per dia de retard
Incompliment reiterat (3 o més en 3 mesos)	Possible resolució del contracte

6. Obligacions de documentació i lliurament

6.1. Documentació de posada en marxa

En el termini màxim de **5 dies hàbils** des de la finalització de la posada en marxa, el proveïdor haurà de lliurar:

- **Document de configuració inicial (*as-built*)**: descripció completa de tota la configuració implementada (zones DNS, regles WAF, redireccions, SSO, certificats, etc.).
- **Informe del període de *log mode***: resum dels falsos positius detectats, les accions correctores aplicades i l'estat final de les regles.
- **Manual d'operació bàsic**: guia per al personal tècnic de Barcelona Activa per a la gestió quotidiana de la plataforma (accés a la consola, consulta de registres, obertura d'incidències, etc.).

6.2. Informes periòdics

Durant tota la vigència del contracte, el proveïdor haurà de lliurar els informes següents:

Informe	Periodicitat	Termini de lliurament
Informe mensual d'activitat	Mensual	Abans del dia 10 del mes següent
Informe de consum de la borsa d'hores	Trimestral	Abans del dia 15 del mes següent al trimestre
Informe de seguretat i amenaces	Trimestral	Abans del dia 15 del mes següent al trimestre
Informe de revisió de configuració	Semestral	Abans del dia 20 del mes següent al semestre

L'informe mensual d'activitat haurà d'incloure, com a mínim: resum d'amenaces bloquejades, trànsit total i per subdomini, incidències obertes i tancades, consum acumulat de la borsa d'hores i alertes de seguretat rellevants.

6.3. Documentació de fi de contracte

Amb una antelació mínima de **3 mesos** respecte a la data de finalització del contracte, el proveïdor haurà de lliurar:

- Documentació tècnica actualitzada de tota la configuració vigent.
- Exportació de tots els registres i logs disponibles.
- Credencials d'accés i inventari de tots els recursos configurats.
- Informe de recomanacions per a la continuïtat del servei.

A la finalització del contracte, caldrà que l'adjudicatari sortint transfereixi la propietat del compte cloud de la solució WAF a Barcelona Activa o a l'adjudicatari entrant, de manera que es garanteixi la continuïtat del servei sense perdre les configuracions i ajustos creats.

6.4. Formació i transferència de coneixement

Amb l'entrega del projecte, l'adjudicatària haurà d'impartir una formació en l'operació de la plataforma al personal tècnic de Barcelona Activa.

Alternativament, l'empresa adjudicatària haurà d'impartir, almenys **una vegada per any contractual**, una sessió de transferència de coneixement adreçada al personal tècnic de Barcelona Activa, amb una durada mínima de 2 hores, sobre novetats de la plataforma contractada i bones pràctiques de configuració.

Sergi Ruiz Talavera
Responsable de sistemes i ciberseguretat