

L'òrgan de contractació de l'Agència de Ciberseguretat de Catalunya, emet la següent memòria justificativa de la contractació

MEMÒRIA

Justificativa de la necessitat i idoneïtat de la contractació del subministrament , instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya Lot 1: Evolució de la plataforma d'emmagatzematge i correlació d'esdeveniment de seguretat; Lot 2: Evolució de la plataforma de còpies de seguretat

De conformitat amb l'article 28 de la Llei 9/2017, de 8 de novembre, de Contractes del Sector Públic (en endavant, LCSP), la present memòria s'emet als efectes de justificar la naturalesa i extensió de les necessitats que es pretenen cobrir mitjançant el present contracte, així com la idoneïtat del seu objecte i contingut per satisfer-les.

Primer.- Necessitats a satisfer: Les necessitats a satisfer mitjançant el present contracte consisteixen en:

➤ **Lot 1:**

La monitorització de les alertes de seguretat que les diferents plataformes i sistemes d'informació és un dels serveis clau a la hora de gestionar de forma eficient la seguretat dels mateixos. Per aquest fet, i derivat del gran increment de registres de seguretat de les noves aplicacions i infraestructures (tant associades al COVID-19 com al Teletreball) que són necessaris gestionar, es precisa incrementar les capacitats de ingesta i tractament dels mateixos.

Concretament, i pel que fa al major pes contractual, es requereix d'un subministrament de maquinari necessari per incrementar les capacitats del Data Lake actual de la Agència de Ciberseguretat de Catalunya, tant a nivell de llicenciament de events per segons a poder gestionar, com en relació als nodes necessaris per tractar i emmagatzemar aquestes dades claus. A aquests efectes, cal dur a terme la migració d'un Data Lake intern del SOC, així com l'afinament de la solució final per a que aquesta resulti estable i amb capacitat suficient d'ingesta i de consulta de la informació continguda.

La raó de ser d'aquesta contractació, doncs, ve determinada per la necessitat d'estabilització de la infraestructura Elastic, implementant el repositori centralitzat d'esdeveniments de seguretat i realitzant les tasques de manteniment correctiu i evolutiu requerit en l'àmbit de les tecnologies que formen l'stack de productes Elasticsearch de l'Agència.

Memòria justificativa del contracte de subministrament , instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya
Número d'Expedient: CO.03.2020

A tal efecte, cal incorporar més nodes al clúster, per així poder incorporar noves fonts d'informació, respectant els estàndards de bones pràctiques existents. L'Agència actualment disposa d'un clúster Elastic implementat en el seu propi CPD que no té el dimensionament necessari per poder suportar les fonts i retenció requerides.

Es requereix la millora funcional de la solució, principalment pel que fa a la ingesta i parseig de fonts.

Fent una primera anàlisi de les necessitats d'increment d'infraestructura, s'han identificat 3 aspectes:

- El dimensionament dels recursos d'informació que s'està processant.
- L'arquitectura actual ha de ser resilient davant d'una fallada dels servidors i, per tant, evitar la possible pèrdua de les dades. A tal efecte, cal redefinir l'arquitectura per evitar aquesta possible indisponibilitat.
- L'arquitectura que es vol implementar ha de poder optimitzar l'entrada i sortida de dades dels elements d'emmagatzematge, evitant les dependències i augmentant la disponibilitat de la plataforma.

➤ **Lot 2:**

La continuïtat de les diferents plataformes i sistemes d'informació vinculats a l'Agència de Ciberseguretat de Catalunya que vetlla per la Ciberseguretat dels actius de la Generalitat de Catalunya, , precisa d'una protecció necessària davant d'un atac de *ransomware* que pugues xifrar els actuals sistemes d'informació i repositoris de *backup*. Per tant resulta necessari garantir que la Agència de Ciberseguretat de Catalunya disposi d'un nou sistema de *Backup*.

Per tant, degut a l'increment de temps i recursos necessaris de les noves aplicacions i infraestructures per la situació actual que són necessaris gestionar, es precisa incrementar les capacitats de *backup* així com de servidors de fitxers, tot disminuint la capacitat de retenció i restauració i el temps dedicat a la gestió dels mateixos.

Concretament, es requereix el subministrament d'una plataforma hiperconvergent de *backup* inmutable i servidor de fitxers i objectes en la mateixa plataforma de gestió amb capacitat de desbordament a cloud.

A tal efecte, cald dur a terme la configuració de la plataforma amb integració i protecció de l'actual entorn de virtualització, així com la configuració del emmagatzemament NAS, documentació i traspàs de coneixement.

Per la naturalesa del subministrament resulta necessari un manteniment del subministrament trimestral per la revisió i proposta de millores sobre la plataforma i amb una durada de 3 anys.

Assenyalat l'anterior, val a dir que resulta necessari millorar el sistema de de backups de la ACC. L'actual sistema de backups conta d'un servidor amb el SW backup.exe i 2 robots de cinta HPE MSL4048. Actualment el sistema no pot realitzar la totalitat dels backups de les màquines virtuals del la ACC i molt menys amb la freqüència desitjada, per tant el RPO (Recovery Point Objective) no es el necessari segons criteri de negoci

*Memòria justificativa del contracte de subministrament , instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya
Número d'Expedient: CO.03.2020*

i Compliance. Es pretén millorar la capacitat d'emmagatzematge, la rapidesa i recerca dels backups i de la restauració, aconseguint un RPO molt més baix. En quan al RTO (Recovery Time Objective), el sistema ha de permetre que aquest paràmetre sigui el més inferior possible.

Així les coses, es fa palès que resulta necessari substituir la plataforma actual per una homogènia amb gestió unificada, de tipus hiperconvergent tant en computació com en emmagatzematge, basada en maquinari generalista de tipus x86 i composta per un nombre de nodes, organitzats en un o més clústers, suficient per a proporcionar el servei descrit.

Aquesta solució haurà de permetre un arxivat i gestió conjunta amb entorns Cloud: Azure i AWS principalment. El sistema deuria poder permetre que la sincronització del sistema On-Promise i el Cloud depengués únicament de la capacitat de les línies WAN/Internet d'ambdós sistemes.

Per tot l'anterior, l'entitat precisa el subministrament, instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya (Lot 1: Evolució de la plataforma d'emmagatzematge i correlació d'esdeveniment de seguretat; Lot 2: Evolució de la plataforma de còpies de seguretat), ja que no disposa d'elements propis suficients per a realitzar aquesta prestació.

Segon.- Objecte del contracte:

➤ Lot 1:

L'objecte del Lot 1 és evolució de la plataforma actual consistent en un sistema centralitzat d'explotació d'esdeveniments de seguretat, amb l'objectiu d'ampliar les capacitats de l'esmentada plataforma, on actualment es duu a terme la ingesta de dades provinent de la recollida d'informació diversa en format d'esdeveniment, el processament de les dades consistent en l'aplicació d'algoritmes, agregacions o enriquiments sobre les dades que permetin ampliar la informació recollida, emmagatzemar els esdeveniments de seguretat i, finalment, analitzar les dades a partir de quadres de control que permetin la visualització a temps real, podent fer cerques a mida per obtenir aquella informació que es requereixi.

En concret, pel que fa a la ingesta de fonts, el Lot1 comprèn els següents punts:

- a) Millora de la infraestructura actual.
- b) Migració d'un ELK específic del servei Anàlisi d'amenaces, amb l'objectiu d'unificar la plataforma.
- c) Afinament de la solució final, la qual inclou la ingesta de noves fonts.

*Memòria justificativa del contracte de subministrament , instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya
Número d'Expedient: CO.03.2020*

➤ **Lot 2:**

L'objecte del Lot 2 és el subministrament d'una plataforma hiperconvergent de *backup* immutable i servidor de fitxers i objectes en la mateixa plataforma de gestió amb capacitat de desbordament a cloud.

També caldrà dur a terme la configuració de la plataforma ofertada amb integració i protecció de l'actual entorn de virtualització, així com la configuració del emmagatzemament NAS, documentació i traspàs de coneixement.

Aquest subministrament inclourà un manteniment trimestral durant un període de 3 anys per la revisió i proposta de millores sobre la plataforma.

Tercer.- Termini per al subministrament, instal·lació muntatge i posada en marxa de les aplicacions: Lot 1 es fixa en QUATRE (4) mesos; Lot 2 es fixa en TRES (3) mesos no s'admeten pròrrogues.

Això sense perjudici de l'exigència de la durada de les garanties, de les llicències i, en el seu cas, del manteniment que es requereixi i que es fixarà a la documentació que revesteix caràcter contractual.

Quart.- Idoneïtat de l'objecte i contingut del contracte: Mitjançant el present contracte se satisfaran les necessitats que s'especifiquen en el punt primer de la present memòria, d'acord amb la justificació tècnica que s'adjunta a la present memòria.

Es considera que mitjançant la licitació se satisfaran de forma directa, clara i proporcional les necessitats establertes al punt primer de la present memòria.

Cinquè.- Justificació del procediment utilitzat per l'adjudicació del contracte: El present contracte s'adjudicarà mitjançant procediment obert, de conformitat amb el que s'estableix a la LCSP, essent necessària la preparació dels plecs de clàusules administratives particulars i de prescripcions tècniques que regeixin la corresponent licitació.

Pels motius exposats es justifica la necessitat i idoneïtat de procedir a la contractació dels esmentats serveis, i a tal efecte,

RESOLC, iniciar el present expedient de contractació.

Memòria justificativa del contracte de subministrament , instal·lació muntatge i posada en marxa d'aplicacions i infraestructura de Ciberseguretat per a l'Agència de Ciberseguretat de Catalunya
Número d'Expedient: CO.03.2020

L'Hospitalet de Llobregat, a 4 d'agost de 2020

Oriol Torruella Torres
Director