Ajuntament de L'Hospitalet

CODI DE VERIFICACIÓ	65600O6K4V4O13200RME		
PROCEDIMENT	V220 Contractacions de subministraments		
EXPEDIENT NÚM.	AJT/23040/2020	DOCUMENT NÚM.	193991/2020
ÀREA	Planificació, Projectes Estratègics i Hisenda		
UNITAT	Contractació		

APROVAR LA CONTRACTACIÓ D'EMERGÈNCIA DEL SUBMINISTRAMENT I IMPLANTACIÓ D'UNA NOVA ESTRUCTURA TALLAFOCS PERIMETRAL I INTERN (DOBLE CORONA).

El tinent d'alcaldia, titular de l'Àrea de Planificació, Projectes Estratègics i Hisenda, en ús de les competències delegades per a la gestió de la contractació com a conseqüència del COVID-19, per l'acord de la Junta de Govern Local adoptat en la sessió AJT/JGL/12/2020 de 18 de març de 2020, publicat en el BOPB de 23 de març de 2020.

VIST que és considera necessari l'adopció de mesures destinades a la protecció de les persones i la garantia en la prestació dels serveis públics que presta aquest ajuntament, davant la situació actual de pandèmia declarada per l'OMS l'11 de març de 2020, derivada del nou coronavirus SARS-CoV-2, aquest govern local considera que ha de contribuir amb la resta d'autoritats estatals i autonòmics i la pròpia societat civil a fer front a la malaltia COVID-19. Per això considera necessari activar els mecanismes que permetin fer una resposta ràpida i eficient a aquelles situacions destinades a protegir a les persones que es puguin presentar en l'àmbit de les seves competències i dels serveis que presta aquest ajuntament.

ATÈS que la Junta de Govern Local, en sessió de data 13 de març de 2020, va adoptar els acords següents:

PRIMER.- DECLARAR que concorre la situació de perill que exigeix l'article 120 de la LCSP per a la contractació d'emergència en relació a tots aquells contractes administratius: d'obres, serveis i/o subministraments, així com els contractes especials o privats, que tinguin per finalitat, en exercici de les competències municipals, prevenir i/o contenir l'expansió del COVID-19, garantir la prestació dels serveis municipals als/a les seus/seves usuàries i/o protegir els/les treballadors/es municipals i els/les membres de la Corporació.

SEGON.- DELEGAR en el 1r. Tinent d'alcaldia, i en cas de la seva absència en el Gerent municipal, la contractació pel tràmit d'emergència que preveu l'article 120 de la LCSP per a la contractació vinculada a la declaració prevista a l'anterior acord.

ATÈS que en l'esmentat acord de delegació s'han establert les condicions per a l'exercici de l'esmentada delegació.

ATÈS que per l'Àrea de Planificació, Projectes Estratègics i Hisenda, s'ha procedit a la justificar la contractació d'emergència del Subministrament i implantació d'una nova infraestructura de tallafocs perimetral i intern (doble corona), com segueix:

1. **Justificació de la necessitat de la contractació, justificació de l'emergència i de l'adequació al projecte COVID-19**

Davant l'actual situació d'emergència de Salut Pública d'importància internacional decretada amb data 11 de març de 2020 pel l'Organització Mundial de la Salut (OMS), el Reial Decret 463/2020 de 14 de març, de declaració d'estat d'alarma , han determinat la necessitat de prestar de manera general els serveis de l'Ajuntament de l'Hospitalet en modalitat no

presencial, s'ha fet necessari habilitar una infraestructura tecnològica que habiliti la possibilitat del teletreball.

En el moment actual el Servei d'Informàtica i Tecnologies de la Informació i Comunicació (SIiTIC) ha pogut proveir un sistema de connexió remota amb VPN, que habilita el teletreball mitjançant la infraestructura de tallafocs existent, basada en el producte Checkpoint Security Gateway 77.30, funcionant en un cluster actiu/passiu sobre plataforma de maquinari HP Proliant G6. Aquest equipament està dimensionat per possibilitar la connexió remota mitjançant VPN de fins a 50 usuaris concurrents, però la situació d'emergència actual ha comportat un increment dràstic de les connexions remotes, fins arribar a multiplicar per 20 aquest dimensionament.

Aquest increment en el número d'usuari ha posat de relleu mancances de l'actual sistema, entre elles:

- Saturació de la capacitat del sistema en hores puntes, havent de desactivar els sistemes de prevenció d'intrusions per tal de garantir el rendiment de les connexions per VPN en teletreball.

- Incapacitat de monitoritzar les connexions establertes des de clients VPN degut a que són prestacions que no estan disponibles en la versió actual, que data de l'any 2015 i està fora de suport de fabricant.

- Impossibilitat de filtrar l'accés a la subxarxa de servidors degut a que no es disposa d'un Firewall intern, que separi la xarxa d'estacions de treball de la xarxa de servidors. Això té especial importància en el context actual ja que les probabilitats de penetració en un dels ordinadors dels usuaris es multipliquen degut a l'exposició d'aquests ordinadors a Internet per permetre les connexions VPN.

Tot això suposa un risc real i imminent de possible fallada en un escenari en que es fa necessari donar suport amb un nivell de servei adequat a un volum continu d'usuaris en teletreball, a la vegada que es produeix un increment constant de les activitats de ciberdelinqüència reportades pel Centro Criptológico Nacional (CCN-CERT) i l'Agència de Ciberseguretat de Catalunya (CESICAT).

Per tant, davant la situació excepcional sobrevinguda causada per l'emergència sanitària actual per atendre les noves necessitats de capacitat i disponibilitat per a la connexió VPN a la xarxa de l'ajuntament de L'Hospitalet, resulta necessària l'adquisició de manera urgent d'una nova infraestructura de tallafocs perimetral i intern (doble corona) per la xarxa de comunicacions de l'Ajuntament de l'Hospitalet de Llobregat que permeti millorar l'actual infraestructura, per incrementar la càrrega concurrent d'usuaris, així com millorar la disponibilitat del servei per fer front a eventuals caigudes.

Per tal de facilitar la migració del sistema actual en el menor temps possible es requereix continuar amb productes del mateix fabricant, i a continuació es descriuen les especificacions tècniques i característiques de l'arquitectura i dels sistemes a implantar per tal de poder atendre a les noves necessitat de capacitat, seguretat i disponibilitat derivades de la situació actual, necessàries per poder donar servei a la necessitat imminent.

El sistema opera com un sistema indivisible per al correcte funcionament i tots són elements necessaris i inseparables per assolir l'objectiu establert.

Es demanen dues parelles de tallafocs que s'instal·laran en els respectius CPDs (La Farga i Ca n'Arus) per tal de proveir redundància en cas de fallada d'un d'ells. Cada parella treballarà en mode cluster actiu/passiu. El nou sistema estarà basat en "appliances", això és, dispositius que integren la solució de maquinari i programari en un únic element.

L'arquitectura del sistema necessària i imprescindible per donar servei a les necessitats descrites anteriorment ha d'estar composada dels següents elements:

- *Corona externa o firewall perimetral:* Inclourà 2 nodes Checkpoint 6600 o similar amb paquet de programari NGTX
- *Corona interna o Firewall intern.i*nclourà 2 nodes Checkpoint 6600 o similar amb paquet de programari NGTP
- *Consola d'administració unificada per la gestió,* es permet aprofitar la plataforma de gestió actual en ser del mateix fabricant, incloent addicionalment els mòduls "Smartevent", Smartreporter" i "Compliance".
- *Llicenciament per connexions VPN: e*l sistema ha de permetre la connexió sense límits d'usuaris remots a través del portal Mobile Access, mitjançant tecnologia VPN SSL.

L'oferta ha d'incloure el suport necessari per al programari especificat, i ha de ser suficient per permetre el correcte funcionament en tots els aspectes que s'han detallat.

Pel que fa a la implantació, cal que l'empresa adjudicatària prepari una nova política de seguretat per Firewall intern i migri i adapti la actual política de seguretat del Firewall perimetral al nou. Cal tenir en compte en aquestes polítiques tots els elements d'aquests Firewalls, nivell 4, IPS, Sandblast, filtre d'aplicacions, etc. Aquests serveis s'hauran de finalitzar en un màxim de 30 dies a partir de quan s'executi la comanda.

2. Dades bàsiques de la contractació o de la despesa

Àrea sol·licitant	Planificació, Projectes Estratègics i Hisenda
Servei	Servei d'Informàtica i Tecnologies de la Informació i Comunicació
Denominació del contracte	COVID-19 Subministrament i implantació d'una nova infraestructura de tallafocs perimetral i intern (doble corona)

Calendari execució prestacions Art. 120.c) LCSP el període execució no podrà ser superior a 1 mes des de l'ordre d'execució
1 mes

3. Dades econòmiques i pressupostàries

Proveïdor	**SIRT - SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L.**
Import (IVA inclòs)	**200.330,04€**
NIF/CIF	**B61588737**
Concepte econòmic pressupostari (*)	**02.9205.2.641.00.99**
Codi de projecte i denominació	**2120 20 2.COVID ACTUACIONS CONTINGENCIES COVID-19**
DOTACIÓ PRESSUPOSTÀRIA	Condicionada a l'aprovació pel Ple municipal i resultat de la publicació de l'expedient de modificació de crèdit núm 92/2020_

VIST el plec de prescripcions tècniques que contenen les especificacions del subministrament, que són d'obligatòria prestació.

Vist l'informe jurídic i la resta de documentació obrant a l'expedient.

Atès que resten exclosos del règim de suspensió previst a la disposició addicional tercera, del Reial Decret Reial Decret 463/2020, de 14 de març, pel qual es declara l'estat d'alarma per a la gestió de la situació de crisis sanitària ocasionada pel COVID-19, modificat pel Reial Decret 465/2020, de 17 de març, els procediments de contractació d'emergència, de conformitat amb l'art. 16 del Reial Decret 7/2000, en relació amb la Disposició final segona del Reial Decret Llei 9/2020.

El Tinent d'Alcaldia de Planificació, Projectes Estratègics i Hisenda, en exercici de les competències delegades per la Junta de Govern Local en sessió de data 13 de març de 2020,

RESOL

Primer:- APROVAR la contractació efectuada a l'empara del que disposa l' art 120 de la Llei de Contractes del Sector Públic, del subministrament i implantació d'una nova estructura tallafocs perimetral i intern (doble corona), amb les següents dades bàsiques:

Àrea sol·licitant	Planificació, Projectes Estratègics i Hisenda
Servei	Servei d'Informàtica i Tecnologies de la Informació i Comunicació
Denominació del contracte	COVID 19 Subministrament i implantació d'una nova infraestructura de tallafocs perimetral i intern (doble corona)
Proveïdor	SIRT - SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L. – B61588737
Import total (net + IVA)	200.330,04 EUROS (165.562,02 euros més 34.768,02 euros corresponents al 21% IVA)
NIF/CIF	B61588737
Dotació pressupostària	Condicionada a l'aprovació pel Ple municipal i resultat de la publicació de l'expedient de modificació de crèdit núm 92/2020_
Aplicació pressupostària	02.9205.2.641.00.99

Segon.- APROVAR les especificacions tècniques del subministrament i implantació d'una nova estructura tallafocs perimetral i intern (doble corona), que esdevenen obligacions contractuals:
Davant la situació excepcional sobrevinguda causada per l'emergència sanitària actual per atendre les noves necessitats de capacitat i disponibilitat per a la connexió VPN a la xarxa de l'ajuntament de L'Hospitalet, resulta necessaria l'adquisició de manera urgent d'una nova infraestructura de tallafocs perimetral i intern (doble corona) per la xarxa de comunicacions de l'Ajuntament de l'Hospitalet de Llobregat que permeti millorar l'actual infraestructura, per incrementar la càrrega concurrent d'usuaris, així com millorar la disponibilitat del servei per fer front a eventuals caigudes.

L'abast del contracte inclourà els elements hardware i software, així com els serveis professionals necessaris per migrar i convertir l'actual infraestructura de tallafocs a una nova infraestructura que permeti evolucionar i millorar els paràmetres de seguretat i les mesures de control necessàries per complir amb les normatives vigents.

El número segons la classificació CPV-2008 corresponent és 32420000-3, Equips de xarxa.

1. CONDICIONS TÈCNIQUES

Per tal de donar cobertura a la segmentació i control de seguretat de la xarxa actual, cal proporcionar una solució formada per dos tallafocs en cluster per donar cobertura a la corona

externa i dos tallafocs en cluster per donar cobertura a la corona interna. Cadascuna de les dues parelles de tallafocs s'instal·larà en els respectius CPDs de què disposa el SIiTIC.

Corona externa o firewall perimetral

Dos nodes Checkpoint 6600 o similar, proporcionant les següents funcionalitats:

- Tallafocs L4: cal promocionar la possibilitat de definir que el tallafocs treballi en L4 pels fluxes desitjats.

- Control d'aplicacions: proporcionar la visibilitat i control d'un mínim de 8000 aplicacions.

- Control d'URL: la solució ha de proporcionar control de navegació de URL, per tal de poder definir regles d'accés fent ús de categories (sexe, malicious sites, anonymizer,...). Caldrà que és pugui definir accions sobre la regla de control de navegació més enllà de accept o drop, es a dir, calen accions com: inform o ask to user, per tal que puguem definir excepcions temporals per part de l'usuari en temps real i per les categories que escolleix l'administrador.

- Eina Anti-Bot, amb capacitat de detectar dispostius infectats que realitzen peticions malicioses com per exemple Command&Control (C&C).

- Sistema de Prevenció d'intrusions (IPS), amb les següents característiques mínimes:

  - Disposar d'una base de dades precarregada superior a 10.000 signatures del mateix fabricant i que permeti la importació de signatures d'snort des del propi interfase gràfic de gestió.
  - Proporcionar la possibilitat de definir prefiltres sobre les signatures en funció de per exemple: tecnologia, sistema operatiu,etc. De forma que es pugui realitzar una preselecció de signatures actives sobre un perfil.
  - Es requereix que el mòdul IPS realitzi un bypass automàtic en cas d'una sèrie de condicions de CPU i memòria, que es parametritzen des del mateix client de gestió, d'una forma gràfica.

- Protecció "zero day": entesa com un conjunt de tecnologies que permeti la prevenció d'atacs de dia zero, això és, atacs que aprofitin vulnerabilitats desconegudes pel propietari i pel fabricant del producte. Entre aquestes tecnologies cal comptar com a mínim amb Sandbox, això és, capacitat d'analitzar una amenaça analitzant el comportament sobre un sistema operatiu en un entorn controlat. La solució ha de permetre atura l'entrega del fitxer a l'usuari final fins que no es disposa d'un veredicte de benigne de la plataforma de Sandbox.

  En cas de rebre fitxers ofimàtics/pdf cal que la solució proporcioni una còpia 100% Lliure d'amenaces en temps real, inclús donant la possibilitat que l'entrega del fitxer en format PDF i oferint la possibilitat a l'usuari final una autogestió per tal de recuperar el fitxer original, sempre que la solució de Sandbox (cloud o On-premise) hagi proporcionat un diagnòstic sobre el fitxer de benigne. Aquest mecanisme ha de ser vàlid tant per fitxers que arribin per http/s i per SMTP, i tal com s'ha dit prèviament, que la solució sigui valida encara que fem ús d'una solució de sandbox al cloud.

- Cadascun dels perfils utilitzats en les regles en l'àmbit de seguretat (no control d'accés), ha de tenir un pre-filtre que ens permeti fer ús d'una primera selecció de signatures en funció de l'impacte en rendiment, severitat i confiança de la mateixa signatura.

Corona interna o Firewall intern

Dos nodes Checkpoint 600 o similar, proporcionant les següents funcionalitats:

- Tallafocs L4: cal proporcionar la possibilitat de definir que el tallafoc treballi en L4 pels fluxes desitjats.
- Control d'aplicacions: proporcionar la visibilitat i control d'un mínim de 8000 aplicacions.
- IPS: cal que l'eina tingui un BDs precarregada superior a 10.000 signatures del mateix fabricant i permeti la importació de signatures d'snort des del propi interfase gràfic de gestió
- Per tal de poder treballa d'una forma eficient sobre el mòdul IPS, cal poder definir una excepció amb un sol clic sobre la pròpia entrada en el log, tenint en compte que és la mateixa eina de gestió qui omple els camps necessaris perquè l'excepció sigui eficient (origen, destino, servei i signatura).
- Es requereix que el mòdul IPS realitzi un bypass automàtic en cas d'una sèrie de condicions de CPU i memòria, que es parametritzen des del mateix client de gestió, d'una forma gràfica.

Consola d'administració unificada per la gestió

La solució de seguretat ha d'estar formada per una plataforma de gestió **única** totalment diferenciada del gateways i per altre costat els elements tallafocs que formen la solució.

La gestió de la política de seguretat, en cap cas es realitzarà mitjançant https o similar, sinó que es realitzarà exclusivament des d'un client instal·lat a cadascun dels administradors de la solució, evitant d'aquesta forma que un mal comportament del navegador provoqui una mala configuració sobre la plataforma de gestió.

Per tal de poder definir el tipus de política requerida per aquest entorn, cal que la solució tingui la capacitat de definir una política de control d'accés amb el següent format: no és suficient amb un simple llistat de regles, sinó que cal tenir la capacitat de definir regles niades, és a dir una regla de control d'accés marca les condicions, per verificar novament el tràfic fent ús d'un altre nivell de regles (fins a 5 nivells de profunditat), per tant, aquest subconjunt de regles només entren en joc quan una regla mare fa match, donant com a resultat una política molt més simple de gestionar. A més permetent restringir a un usuari específic la gestió d'aquest subconjunt de regles. Cal dir que també es requereix que aquest conjunt de regles niuades poden ser compartides en block amb altres polítiques de seguretat.
La política de seguretat també pot fer ús de conjunt de regles (capes) que s'avaluen de forma consecutiva, una capa està formada per un conjunt de regles.

Una vegada el paquet arriba al tallafocs, és avaluat per la capa superior, si la primera regla que fa match té una acció de allow, aquest mateix tràfic és avaluat per el següent conjunt de regles (capa), amb el mateix criteri, s'aplica l'acció de la primera regla que fa match, en cas de ser un tràfic permès per aquesta capa, tornem a realitzar aquesta mateixa tasca per la següent capa. El paquet només serà permès si totes les capes, després de fer l'avaluació descrita, permeten l'accés. S'ha de poder treballar amb un mínim de 10 capes d'aquesta mena i alhora amb capes aniudades descrites anteriorment.

Serà necessari, que si la nostra política està formada per diferents capes en línia, el log representi d'una forma clara, sobre quines regles i capes ha sigut permès el tràfic i sobre quines ha sigut denegat.

Reporting

En l'àmbit de logs i reporting, cal no només fer ús de vistes personalitzades per tal de poder visualitzar la informació tal com la desitja el client, sinó tindre la possibilitat de veure els esdeveniments/logs d'una regla especifica, sobre el mateix pla de visualització de les regles de control d'accés o inclús sobre el pla de regles de seguretat.

També cal tenir la possibilitat de definir vistes i reports utilitzant filtres granulars, inclús fen ús de grups de l'Active Directory des de la mateixa eina de gestió.

Es requereix també la possibilitat de generar alertes automàtiques en cas d'incidents de seguretat, generar informes periòdics sobre incidents i ús el sistema, i l'adequació d'aquest a les normes de seguretat establertes per estàndards internacionals.

Arquitectura de xarxa

Cal proporcionar una solució de cluster físic, tant per la corona externa com per la corona interna. Aquest cluster pot treballar en mode Actiu/passiu o en Actiu/Actiu. En cas de treballar en mode Actiu/Actiu no ha de provocar canvis en l'arquitectura o fluxos de tràfic, és a dir, cal que cadascun dels segments de xarxa tingui una única IP de servei que representi punt d'encaminament dels diferents actius d'aquest segment.

Encara que no sigui fruit de requisits actuals, si cal que la solució presentada proporcioni la possibilitat, d'afegir nous membres a la solució (fins a 50 membres), proporcionant escalabilitat de rendiment lineal a mesura que afegim nous membres a la solució. En cas de requerir algun element addicional ha de ser del mateix fabricant. Ha de quedar clar el fet de voler gaudir d'aquesta escalabilitat lineal, seguim mantenint una sola IP de servei per cadascun dels segments que protegeix els tallafocs, és a dir en cap cas es modifiquen els flujes de tràfic originals.

Connexions VPN

El sistema ha de permetre la connexió sense límits d'usuaris remots a través d'un portal corporatiu mitjançant la tecnologia VPN SSL

Llicències i subscripcions de programari associat

L'oferta ha d'incloure el suport necessari pel programari especificat, i ha de ser suficient per permetre el correcte funcionament en tots els aspectes que s'han detallat en el present plec de condicions tècniques.

Tots els productes i serveis adquirits són per a la seva utilització en l'àmbit de l'Ajuntament de l'Hospitalet de Llobregat i dels seus organismes. No es contemplen modalitats de llicències de programari per a educació, ni per a professionals amb condicions especials de llicència.

Cal incloure la versió habitual més recent del producte de programari disponible en el moment d'efectuar l'oferta, d'acord amb les característiques especificades en aquest plec de condicions. En el cas que existeixi la versió en català del programari especificat, o opcions del mateix, cal que l'oferta contempli aquesta opció.

A efectes de reduir costos, l'oferta cal que tingui en compte les opcions i els preus del fabricant aplicables a l'Ajuntament de l'Hospitalet de Llobregat.

El subministrament de tots els elements s'ha d'efectuar d'acord amb els requeriments que en el seu moment determini el Servei d'Informàtica de l'Ajuntament de l'Hospitalet de Llobregat.

Serveis d'implantació

Cal que la empesa adjudicatària prepari una nova política de seguretat per Firewall intern i migri i adapti la actual política de seguretat del Firewall perimetral al nou. Cal tenir en compte en aquestes polítiques tots els elements d'aquests Firewalls, nivell 4, IPS, sandblast, filtre d'aplicacions, etc.

Garanties i suport tècnic

Els dispositius demanats com a objecte del contracte han de tenir com a mínim 2 anys de garantia i 1 any addicional de suport tècnic del fabricant. Durant tot aquest període el fabricant ja sigui directament o a través de l'empresa licitadora ha d'oferir un servei de helpdesk per consultes, gestió d'incidències i avaries dels equips amb suport per part de l'adjudicatari 24x7 amb contacte per telèfon i correu electrònic, i possibilitat d'escalar aquests problemes al fabricant en format 8x5.

2. CONFIDENCIALITAT I SEGURETAT.

L'adjudicatari queda expressament obligat a mantenir la confidencialitat i a la no difusió de les dades a què tingui accés o hagi elaborat per raó de l'execució del contracte i, a tal efecte, l'adjudicatari manifesta que té implantades i/o adoptarà abans de l'inici del contracte les mesures de tipus tècnic i organitzatiu necessàries per tal de garantir la seguretat i evitar l'alteració, pèrdua, tractament o accés no autoritzat, en atenció a l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estiguin exposades. El deure de secret i no difusió subsistiran inclòs quan hagin finalitzat les relacions contractuals mútues.

També haurà de guardar la deguda confidencialitat respecte a tota la informació obtinguda i documentació elaborada per raó de l'execució del contracte i aquesta documentació no podà ser reproduïda, cedida, difosa, publicada o utilitzada per a finalitats diferents de les establertes en aquest plec, fins i tot un cop extingit el contracte.

L'adjudicatari es comprometrà a la no difusió de cap tipus de codi d'accés o qualsevol altre tipus d'informació que pugui facilitar l'entrada als sistemes de l'Ajuntament, així com a no fer un ús incorrecte dels permisos i privilegis que es concedeixin al seu personal per a l'execució del contracte.

L'adjudicatari es farà responsable dels perjudicis que se li puguin ocasionar a l'Ajuntament degut a l'incompliment de qualsevol de les condicions esmentades.

Tercer.- Efectuades les prestacions objecte del contracte, per part dels serveis tècnics s'haurà d'emetre informe que haurà de posar de manifest que les prestacions s'han efectuat correctament i dins del termini d'1 mes des de l'ordre de la seva execució tal com estableix l'article 120 c) de la LCSP i que procedeix la seva recepció de conformitat; i s'efectuarà la proposta de liquidació del mateix per l'import que correspongui.

Quart.- La notificació de la present resolució al contractista tindrà efectes de formalització del contracte i en la seva conseqüència, del seu perfeccionament.

Cinquè.- De conformitat amb l'esmentat acord de la Junta de Govern Local de data 13 de març de 2020, es disposa que, executades les actuacions objecte del contracte, prèvia comprovació de la seva correcta execució, efectuarà les operacions destinades a la liquidació de la prestació i ordenarà el seu pagament.

Sisè.- SENYALAR que la fiscalització dels acords anteriors es realitzarà d'acord amb l'aprovat pel decret de l'Alcaldia núm. 7 (res/4179/2020) de 27 de març, de mesures mures extraordinàries relacionades amb el COVID-19, relatives a l'autorització a la intervenció general municipal per l'exercici del control intern mitjançant control financer en determinats supòsits amb ocasió de l'impacte econòmic i social derivat de la crisi sanitària.

Setè.- NOTIFICAR la present resolució al contractista SIRT - SISTEMAS INTEGRALES DE REDES Y TELECOMUNICACIONES S.L. fent constar que els terminis per a la interposició dels recursos que s'indiquen a continuació es troben suspesos durant la vigència de l'estat d'alarma, per aplicació de les disposicions addicionals segona i tercera del l Reial decret 463/2020, de 14 de març, pel qual es declara l'estat d'alarma per a la gestió de la situació de crisi sanitària ocasionada pel COVID-19. El còmput dels terminis s'iniciarà des del dia hàbil següent a la data de finalització de la declaració de l'estat d'alarma.

Vuitè.- Comunicar la present resolució a l'Àrea gestora d'Equitat, Drets Socials i Recursos Humans, al Servei de Programació i Pressupostos, a la Intervenció General, a la Tresoreria Municipal i a la Gerència Municipal

Novè.- Comunicar la present resolució al Servei de Contractació i Patrimoni, per tal que procedeixi a la seva publicació en el portal de transparència i en els registres públics i al compliment de la resta de les obligacions formals derivades de la normativa de contractes.

Contra aquest acte, que exhaureix la via administrativa, es podrà interposar, de manera optativa i no simultània, un dels recursos següents:

- Recurs potestatiu de reposició: davant el mateix òrgan que l'ha dictat, en el termini màxim d'un mes, comptat de l'endemà a la recepció de la seva notificació. El termini màxim per a la resolució d'aquest recurs és d'un més des de la seva interposició, transcorregut el qual sense que s'hagi rebut notificació de la seva resolució expressa, s'entendrà desestimat per silenci administratiu. Contra la desestimació presumpta es podrà interposar, en el termini de 6 mesos a partir de l'endemà a aquell en què s'entengui desestimat, recurs contenciós administratiu davant els jutjats contenciosos administratius de Barcelona, en la forma i amb els requisits establerts a Llei 29/1998, de 13 de juliol, reguladora de la Jurisdicció contenciós administrativa.

- Recurs contenciós administratiu: directament, davant els jutjats contenciosos administratius de Barcelona, en el termini de dos mesos a partir de l'endemà a la seva notificació, en la forma i amb els requisits establerts a la Llei 29/1998, de 13 de juliol, reguladora de la Jurisdicció contenciosa administrativa.

Tot això, sense perjudici de la interposició de qualsevol altre recurs o de l'exercici de qualsevol acció que es considerin adients.