Ajuntament de Castelldefels

Sistemes d'Informació
Núm. Exp.: 2022/4532
Previ de necessitats

INFORME DE NECESSITAT I IDONEÏTAT DEL CONTRACTE DE CONTRACTE MIXT DE SUBMINISTRAMENT, IMPLANTACIÓ, POSADA EN MARXA I OPERACIÓ D'UN CENTRE D'OPERACIONS DE CIBERSEGURETAT A L'AJUNTAMENT CASTELLDEFELS.

- Necessitat i idoneïtat de la contractació

La figura del Centre d'Operacions per Ciberseguretat es recull normativament a l'Ordre PCI/487/2019, de 26 d'abril, per la qual es publica l'Estratègia Nacional de Ciberseguretat 2019, aprovada pel Consell de Seguretat Nacional (Butlletí Oficial de l'Estat de 30 d'abril de 2019). En aquesta ordre, al capítol de Línies d'acció i mesures i, a la línia d'acció 2 on s'especifiquen les mesures per garantir la seguretat i la resiliència dels actius estratègics de l'estat espanyol es fa referència al impuls en el desenvolupament de Centres d'Operacions de Ciberseguretat a les entitats locals.

A més, el Centre d'Operacions de Ciberseguretat que es desplega amb caràcter obligatori formarà part de la Xarxa Nacional de Centres d'Operacions de Ciberseguretat, on el Centre Criptològic Nacional ja està treballant, i que integrarà el Centre d'Operacions de Ciberseguretat de la Administració General de l'Estat i els de les altres administracions públiques de l'àmbit nacional. La coordinació dels centres integrats en aquesta xarxa nacional es durà a terme a través de la Plataforma Nacional de Notificació i Seguiment de Ciberincidents, prevista a l'article 11 del Reial decret 43/2021, de 26 de gener, pel qual es desenvolupa el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.

En conseqüència, es proposa la contractació referida pel Departament de Sistemes d'Informació que depèn de la regidoria de Presidència, Comunicació, Noves Tecnologies, Serveis Socials i Dependència. Per la necessitat que té l'Ajuntament de Castelldefels d'ampliar i millorar les seves capacitats en ciberseguretat i cibervigilància, ampliant la monitorització de seguretat, la detecció primerenca de incidents, la vigilància i l'anàlisi de diverses fonts d'amenaça i vulnerabilitats i finalment optimitzant la capacitat de reacció, resposta i recuperació davant de qualsevol possible incident de ciberseguretat.

L´objecte d´aquesta licitació és la contractació d´un Centre d´Operacions de Ciberseguretat (conegut per les sigles SOC) que doni resposta a les necessitats actuals de l'entitat d'acord amb els requeriments que s'indicaran al plec de prescripcions tècniques.

Es tracta d'un contracte públic al qual és aplicable a més de les normes generals de contractació pública, els principis de gestió específics del Pla, definits a l'article 2 de l'Ordre HFP/1030/2021 de 29 de Setembre (BOE 30 de Setembre de 2021), pel qual es configura el sistema de gestió del Pla de Recuperació, Transformació i Resiliència.

El projecte de subministrament, implantació, posada en marxa i operació del SOC de l'Ajuntament de Castelldefels comprèn les fases que s'indiquen a continuació:

1. Subministrament, implantació i posada en marxa d'eines per a funcionament del SOC.

Aquesta fase inclou l'estudi previ, subministrament de hardware i software, llicenciament, implantació, proves de funcionament i suport durant la vigència del contracte de les eines necessàries per al correcte funcionament del Centre d'Operacions de Ciberseguretat. Com a mínim l'adjudicatari realitzarà la posada en marxa, subministrament, llicenciament i actualització de les eines següents:

- Plataforma de correlació d'esdeveniments de la seguretat de la informació amb el SIEM MONICA del CCN-CERT .
- Implantació de l'eina d'intercanvi de ciberincidents LUCIA del CCN-CERT que permet l'intercanvi automàtic i fluid de ciberincidents amb la Plataforma Nacional de Notificació i Seguiment de ciberincidents del Centre Criptològic Nacional.
- Implantació del sistema d'alerta temprana d'internet (SAT INET) de CCN-CERT.
- Posada en marxa i gestió del servei d'alerta temprana de vulnerabilitats, que mantingui els actius adequadament actualitzats davant possibles amenaces.
- Realitzar una revisió de la instal·lació i completar la configuració de l'eina microCLAUDIA del CCN-CERT de vacunació contra el ransomware.
- Implantació de la eina REYES de CCN-CERT per agilitzar la labor d'analisis dels ciberincidents.

2. Operació del Centre d'operacions de Ciberseguretat.

Un cop realitzada la implantació de les eines indicades al punt anterior i fent ús de les mateixes i de les eines ja disponibles a l'Ajuntament de Castelldefels, l'adjudicatari constituirà un equip d'operació del SOC 24x7, que participarà a les etapes del monitoratge d'amenaces, descobriment, avaluació i notificació amb proposta de mesures contenció i remediació en resposta a incidents i intel·ligència d'amenaces.

Una vegada avaluat l'incident Es comunicarà amb proposta de remediació al responsable de operació del actiu d'informació compromès.

Es contractarà una bossa d'hores per les funcions de contenció i remediació per quan no sigui suficient l'acció dels responsables de cada actiu d'informació. Per utilitzar i facturar nomes en el cas de que siguin necessaris serveis de contenció i remediació per la gestió de incidents de seguretat, que desbordi la capacitat de l'Ajuntament o del proveïdors que gestionen els diferents actius d'informació execució.

L'equip s'encarregarà del manteniment i actualització de les eines i solucions de seguretat implantades al present contracte. El Centre d'Operacions de Ciberseguretat (SOC) s'ubicarà físicament al territori de la Unió Europea i l'atenció del mateix es farà en castellà o català.

3. Servei de conscienciació Ciberseguretat per al menys 700 usuaris.

Provisió d'una plataforma online de capacitació i conscienciació en seguretat de la informació, amb la capacitat de simular atacs dirigits a l'usuari final per avaluar el grau de conscienciació i formació en Ciberseguretat i tots els serveis associats a la seva implantació.

4. Eines EPP, EDR i protecció de correu electrònic.

Implantació i posada en marxa de d'un EPP (EndPoint Protection, l'antivirus) i un sistema EDR (EndPoint Detection Response) amb les característiques i funcionalitats que es detallaran al plec de prescripcions tècniques, inicialment per 700 usuaris des de qualsevol equip corporatiu i pels servidor físic i virtuals de l'Ajuntament.

Sistema de protecció de correu electrònic per al menys 700 usuaris de correu electrònic, sense limitació de bústies departamentals o de serveis.
Aquests desplegament per la millora radical de la Ciberseguretat de l'Ajuntament no es poden exercir amb els mitjans amb què l'Ajuntament de Castelldefels compta actualment, ja que es requereix formació especialitzada en ciberseguretat i detecció d'amenaces, així com un coneixement exhaustiu de l'eina i una àmplia experiència d'ús, així com una dedicació exclusiva en hores de treball que no es disposa, es per això que es fa necessari recórrer a la contractació d'aquest serveis.

Serà possible la divisió en lots de la present licitació en tres lots

- Posada en marxa i operació de un Centre Operacions de Seguretat (SOC) punts 1 i 2.
- Servei de conscienciació Ciberseguretat per al menys 700 usuaris.
- Eines EPP, EDR i protecció de correu electrònic per al menys 700 usuaris.

El projecte està cofinançat pel Pla de Recuperació, Transformació i Resiliència – Finançat per la Unió Europea- NextGeneration EU, amb participació del Ministeri de Política Territorial, tractant-se el citat finançament de subvencions destinades a la transformació digital i modernització de les administracions de les entitats locals, en el marc del component 11, inversió 3, del Pla de Recuperació, Transformació i Resiliència.

El component 11 del Pla de Recuperació Transformació i Resiliència aborda la reforma i modernització de l'administració pública, per tal d'adaptar-la als reptes de la societat contemporània. S'estructura en un conjunt de 5 reformes i 5 inversions. La inversió 3 component 11 està dirigida a la transformació digital i modernització de les diferents administracions públiques.

El SOC es constitueix com un projecte de prioritat 1 (Posada en marxa d'un Centre d'Operacions de Ciberseguretat) objectivitzat a la Línia estratègica 5 (Ciberseguretat) de l'Ordre TER/1204/2021, de 3 de novembre, per la qual s'aproven les bases reguladores i s'efectua la convocatòria corresponent a 2021, de subvencions destinades a la transformació digital i modernització de les administracions de les Entitats Locals, en el marc del Pla de Recuperació, Transformació i Resiliència, i com a tal, ajustarà al que estableix la Guia tècnica emesa per a aquest efecte tal com s'indica a l'article 5 de l'esmentada ordre.

- Justificació d'insuficiència de mitjans personals

La insuficiència de mitjans queda suficientment justificada pel/pels motiu/s següent/s:

☒Que en la plantilla de llocs de treball no consta personal suficient per atendre les funcions que es requereixen en aquest servei i/o que pel volum de treball no es pot portar a terme pel personal propi d'aquesta Corporació.

☒Que es tracta de funcions específiques i concretes no habituals que només es poden prestar per una empresa externa, ja que tenen una especificitat que dificulta o impossibilita tenir personal especialitzat.

☐Que requereix d'una habilitació professional específica de la que manca el personal propi d'aquesta Corporació, així com d'uns coneixements altament especialitzats i/o titulacions acadèmiques específiques necessàries per prestar el servei.

- Valor estimat orientatiu

El valor estimat del contracte aproximat serà de 668.530 euros

- Responsable del contracte i regidor del qual depèn.

El responsable del contracte serà, Cap de Sistemes d'Informació, José Luis Guerrero Pérez, que depèn de la Regidora-delegada de Presidència, Comunicació, Noves Tecnologies, Serveis Socials i Dependència, Esther Niubó Cidoncha.

- Projecte finançat amb fons del Mecanisme de Recuperació i Resiliència:

☒SI
☐NO

- Projecte finançat amb fons REACT-EU:

☐SI
☒NO

Càrrec: