Ajuntament d'Igualada

PLEC DE PRESCRIPCIONS TÈCNIQUES PER LA CONTRACTACIÓ DEL SUBMINISTRAMENT I SERVEIS DE CONFIGURACIÓ I MIGRACIÓ DE LES INFRAESTRUCTURES TECNOLÒGIQUES CENTRALS I LES SEVES XARXES D'INTERCONNEXIÓ (LÍNIA 4 ACTUACIONS 2 i 3) DEL PLA DE RECUPERACIÓ, TRANSFORMACIÓ I RESILIÈNCIA, FINANÇAT PER LA UNIÓ EUROPEA – NEXT GENERATION EU

Exp. 35/2024

GOBIERNO DE ESPAÑA
MINISTERIO DE POLITICA TERRITORIAL Y MEMORIA DEMOCRÁTICA
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU

1. ANTECEDENTS

L'Ajuntament d'Igualada ha rebut una subvenció en el marc de l'Ordre TER/836/2022, de 29 d'agost, per la qual s'aproven les bases reguladores 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.

La subvenció rebuda és per al desenvolupament de la **Línia 4, de Renovació i Modernització de les infraestructures tecnològiques centrals i les seves xarxes d'interconnexió, concretament per a la modernització dels sistemes de virtualització de CPDs i increment de les mesures de seguretat activa i passiva de la xarxa**.

2. OBJECTE

L' objecte del present procediment és el subministrament, migració i configuració de la plataforma de sistemes d'informació de l'Ajuntament d'Igualada, en endavant, l'Ajuntament. L'adjudicatari del present contracte ha de realitzar les tasques de subministre, instal·lació, configuració i posada en marxa dels nous equips, així com també fer la migració de tota la infraestructura de virtualització i emmagatzemament de dades existents en el clúster actual cap als nous sistemes implementats. També haurà de prestar el manteniment dels nous equips un cop quedin instal.lats i en funcionament a l'Ajuntament.

Amb això es pretén la modernització de les infraestructures tecnològiques centrals i les seves xarxes d'interconnexió, més concretament amb la substitució dels actuals sistemes de virtualització de CPDs i aconseguir incrementar les mesures de seguretat activa i passiva de la xarxa amb el desplegament d'un nou subsistema de seguretat informàtica (tallafocs) .

Els objectius generals del projecte són els següents:

- Millorar la redundància del sistema actual, aconseguint redundància de la plataforma entre CPDs i sense punts únics d'errada.
- Millorar l'optimització del sistema. A través d'una evolució respecte dels equips actuals i una reestructuració a nivell d'arquitectura.
- Reduir la quantitat de maquinari per tal de millorar l'impacte energètic i tenir una solució més sostenible.
- Incrementar les velocitats de connexió en el conjunt de la plataforma.
- Disposar d' equips amb firmware recent i de màquines virtuals amb sistemes operatius actuals i segurs.
- Millorar la seguretat activa i pasiva de la instal.lació de xarxa.

L'abast del projecte es centra en l'àmbit tecnològic i dels serveis associats al subministrament i contempla:

A) El subministrament d'una solució d'infraestructura de servidors als CPD's, que utilitzi la tecnologia d'Hiperconvergència (HCI) basada en un cluster de 2 nodes (1 per a cada CPD) funcionant 100% en alta disponibilitat (HA) en CPU, RAM i emmagatzematge i que tingui la capacitat de gestionar eficaçment el còmput i emmagatzematge necessaris pels diferents serveis de l'Ajuntament.

   La solució estarà configurada en alta disponibilitat de dades i de connexió a internet per a tolerància a errors en cas de caiguda d'un dels dos CPD's.

   S'hi inclouran els serveis professionals per realitzar la posada en marxa dels servidors HCI, així com totes les llicències necessàries per a la plataforma hiperconvergent i del producte VmWare vSphere ESX i vCenter Standard en les seves versions més recents i estables, durant un periode d'un any; la instal·lació, migració i configuració de l'actual clúster (dades, màquines virtuals etc.)

B) El subministrament, els serveis d'instal·lació, posada en règim d'explotació, manteniment i suport, d'un nou subsistema de seguretat informàtica (en endavant tallafocs) per tal d'incrementar les mesures de seguretat activa i passiva de la xarxa i la protecció de tot l'entorn informàtic de l'Ajuntament d'Igualada en front a possibles ciberatacs.

En ambdós casos, l'abast del projecte inclourà:

- La garantia del conjunt de la solució, durant un periode de tres anys.
- El llicenciament del conjunt de la solució durant els periodes establerts.
- Formació al personal de l'Ajuntament de les noves solucions proposades.
- Manteniment i suport tècnic de les solucions: Els serveis de manteniment tant proactiu com reactiu necessaris de la plataforma. El suport de la plataforma haurà d'oferir-se per 3 anys, en règim de 24x7 i temps de resposta 4h. El preu dels 3 anys està inclòs en l'import del pressupost base de licitació.

Aquesta actuació s'emmarca en el Pla de Recuperació, Transformació i Resiliència - Finançat per la Union Europea-NextGenerationEU, Mecanisme de Recuperació i Resiliència, establert per al Reglament (UE) 2021/241 del Parlament Europeu i del Consell, de 12 de febrer de 2021.

L'actuació s'inclou dins del Component 11, Inversió 3, del PRTR, gestionat per al Ministeri de Política Territorial i Funció Pública.

3. NECESSITAT I IDONEÏTAT DEL CONTRACTE

És necessària la contractació d'aquest servei que doni resposta a les necessitats d'assistència tècnica i de gestió en el desenvolupament de les accions previstes en el

projecte de **Renovació i Modernització de les infraestructures tecnològiques centrals i les seves xarxes d'interconnexió**. Sense aquesta contractació la necessitat a cobrir no seria factible.

Per a la correcta execució tècnica del projecte, així com per a la millor coordinació i optimització del control de l'execució del contracte, resulta convenient la no divisió en lots de les prestacions compreses a l'objecte d'aquest plec, atesa la complexitat de la integració entre els equips subministrats, la seva configuració i posada en funcionament així com també el manteniment d'aquests.

Les necessitats administratives a satisfer mitjançant el contracte són necessitats d'interès públic i general i que entren dins l'àmbit de competències de l'Ajuntament, de conformitat amb el que disposa l'article 25.2.e) de la Llei 7/1985, de 2 d'abril, RBRL; art. 66. k) del DL 2/2003, de 28 d'abril TRLMRLC i art. 84.2 m) de l'Estatut d'Autonomia de Catalunya i, per altra banda, en el sí del marc europeu i de foment de la digitalització cal fer constar que:

- El 21 de juliol de 2020, el Consell Europeu va aprovar la creació del programa Next Generation EU (NGEU) per estimular la recuperació econòmica i la reparació dels danys causats per la pandèmia de la COVID-19 i construir l'Europa de la nova generació, impulsant la transició ecològica, digital i resilient dels països membres de la Unió Europea.

- El PRTR va ser aprovat per la Comissió Europea el passat 16 de juny de 2021, i pel Consell de la Unió Europea el 13 de juliol de 2021 i pretén reformes i inversions en els àmbits prioritaris a nivell europeu. Per a això, l' esmentat Pla s' estructura en quatre eixos dedicats a la transició ecològica, transformació digital, cohesió social i territorial i igualtat de gènere, que alhora orienten deu polítiques palanca i trenta components.

- La quarta política palanca és una Administració per al segle XXI, que planteja una modernització de l'Administració per respondre a les necessitats de la ciutadania i l'economia a tot el territori. El component 11, que desenvolupa aquesta política a través d' un conjunt de reformes i inversions, xifra com a objectius estratègics la digitalització i modernització de les administracions públiques, la transició energètica i el reforç de les capacitats administratives. La inversió 3 del component 11 està dirigida a la transformació digital i modernització de les diferents administracions públiques a través del compliment de les fites 167 i 169 i de l'objectiu 168 del PRTR i disposa d'un finançament que ascendeix a 1.000 milions d'euros en el període 2021-2023 D'aquesta quantitat es destinaran, al llarg del període 2021-2023, 391,4 milions d'euros a les entitats locals.

Les tasques que es descriuen en aquest plec no es poden dur a terme només amb els mitjans de què disposa l'Ajuntament en el si del departament d'Organització i Tecnologies de la Informació, que compta amb recursos limitats i que es focalitza en abastar els serveis ordinaris de l'Ajuntament.

Per altra banda, el projecte està finançat en l'import de 280.649,06 euros (IVA inclòs) en el marc de la Resolució de data 31de maig de 2023 de la Direcció General de Cooperació Autonòmica i Local del Ministeri de Política Territorial, en el marc del Pla de Recuperació, Transformació i Resiliència.

4. CODI DE L'ACTIVITAT

Les codificacions estadístiques i el sistema de classificació aplicable a què fa referència aquest contracte són:

48800000 Sistemes i servidors d'informació.
30211200-3 Equips informàtics d'unitat central.
32413100-2 Encaminadors de xarxa.
51610000-1 Serveis d'instal.lació d'ordinadors i d'equips per al processament de la informació.

5. SOLVÈNCIA ECONÒMICA I FINANCERA I TÈCNICA PROFESSIONAL

A més dels requisits generals de capacitat per contractar, s'haurà d'acreditar la solvència econòmica financera i la solvència tècnica professional pels mitjans següents:

Solvència econòmica i financera

S'haurà d'acreditar per algun dels mitjans següents:

a) **El volum anual de negocis** del licitador que, referit a l'any de major volum de negoci en l'àmbit al qual es refereix el contracte, en els últim cinc anys disponibles en funció de les dates de constitució o d'inici de les activitats de l'empresari, haurà de ser, almenys, d'una vegada i mitja el valor estimat del contracte o el valor anual mig si aquest és inferior.
El volum anual de negocis del licitador s'haurà d'acreditar mitjançant les seves comptes anuals aprovades i dipositades en el Registre Mercantil o en el Registre Oficial en què hagi d'estar inscrit. Els empresaris individuals no inscrits en el Registre Mercantil acreditaran el seu volum anual de negocis mitjançant els seus llibres d'inventaris i comptes anuals legalitzats pel Registre Mercantil o bé presentant els tres últims anys de l'IRPF acompanyant els Resums Anuals d'IVA (model 390) i el registre de les factures emeses corresponents a cadascun d'aquest anys (art.87.1.a) i 3.a) LCSP).

b) **Justificant de l'existència d'una assegurança d'indemnització per riscos professionals per import igual o superior a 300.000 euros per sinistre i any;** a més d'aportar el compromís de la seva renovació o pròrroga que garanteixi el manteniment de la seva cobertura durant tota l'execució del contracte. Aquest requisit s'entendrà

acomplert pel licitador quan inclogui en la seva oferta un compromís vinculant de subscripció, en cas de resultar adjudicatari, de l'assegurança exigida, compromís que haurà de ser complert dins del termini de deu dies hàbils referit en l'article 150.2 de la LCSP. L'acreditació serà a través d'un certificat expedit per l'assegurador, on constin els imports i riscos assegurats i la data de venciment de l'assegurança i, a través del document de compromís vinculant de subscripció, pròrroga o renovació de l'assegurança, en els cassos en què procedeixi. (article 87.1.b) i 3.b) LCSP).

Solvència tècnica professional

S'haurà d'acreditar de la manera següent:

L'experiència en la realització de treballs del mateix tipus o naturalesa que l'objecte del contracte (art.90.1.a) LCSP).

L'experiència s'haurà d'acreditar mitjançant una relació dels principals subministraments realitzats de naturalesa igual o similar que els que constitueixen l'objecte del contracte en el curs de, com a màxim els tres últims anys, en què s'indiqui l'import, la data i el destinatari, públic o privat dels mateixos.

S'haurà d'avalar amb la presentació de certificats de bona execució, en relació als serveis més importants, quan el destinatari sigui una entitat del sector públic; quan el destinatari sigui un subjecte privat, mitjançant certificat expedit per aquest i a falta de certificat d'aquest, mitjançant una declaració del licitador, acompanyada de document original signat electrònicament o còpia autentica del document emes o còpia escanejada signada per licitador que acrediti de manera fefaent les dades indicades en la relació responsable.

Tant en la relació com en els certificats a presentar, cal indicar objecte, import, dates, lloc d'execució i destinatari públic o privat.

El requisit mínim serà que l'import anual acumulat en l'any de major execució ha de ser igual o superior al 70% del valor estimat del contracte o el valor anual mig si aquest és inferior.

Certificacions professionals exigides

Es demana comptar amb les següents certificacions per tal de validar la capacitat tècnica. L'adjudicatari ha de disposar de les següents certificacions oficials en vigor:

- Certificació ISO 27001 o equivalent.
- Certificat a l'Esquema Nacional de Seguretat -nivell alt en suport i gestió de dispositius de seguretat.

- Partner oficial del fabricant de la solució d'infraestructura de servidors de nivell “Platinum” o equivalent.
- Vmware VCSP Pinnacle.
- Partner GOLD de Microsoft.

L'empresa adjudicatària ha de disposar en plantilla d’un equip de treball que comptarà amb enginyers superiors o llicenciats en informàtica o telecomunicacions (almenys un) amb més de cinc anys d’experiència i que disposin de referències acreditades en treballs similars. S’acreditarà mitjançant la presentació d’una còpia de la titulació i l’experiència professional mitjançant certificats expedits per l’òrgan competent de l’Administració Pública o de les empreses on s’hagin prestat aquests serveis.

La licitadora que obtingui la millor puntuació haurà d'enumerar les persones que formen part de l'equip, titulacions de cadascuna i certificació o certificacions de què disposin, a més d'acreditar-les.

6. DESCRIPCIÓ DEL SERVEI I TASQUES A EXECUTAR

6.1 DESCRIPCIÓ DE LA SITUACIÓ ACTUAL

L’Ajuntament d’Igualada, consta d’un conglomerat de seus municipals interconnectades entre si mitjançant fibra òptica propietària en la majoria dels casos.

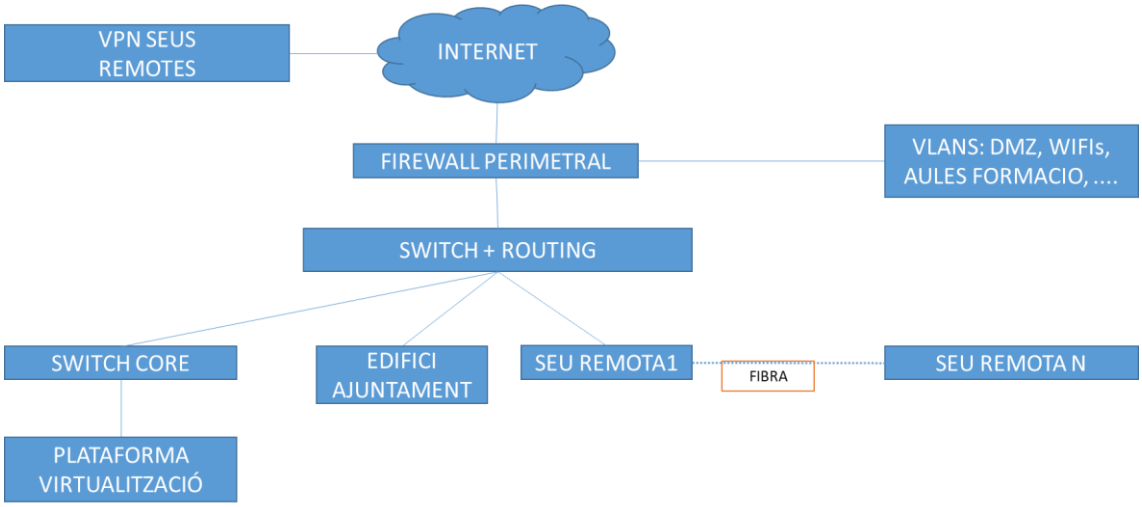
Cadascuna de les xarxes d’aquestes seus municipals, tenen un punt d’unió on es realitzen totes les tasques d’enrutament i accés entre elles i cap a la connexió a internet mitjançant un Firewall, per tal de protegir la nostra xarxa d’amenaces externes.

El dispositiu que gestiona aquest enrutament intern de xarxes, està actualment descatalogat pel fabricant (Cisco Catalyst 4500). A més a més, és l’únic dispositiu que actualment gestiona aquest enrutament. Es troba ubicat físicament al CPD primari de l’ajuntament, situat a l’edifici central de la Pl. Ajuntament, 1.

El fet que aquest dispositiu sigui l’únic que s’encarrega de l’enrutament entre les diferents xarxes corporatives de l’Ajuntament, suposa una mancança important en el disseny de la xarxa corporativa, pel fet de no estar redundat. Tampoc incorpora cap mecanisme de seguretat de segmentació entre xarxes, que permeti una millor resposta en cas de possibles intrusions informàtiques a la xarxa. Per aquest motiu, amb la implantació dels dos nous equips de firewall, deixarà de realitzar aquesta funció d’enrutament, que serà assumida pels nous equips.

Aquest mateix dispositiu (Cisco Catalyst 4500), també funciona com a switch d’accés de tot el personal situat a l’edifici central de l’ajuntament, funció que continuarà conservant un cop instal.lats els nous dispositius.

La figura representa el diagrama de funcionament de la xarxa municipal.



Infraestructura de virtualització existent

Es disposa d'una solució del fabricant Vmware-Vsphere de virtualització en la seva versió 6.5U2 i consta de 2 Hosts configurats en clúster amb el servei de HA per poder donar resposta a possibles fallades de cada un d'ells.
L'ajuntament té 2 CPDs, separats geogràficament i units per 2 fibres directes monomode.

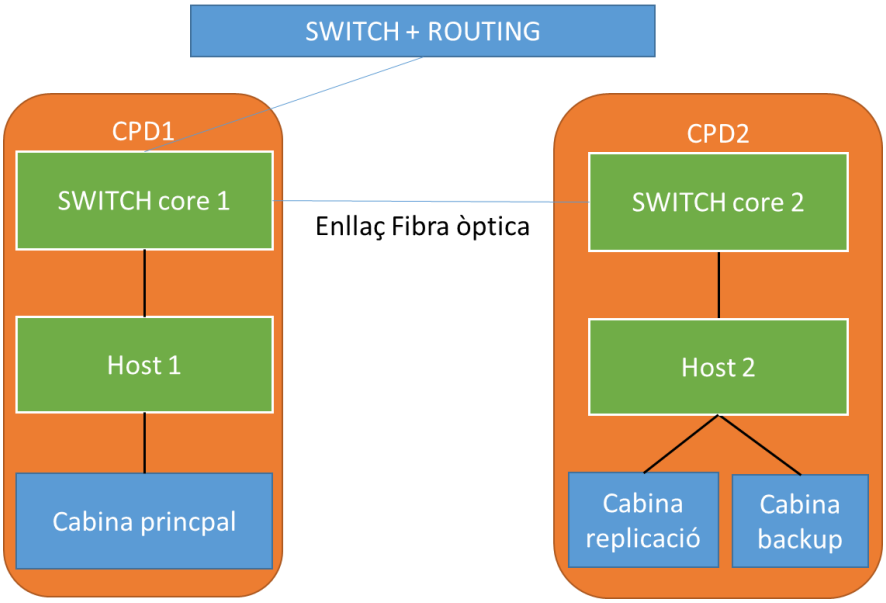
Al CPD primari, situat a l'edifici de l'Ajuntament, hi ha un Host HP Proliant DL380G8 amb 264GB de memòria RAM, un processador Intel(R) Xeon(R) CPU E5-2620 0 @ 2.00GHz amb 24 processadors lògics i 6 NICs que dona servei a 26 màquines virtuals. Està connectat mitjançant FiberChannel a una cabina principal de dades (HP P2000) amb capacitat d'uns 20 Terabytes totals, distribuïts en diversos datastores configurats amb RAID5 i RAID1.

Al CPD secundari, es troba el segon Host del Cluster, un HP Proliant DL380G10 amb 256GB de memòria RAM, un processador Intel(R) Xeon(R) Silver 4208 CPU @ 2.10GHz amb 32 processadors lògics i 6 NICs, que dona servei a 13 màquines virtuals.
Aquest CPD secundari, també conté 2 Cabines de dades dedicades a repliques i còpies de seguretat.

Aquests sistemes han estat funcionant durant 10 anys i actualment l'evolució en les necessitats tecnològiques de l'ajuntament fan que sigui molt difícil donar-hi resposta

amb la qualitat exigida. Tampoc és un sistema que garanteixi una redundància en el seu funcionament, ja que la cabina principal d'emmagatzematge, és única i no podem distribuir les dades en cas de talls elèctrics o mal funcionament d'aquesta.

La figura representa l'estat actual d'aquest sistema.



Infraestructura de tallafocs i ciberseguretat actuals

Actualment l'Ajuntament d'Igualada, disposa d'un servei de subscripció de Firewalling de propera generació (NGFW) de l'empresa PaloAlto Networks, que és la convergència de la tecnologia de tallafocs tradicional amb altres funcions de filtratge de dispositius de xarxa, com el control d'aplicacions en línia, un sistema integrat de prevenció d´intrusions (IPS), capacitats de prevenció d´amenaces i protecció antivirus.

Aquesta seguretat està encaminada a protegir les estructures tecnològiques des del punt de vista perimetral del sistema. És a dir, tenim especial cura i control sobre atacs externs de la xarxa.

Observant l'evolució dels atacs informàtics esmentats, i analitzant els últims atacs produïts en diferents organismes i empreses, molts d'aquests poden produir-se també des de màquines internes al sistema. Cal notar que una administració pública dóna servei a múltiples serveis amb múltiples necessitats i amb usuaris de procedència molt diferent. És per tant imprescindible dotar l'administració d'eines de seguretat actives i passives amb poder de segmentació, aïllament i mitigació d'atacs, de manera que, en cas d'infecció, les pèrdues i les afectacions siguin mínimes, i la recuperació del sistema sigui el més ràpid possible.

6.2 ESPECIFICACIONS TÈCNIQUES DELS SERVEIS A CONTRACTAR

Totes les especificacions i requeriments relacionats en aquest punt, es consideren essencials.

Infraestructura de servidors als CPD's utilitzant la tecnología d'hiperconvergència (HCI).

Descripció general de la infraestructura a incorporar i implementar

- Incorporar una plataforma HCI en rol de clúster principal, amb nodes que per motius de compatibilitat hauran d'usar l'hipervisor VMware vSphere ESX, en les seves versions més recents i estables.
- El clúster haurà d'estar format per un mínim de dos (2) nodes, un per cada CPD que disposa l'ajuntament per tal de conformar una solució altament disponible (HA 100%) en CPU, RAM i emmagatzematge.
- Realitzar la instal·lació i configuració de la nova infraestructura, i posada en producció del nou equipament.
- Migració de les dades de la plataforma actual cap a la nova plataforma implementada.
- Oferir els serveis de manteniment tant proactiu com reactiu necessaris de la plataforma durant tota la durada del contracte del projecte.

L'arquitectura requerida s'haurà de satisfer mitjançant nodes HCI purs, no s'admetran solucions desagregades on el còmput i l'emmagatzematge estiguin separats. De forma independent als components que defineixi cada solució, cada node haurà de d'incorporar, com a mínim:

Requeriments hardware genèrics, per node:

- 32 nuclis físics (cores) de mínim 2,0 GHz cadascun, en base Intel Xeon.
- 512 GB de memòria RAM.
- 4 ports de 10/25GbE.
- 1 ports de 1GbE.
- Doble font d'alimentació Titanium hot-plug.
- Emmagatzematge de dades "all-flash" SSD (no s'accepten opcions híbrides).
- Emmagatzematge per a sistema d'arrancada (boot) en RAID1, format per dos (2) discs dedicats de tamany mínim 480GB.
- Controladores de discs independents per dades i sistema/boot.

Requeriments pel llicenciament del software d'HCI:

- Tantes llicències com siguin necessàries per cobrir els nodes proposats.

- En cas que la solució HCI disposi de diferents edicions, caldrà subministrar la versió més rica en funcionalitats, per tal d'evitar costos ocults a futur.
- Caldrà assegurar també que la proposta integri les llicències/funcionalitats necessàries per establir un model Stretched-Cluster per al clúster requerit, en independència de com la solució s'instal·li inicialment.

El sistema ha de permetre l'ampliació en calent (amb l'addició de nodes addicionals), es a dir, sense necessitat de reconfigurar tot el clúster o realitzar una apagada complerta, o necessitat de fer canvis en el llicenciat existent (del software HCI).

El fabricant de la solució proposada ha d'aportar per escrit algun tipus de garantia escrita que asseguri que es complirà el següent:

- El % d'estalvi de capacitat d'emmagatzematge, el temps a realitzar un backup (p. e. 1 minut per a 1TB…), el número de passos per fer una còpia de seguretat, restauració o clonació d'una màquina virtual, el temps en crear polítiques de còpia de seguretat, etcètera.

Requeriments tècnics

Serveis sobre les dades

- La solució proposada ha de tenir actius tots els seus motors d'eficiència (no només disposar de les funcionalitats). Els motors d'eficiència in-line requerits són: compressió, deduplicació i optimització d'escriptures en discs de dades. La solució pot oferir més motors d'eficiència, sempre que no afectin als tres requerits.

- La solució ha de tenir habilitada la funcionalitat de xifratge de dades. En concret, aquella funcionalitat que permeti xifrar directament el contingut dels discs de dades. És necessari que si un disc de dades queda exposat (per retirada, substitució, robatori o similar) no pugui ser llegit en cap altre sistema. Aquesta funcionalitat de xifratge s'oferirà en la capa HCI, al marge de les opcions que pugui oferir el nivell hipervisor.

- Els motors d'eficiència i el xifratge de dades han de quedar habilitats per al 100% de les càrregues de treball i sense restriccions ni limitacions entre elles. En cas que la solució proposada no pugui complir de manera intrínseca amb aquest requeriment, caldrà que les limitacions tècniques quedin reflectides en la resposta al plec.

- Les propostes hauran d'identificar de manera clara la quantitat de vCPU (o GHz) i vRAM que el programari HCI consumirà a cada node. En cas que aquests consums no siguin fixes, o estiguin vinculats a les diferents funcionalitats habilitades, o no estiguin degudament informades a la documentació del fabricant, les propostes hauran d'afegir com a mínim un 20% extra sobre el recursos (CPU/RAM) sol·licitats.

- Aquelles propostes que no identifiquin aquests consums i/o l'increment de recursos sol·licitats seran automàticament descartades.

- L'adjudicatari haurà d'incorporar documentació sobre l'arquitectura a implementar, així com del comportament esperat de la plataforma en base als diferents escenaris de fallada esperables.

Resiliència i capacitats de la solució

- El clúster HCI ha de proporcionar un emmagatzematge d'alta resiliència, semblant a l'obtingut en una cabina de discos amb doble controladora activa-activa i configuració RAID6 o superior.

- La solució proposada haurà de realitzar una protecció de la dada tant dins de cada node, mitjançant un RAID6 entre discs, com entre els diferents nodes que formin la proposta, mitjançant un mecanisme de rèplica síncrona.

- El clúster principal ha de proporcionar els mecanismes necessaris per permetre la pèrdua simultània d'un (1) node i dos (2) discs de dades de cada node supervivent, sense que aquesta condició afecti la disponibilitat de la informació emmagatzemada.

- Si la solució proposada necessita reconstruccions lògiques (sense RAID físic) davant la pèrdua d'algun disc, s'han de proporcionar nodes amb discs no més grans de 2TB per tal de minimitzar el temps de reconstrucció i el seu impacte en el rendiment.

- En cas que la solució només hagi de reconstruir dades en el canvi d'un disc i no en la pèrdua (RAID a cada node), haurà de disposar de mecanismes que limitin l'impacte en el rendiment de la reconstrucció.

- La tecnologia ha de permetre implementar, en un futur si es desitja, solucions asimètriques entre el clúster principal i un eventual centre de contingència. Per exemple: dos (2) nodes en centre principal i un (1) futur node de contingència.

- La tecnologia també ha de ser capaç d'acceptar configuracions en un (1) sol node, sense limitacions en les funcionalitats. Com a mínim haurà de complir amb els serveis de Deduplicació i Compressió habilitats, així com resiliència local en la fallada d'un disc en RAID5.

- La solució ha de proporcionar un mínim de 9,7 TiB (10 TB) nets usables.

- Es considera la capacitat neta usable com: el resultat de restar la capacitat bruta del sistema (RAW) l'espai necessari per a la implementació de la protecció de la informació (resiliència, rèplica, tolerància a fallada/paritats, etcètera), restar l'espai reservat per a índexs i operatives internes, i sense aplicar cap tècnica d'estalvi en disc com deduplicació i compressió.

- La proposta tècnica haurà de mostrar el detall del dimensionament realitzat per arribar a l'espai net usable presentat. Totes aquelles propostes que només proporcionin un llistat de materials físics, o només la suma dels mateixos, seran descartades.

Gestió de la solució

- La solució presentada ha d'estar totalment integrada amb l'Hipervisor VMware (vCenter), de forma que no sigui necessària cap consola de gestió addicional. En cas d'existir o requerir alguna altra consola de gestió, la solució haurà de proporcionar els seus propis recursos CPU/RAM/disc, de forma independent als sol·licitats i aportar les llicències necessàries a l'edició o versió més completa i rica en funcions.

- En cas de caiguda, pèrdua o apagat del vCenter, la solució ha de continuar treballant amb tota normalitat, i fins i tot permetre accions de "backup/restore". Si la solució presentada considera el component vCenter com a crític o indispensable per mantenir i operar la solució, s'haurà de proporcionar una solució d'alta disponibilitat (HA) pel propi vCenter.

- Al marge de la gestió integrada, la solució ha de disposar d'una interfície d'ordres i una interfície Rest-API per a qualsevol integració, desenvolupament de seqüències o accions en caiguda de vCenter. Aquestes interfícies han d'estar totalment llicenciades i documentades.

Sistema de backup integrat

- Al marge de la solució de còpia de seguretat (*backup*) externa existent a l'ajuntament, la solució proposada ha de ser capaç d'auto protegir les dades,

mitjançant funcionalitats de *backup* integrades, així com de funcionalitats per fer rèpliques remotes d'aquestes còpies a altres nodes/clúster extern/s.

- Aquestes funcionalitats no han de ser tipus *snapshot* de l'Hypervisor ni de volum, sinó una funcionalitat de còpia de seguretat real, amb granularitat a nivell de màquina virtual.

- S'ha de permetre recuperar les còpies de seguretat fins i tot quan la màquina virtual original hagi estat esborrada, a més de permetre recuperar qualsevol d'aquestes còpies sense afectació a la seqüència de protecció. Funcionalitat del tipus *Full Backup*.

- En aquest context, les funcionalitats mínimes requerides seran:

    - Protegir i recuperar màquines virtuals independents (no Datastores) amb sobre escriptura o generant una nova VM (GUID diferent).
    - Recuperació de fitxers i carpetes.
    - Integració amb VMware Tools i Microsoft VSS per consistència d'aplicació.
    - Modificació de la retenció en una còpia específica.
    - Eliminació de qualsevol còpia sense afectar la seqüència del *backup* .
    - RTO/RPO garantits, o com a mínim, identificar temps assumibles.
    - No ha de limitar la solució de còpia de seguretat existent.

- La tecnologia ha de permetre la capacitat de fer rèplica de les còpies de seguretat entre clústers HCI en ubicacions diferents, i ha d'optimitzar el tràfic de WAN nativament (també poder-lo limitar si fos necessari); permetent en un futur l'eventual inclusió d'un node/nodes addicional/s en rol de DR (formació X+1).

- En cas que la solució proposada no disposi d'aquestes característiques de forma nativa, haurà de proporcionar algun programari addicional (incloent-hi llicenciament), certificat pel fabricant, que permeti fer-les. Aquest programari addicional ha de ser compatible amb el ja existent.

Autosuport i ús d'intel.ligència artificial/ML

- La solució proposada haurà de disposar d'un servei o solució basada en Intel·ligència Artificial que permeti beneficiar-se de totes les experiències compartides, de forma anònima, per altres clients amb entorns similars al d'aquesta proposta.

- Aquest servei, o solució, ha d'aportar informes, prediccions, recomanacions i fins i tot que pugui arribar a obrir casos de suport de manera automàtica i directa amb el fabricant. Aquesta solució de programari no podrà utilitzar recursos maquinari del client, sinó que estarà desplegada al núvol del fabricant (en format SaaS).

Sistema de tallafocs i mesures de seguretat a la xarxa

Requeriments generals dels equips de seguretat

- La proposta haurà d'incloure durant la totalitat de la duració del contracte, així com les possibles pròrrogues, totes les llicències i subscripcions necessàries per activar, en el cas que sigui necessari, totes les funcionalitats associades als requeriments obligatoris que es llisten a continuació.

- Els equips tallafocs han de ser en format appliance d'un únic fabricant, quedant exclosos màquines virtuals ni servidors de propòsit general. Han de poder ser instal·lats en un rack estàndard de 19''.

- Els dos equips físics (un en cada CPD que disposa l'Ajuntament) han de ser de idèntiques característiques, redundats i en alta disponibilitat (HA, High availability). Han de permetre treballar en mode HA actiu-actiu i actiu-passiu. En el cas d'activar sistemes virtuals, aquests poden funcionar en qualsevol dels dos nodes, de forma que s'aconsegueixi un actiu-actiu.

- Aquests dos equips, hauran d'assumir les tasques d'enrutament de les diferents xarxes internes de l'ajuntament corresponents a totes les seus municipals.

- La solució ha d'incloure funcionalitats de control d'aplicacions, IPS, Antimalware amb Cloud Sandbox inclós, Webfilter, DNS Filter, Antispam, protecció antiDoS i Web Application Firewall. Totes aquestes funcionalitats han d'estar llicenciades per tota la duració del contracte.

- S'hauran de subministrar fonts d'alimentació redundants per a cada equip.

- Els equips han de disposar de la funcionalitat de Firewalls virtuals per tal de crear entorns completament diferencials. Ha d'incloure com a mínim 10 Firewalls virtuals per equip.

- La solució de seguretat ha de permetre diferents modes de funcionament, podent-se combinar entre els diferents Firewalls virtuals:
    - Mode transparent
    - Mode routed

- Mode sniffer

- S'haurà d'incloure a la proposta, dintre dels mateixos appliance, la funcionalitat d'auditoria pròpia del Sistema, que com a resultat tingui un indicador o valor numèric de risc, així com puntuació negativa per cada paràmetre auditat no complert. Aquests paràmetres que s'han de comprovar son com a mínim: política de seguretat sense ús en els últims 90 dies, política de contrasenyes dèbils i comprovació del llicenciament/suport.

- La pròpia plataforma ha de tenir connectors automàtics amb l'objectiu d'integrar-se amb identitats terceres i poder recollir informació, adreçament ip, inventari d'objectes i etiquetes. Aquesta funcionalitat haurà d'estar suportada en els appliances de seguretat (sense necessitat de consola addicional). En concret es requereixen les següents:
  - Cloud pública: Google Cloud, Azure, AWS, Oracle i AliCloud.
  - Cloud privada: VMware NSX i ESXi, Openstack, Kubernetes, Cisco ACI i Nuage.
  - Fonts d'identitat: Active directory i Radius.
  - Fonts d'amaneces: Llistat d'ip, dominis, URLs i hash's de malware customitzats.

- La mateixa solució de seguretat ha de permetre la creació d'automatismes per tal de:
  - Davant la detecció d'un host compromès, els tallafocs enviïn (tots alhora): un email, una notificació tipus push a dispositius Iphone, poder banejar l'adreça ip, invocar funcions AWS Lambda, Google functions, Azure Functions i Webhook.
  - Davant el canvi de configuració del tallafocs, un failover, reboot, actualització de firmes, de forma programada i qualsevol event del tallafocs, aquest enviï (tots alhora): un email, una notificació tipus push a dispositius Iphone e invocar funcions AWS Lambda, Google functions, Azure Functions, AliCloud Function, comanda per CLI i Webhook.

- Capacitat de configuració de Proxy explícit per Interface, amb la funcionalitat de Proxy chaining en cas necessari, a més de capacitat de caching.

Requeriments de capacitat i rendiment

- Els equips tallafocs tindran hardware específic (de tipus ASIC) per tal d'assegurar el rendiment requerit; en detall, ha de tenir un hardware específic per analitzar el tràfic a nivell 4 i un altre totalment diferent, a nivell 7 i garantir baixa latència.

- El tallafocs disposarà de fins 139 / 137 / 70 Gbps de rendiment de firewall per paquets de 1518, 512 i 64 bytes en IPv4 ; i de 139 / 137 / 70 Gbps de rendiment de firewall per paquets de 1518, 512 i 86 bytes en IPv6 .

- El tallafocs ha de ser capaç de gestionar fins 8 Milions sessions concurrents. Així com a mínim 550.000 noves sessions per segon.

- El tallafocs ha de tenir una latència inferior a 4.12 µs (per paquets 64 byte UDP) que caldrà acreditar amb el datasheet oficial del fabricant.

- Ha de tenir capacitat per com a mínim de 20.000 polítiques de firewall.

- El rendiment per tràfic SSL VPN ha de ser de com a mínim 4.3 Gbps i per tràfic IPSEC VPN (512 bytes) de 55 Gbps.

- A nivell 7, l'equip ha de disposar de com a mínim el següent rendiment:

    - Rendiment IPS: 14 Gbps per tràfic Enterprise MIX.
    - Rendiment NGFW (IPS i control d'aplicacions): 11.5 Gbps per tràfic Enterprise MIX.
    - Rendiment amb Threat Protection (Firewall mes IPS, control d'aplicacions i motor antimalware actius): 10.5 Gbps per tràfic Enterprise MIX.

      Caldrà acreditar que aquestes tres últimes dades siguin amb logging actiu.

    - Rendiment Inspecció SSL amb IPS: 9 Gbps mesurat amb diferents Ciphers.
    - Rendiment per control d'aplicacions: 32 Gbps mesurat per http 64K.

Característiques físiques i requeriments funcionals

Els datacenters de nova generació, amb adopció de tecnologies de connectivitat 25G/40G requereixen de tallafocs de nova generació amb hardware específic. Caldrà que els equips ofertats suportin les següents funcionalitats:

- Processadors Hardware (SPU) preparats per datacenters hyperescalars amb acceleració hardware.
- Suport de processament hardware amb alt rendiment i molt baixa latència amb acceleració de tràfic IPv4, IPv6, CAPWAP, VXLAN, GRE i IPSEC.
- Capacitat de protecció antiDoS (Denegació de Servei) implementada per hardware contra atacs volumètrics.
- Suport de QoS per hardware incloent traffic shaping i queuing.

- La solució ofertada haurà d'incloure coprocessadors hardware per accelerar el tràfic criptogràfic així com la inspecció de seguretat per hardware, incloent la recerca de signatures d'atacs.
- Suport de protocols RIP v1/v2, OSPF, ISIS, BGP, WCCP i Multicast per IPv4 e IPv6, Routing basat en política o PBR i funcionalitats avançades SD-WAN.
- Suport de VRFs (múltiples taules de Routing) i multiVRF Routing (per BGP i OSPF).
- Suport Dual Stack IPv4 e IPv6 simultàniament.
- Network address translation NAT IPv4, NAT64 i NAT66.
- DHCP server / DHCP Relay /DNS Server / DNS Proxy / NTP Server.
- 802.1Q VLANs i Point-to-Point Protocol over Ethernet (PPPoE).
- 802.3ad Capacitat de crear enllaços LACP per l'agregació de ports
- Capacitat de balanceig de servidors a nivell 4 per tots els serveis, com també possibilitat de fer SSL off-loading pel tràfic HTTPS.
- Cal que la solució de seguretat tingui capacitats integrades de SD-WAN, en concret:

    - Balanceig intel·ligent de connexions físiques i lògiques, indiferentment del tipus de connexió WAN (MPLS, 3G/4G, FTTH, VPN, etc..).
    - El número mínim de connexions físiques i lògiques que es poden afegir a l'SD-WAN ha de ser de 256.
    - Verificació de la disponibilitat d'Internet per cadascuna de les línies, per protocols http, ping, dns i TWANP. El numero de Health-checks ha de ser de com a mínim 100.
    - Verificació de qualitat en temps real: jitter, packet loss i latència per línia.
    - Configuració de polítiques de SD-WAN intel·ligent basat en origen (usuaris AD i direcció IP), en el destí (direcció IP, aplicacions i/o serveis d'Internet/aplicacions) i en la línia amb millor qualitat d'aquell moment basat en valors de jitter, packet loss, latència, tràfic de pujada/baixada o ampla de banda, així com una combinació per pesos.
    - En el cas de necessitat de llicenciament o subscripcions per activar aquestes funcionalitats, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

- Suport d'VXLAN i VXLAN VTEP per extensió de nivell 2 sobre xarxes de nivell 3.

- El sistema proposat ha de tenir una funcionalitat integrada de Traffic Shaping tant de trànsit sortint com a entrant sent capaç de reservar ample de banda i marcar el trànsit amb DSCP. Aquest traffic shaping ha de basar-se en aplicacions i URLs a nivell global de perfil o per ip.

Connectivitat i caracteristiques fisiques

Els tallafocs han de incloure en la oferta presentada el següent número de interfícies com a mínim (per cada equip):

- 1 port de consola.
- 2 port d'USB 3.0 per a la connexió de modem 3G/4G i/o pendrive.
  El port USB ha de permetre la instal·lació desassistida del firmware i aplicació de configuració en el booting de l'equip per realitzar tasques automàtiques d'instal·lació i canvis d'equipament.
- 4 ports 10GE SFP+
- 4 ports 25GE/10GE SFP28/SFP+
- 24 ports 1GE (16 ports 1GE RJ45 + 8 ports 1GE SFP)
- 2 ports HA/Gestió dedicats
- Instal·lació en rack de 19'' i no més de 1 RU.
- Consum màxim inferior a 255 W.
- En el cas que l'equipament permeti ampliacions modulars d'interfaces, caldrà que tots els mòduls d'ampliació estiguin equipats amb interfícies com a mínim de les mateixes velocitats que es sol·liciten pels ports mínims obligatoris.
- En el cas que l'equip suporti ampliacions de memòria RAM i Disc Dur, caldrà que l'appliance estigui equipat amb el màxim de capacitats RAM i de Disc suportats pel fabricant.
- Fonts d'alimentació redundants i amb Hot Swap.

Alta disponibilitat

- La funcionalitat d'alta disponibilitat ha d'estar disponible sense necessitat de llicencia.
- Suport HA tipus Actiu – Passiu, Actiu - Actiu i mode mixta. El mode mixte implica poder tenir Firewalls virtuals actius i passius de forma barrejada, es a dir, el màster de certs Firewalls virtuals sigui la primera unitat de tallafocs, mentre que la segona unitat de tallafocs es màster de la resta de firewalls virtuals alhora.
- La transferència de servei d'un equip a l'altre s'ha de poder fer sense talls, ni pèrdua de les connexions tcp, ni aturada de servei.
- Les configuracions s'han de traspassar de manera automàtica entre els dos equips.

- Capacitat de funcionament en mode actiu/actiu sincronitzant sessions entre els dos nodes però mantenint adreçament IP diferenciat en les interfícies de cada node del clúster.
- En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

Visibilitat

- Els equips tallafocs han de poder generar topologies gràfiques físiques i lògiques, amb la integració d'altres tallafocs del fabricant, per tal de poder ser capaç de veure en un extrem a extrem que esta passant en tota la xarxa.
- Funcionalitat de consolidació de logs amb diferents nivells d'agrupació, en concret: per origen, destí, aplicació, amenaça, websites i polítiques per a la seva visualització.
  Aquesta visualització ha de ser tipus "Drill-down", és a dir, poder seleccionar uns dels objectes agrupats i anar filtrant el resultat en base a aquesta selecció, fins a saber el detall complet.

Aquests requeriments hauran de poder acomplir-se des de la mateixa GUI dels appliances, en temps real, i sense necessitat d'una consola central de gestió.

Seguretat

- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant els següents paràmetres de coincidència:

  - Com a origen (totes les opcions):
    - Capacitat de definir una i/o més d'una Interface d'origen, incloent "any". Així com també "zones".
    - Capacitat d'utilitzar direccions ip, rangs i/o xarxes, FQDN, països, serveis d'internet i direccions ip's reconegudes com origen de xarxes TOR, proxies anònims (aquestes direccions han d'actualitzar-se automàticament), així com els objectes exportats dels connectors esmentats a l'apartat de caracterisques generals de l'equip.
    - Capacitat d'utilitzar usuaris/grups locals o remots mitjançant connectors AD, NAC o altres repositoris d'identitat.
    - Capacitat per declarar horaris o "schedule" tant per dia/hora com a data màxima de venciment.
    - Capacitat de selecció del servei a utilitzar.

  - Com a destí:

- Capacitat de definir una i/o més d'una Interface de destí, incloent "any". Així com també "zones".
- Capacitat d'utilitzar direccions ip, rangs i/o xarxes, així com objectes FQDN, països i serveis d'internet.

- Capacitat de definir polítiques de seguretat IPv4/v6 utilitzant la següent parametrització:

  - S'ha de poder seleccionar quin tràfic s'analitzarà a nivell 4 i quin a nivell 7, per política, sense excepció.
  - La configuració del NAT sortint s'ha de poder configurar dintre de cadascuna de les polítiques de seguretat, de forma granular.
  - Les diferents funcionalitats de seguretat avançades de nivell 7 s'activaran de forma individual a nivell de política, mai a nivell global. A més aquestes es gestionaran amb perfils per tal de ser granulars en els permisos. Aquestes funcionalitats son: antivirus, webfilter, DNS filter, Web Application Firewall, Control d'aplicacions, IPS, i DLP.
  - Decidir a nivell de política quin tràfic SSL serà desxifrat pel seu anàlisis i quin només a nivell de certificat.

  - A nivell de logging, cal que la solució permeti activar el logging de només nivell 7, o tant de nivell 4 més nivell 7. Cal també fer captura de packets en la pròpia política.

- Capacitat de creació de regles de DoS a nivell 3 i 4, podent aplicar umbrals per serveis publicats on poder filtrar per direccions ip o països per: ip_src_session, ip_dst_session, tcp_syn_flood, tcp_port_scan, tcp_src_session, tcp_dst_session, udp_flood, udp_scan, udp_src_session, udp_dst_session, icmp_flood, icmp_sweep, icmp_src_session, icmp_dst_session, sctp_flood, sctp_scan, sctp_src_session i sctp_dst_session.

- Capacitat de definir polítiques a nivell d'Interface per tal de denegar tràfic i no ser processat per la política de seguretat global. S'han de poder utilitzar direccions IP's, països, així com rangs i xarxes ip com a origen.

- Per tal d'evitar l'accés de xarxes botnet, els tallafocs han de tenir una base de dades de reputació dinàmica que bloquegi els accessos a nivell d'Interface.

- Visualització del número d'usos i quantitat de tràfic de cada regla de seguretat, de forma àgil tant en la pròpia secció de polítiques de seguretat, això com també dintre de la configuració de cada política . També cal veure l'ultima vegada que s'ha utilitzat.

Control d'aplicacions

- Capacitat per identificar un mínim de 4400 aplicacions actives actuals (incloent aplicacions web 2.0), com per exemple distingir Facebook, d'una sub-aplicació Facebook-chat o post.

- La solució ha de classificar les aplicacions en diferents categories i subcategories, per poder aplicar regles d'acord amb aquestes categories / subcategories (control granular dins de l'aplicació).

- Aplicar tècniques d'identificació d'aplicacions a tots els ports TCP / UDP i no només en els més comuns.

- Capacitat per identificar les aplicacions sota túnels HTTPS.

- Capacitat per identificar aplicacions Industrials com Modbus.

- Capacitat de creació de firmes d'aplicacions per un reconeixement personalitzat. Es obligatori que en aquelles aplicacions customitzades, també siguin analitzades per motors de protecció (IPS i antimalware).

IPS

- Capacitat per protegir tant servidors com clients amb un mínim de 11000 firmes d'IPS, agrupades per categoria, severitat, objectiu i protocol. Davant la identificació d'un atac per IPS, cal que el tallafocs capturi el tràfic en un arxiu pcap per tal d'evidenciar-ho i fer un estudi posterior.

- Capacitat per identificar patrons d'atacs basats en comportament o rated-base, per tal de bloquejar intents d'atacs un cop superat un umbral d'ús en un temps determinat.

- Capacitat de creació de firmes d'IPS per un reconeixement personalitzat.

Antimalware

- Capacitat de detecció de malware (virus, grayware, worns, etc…) basat en firmes conegudes o mètodes avançats de detecció.

- Suport de sandboxing en el cloud, amb un tamany mínim de fitxer de 100 MB indistintament del tipus de fitxer.

- Capacitat per l'eliminació del contingut dinàmic (macros, javascript, URL) explotable dintre de documents ofimàtics i pdf, que es distribueixen per protocols SMTP, IMAP i http.

- Capacitat de comprovació de si es tracta d'un fitxer bo o dolent, en funció del hashing i comparat amb la BBDD del fabricant. Així com bloquejant mitjançant malware de repositoris externs de threat inteligence.

Webfilter

- Capacitat de categoritzar més de 250 milions de pàgines web en més de 60 categories web per tal d'aplicar: block, monitor i aplicació de cuotes de temps o tràfic per categoria.

- Suport de protocols http v1.0, 1.1 i 1.2.

- La base de dades de categories web caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les url's el més actualitzat possible.

- Suport per restringir l'accés a Youtube i Google en mode "safe search".

- Suport de rating per imatges per URL.

- Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.

DNS Filter

- Capacitat de categoritzar domins DNS en més de 60 categories per i poder realitzar intercepció del tràfic DNS amb les següents accions: block, monitor i redirect (redirigir les consultes cap a un portal web cloud o personalitzat de bloqueig).

- La base de dades de categories dns caldrà consumir-se com un servei cloud en temps real i no podrà basar-se únicament en llistats locals per tal de tenir la categorització de les url's el més actualitzat possible.

- Suport per restringir l'accés a Youtube i Google en mode "safe search".

- Suport per a la creació de llistes blanques/negres externes sense necessitat de llicencia.

Altres funcionalitats de nivell 7

- Altres funcionalitats de nivell 7 que la proposta ha d'incloure i han d'estar llicenciades son:
    - DLP
    - ICAP
    - Web application firewall

VPN

- El dispositiu admet fins a un màxim de 10.000 usuaris simultanis VPN SSL, ja sigui amb agent o sense, però en qualsevol cas sense llicència addicional.

- El sistema proposat haurà de complir els estàndards de la indústria, sense el suport extern addicional de maquinari o mòduls: IPSEC VPN (IPv4 i IPv6), PPTP VPN, L2TP VPN, SSL VPN i GRE sobre IPSEC.

- El sistema proposat haurà de suportar 2 modes de funcionament SSL VPN:
    - Sense client - Accés web: per a clients remots que només necessiten un navegador i no requereix la instal·lació de cap agent, per tal d'accedir via web a: HTTP / HTTPS Servidor intermediari, FTP, Telnet, SMB / CIFS, SSH, VNC i RDP.
    - Mode túnel: per a equips remots que executen una varietat d'aplicacions de client i servidor.

- Suport d'agregació de túnels VPN i balanceig per packet podent així afegir l'ampla de banda dels accessos VPN IPsec entre seus.

- Capacitat d'integració del mateix fabricant de doble factor d'autenticació via token mòbil, així com per SMS i correu electrònic, integrat en la mateixa plataforma de seguretat. Aquest token també s'ha de poder fer servir per l'accés a la GUI dels equips tallafocs.

Controladora d'accés segur integrada

- El sistema ha de ser capaç d'actuar com controladora de punts d'accés wireless així com de switches del mateix fabricant.

- La capacitat mínima de 1024 punts d'accés wifi gestionats del mateix fabricant, i de switchs de 96 gestionats i del mateix fabricant.

- En el cas de necessitat de llicenciament o subscripcions per activar l'alta disponibilitat, caldrà que aquestes estiguin incloses en la proposta durant la duració completa del contracte.

- La gestió dels APs i Switches es farà des de la mateixa interfície gràfica i CLI des de la qual es gestiona el Firewall o des de la consola central de gestió.

Sistemes de logging i reporting

Pel logging i reporting caldrà instal·lar una màquina virtual/appliance per tal que els tallafocs enviïn en temps real els logs generats, amb l'objectiu de que sigui una:

- Eina de monitoreig a temps real del trànsit filtrat pels diferents mòduls dels equips.
- Eina de monitoreig històric externa als dispositius, emmagatzematge de logs, reports, del tràfic analitzat pels equips amb capacitat de fer informes de 6 mesos aproximadament (incloure llicenciament i suport necessari durant tota la durada del contracte).
- Reports i alarmes en funció de adreces, ports, protocols.
- Reports i alarmes en funció de usuaris i/o grups d'usuaris (AD/LDAP).
- Poder analitzar, correlacionar i fer informes de la informació de seguretat de manera centralitzada.
- Panell de control amb vista general d'usuaris destacables, aplicacions, destinacions, llocs web, vulnerabilitats, etc.
- Models d'informes preconfigurats, editables, modificables i exportables.
- Gestió d'events amb generació d'alertes automàtiques a administradors.
- Visor de logs en temps real o històric, que permeti distingir-los entre trànsit, events i seguretat.
- Visió de logs per dispositiu, dominis d'administració o agregats.
- Capacitat de filtratge i granuralitat d'anàlisi de logs.
- Dissenyador d'alertes comprensible .
- Possibilitat de generació d'alertes per nivells de seguretat, events específics, accions o destinacions i nombre d'events en un determinat temps.
- Capacitat de cercar alertes històriques.
- Notificació d'alertes per correu electrònic, SNMP o syslog.

- Rotació de logs recopilats automàtica amb enviament d'històrics a d'altres sistemes per email, FTP, HTTP, etc.
- Visibilitat dels logs en format TXT descarregables.
- Vista comparada de patrons de trànsit i amenaces.
- Anàlisi exhaustiva de totes les activitats relacionades amb el trànsit i els dispositius.
- Elaboració d'informes sobre totes les activitats de trànsit i de dispositius.

6.3 Provisió dels sistemes

L'import estimat del contracte inclou la provisió de les infraestructures i sistemes sol·licitats i tots els possibles elements de cost associats al subministrament, implementació, migració i garantia dels sistemes inclosos en l'abast del present document, incloent:

- Subministrament
- Instal·lació
- Migració
- Pla de proves
- Formació
- Manteniment
- Garantia

D'altra banda, els licitadors han de preveure tot aquell material necessari per a la posada en marxa dels sistemes contemplats. Addicionalment, es requereix la prestació dels serveis de garantia.

És a dir, l'Ajuntament no assumirà cap altre cost associat a la implantació dels sistemes contemplats, a banda de les necessitats per als licitadors en les seves propostes.

D'altra banda, les licitadores no han de preveure part del personal de l'Ajuntament excepte per assistir a l'adjudicatari en les tasques de migracions dels serveis.

6.4 Model Organitzatiu

a) Comitès del projecte

El model organitzatiu i de relació per a la gestió del projecte es basa en l'establiment i realització dels següents comitès:

- Comitè de Direcció del projecte:

- Assistència del responsable del projecte per a part de l'Ajuntament.
- Assistència del responsable del projecte per part del proveïdor.
- Lliurament i revisió de l' informe executiu de seguiment per al Comitè de Direcció.
- Revisió dels aspectes rellevants de l'informe executiu de tal manera que s'identifiquin les criticitats i riscos, avaluació de problemes, etc.
- Presa de decisions i accions de millora derivada de l'anàlisi de l'informe executiu.
- Elaboració de l'acta del Comitè de Direcció.
- Reunions de periodicitat mensual i/o sota demanda segons riscos i/o criticitats del projecte.

- Comitè de Seguiment del projecte:
  - Assistència dels responsables del projecte per part de l'Ajuntament.
  - Assistència dels responsables del projecte per part del proveïdor.
  - Lliurament i revisió de la documentació de seguiment per al Comitè de Seguiment.
  - Revisió de les activitats realitzades des de l'últim Comitè de Seguiment, problemàtiques, aspectes crítics, etc.
  - Elaboració de l' acta del Comitè de Seguiment.
  - Reunions de periodicitat quinzenal i/o sota demanda segons riscos i/o criticitats del projecte.
  - Les reunions de Comitè de Seguiment poden derivar en la convocatòria de reunions extraordinàries de Comitè de Direcció si així s' estima convenient.

b) Equip tècnic del projecte

Les persones que formaran part de cada un dels equips tècnics de les parts són les següents:

L'Ajuntament té prevista l'assignació del següent equip per al projecte:

- El Cap del Servei d'Organització i Tecnologíes de la informació serà el màxim responsable del projecte per part de l'Ajuntament.
- 2 Responsables tècnics de sistemes per al seguiment diari del projecte.

Per part del proveïdor i a fi de garantir el model de relació i gestió explicitat, l'equip mínim següent:

- Responsable/Director del projecte, que serà el màxim responsable per part del proveïdor. Les seves responsabilitats principals són:
    - Interlocució amb els responsables de l'Ajuntament.
    - Anàlisi d'incidències i propostes d'acció correctores.
    - Responsable de la definició organitzativa del projecte.
    - Seguiment intern del projecte i identificació d'accions de millora.
    - Supervisió dels recursos assignats al projecte.
    - Elaboració de la documentació de seguiment per al Comitè de Direcció del projecte.
    - Assistència al Comitè de Direcció del projecte.
- Responsables tècnics: Responsables del dia a dia del projecte i de la coordinació de la resta de recursos assignats al projecte. Les seves responsabilitats principals són:
    - Interlocució amb els recursos de l'Ajuntament que gestionen les plataformes de sistemes d'informació.
    - Primer nivell d'escalat del proveïdor.
    - Seguiment del dia a dia del projecte. Supervisió de la resta de tècnics de camp assignats al projecte ja sigui de forma permanent o puntual. Elaboració de la documentació de seguiment per al Comitè de Seguiment del projecte. Assistència al Comitè de Seguiment i al Comitè de Direcció si així es requereix.
- Tècnics de camp: Tècnics operatius del projecte.
    - Les seves responsabilitats principals seran el desenvolupament de les tasques associades al projecte.
    - Assistència al Comitè de Seguiment i al Comitè de Direcció del servei, en cas que així es requereixi de forma específica.

Es requereix que, com a mínim, dos dels tècnics adscrits a l'equip de projecte proposat per al proveïdor comptin amb una certificació tècnica pròpia del fabricant dels equips a subministrar en el present procediment. Aquesta certificació ha de permetre garantir que aquests tècnics disposin dels coneixements i habilitats per a la gestió, operació i configuració dels equips proposats per a l' adjudicatari.

6.5 Model d'implantació

a) Pla d'implantació

El pla d' implantació detallat dels sistemes objecte del present plec es presentarà en forma de pla de projecte tal i com es descriu a l'apartat 8- Criteris d'adjudicació del contracte.

Aquest pla d'implantació ha de tenir en compte els equips que actualment es troben en funcionament per part de l'Ajuntament. En aquest sentit es pot donar el cas que el licitador hagi de reubicar el maquinari existent per donar cabuda als nous sistemes.

Per últim, el licitador ha de tenir en compte la retirada de l'embalatge dels diferents sistemes instal·lats, així com indicar a l'Ajuntament els embalatges que calgui conservar.

b) Documentació “as-built”.

Una cop finalitzada la implantació serà necessari lliurar la documentació que indiqui de forma exhaustiva totes les instal·lacions i implementacions realitzades sota l'abast del present plec. La documentació ha d'incloure, com a mínim:

- Memòria tècnica de les instal·lacions i implementacions, incloent l’inventari d'equipament i, quan correspongui, el detall de les parametritzacions efectuades durant la instal·lació / implementació.
- Manuals d' operació i d’explotació.
- Certificació de la instal·lació conforme a la normativa d’aplicació.

6.6 Manteniment i suport

El proveïdor ha de realitzar les tasques preventives, correctives i evolutives de l'equipament subministrat que així ho requereixi el seu pla de manteniment i suport, inclòs en l' adjudicació del procediment, essent la seva responsabilitat i assumint el seu cost.

A tots els efectes, la duració mínima dels serveis de manteniment serà de 5 anys.

A continuació, es detallen les característiques per tenir en compte pel que fa als serveis de manteniment i suport.

a) Manteniment preventiu

El manteniment preventiu té coma objectiu detectar amb antelació possibles fallades de les noves sistemes instal·lades i evitar situacions futures que poden dificultar l'operativa dels serveis, així com minimitzar el risc d'incidències.

En aquest sentit, el licitador ha de detallar en el pla de manteniment i suport un apartat sobre el manteniment preventiu pels sistemes que es detallen en el present document, detallant les seves tasques, així coma la freqüència d'aquestes, sent la periodicitat per a la realització d'aquestes tasques de caràcter semestral.

Cap de les tasques detallades no pot afectar el funcionament dels sistemes de l'Ajuntament. En cas que el manteniment d'un sistema comporti la seva no operativa,

els tècnics de l' Ajuntament hauran de determinar l' interval horari de menor productivitat de l'Ajuntament per a la realització de les tasques preventives. Els licitadors hauran de contemplar, si és necessari, fer aquestes actuacions fora de l'horari de treball establert a l'Ajuntament en les seves propostes.

Per últim, l'adjudicatari ha de contemplar el monitoratge dels següents paràmetres:

- Mesura i monitorització en temps real dels paràmetres de qualitat SLA associats al servei.
- Mesura i monitorització dels paràmetres de qualitat SLA associats a la gestió de les incidències: temps mitjà entre fallades, temps mitjà de detecció, diagnòstic i resolució de les incidències, etc.
- Els diferents equips que conformen la plataforma s'han de poder integrar en una plataforma en modalitat Saas en cloud, que permeti oferir analítiques predictives (relacions amb seguretat i possibles falles del maquinari, per exemple), aprenentatge global (per exemple, inventariats, reports d'estat) i informació avançada de suport (recol·lecció automatitzada de dades telemètriques, accés a arxius de registre, notifiquen nous programaris firmware i drivers disponibles, així com a creació manual i automàtica de casos de suport).

b) Manteniment correctiu

El manteniment correctiu es realitza per part de l' adjudicatari una vegada es detecti qualsevol averia o incidència en els sistemes subministrats.

Serà responsabilitat de l' adjudicatari i sense cost per a l'Ajuntament la reparació de les averies, encara que impliquin la substitució d'equips, desplaçament de personal, mà d'obra, etc.

S'ha de detectar i reparar qualsevol averia, encara que aquesta no produeixi indisponiblitat ni degradació del servei. Aquestes incidències seran gestionades per l' adjudicatari seguint els SLA establerts.

Dins del manteniment correctiu el licitador ha de contemplar la possible destrucció segura i confidencial de qualsevol suport d'emmagatzematge que es consideri avariat i sense possibilitat de reparació. Aquesta acció podrà ser auditada i en qualsevol cas ha de ser validada pels tècnics de l'Ajuntament.

c) Manteniment evolutiu

El manteniment evolutiu té com a objectiu introduir per part de l'adjudicatari les possibles millores, bàsicament a nivell de versions de programari, que sorgeixin durant la duració del present contracte. Això implica una actitud proactiva per part del proveïdor per garantir els següents aspectes:

- Aplicar les actualitzacions "minor release" associades al programari subministrat que sorgeix durant la durada del contracte.
- Informar a l'Ajuntament dels nous sistemes i/o facilitats que puguin ser d'interès en l'àmbit local.
- Proposar accions proactives de manteniment preventiu. Totes les accions proactives hauran de ser notificades prèviament a l'Ajuntament, que validarà la seva implementació.

7. OBLIGACIONS DE L'ADJUDICATARI

7.1 Generals

- L'adjudicatari no podrà subcontractar, cedir o traspassar els drets o obligacions derivats del contracte sense autorització de l'Ajuntament d'Igualada.

7.2 Coordinació

S'establirà un sistema de coordinació entre l'Ajuntament d'Igualada i l'empresa contractada. En les reunions de coordinació es tractaran temes relacionats amb el desenvolupament del contracte i resultats.

7.3 Protecció de dades

El contractista i el seu personal hauran de respectar les prescripcions del Reglament (UE) 2016/679 del Parlament i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades així com la Llei orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a finalitats de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions.

Sota cap circumstància, el contractista no podrà obtenir altres dades (escrites, gravades, filmades o efectuades per qualsevol altre mitjà audiovisual) de l'usuari/ària, que les aportades per l'Ajuntament.

8. CRITERIS D'ADJUDICACIÓ DEL CONTRACTE

Les ofertes presentades a licitació es valoraran entre 0 i 100 punts. Per valorar-les es tindrà en compte una pluralitat de criteris en base a la millor relació qualitat-preu, amb la ponderació relativa atribuïda a cadascun. El mètode per determinar la millor oferta serà la suma dels diferents punts assignats en cadascun dels criteris de valoració que a continuació s'indiquen:

Criteri de valoració	Tipus de criteri	Puntuació
Criteri subjectiu	Criteris que depenen d'un judici de valor. Presentació d'un pla de projecte detallant la implementació	Fins a 25 punts
Criteri avaluable de forma automàtica	Oferta econòmica i millores aportades	Fins a 75 punts
PUNTUACIÓ MÀXIMA		Fins a 100 punts

8.1 Criteris que depenen d'un judici de valor (fins a 25 punts)

Presentació d'una memòria-pla de projecte, de presentació obligatòria: Els licitadors presentaran un pla de projecte on es detallarà la proposta ofertada, en un màxim de 50 pàgines (font de lletra, tamany mínim 10p).

El contingut mínim que ha de tenir aquest pla és el següent:

1. Índex

2. Solució tècnica detallada incloent-hi els datasheets del fabricant amb les característiques tècniques exigides en aquest plec. Valoració màxima 10 punts.

    - Es descriu de forma detallada i clara la solució tècnica, les característiques tècniques presten una màxima funcionalitat i hi ha una màxima adequació entre les necessitats que planteja el projecte i el maquinari i programari a instal·lar… 10 punts.
    - Nivell mitjà de detall en la descripció i claredat de la solució tècnica o les característiques tècniques presten una funcionalitat mitjana i una adequació mitjana entre les necessitats que planteja el projecte i el maquinari i programari a instal·lar… 5 punts.
    - Nivell baix de detall en la descripció i claredat de la solució tècnica o les característiques tècniques presten una funcionalitat baixa i una adequació baixa entre les necessitats que planteja el projecte i el maquinari i programari a instal·lar… 1 punts.
    - Sense descripció o amb errors considerables... 0 punts.

3. Pla d'instal.lació, migració i cronograma. Valoració màxima 10 punts.

    - Descriu de forma detallada i clara la instal·lació i migració de les dades i el pla d'execució, la senzillesa en la instal·lació i migració amb un perjudici mínim a l'activitat normal de l'Ajuntament… 10 punts.

    - Nivell mitjà de detall i claredat de la instal·lació i la migració de les dades i el pla d'execució o un procés d'instal·lació i migració de complexitat mitjà o un perjudici mitjà per a l'activitat normal de l'Ajuntament… 5 punts.

    - Nivell baix de detall i claredat al pla d'instal·lació i migració o una complexitat alta a la instal·lació i migració o un perjudici alt a l'activitat normal de l'Ajuntament… 1 punt.

    - Sense descripció o amb errors considerables … 0 punts.

4. Pla de formació. Pla de capacitació als empleats de l'Ajuntament en les tecnologies implantades, tot contemplant detall i amplitud de la formació i del temari que haurà d'incloure necessàriament exemples pràctics. Valoració màxima: 5 punts.

    - Descriu de forma detallada i clara la formació i del temari i la seva amplitud… 5 punts.
    - Nivell mitjà de detall i claredat de la formació i temari o amplitud mitjana… 3 punts.
    - Nivell baix de detall i claredat de la formació i temari o amplitud mínima… 1 punt.
    - Sense descripció del Pla de formació… 0 punts.

8.2 Criteris avaluables de forma automàtica (fins a 75 punts)

OFERTA ECONÒMICA: PREU - fins a 60 punts.

L'oferta econòmica, que és obligatòria, s'ha de presentar segons el model que s'estableix en el plec de clàusules administratives.

A l'oferta econòmica més baixa, que no incorri en valors anormals o desproporcionats, se li atorgarà la màxima puntuació.

La puntuació de la resta de les ofertes s'avaluarà de la següent manera:

$$Pv = [1-(\underline{Ov-Om}) \times (1/VP)] \times 60$$
$$IL$$

On:
Pv =Puntuació de l'oferta a valorar
Ov = Oferta que es valora
Om = Oferta més baixa
IL = Import de licitació
VP = Valor de ponderació

CRITERIS DE MILLORA:

Fins a 15 punts.

Els licitadors podran presentar, de forma potestativa, les següents millores tècniques:

- **Extensió de la garantia dels equips instal.lats (fins a 10 punts).**

  Per cada any addicional aportat de garantia dels equips: 5 punts.

- **Ampliació de l'emmagatzemament SSD als dispositius firewall (fins a 5 punts).**

  Oferir 1 disc dur SSD de 240Gb addicional per a cadascun dels dispositius de firewall: 5 punts.

9. INICI I DURADA DEL CONTRACTE

El contracte s'iniciarà a la data de la seva signatura i atesos els terminis d'execució que disposa l'Ordre TER/836/2022, de 29 de agosto, per la qual s'aproven les bases reguladores de la subvenció Next Generation sobre Modernització dels serveis d'atenció ciutadana citada anteriorment, la finalització del contracte serà el 13 de setembre de 2024.

10. PREU I FORMA DE PAGAMENT

El preu del contracte es fixa en la quantitat **de 214.950 euros IVA exclòs (260.089,5 euros -IVA 21% inclòs-).** No podran acceptar-se proposicions econòmiques que superin aquest import.

La despesa s'imputarà a les partides i en els imports que segueixen, del programa 30003.92005 MRR MODERNITZACIÓ I DIGITALITZACIÓ ADMINISTRACIÓ LOCAL del pressupost general de la Corporació per aquest 2024.

PARTIDA	IMPORT IVA EXCLÒS	IMPORT AMB IVA
30003.92005.64100	214.950 €	260.089,5 €

L'adjudicatari presentarà una factura, una vegada realitzats els treballs, que correspondrà a les partides descrites en el quadre, en el termini màxim del dia 13 de setembre de 2024, adaptades les quanties als imports de l'oferta guanyadora.

11. MODIFICACIÓ DEL CONTRACTE

No es preveuen supòsits específics de modificació del contracte.

12. REVISIÓ DE PREUS

No es preveu revisió de preus atès que no es preveu cap inversió que requereixi un període de recuperació igual o superior a 5 anys.

13. RESPONSABILITAT CIVIL

El contractista, abans de la signatura del contracte, si és que no ho ha fet amb anterioritat, haurà de presentar còpia de la seva pòlissa de responsabilitat civil, amb un risc assegurat per un import mínim de 300.000 € per sinistre i any. Per causes justificades, el president podrà prorrogar el termini per presentar la pòlissa de responsabilitat civil. Si transcorregut el termini no es presenta, serà causa de resolució del contracte.

14. REGLES ESPECIALS RESPECTE DEL PERSONAL LABORAL DE L'EMPRESA CONTRACISTA

Correspon exclusivament a l'empresa contractista la selecció del personal que, acreditant els requisits de titulació i experiència exigits en els plecs, formarà part de l'equip de treball adscrit a l'execució del contracte, sense perjudici de la verificació per part de l'Administració del compliment d'aquells requisits.

L'empresa contractista procurarà que existeixi estabilitat en l'equip de treball, i que les variacions en la seva composició siguin puntuals i obeeixin a raons justificades, en ordre a no alterar el bon funcionament del servei, informant en tot moment a l'Administració.

En relació amb els treballadors destinats a l'execució d'aquest contracte, l'empresa contractista assumeix l'obligació d'exercir de manera real, efectiva i continua, el poder de direcció inherent a tot empresari. En particular, assumirà la negociació i el pagament dels salaris, la concessió de permisos, llicències i vacances, les substitucions dels

treballadors en els casos de baixa o absència, les obligacions legals en matèria de Seguretat Social, inclòs l'abonament de cotitzacions i el pagament de prestacions, quan procedeixi, les obligacions legals en matèria de prevenció de riscos laborals, l'exercici de la potestat disciplinaria, així com quants drets i obligacions es deriven de la relació contractual entre empleat i ocupador.

L'empresa contractista vetllarà especialment perquè els treballadors adscrits a l'execució del contracte desenvolupin la seva activitat sense extralimitar-se en les funcions desempenyorades respecte de l'activitat delimitada en els plecs com a objecte del contracte.

L'empresa contractista prestarà el servei des de les seves dependències, havent de personar-se a l'Ajuntament per a les reunions que es convoquin i tantes vegades com es consideri convenient a fi i efecte de no obstaculitzar el bon servei a prestar.

L'empresa contractista haurà de designar, al menys, un coordinador tècnic o responsable integrat en la seva pròpia plantilla, que tindrà entre les seves obligacions les següents:
- Actuar com a interlocutor de l'empresa contractista davant l'Administració, canalitzant, d'una banda, la comunicació entre aquella i el personal integrant de l'equip de treball adscrit al contracte i, d'una altra banda, de l'Administració, en tot el relatiu a les qüestions derivades de l'execució del contracte.
- Distribuir el treball entre el personal encarregat de l'execució del contracte, i impartir a aquests treballadors les ordres i instruccions de treball que siguin necessàries en relació amb la prestació del servei contractat.
- Supervisar el correcte compliment per part del personal integrant de l'equip de treball de les funcions que té encomanades.
- Organitzar el règim de vacances del personal adscrit a l'execució del contracte, havent de coordinar-se adequadament l'empresa contractista com l'Administració contractant, per no alterar el bon funcionament del servei.
- Informar a l'Administració sobre les variacions, ocasionals o permanents, en la composició de l'equip de treball adscrit a l'execució del contracte.

15. RÈGIM SANCIONADOR

Les **infraccions** que cometi el contractista en l'execució del servei es classifiquen en molt greus, greus i lleus.

Es classificaran o es consideraran infraccions molt greus:

a) Prestar negligentment el servei.
b) Incompliment, molt greu del termini de prestació del servei, segons l'establert en aquest Plec.

c) No prestar el servei amb la continuïtat i regularitat exigida en el contracte, que impliqui unes conseqüències molt greus.
d) En cas d'extinció del contracte per part de l'adjudicatari, no prestar el servei fins que un altre adjudicatari es faci càrrec de la seva gestió.
e) No trobar-se al corrent en el pagament de l'assegurança requerida en aquest Plec.
f) No sufragar les següents despeses:
- Les de caràcter tributari que es desprenguin de l'activitat desenvolupada.
- Les que origini la contractació del personal necessari per a la correcta gestió del servei.
g) No complir totes les disposicions vigents en matèria fiscal, laboral, de Seguretat Social i de Seguretat i higiene en el treball.
h) No indemnitzar els danys que es causin a tercers com a conseqüència de les operacions que requereixi el desenvolupament del servei.
i) Cedir, subcontractar o traspassar totalment o parcial els serveis, sense autorització expressa de l'òrgan competent de l'Ajuntament d'Igualada.
j) Cessar en la prestació del servei pel contractista, sense la concurrència de les circumstàncies legals que la facin legítima.
k) La reiteració de faltes greus.
l) Les altres previstes en aquest plec.

Tindran la consideració d'infraccions greus :

a) Incomplir de forma greu el calendari de prestació del servei, segons l'establert en aquest Plec.
b) No coordinar-se amb el Servei d'Organització i Tecnologies de la Informació de l'Ajuntament.
c) No prestar el servei amb la continuïtat i regularitat exigida en el contracte, que impliqui conseqüències greus.
d) No informar a l'Ajuntament sobre la prestació del servei.
e) No presentar la documentació requerida, dins dels terminis establerts en aquest Plec.
f) No complir les ordres i instrucció donades per l'Ajuntament.
g) Obstaculitzar la fiscalització de la gestió per part de l'Ajuntament.
h) L'incompliment d'acords o decisions municipals sobre variacions de detall dels serveis que no impliquin despeses per al contractista.
i) Les irregularitats inadmissibles en la prestació dels serveis d'acord amb les condicions fixades en el present plec.
j) L'ocultació o falsejament exprés de la informació.
k) L'incompliment de les obligacions de l'ús de la llengua catalana.
l) La reiteració en la comissió de faltes lleus.

Tindran la consideració d'infraccions lleus:

Totes les altres no previstes anteriorment i que infringeixin d'alguna manera les condicions establertes en aquest plec de condicions i sempre en perjudici lleu del servei.

Les **sancions** que podrà imposar l'Ajuntament al contractista seran les següents:

- Les infraccions lleus es sancionaran amb la imposició d'una multa de 60 a 300 €.
- Les infraccions greus es sancionaran amb la imposició d'una multa de 300 a 900 €.

La comissió de tres infraccions greus podrà ser sancionada amb la rescissió del contracte, incautació de la fiança i indemnització de danys i perjudicis, en el seu cas.

- Les infraccions molt greus es sancionaran amb la imposició d'una multa de 900 a 1.300 €.

La realització de dues infraccions molt greus podrà ser sancionada amb la rescissió del contracte, incautació de la fiança i indemnització de danys i perjudicis, en el seu cas. Alhora, en el seu cas, el contractista procedirà a la indemnització de danys i perjudicis.

La imposició de sancions requerirà la incoació de l'oportú expedient.

En l'esmentat expedient es donarà audiència al contractista, es practicarà la informació i prova necessària a la justificació dels fets i s'observaran les garanties jurídicoadministratives prescrites en la normativa reguladora.

La resolució de l'expedient incumbeix a l'Alcalde.

L' import de les sancions econòmiques podrà ser descomptat del preu a percebre pel contractista o bé podrà carregar-se sobre la fiança constituïda. En aquest darrer cas, el contractista haurà de reposar l' import de la fiança en la seva totalitat, a requeriment de l'Alcaldia i en el termini que aquesta assenyali.

16. TRANSPARÈNCIA I ACCÉS A LA INFORMACIÓ PÚBLICA

De conformitat amb l'article 4 de la Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern i article 3.2 de la Llei 19/2014, de 29 de desembre, de transparència i accés a la informació pública i bon govern, l'Ajuntament podrà publicar o posar a disposició de qui la sol·liciti, tota la informació relativa a la present licitació, amb la única excepció de la informació tècnica aportada per les empreses licitadores que quedi coberta pel secret comercial.

L'Ajuntament d'Igualada podrà sol·licitar a l'empresa adjudicatària qualsevol informació relativa a l'objecte del contracte i les circumstàncies de la seva execució quan sigui d'interès pels ciutadans, havent l'empresa facilitar-la en un format apropiat i en el

termini màxim de deu dies, tret que del seu volum o complexitat es justifiqués la seva ampliació.

Si l'empresa considera que és aplicable alguna de les limitacions a la publicitat prevista en la normativa sobre la transparència i lliure accés a la informació i/o protecció de dades, podrà al·legar-ho davant l'òrgan competent en matèria de publicitat de la informació. Aquesta obligació subsistirà durant els dos anys posteriors a la finalització de les obligacions principals del contracte.

L'empresa adjudicatària haurà de proporcionar, al llarg de tot el període d'execució del contracte, la informació relativa a la prestació de serveis públics o a l'execució de potestats administratives delegades que l'Ajuntament consideri que ha de ser publicada d'acord amb el que disposa la normativa sobre transparència i lliure accés a la informació. La publicació a Internet serà realitzada per l'Ajuntament a través del portal de transparència.

Els formats a utilitzar per la publicació i/o comunicació de les dades serà en paper i format PDF (suports físics digitals: CD, DVD, memòria USB), havent-se de coordinar l'adjudicatari amb el servei responsable del Portal de transparència per a determinar i concretar l'estructura de les dades i la implementació i engegada dels mecanismes tècnics que resultin precisos.

L'incompliment de la normativa sobre transparència és sancionarà de conformitat amb l'esmentada normativa.

Signat,