



PLEC DE PRESCRIPCIONS TÈCNiques (PPT) PER LA LICITACIÓ DEL CONTRACTE MIXT DE SUBMINISTRAMENT D'UNA LLICÈNCIA DE GESTIÓ I CONTROL D'ACTIUS I SERVEIS DE SUPORT ASSOCIATS

1. ANTECEDENTS

Barcelona Activa té la missió de contribuir a la millora de la qualitat de vida de les persones promovent la competitivitat econòmica de la ciutat i el reequilibri dels territoris, a través del foment de l'ocupació de qualitat, l'impuls a l'emprenedoria i el suport a un teixit empresarial plural, divers i sostenible, des d'una perspectiva econòmica, social i ambiental.

La nostra visió és fer de Barcelona una ciutat de referència internacional per treballar, emprendre i viure amb valors socials i ambientals. Una de les principals prioritats municipals dels darrers anys ha estat la lluita contra l'atur i la precarietat laboral. Fomentar l'ocupació de qualitat és essencial per a la ciutat i constitueix un element clau per a la millora de la cohesió social i l'avenç cap a un nou model de desenvolupament just i sostenible.

Per aconseguir-ho, Barcelona Activa acompanya les persones en el seu procés de recerca de feina basant-se en els eixos que la defineixen (persona, aspectes psicosocials i mercat de treball), per tal d'augmentar les seves oportunitats d'accedir a un lloc de treball de qualitat.

Actualment, Barcelona Activa està sotmesa a diverses obligacions de conformitat en matèria de seguretat informàtica, derivades de la normativa vigent i dels estàndards de seguretat reconeguts, el compliment de les quals és imprescindible per evitar sancions i garantir una gestió responsable de les dades personals i la informació sensible.

En conseqüència, Barcelona Activa té com a objectiu millorar la gestió dels seus actius tecnològics i garantir la seguretat de la seva infraestructura informàtica. La implementació d'una solució de gestió i control d'actius informàtics ajudaria a garantir el normal funcionament i reduir les vulnerabilitats dels sistemes i les aplicacions corporatives.

La implementació d'aquesta eina per al servei de gestió i control d'actius informàtics, contribuiria a que l'activitat de Barcelona Activa s'adeqüés als requisits mínims de seguretat, protegint la informació confidencial i assegurant la privacitat de les persones usuàries i les parts interessades, donant compliment a la missió i objectius d'aquesta, del Barcelona Green Deal i del Pla d'Actuació Municipal.

2. SITUACIÓ ACTUAL

Barcelona Activa té com a objectiu millorar la gestió dels seus actius tecnològics, així com mantenir un control eficaç de la seguretat de la seva infraestructura informàtica. Amb aquesta finalitat, es requereix contractar una solució de gestió i control d'actius que permeti una supervisió detallada del parc informàtic i una gestió efectiva de les vulnerabilitats en matèria de ciberseguretat.

Actualment, Barcelona Activa necessita una eina que faciliti la gestió centralitzada dels seus actius informàtics, incloent-hi equips de treball, dispositius de xarxa i altres recursos tecnològics. A més, és essencial disposar d'una funcionalitat de gestió de vulnerabilitats que permeti identificar i abordar de manera proactiva les possibles amenaces de seguretat.



3. NORMATIVA I OBLIGACIONS DE CONFORMITAT

Barcelona Activa està sotmesa a diverses obligacions de conformitat en matèria de seguretat informàtica, les quals es deriven de la normativa vigent i dels estàndards de seguretat reconeguts. A continuació, s'estableixen les principals referències normatives i les seves implicacions per a la gestió dels actius informàtics:

- **Esquema Nacional de Seguretat (ENS):**
 - En virtut del Reial Decret 311/2022, del 3 de maig, l'ENS és d'aplicació a les entitats del sector públic i a aquelles del sector privat que presten serveis competencials. Aquesta normativa estableix les directrius i els requisits mínims per a garantir la seguretat de la informació en els sistemes d'informació.
 - Atenent la naturalesa jurídica dual de Barcelona Activa, aquesta entra dins de la descripció d'entitat definida a l'apartat d) de l'article 77.1 de la LOPDGDD i, per tant, li resulta d'aplicació l'obligatorietat de la Disposició Addicional Primera del mateix text legal en quant a l'adequació a l'ENS.
 - L'aplicació de l'ENS per a aquest servei és fonamental per garantir que la gestió i control d'actius informàtics compleixen amb els estàndards de seguretat requerits, protegint així la informació sensible i assegurant la confidencialitat, integritat i disponibilitat de la mateixa.
- **Reglament General de Protecció de Dades (RGPD):**
 - El RGPD, que va entrar en vigor el 25 de maig de 2018, té com a objectiu principal protegir els drets i les llibertats fonamentals de les persones físiques, especialment el dret a la protecció de dades personals. Aquesta regulació estableix normes sobre la recollida, el tractament i la protecció de dades personals dins de la Unió Europea i l'Espai Econòmic Europeu.
 - L'aplicació del RGPD és crucial per a aquest servei, ja que involucra la gestió i el control d'actius informàtics que poden contenir dades personals. Garantir el compliment del RGPD és fonamental per protegir la privacitat dels titulars de les dades i evitar sancions per incompliment de la legislació de protecció de dades.
- **Llei Orgànica de Protecció de Dades Personals i Garantia dels Drets Digitals (LOPDGDD):**
 - La LOPDGDD, aprovada el 5 de desembre de 2018, complementa el RGPD en l'àmbit nacional i estableix disposicions específiques per a la protecció de les dades personals i la garantia dels drets digitals a Espanya.
 - L'aplicació de la LOPDGDD és rellevant per a aquest servei ja que regula la protecció de les dades personals i els drets digitals dels ciutadans espanyols. És essencial garantir el compliment d'aquesta llei per protegir la privacitat i els drets de les persones usuàries en relació amb les dades personals emmagatzemades i processades pels sistemes informàtics de Barcelona Activa.
- **Altres Normatives Sectorials:**
 - A més de les disposicions generals en seguretat informàtica, Barcelona Activa pot estar subjecta a altres normatives sectorials o específiques del seu àmbit d'activitat. Aquestes normatives poden incloure requisits addicionals en matèria de seguretat informàtica i protecció de la informació.

La integració d'aquesta normativa és essencial per al servei de gestió i control d'actius informàtics de Barcelona Activa, ja que establint els requisits mínims de seguretat, es protegeix la informació confidencial i s'assegura la privacitat de les persones usuàries i les parts interessades. El compliment d'aquestes normatives és imprescindible per a Barcelona Activa per evitar sancions i garantir una gestió responsable de les dades personals i la informació sensible.

4. OBJECTE

L'objecte del present servei és el subministrament d'una llicència Pro de l'eina Lansweeper per a 6.000 assets (actius), així com la prestació de 20 hores de consultoria de suport. L'eina Lansweeper és una solució



de gestió i control d'actius informàtics, amb capacitat per a la supervisió detallada dels equips i la xarxa, així com la gestió de vulnerabilitats sense necessitat d'instal·lar un agent als dispositius finals.

5. OBJECTIUS

Els objectius específics de la solució són:

Gestió Eficient dels Actius Informàtics:

- Proporcionar una visió global i detallada dels actius informàtics de Barcelona Activa, incloent-hi equips de treball, dispositius de xarxa, servidors i altres recursos tecnològics.
- Mantenir un inventari actualitzat dels actius, incloent-hi informació rellevant com ara configuracions, especificacions tècniques i ubicacions físiques.

Supervisió i Monitoratge Continu:

- Oferir una supervisió en temps real de l'estat dels actius informàtics, incloent-hi el rendiment dels equips, l'ús dels recursos de xarxa i altres indicadors rellevants.
- Detectar de manera proactiva problemes potencials i alertar sobre situacions anòmales o irregularitats en el funcionament dels sistemes.

Gestió de Configuració i Pegats de Seguretat:

- Administrar la configuració dels equips de treball i dispositius de xarxa, garantint la coherència i la conformitat amb els estàndards de seguretat establerts per l'organització.
- Gestionar de manera eficient els pegats de seguretat i les actualitzacions de seguretat, assegurant que tots els sistemes estiguin actualitzats i protegits contra vulnerabilitats conegudes.

Generació de Informes i Anàlisis:

- Generar informes detallats i personalitzats sobre els actius informàtics, proporcionant informació rellevant per a la presa de decisions i la planificació estratègica.
- Realitzar anàlisis i informes específics sobre la seguretat dels sistemes, incloent-hi la identificació de possibles punts febles i recomanacions per a la millora de la seguretat.

Gestió de Vulnerabilitats:

- Identificar i classificar les vulnerabilitats dels sistemes informàtics, incloent-hi els equips de treball, els servidors i altres dispositius de xarxa.
- Prioritzar les vulnerabilitats segons el seu grau de criticitat i proporcionar recomanacions per a la seva correcció o mitigació.

Seguretat i Conformitat Normativa:

- Garantir el compliment dels requisits normatius i les polítiques de seguretat de Barcelona Activa, incloent-hi la protecció de dades, les regulacions sectorials i els estàndards de seguretat.
- Proveir informació i eines per a les auditories de conformitat i la preparació per a les certificacions de seguretat pertinents.

Optimització de Recursos i Reducció de Riscos:

- Optimitzar l'ús dels recursos informàtics i minimitzar els riscos de seguretat mitjançant una gestió efectiva dels actius i una resposta proactiva a les amenaces.
- Identificar oportunitats d'optimització i millora de la infraestructura informàtica per aconseguir una millor eficiència i reduir els costos operatius.

Millora Continua:

- Fomentar una cultura de millora contínua en matèria de gestió i seguretat informàtica, mitjançant la revisió i l'avaluació regular dels processos i les pràctiques existents.
- Proporcionar eines i recursos per a la formació i el desenvolupament del personal de Barcelona Activa en temes relacionats amb la gestió i la seguretat informàtica.



6. ABAST I CARACTERÍSTIQUES

Barcelona Activa té com a objectiu millorar la gestió dels seus actius tecnològics i garantir la seguretat de la seva infraestructura informàtica mitjançant la implementació d'una solució de gestió i control d'actius informàtics. Per aconseguir aquesta meta, s'ha decidit contractar les llicències de la solució Lansweeper.

Aquest contracte abasta l'adquisició d'una llicència Pro de l'eina Lansweeper per a 6.000 *assets* (actius) per a la solució de gestió i control d'actius informàtics, així com una borsa de 20 hores de suport. Les característiques específiques del producte són, entre d'altres, la seva capacitat per a supervisar i gestionar els actius informàtics, la seva eficàcia en la detecció de vulnerabilitats, així com altres funcionalitats rellevants per a les necessitats de Barcelona Activa.

Llicència i Característiques del Producte:

La solució que s'està buscant ha de ser capaç d'oferir una àmplia gamma de funcionalitats per a la gestió exhaustiva d'actius informàtics i la gestió de vulnerabilitats. Es busca una solució integrada que proporcioni una visió completa de tots els dispositius i recursos de la xarxa, així com una manera eficaç de gestionar i mitigar els riscos de seguretat associats. A continuació, es detallen amb més profunditat les funcionalitats específiques que s'esperen de la solució:

Descobriment i Inventari Detallat:

- La solució ha de tenir la capacitat de realitzar un descobriment detallat de tots els actius de la xarxa, incloent-hi equips de sobretaula, portàtils, servidors físics i virtuals, dispositius de xarxa, impressores, equips mòbils i altres elements actius. Utilitzant tecnologies d'escaneig avançades, la solució ha d'identificar tots els dispositius connectats a la xarxa, recopilant informació exhaustiva sobre la seva configuració, software instal·lat, actualitzacions pendents, adreces IP i altres detalls rellevants.

Monitoratge Proactiu i Supervisió Continuada:

- S'espera que la solució ofereixi la capacitat per a monitorar proactivament els actius de la xarxa i supervisar-los de forma continuada per a la detecció de problemes de rendiment, falles de hardware o software i altres incidents potencials. Mitjançant alertes personalitzables i notificacions en temps real, els administradors han de poder identificar i abordar ràpidament qualsevol anomalia o problema.

Gestió de Configuracions i Polítiques de Seguretat:

- La solució ha de permetre als administradors gestionar centralitzadament les configuracions dels actius i aplicar polítiques de seguretat cohesives a tota l'organització. Amb funcions de desplegament de software, gestió de paquets d'actualització i control de polítiques de grup, la solució ha de facilitar la implementació i l'aplicació de mesures de seguretat estandarditzades per a protegir els actius de la xarxa.

Automatització de Tasques i Orquestració de Processos:

- S'espera que la solució inclogui eines d'automatització potents per a realitzar tasques repetitives i orquestrar processos complexos relacionats amb la gestió d'actius i la seguretat informàtica. Amb funcions de programació de tasques, fluxos de treball automatitzats i integració amb altres sistemes a través d'APIs, la solució ha de permetre als administradors simplificar i accelerar les operacions quotidianes de gestió.

Gestió de Vulnerabilitats i Anàlisi de Riscos:

- La solució ha de ser capaç d'identificar i gestionar vulnerabilitats en els actius de la xarxa. Utilitzant escaneigs de seguretat en profunditat i bases de dades actualitzades de signatures de vulnerabilitats, la solució ha de detectar punts febles de seguretat i proporcionar recomanacions per a la seva mitigació. A més, ha d'oferir funcions avançades d'anàlisi de riscos per a avaluar la severitat i l'impacte potencial de les vulnerabilitats detectades.



Integració amb Altres Tecnologies i Plataformes:

- S'espera que la solució sigui compatible i integrable amb una àmplia gamma de tecnologies i plataformes utilitzades a Barcelona Activa, incloent-hi sistemes de gestió d'incidències (ITSM), portals de servei d'usuari (SSP), sistemes de gestió de xarxes (NMS) i altres solucions de seguretat i gestió de la informació. Mitjançant connectors i integracions API, la solució ha de permetre una interoperabilitat fluida i una gestió més eficient dels recursos tecnològics.

Seguretat Avançada i Privacitat de Dades:

- La solució ha de incorporar funcions avançades de seguretat per a protegir la confidencialitat i la integritat de les dades de la xarxa. Amb mesures de xifrat, controls d'accés granulars, auditories detallades i altres mecanismes de protecció, la solució ha de garantir la seguretat i la privacitat de les dades sensibles emmagatzemades a la plataforma.

Funcionament Sense Agent:

- La solució ha de poder operar sense la necessitat d'instal·lar agents en cada dispositiu de la xarxa, simplificant així la implementació i la gestió de la solució.

Integració SSO i MFA:

- És essencial que la solució ofereixi integració amb sistemes de Single Sign-On (SSO) i autenticació multi factor (MFA) per a garantir una autenticació segura i eficient dels usuaris.

Cloud Discovery:

- La solució ha de proporcionar funcionalitats avançades de descobriment d'actius al núvol, permetent identificar i monitorar els recursos que resideixen en entorns cloud, com ara instàncies de màquines virtuals, bases de dades, emmagatzematges, entre altres. Això possibilita una visibilitat completa de l'entorn de TI, incloent-hi els actius que es despleguen en plataformes de núvol públiques, privades i híbrides.

Generació de Informes Personalitzats i Dashboards Interactius:

- La solució ha de disposar d'eines avançades per a la generació de informes personalitzats sobre l'estat dels actius, els riscos de seguretat, el compliment normatiu i altres aspectes rellevants per a la gestió de la infraestructura tecnològica. Amb una àmplia gamma de plantilles de informes predefinides i la capacitat de crear informes personalitzats mitjançant un generador d'informes flexible, la solució ha de permetre als administradors obtenir una visió completa i detallada de la seva xarxa.

- Alguns dels informes que ha de ser capaç de generar de forma automàtica són:

- Informe d'estat dels actius
- Informe de riscos de seguretat
- Informe de compliment normatiu
- Informe d'auditoria de seguretat
- Informe d'inventari de software
- Informe d'ús de llicències de software
- Informe d'activitat de l'usuari
- Informe d'activitat de la xarxa
- Informe d'estat de la seguretat
- Informe de vulnerabilitats
- Informe d'incident de seguretat
- Informe de seguiment de tasques
- Informe de diagnòstic de la xarxa
- Informe d'ús del núvol (Cloud Usage Report)
- Informe d'estructura de l'actiu
- Informe de disponibilitat de l'actiu
- Informe d'ús dels recursos del sistema
- Informe de manteniment preventiu



- Informe de control d'accés
- Informe de gestió d'incidents

7. LLIURABLES

1. **Documentació de Llicències:**
 - Especificacions detallades de les llicències adquirides, incloent-ne el nombre de llicències, la durada de la subscripció i qualsevol restricció associada.
2. **Informació de Suport:**
 - Detalls sobre els serveis de suport proporcionats pel proveïdor, incloent-ne els nivells de suport disponibles, els horaris d'assistència i els canals de comunicació.
3. **Informació de Facturació:**
 - Detalls sobre els procediments de facturació associats a les llicències adquirides, incloent-ne els termes de pagament, els terminis de renovació i qualsevol informació rellevant sobre la gestió de pagaments.
4. **Clau de Llicència:**
 - Entrega de claus de llicència vàlides i úniques per a cada llicència adquirida, garantint-ne la autenticitat i la legalitat d'ús.
5. **Contracte de Llicència:**
 - Acord contractual formal que estipula els termes i condicions de l'adquisició de les llicències de Lansweeper, incloent-ne les disposicions sobre garanties, responsabilitats i resolució de conflictes.
6. **Certificat de Propietat:**
 - Certificació oficial que acredita la propietat de les llicències adquirides, proporcionant-ne una prova de validesa i autenticitat.

8. CONDICIONS TÈCNIQUES PARTICULARS

A continuació fem esment de les condicions tècniques particulars que caldrà complir:

Modalitat del contracte: L'empresa adjudicatària serà l'encarregada de tramitar amb Lansweeper el contracte llicències Pro de Barcelona Activa així com d'oferir les hores de consultoria.

Vigència del contracte: 3 anys comptadors a partir de la data següent a la de formalització del contracte.

Revisió i comanda anual: Per a cadascuna de les 3 anualitats del contracte, dos mesos abans del venciment (finals de gener) caldrà mantenir una reunió entre l'empresa adjudicatària del contracte i Barcelona Activa per tal d'acordar el nombre d'unitats de cada llicència que s'inclouran a la comanda i el nombre d'hores de consultoria restants.

Facturació: el contracte es facturarà en períodes d'anys naturals. En el cas de comandes que incloguin més d'una anualitat (reserves) s'aplicarà exactament la mateixa lògica de facturació.

Marc Puente Vila-Masana
Director de Tecnologia