PLEC DE PRESCRIPCIONS TÈCNIQUES

Expedient CM-2024-85851

Acord Marc

per al subministrament de subscripcions de productes Splunk i serveis professionals associats

IThink UPC

Contingut

1. Objecte del contracte

El present plec té com objecte definir les prescripcions tècniques particulars i fixar uns valors de qualitat en l'adquisició de productes Splunk així com els serveis professionals associats a la instal·lació i suport que del seu ús es deriven.

Per als articles que composen l' equipament estimat per aquest contracte, es busca poder disposar d'un proveïdor que pugui subministrar en comandes successives, els productes sol·licitats, a un preu estable i fora dels fluxos del mercat sempre d'acord amb les clàusules de revisió de preus que es determinin en el Plec de clàusules administratives, permetent d'aquesta manera, una planificació acurada dels recursos necessaris per a optimitzar els costos dels nous projectes de IThinkUPC i garantir la seva viabilitat econòmica. L'adjudicació del contracte marc portarà implícita la continuïtat del subministrament de productes proposats durant tota la seva vigència.

2. Béns objecte del contracte

El béns que composen l'objecte del contracte es detallen a l'Annex 1.

Aquest inclou la quantitat estimada de cadascun dels productes que s'hauran de subministrar durant la vigència del present acord marc, així com les unitats per a calcular l'import màxim de referencia per a la valoració econòmica.

3. Característiques dels productes

Els principals productes Splunk que es podrien adquirir són els següents:

- Splunk Cloud Platform.
- Splunk Enterprise.
- Splunk Security Essentials + InfoSec.
- Splunk User Behavior Analytics.
- Phantom.
- Splunk IT Service Inteligence.
- SignalFx.
- VictorOps.
- Splunk Insights para AWS Cloud Monitoring.
- Splunk App for Infrastructure.
- Splunk para IoT.
- Splunk Business Flow.

Splunk Cloud

Splunk Cloud és un producte SaaS de programari que permet cercar, analitzar i visualitzar les dades recopilades dels components d'una infraestructura de TI. Splunk pren dades de llocs web, aplicacions, sensors, dispositius, etc. Després de definir l'origen de dades, Splunk indexa el flux de dades i l'analitza en una sèrie d'esdeveniments individuals que es poden veure i cercar.

Splunk Security Essentials

És la solució principal que proposa Splunk com a SIEM. Splunk Security Essentials utilitza les capacitats de cerca i informes de la plataforma Splunk per proporcionar al professional de seguretat una visió general de seguretat a una organització. Security Essentials utilitza cerques de correlació per proporcionar visibilitat de les amenaces rellevants per a la seguretat i generar esdeveniments notables per al seguiment de les amenaces identificades. Es poden capturar, monitoritzar i informar sobre dades de dispositius, sistemes i aplicacions a l'entorn.

Els preus adjudicats operaran com a preus **màxims** durant tota la durada de l'acord marc.

4. Requisits i obligacions essencials del contracte

Els licitadors han de complir els següents requisits per poder presentar-se a aquesta licitació:

- El certificat ISO 27001 o equivalent vigent a la data de presentació de la sol·licitud de participació. Es presentarà còpia del certificat de qualitat vigent i en el cas que la ISO hagi caducat una vegada presentada la sol·licitud de participació s'ha d'acreditar mitjançant el certificat de l'empresa qualificadora haver sol·licitat la renovació de la certificació i assolit amb èxit l'auditoria corresponent amb anterioritat a la data de pèrdua de vigència.

- El certificat ISO 9001 Sistema de Gestió de la Qualitat o equivalent vigent a la data de presentació de la sol·licitud de participació. Es presentarà còpia del certificat de qualitat vigent i en el cas que la ISO hagi caducat una vegada presentada la sol·licitud de participació s'ha d'acreditar mitjançant el certificat de l'empresa qualificadora haver sol·licitat la renovació de la certificació i assolit amb èxit l'auditoria corresponent amb anterioritat a la data de pèrdua de vigència.

- Certificació en Esquema Nacional de seguretat (mig o superior) en serveis de SOC i/o en gestió de plataformes SIEM vigent a la data de presentació de la sol·licitud de participació. Aquest apartat es considera requisit essencial i serà exclòs aquell licitador que no compleixi amb ell.

5. Característiques dels serveis associats

5.1. Serveis Professionals

Els serveis professionals poden arribar a incloure tot el conjunt de tasques necessàries des de l'anàlisi de requeriments per a la preparació d'una proposta de projecte, el suport tècnic per a la instal·lació i explotació de la infraestructura.

També es pot requerir participar en una part de l'execució de projectes.

5.2. Perfils

Es valoraran en format bossa d'hores dos perfils:

- Analista/consultor expert per Consultoria i arquitectura de projectes expert en productes Splunk. Per aquest perfil es requereix més de tres anys d'experiència en disseny, manteniment, integracions amb tercers i evolució de plataformes SIEM.
- Tècnic de suport per Suport tècnic i projectes, amb més d'un any d'experiència en l'ús i manteniment de plataformes SIEM i integracions de tercers amb Splunk.

6. Suport tècnic i garantia

6.1. Garantia

Tots els productes inclouen garantia per part del fabricant, sense perjudici que sigui gestionada per la empresa proveïdora.

6.2. Suport tècnic

L'adjudicatari disposarà d'un sistema d'atenció i suport tècnic per aquest acord que garanteixi la recepció d'incidències durant 8 hores al dia en l'horari de dilluns a divendres laborables de 8:00h a 21:00h agost i festius locals de: 08:00h a 15:00.

Els tècnics hauran de seguir les normes de documentació, seguiment, resolució i escalat de les incidències establertes per IThinkUPC.

6.3. Temps de resposta

El temps de resposta, definit com el període màxim de temps entre la notificació de l'avaria i la resposta d'un tècnic especialitzat, haurà de ser de quatre hores laborables.

6.4. Temps de resolució

El temps de resolució, definit com el període màxim de temps entre la notificació de l'avaria i la seva resolució, ha de ser de dos dies laborables.

7. Contingut oferta tècnica

L'oferta tècnica a presentar haurà de recollir entre d'altres els següents punts:

- Relació de partnership amb Splunk de primer ordre.
- Referències en projectes d'implantació similars a Catalunya i Espanya.
- Experiència en integracions d'aquestes solucions amb altres fabricants.
- Certificacions dels tècnics o en curs.
- Possibilitat d'altres serveis de suport en temes de ciberseguretat

Annex 1 - Volumetria

La volumetria estimada de contractacions derivades de serveis i subministraments de productes durant la vigència de l'acord marc (3 anys) és la següent:

SUBMINISTRAMENTS I SERVEIS	UNITATS
Hores d'Analista/consultor expert per Consultoria i arquitectura de projectes	240
Hores de Tècnic de suport per Suport tècnic i projectes)	240
Subscripcions d'Splunk Cloud Platform i Splunk Security Essentials:	
per 1 any, 20 GB d'ingesta diària i 90 dies de retenció	12
per 1 any, 35 GB d'ingesta diària i 90 dies de retencio	9
per 3 anys, 35 GB d'ingesta diària i 365 dies de retenció	3

La configuració dels productes adquirits durant aquests 3 anys pot variar i es poden afegir mòduls o canviar els GB o la durada de retenció dels logs. El número de subscripcions és estimat i no són xifres garantides.