PLEC DE PRESCRIPCIONS TÈCNIQUES PER A LA CONTRACTACIÓ DELS SERVEIS D'OPERACIÓ DE SEGURETAT (SOC) PER LA PREVENCIÓ, DETECCIÓ I RESPOSTA D'INCIDENTS I DELS SERVEIS INFORMÀTICS DE LES OFICINES DE SERVEIS AVANÇATS DE TELECOMUNICACIONS (OSAT) DE L'AJUNTAMENT DE BARCELONA, AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE

ÍNDEX

1. INTRODUCCIÓ

L'Institut Municipal d'Informàtica (IMI) disposa d´un model de gestió de les tecnologies de la informació i les comunicacions (TIC) a l'Ajuntament de Barcelona.

Aquest model té com a objectiu principal proveir aquelles solucions que millorin l'eficiència tècnica, la seguretat TIC, la gestió administrativa de les contractacions i l'eficiència econòmica dels actuals serveis TIC amb l'objectiu final d'oferir un servei de màxima qualitat i seguretat al ciutadà i fer de Barcelona una ciutat innovadora.

El model TIC es vertebra en tres eixos:

- Modernització i consolidació tecnològica:
  - Incorporar el model de cloud computing, amb la creació d'un cloud privat i cloud públic per a l'Ajuntament de Barcelona
  - Aprofitar les millores tecnològiques, presents i futures, del mercat TIC.
- Eficiència i transformació del model de serveis TIC:
  - Obtenir més i millors prestacions per a l'Ajuntament de Barcelona amb els mateixos recursos econòmics
  - Dedicar els recursos humans de l'IMI a la prestació de serveis de valor afegit
  - Transformar la prestació de serveis cap a models basats en l'adquisició de la computació com un servei corrent.
- Gestió de la Seguretat:
  - Incrementar i millorar l'efectivitat dels Serveis de seguretat i telecomunicacions TIC
  - Dotar a l'Ajuntament d'una estructura que asseguri el compliment de la seguretat i la minimització dels riscos de Telecomunicacions i Seguretat TIC corporatius amb vigilància activa, reactiva i preventiva
  - Implantar Projectes tecnològics per donar resposta a les necessitats TIC en matèria de telecomunicacions, seguretat i protecció.

Els **serveis Avançats de Telecomunicacions (OSAT**) van néixer com a resposta a la necessitat de millorar les capacitats tècnic-operatives de la xarxa i assegurar la governança i la seguretat operativa fent ús del nucli de l'arquitectura amb els següents eixos motivadors:

GARANTIA DE QUALITAT
Estableix i implementa polítiques clares d'interconnexió i seguretat en les comunicacions

INNOVACIÓ
Permet fer un salt endavant en el servei mitjançant projectes de transformació tecnològica

RETENCIÓ DE CONEIXEMENT
Assegura el coneixement mitjançant la estandardització de la documentació i dels processos

ROBUSTESA
Assegura la continuïtat del servei mitjançant la redundància i modularitat de la infraestructura

VALOR AFEGIT
Permet focalitzar l'organització de l'IMI en tasques de més valor afegit en la gestió TIC

TRANSVERSALITAT
Trenca amb els models verticals centralitzant funcions de comunicacions i seguretat

El context actual en matèria de **Ciberseguretat** resulta cada vegada més complex. En un entorn en què la mobilitat i, en conseqüència, els serveis en cloud i el nivell d'exposició dels serveis interns és creixent, el nivell de complexitat de la xarxa de telecomunicacions i de risc conseqüent augmenta amb una proporció exponencial. Per la seva banda, les xarxes criminals són cada vegada més especialitzades i tendeixen a dirigir i elaborar cada vegada més els seus atacs.

En aquest marc i context, esdevé fonamental orquestrar un disseny i desenvolupament de projectes i serveis de telecomunicacions i seguretat amb un Model de Gestió integrat, de cara a millorar les capacitats ja disponibles i incorporar noves capacitats i funcionalitats que permetin fer front a la situació actual.

2. OBJECTE

El present contracte té per objecte el **servei especialitzat de seguretat i telecomunicacions** que ens haurà de proporcionar el servei d'implantació, adaptació, gestió, suport i evolució tècnica de la **infraestructura tecnològica del** nus de comunicacions, dels elements de xarxa i dels CPDs nucli, així com el manteniment de l'equipament amb garanties esteses de fabricant, juntament amb la **prevenció, monitorització d'esdeveniments i gestió d'incidents de seguretat** emprant les eines que disposa l'IMI de SIEM (Security Information and Event Management) corporatiu (QRADAR) i de logs centralitzats ELK (*Elastic Search amb Llicenciament*), amb l'abast dels sistemes d'informació i serveis TIC de l'Ajuntament de Barcelona i amb les

capacitats tecnològiques i volumetries que s'indiquen en aquest plec de prescripcions tècniques.

Això inclourà:

- Disposar de vigilància activa, preventiva i reactiva enfront a intrusions i incidents en els serveis i la xarxa del nus, incloent:
    - Serveis de navegació
    - Serveis de connexió de col•laboradors externs
    - Serveis de comunicacions de sistemes d'informació
    - Serveis de connectivitat remota
    - Serveis de Wireless
    - Serveis de gestió d'adreçament IP Públic i Privat
    - Serveis de Seguretat perimetral
    - Serveis de generació de certificats
    - Serveis de control d'accés a la xarxa corporativa
- Disposar d'un servei de monitorització del nus i d'esdeveniments en temps real de la seguretat 24x7, vigilància i detecció.
- Administrar i monitoritzar tota la plataforma tecnològica així com la resolució de peticions, incidències i problemes per tal de proveir la màxima disponibilitat dels serveis.
- El subministrament de maquinari per renovar el nus de comunicació i evitar l'obsolescència.
- Eines de vigilància de la seguretat.
- Serveis de consultoria orientats al desenvolupament de projectes de transformació de telecomunicacions.
- Suport a l'execució dels projectes del Nus OSAT, nous projectes relacionats amb la infraestructura tecnològica de l'Ajuntament de Barcelona i d'altres relacionats.
- Serveis especialitzats de seguretat per a la prevenció, monitorització d'esdeveniments i gestió d'incidents de seguretat emprant les eines que disposa l'IMI de SIEM (Security Information and Event Management) i de logs centralitzats.

- Serveis d'anàlisi i gestió de vulnerabilitats, per a l'anàlisi de vulnerabilitats dels sistemes d'informació i infraestructures TIC, incloent Hackings ètics.
- Servei de Ciberintel.ligència:
    - Detecció primerenca d'incidents, amenaces i alerta digital.
    - Serveis especialitzats d'anàlisi i resposta d'incidents per l'avaluació d'impacte i gestió de i comunicació d'incidents (s'activa sota demanda).
- Disseny, administració i operació dels processos, tecnologies i eines pròpies del SOC.
- Serveis govern del SOC per la definició de indicadors i quadres de comandament i gestió del coneixement.
- Generació dels procediments de seguretat necessaris pel bon funcionament del servei.

Aquests serveis objecte d'aquest contracte ens hauran de permetre:

- Millorar les capacitats tècnic-operatives
- Assegurar uns processos transparents i una gestió més àgil, implantant nous processos i mantenint actualitzada la documentació
- Realitzar el desenvolupament i posterior manteniment dels nous serveis que es puguin desenvolupar
- Plantejar l'execució dels nous projectes en base a una estratègia conjunta telco-seguretat
- Acomplir els acords de nivell de servei del catàleg dels serveis gestionats
- Implantar els processos de millora contínua durant la fase d'execució del contracte
- Permetre una consolidació de funcionament per serveis en base als indicadors associats
- Garantir que les solucions a nivell de telco-seguretat compleixen unes directrius mínimes, respectant la governança del servei.
- Millorar el temps d'implantació final d'un servei
- Permetre una visió transversal i independent dels serveis: dissenyar i mantenir el catàleg de serveis del nus, gestionar el servei en base a ITIL
- Donar suport a la transició d'altres contractes de l'organització

- Tenir capacitat crítica enfront solucions i problemes complexos multi proveïdor
- Suport a altres serveis que requereixin del Nus OSAT
- Suport a canvis, peticions i projectes relacionats amb els equips de xarxa de l'Ajuntament (migracions, desplegament de nous equips, baixes, trasllats, canvis de tipologia i altres modificacions requerides per projectes de tercers)
- Generació de tota la documentació necessària, documentació operativa i de negoci.
- Suport a la transformació actual i futura que l'IMI realitzi de manera progressiva als *clouds*, ja siguin privats o públics
- Detecció IOCs (Indicators of compromise), implantar-los al SIEM i monitoritzar i traçar els IOCs implementats en eines de Telecomunicacions (FW, Proxy, IPS/IDS...)
- Definir i posar en marxa una metodologia d'integració i filtratge de noves fonts per gestionar l'impacte inicial dels falsos positius, excés d'alertes, etc. que garanteixi l'entrada racional de les alertes al serveis de Monitorització
- Proporcionar els Indicadors de Seguretat sobre aquest servei de Monitorització i Gestió d'incidents al Departament de Seguretat per la millora continua del servei. S'han de poder personalitzar i ser flexibles
- Alimentar el Quadre de Comandament de Seguretat Corporatiu que està implementant el Servei de GRC. Sempre que sigui possible aquesta alimentació es realitzarà de forma automatitzada. Els indicadors de Seguretat es publicaran sempre des del departament de Seguretat/Direcció i Comitè de Seguretat de L'IMI, taules de coordinació de l'Ajuntament
- Elaborar i lliurar els Informes de Servei. Seguiment del Servei d'aquest mateix plec
- Suport tècnic de sistemes per a la monitorització, administració i operació de les plataformes SIEM, Logs Centralitzats i eines d'escaneig de vulnerabilitats
- Gestió de la capacitat (requeriments de adquisició de mes capacitats, control i optimització dels EPS (esdeveniments per segon) i de fonts integrades amb els logs centralitzats, control del consum i outliers i comportaments anòmals dels EPS

3. ABAST

L'abast dels serveis inclou tots els sistemes d'informació, serveis TIC i components de l'Ajuntament de Barcelona gestionats per l'IMI. Això inclou serveis en el cloud públic i en clouds privats.

Concretament, l'abast del contracte inclou tots els serveis TIC de l'Ajuntament de Barcelona i del grup municipal classificats i gestionats per l'IMI, incloent tota la infraestructura que dóna suport als mateixos, tant si estan ubicats a l'IMI com si estan sota contractes de serveis externs realitzats per l'IMI basats en cloud. El serveis TIC inclouen tant els sistemes d'informació com les solucions de treball del personal corporatiu com són les estacions de treball, dispositius de mobilitat, correu corporatiu, eines de col·laboració, gestors documentals, etc.

També forma part de l'abast d'aquest contracte, el suport de consultoria puntual a l'Ajuntament en matèria de seguretat TIC de sistemes no gestionats per l'IMI, per tal d'assessorar i donar suport de consultoria en front incidents o vulnerabilitats crítiques a ens municipals no gestionats per l'IMI però que formen part del grup municipal i que puguin constituir-se en un futur en una Taula de Ciberseguretat en l'Ajuntament de Barcelona. En concret aquestes consultories seran puntuals i es sol·licitaran des del departament de Seguretat de l'IMI sobre alertes de ciberseguretat, vulnerabilitats incipients, alerta temprana o o-Days que puguin exposar a la xarxa corporativa de l'Ajuntament des de altres entitats corporatives amb l'objectiu de minimitzar riscos d'exposició de la xarxa corporativa.

Actualment, l'IMI està immers en la revisió i evolució dels processos operatius i de gestió dels serveis, en especial aquells basats en "cloud". Aquesta revisió està tenint com a resultat la redefinició del conjunt de processos d'aquest nou model. En els propers dos anys es realitzaran canvis progressius orientats a implantar un model de serveis evolucionat i, el contracte derivat d'aquest plec no n'estarà al marge.

Al respecte d'això, cal tenir en compte que:

- L'IMI és en tot moment responsable del disseny dels processos relatius als serveis TIC que proporciona.
- L'IMI facilitarà les eines bàsiques de suport a l'operativa i la gestió dels serveis.
- L'adjudicatari del present contracte serà responsable de la implantació de les diferents versions del model de l'IMI que es vagin consensuant, en el conjunt dels seus equips i en el seu àmbit de servei.
- L'adjudicatari acceptarà tenir una actitud oberta vers aquesta evolució i participarà en la mateixa, proporcionant la realimentació oportuna, alhora que aportant solucions a problemes i riscos identificats.

Les tasques que s'hauran de desenvolupar durant el contracte són les que s'especifiquen en la descripció dels serveis que es recull en l'apartat 4 d'aquest plec.

4. DESCRIPCIÓ DELS SERVEIS

Als apartats següents s'expliquen de forma més detallada cadascun d'aquests grup de serveis.

4.1. SERVEIS SOC

4.1.1. SERVEI DE PREVENTIU

L'objectiu del servei de preventiu és la detecció i gestió de vulnerabilitats. Això suposa realitzar una gestió completa del cicle de vida de les vulnerabilitats i posterior revisió e què els serveis implementin les accions correctores amb la finalitat de garantir que les infraestructures o serveis siguin segurs. Les vulnerabilitats es detecten per múltiples fonts (com són fonts de ciberintel·ligència, proves d'intrusió d'infraestructures i serveis, alertes de seguretat que impliquen a inventari infraestructures corporatives, alerta temprana, etc.).

L'adjudicatari assolirà aquest objectiu identificant de forma anticipada les vulnerabilitats presents en els sistemes d'informació inclosos a l'abast, fent-ne el seguiment i donant suport als equips interns i de serveis de l'IMI implicats fins a la resolució de les mateixes.

El servei de Preventiu s'iniciarà durant la transició de servei del contracte de Preventiu vigent amb codi 19000130 que finalitzarà el 02/06/2022. Aquest període de transició i transferència de coneixement tindrà una durada mínima, màxima i requeriments d'acord amb l'apartat 5.FASES DE LA PESTACIÓ DEL SERVEI del present plec.

L'adjudicatari ha d'executar les següents tasques:

4.1.1.1. Gestió de vulnerabilitats

L'adjudicatari ha de gestionar el cicle de vida de les vulnerabilitats que es detectin, comunicades per fonts externes (ja siguin des del servei d'alerta primerenca d'amenaces emergents o d'avisos de vulnerabilitats tecnològiques comunicades o 0-days) o per escanejos de vulnerabilitats que es realitzen internament aplicables a la infraestructura i serveis corporatius.

El servei ha de donar resposta a les necessitats de prevenir la seguretat de la infraestructura corporativa, i això inclou infraestructura on-premise o de clouds privats o serveis en clouds públics gestionats per l'IMI.

Això implica:

- Priorització
- El seguiment de les vulnerabilitats i suport durant la resolució als equips de l'Ajuntament responsables de la correcció de les mateixes (Serveis, Operació de Sistemes i Suports Tècnics Operatius):
  - Trasllat als equips tècnics encarregats de la remediació

  - Vetllar per la planificació de la remediació
  - Suport durant la remediació
  - Comprovar la correcta remediació
- Reporting executiu de la situació de les vulnerabilitats
- Realització de propostes d'evolució i adaptació del servei per donar cobertura a les amenaces emergents i vulnerabilitats atòpiques.

El servei s'ha de dur a terme amb la màxima qualitat. Per això durà a terme les tasques que s'indiquen a continuació:

- Assegurar que no es proporcionin falsos positius, amb verificacions manuals.
- Garantir que no hi hagi entrades repetides i, en tots els casos, s'haurà d'executar un procediment per assegurar-se que les vulnerabilitats que es presentaran als responsables de seguretat de l'IMI estaran filtrades i lliures de falsos positius i repeticions.
- Re-certificació de vulnerabilitats per a l'assegurament de la seva resolució.
- Realització informes mensuals per Direcció destinats sobre el nivell d'exposició dels sistemes d'informació de l'Ajuntament davant d'atacs.

Les fonts d'entrades de les vulnerabilitats seran múltiples: les derivades dels Serveis de ciberintel·ligència, dels CERTs que reporten vulnerabilitats a Ajuntament (CESICAT, CCN-CERT,..), de les auditories tècniques, publicades pels diferents fabricants dels productes, de les detectades degut a incidents de seguretat reportats, escanejos de vulnerabilitats d'aquest contracte o internes IMI, així com també vulnerabilitats que es detectin fora del contracte i que es reportin al servei.

En aquest apartat cal remarcar que el model de contractació per serveis TIC corporatius implica que hi pot haver disseminació de proveïdors gestionant i administrat la tecnologia de plataformes de sistemes d'informació corporatius i de serveis verticals. Cada contracte tindrà un referent corporatiu. Amb això, la gestió de vulnerabilitats ha de contemplar la complexitat de contractes que gestionaran la infraestructura i serveis.

El servei de gestió de vulnerabilitats haurà de coordinar-se amb els serveis operatius dels diferents contractes de gestió de infraestructures i programaris o serveis de suport tècnic, d'administració i operació de sistemes informació per tal d'automatitzar i industrialitzar al màxim els processos de detecció i correcció de la vulnerabilitat. Amb això crearà un grup de treball amb els equips adients de l'IMI per avaluar tecnologies, automatismes i procediments per aconseguir aquesta industrialització.

El gestor de vulnerabilitats dins del marc de la industrialització del servei haurà de proposar processos i impulsar i coordinar la implementació de millora que redueixin els costos i facin més eficient i eficaç la reducció de riscos de l'exposició de les

vulnerabilitats. Es definirà un pla de millores continua anualment i trimestralment proporcionarà els avenços planificats.

Per la maduració i la industrialització dels serveis, qualsevol servei, subservei o procés del contracte ha de ser susceptible de ser industrialitzat. És a dir, en el procés de disseny i desplegament ha de tenir-se en compte aquest objectiu, per la qual cosa haurà de seguir els criteris d'eficiència i eficàcia en recursos, eines i sinergies amb la resta de processos. Evitant processos que consumeixin grans esforços de recursos o que no reverteixin en millores significatives.

El licitador haurà de plantejar en la descripció del serveis el model d'industrialització proposat i el seu pla de desplegament.

El servei és auto-contingut en el sentit que ha realitzar les tasques relacionades amb la gestió de vulnerabilitats **de forma activa i proactiva**, i això implica que haurà liderar, coordinar i gestionar la implementació de processos i eines en els entorns operatius amb l'equip responsable dels serveis productius corresponents (SAU, lloc de treball, CPD, Telecomunicacions, etc.) on es requereixin gestionar vulnerabilitats tant als sistemes existents com quan apareguin noves necessitats d'escanejos en noves tecnologies o entorns.

El licitador ha d'incloure sense cost addicional eines i les llicències d'ús de les eines necessàries per a l'execució de les tasques del servei de preventiu. Els licitadors indicaran a l'oferta les eines que proposen emprar per la Gestió de vulnerabilitats, considerant dins del cost del contracte tota despesa derivada (llicències, manteniments, actualitzacions, etc.) sense cost addicional per l'IMI.

En alguns contractes d'operació i infraestructures de l'IMI s'exigeixen escanejos i gestió de vulnerabilitats de les infraestructures que operen: Serveis de CPD i de Sistemes, contractes de Clouds per temes específics com pot ser webs corporatives. L'adjudicatari haurà de implementar la gestió de vulnerabilitats podent aprofitar sinergies d'aquests contractes però en qualsevol cas ha de garantir la gestió de vulnerabilitats global corporativa.

Com a mínim, es considera necessària la provisió de les següents eines:

- Eina d'escaneig de vulnerabilitats.
- Eina de gestió de vulnerabilitats.

Una eina o solució d'escaneig de vulnerabilitats que compleixi amb els següents requisits:

- Efectivitat dels escanejos de vulnerabilitats: Justificar la seva efectivitat sobre quins requisits compleix, per exemple si pot ser considerada Approved Scanning Vendors (ASV) del PCI Data Security Standard, o la

certificació FedRAMP certification, o altres certificacions equivalents que siguin garants de un bon servei preventiu.

- Un repositori únic en què abocar les vulnerabilitats detectades com a resultats dels diferents tests de seguretat que es realitzin sobre els sistemes de l'Ajuntament que permeti:
    - Categoritzar les vulnerabilitats en funció de criteris de valoració estàndard CVSS2 i CVSS3.
    - Importa de manera automàtica i mitjançant una interfície API els resultats de diferents eines d'escanejos de vulnerabilitats.
    - L'exportació en format .csv de la base de dades d'actius i de les vulnerabilitats perquè els equips de l'Ajuntament puguin tractar aquesta informació de manera més àgil o distribuïda.
    - Realitzar recerques d'actius afectats per una vulnerabilitat concreta.

- Faciliti indicadors i seguiment de la gestió de les vulnerabilitats, planificació dels treballs i resum del nivell d'exposició de l'organització davant d'atacs, que permeti:
    - Una gestió del risc que possibiliti establir diferents terminis de resolució en funció de la criticitat dels actius i de les vulnerabilitats associades.
    - Modificar manualment el nivell de risc d'un actiu.
    - Elaborar gràfics configurables i quadre de comandament.
    - Mostrar una evolució de la seguretat al llarg del temps.
    - Proporcionar en qualsevol moment una visió actualitzada general de seguretat.
- Disposar d'una interfície web accessible per a l'Ajuntament, que ha de permetre la gestió eficaç.
- El control d'actius que permeti, entre d'altres:
    - Identificar els actius pel seu nom i assignar-los un nivell de criticitat per a la companyia.
    - Etiquetar els actius amb tantes etiquetes com sigui necessari.
    - Agrupar els actius per unitats organitzatives.
    - Designar un responsable per cada actiu.
    - Realitzar recerques dins de l'inventari d'actius per diferents criteris.

- Incorporar de manera automàtica nous actius que es donin d'alta en l'organització.

L'IMI disposa d'una CMDB i el servei pot emprar o implementar certes funcionalitats en la CMDB o integrar-se amb la CMDB de l'IMI, sempre i quant això ofereixi els serveis requerits en el punt anterior.

Es valoraran les propostes d'eines o serveis addicionals a les indicades en el paràgraf anterior que millorin l'eficàcia del servei de gestió de vulnerabilitats.

Gestió de Vulnerabilitats de les imatges Dockers

L'IMI a la seva infraestructura disposa de contenidors amb imatges dockers i una *pipeline* de DEVSECOPS, on hi ha eines per la revisió de la seguretat dels codis que produeix (OWASP, anàlisi imatges dockers,..).

El servei de preventiu haurà de:

- Proporcionar suport puntual al equip de DEVSECOPS sobre les vulnerabilitats complexes que emergeixin.
- Identificar i gestionar les vulnerabilitats del contenidors productius i de les imatges Dockers productives.
- Ingestar les alertes de notificació de les eines d'escaneig al sistema de *ticketing* corporatiu de l'IMI.

4.1.1.2. Auditories tècniques de seguretat i hacking ètic

L'adjudicatari del servei s'encarregarà de la planificació, gestió i execució d'escanejos de vulnerabilitats i proves de seguretat necessàries per identificar possibles vulnerabilitats i debilitats existents en els sistemes d'informació de l'Ajuntament. La tipologia de proves d'aquest servei de detecció de possibles vulnerabilitats que es contemplen són:

- Escanejos periòdics de vulnerabilitats: Escanejos periòdics de vulnerabilitats sobre 800 IPs públiques i 600 Ips internes.
- Auditories Tècniques de seguretat.
  - Test Intrusió extern/Intern – caixa negra. Caixa negra i blanca.
  - Auditories de Sistemes: configuració, arquitectura de sistemes i el seu bastionat de Wifi, sensors, firewall, IPs, proxies i elements de comunicacions etc.
  - Auditories a aplicatius/serveis: aplicacions, aplicacions web, productes i aplicacions mòbils.

L'adjudicatari del servei haurà d'establir un pla d'auditories tècniques d'ofici per a la detecció de vulnerabilitats a les infraestructures corporatives *on-premise* o al núvol, en

el que, com a mínim, s'inclouran les auditories indicades a continuació amb l'esforç que es detalla mes endavant per a cada una d'elles:

Servei d'Escanejos periòdics de vulnerabilitats	Freqüència
Escanejos de vulnerabilitats sobre 800 IPs públiques	2 per any
Escanejos de vulnerabilitats sobre 600 IPs internes de servidors	6 per any
Escanejos de maquetes dels lloc de treball (4 maquetes)	6 per any
Descobriment de la xarxa i identificació d'elements anòmals	2 per any

El proveïdor haurà de disposar d'eines/serveis per a realitzar aquests escanejos.

Es valoraran les propostes dels licitadors que millorin el nombre la freqüència de la volumetria anterior.

Volumetria d'auditories tècniques	Quantitat
Test Intrusió extern/Intern – Caixa negra - Hacking ètic per IP (30 IPs diferents i no necessàriament agrupades i al mateix moment)	40 anuals
Auditoria tècnica de sistemes i configuracions de dispositius de seguretat: DNS, IPS i proxies corporatius (elements de comunicacions), wifis, End Point (EDR si fos el cas), MDM, SIEM, WAF, NGFW, AntiSpam, IDS, Serveis IOT, NAC, etc.	3 anuals
Auditoria d'aplicatius web/Serveis: aplicatius web, apps mòbils, productes (Serveis), de complexitat mitjana	3 anuals

En principi es consideraran auditories de nivell mig de complexitat, amb un valor aproximat de 70 hores cadascuna. Si la planificació requereix auditories de nivell BAIX de complexitat (35 hores aprox.) es repercutiran en dues auditories en lloc d'una. D'igual manera es repercutirà proporcionalment si l'auditoria que es requereix és de complexitat ALTA (140 hores).

Es valoraran les propostes dels licitadors que millorin el nombre mínim d'auditories a realitzar anualment.

El licitador haurà de definir el pla d'auditories tècniques de seguretat del contracte, proposant les auditories en base a riscs de seguretat de les infraestructures TIC i prioritats d'Ajuntament, per anualitats però amb visió global del servei de tot el contracte.

Es valoraran les propostes dels licitadors que facin un pla d'auditories amb millor detall de recursos, activitats i calendarització. En cas de millora oferta per part de l'adjudicatari, serà aquesta la que prevaldrà.

Per reduir els costos de realització d'aquestes auditories tècniques i serveis de hacking es contempla que el licitador pugui emprar els seus serveis regulars de l'empresa

d'execució d'auditories tècniques o també a executar-les comptant parcial o totalment (depenent de l'experiència del perfil) amb el personal dedicat al contracte per la gestió de vulnerabilitats, sempre i quan el perfil tingui les capacitats tècniques exigides al contracte per a la realització d'aquestes tasques.

Formen part d'aquest servei també tasques de detecció o investigació i/o revisió de vulnerabilitats de defectes de disseny de les arquitectures de xarxes, sistemes o desenvolupaments.

En qualsevol cas, la gestió de les vulnerabilitats detectades sempre es realitzarà a través del servei de gestió de vulnerabilitats.

4.1.1.3. Servei de Ciberintel·ligència

L'objectiu de la ciberintel·ligència és ajudar els equips interns de l'IMI a anticipar la detecció de potencials amenaces i amenaces emergents contra l'organització municipal amb l'objectiu de poder prendre mesures que protegeixin per tal d'evitar i prevenir incidents de ciberseguretat sobre els sistemes d'informació de l'Ajuntament. Amb aquest objectiu, l'adjudicatari ha d'executar les següents tasques:

- **Vigilància d'amenaces**. La preparació i planificació de ciberatacs contra una organització pot deixar algun rastre a la internet superficial, la Deep web i també a xarxes socials, fòrums, xats d'accés restringit i mercats negres. Disposar d'aquesta informació pot permetre que l'IMI anticipi la realització d'accions orientades a protegir-se davant els mateixos. Els objectius del servei de vigilància de amenaces són:
  - La detecció, eliminació i control de la divulgació de la informació que es pot utilitzar per a l'elaboració i posada en marxa de ciberatacs contra la infraestructura d'IT corporativa.
  - La monitorització de les activitats dels grups hacktivistes.
  - La detecció de la participació d'actius d'IT corporatius en activitats fraudulentes.
  - La detecció de planificació d'atacs tipus DDoS contra els sistemes de l'organització.
  - La detecció, monitorització i tancament de llocs relacionats amb campanyes de malware dirigides contra l'organització. Cerca d'informació sensible de l'Ajuntament a la *Deep web*, xarxes , fòrums, etc.

- **Alerta d'amenaces emergents**. Es demana la monitorització, detecció primerenca d'alertes de seguretat i notificació d'amenaces emergents fora l'Ajuntament (fuites

d'informació de l'Ajuntament, atacs DDoS, activisme i hacktivisme, vulneració de mecanismes de seguretat, conductes perilloses, suplantacions d'identitat, robatori de credencials, espionatge, monitorització d'amenaces a la Darknet, pastebin, social media, xats, altres fòrums) des de diferents fonts de confiança: Organismes de resposta a Incidents CSIRT o CERTs, serveis especialitzats en avisos de seguretat (públics i privats), fabricants o proveïdors de seguretat, xarxes socials, etc.

Es demana alhora la notificació ràpida d'amenaces publicades a Internet que de forma genèrica poden afectar a l'Ajuntament. El servei està orientat a campanyes globals en principi no associades a un producte concret.

• **Alerta primerenca de riscos d'infraestructura** mitjançant la notificació al servei de Preventiu via *ticketing* corporatiu de vulnerabilitats conegudes relacionades amb el programari i maquinari identificats en el conjunt d'actius i sistemes de l'Ajuntament. Es demana la notificació de vulnerabilitats que s'emeten del programari de tercers que tenim com actius en les instal·lacions municipals amb l'objectiu d'informar de les vulnerabilitats que es vagin publicant, en especial els de tipus 0-day.

Contempla notificacions dels últims pegats de Seguretat publicats així com les possibles i respectives solucions, butlletins de seguretat: CVE i CVSS amb pegats associats que solucionen, avisos de seguretat d'últimes vulnerabilitats descobertes, etc.

• **Recuperació d'informació**. La informació privada corporativa es pot trobar a Internet en llocs que no estan autoritzats per al seu coneixement i difusió. Aquests llocs poden pertànyer a la web superficial, a la xarxa profunda i també a xarxes criminals d'accés restringit i mercats negres. Els objectius del servei de recuperació d'informació són:

- La detecció, eliminació i control dels enllaços de descàrrega d'informació corporativa disponible en servidors no corporatius.
- La detecció i informe de les credencials d'accés d'actius corporatius.

• **Vigilància de marca.** La identitat digital de l'Ajuntament pot ser suplantada per terceres parts malicioses amb l'objectiu de realitzar activitats fraudulentes, aprofitant la imatge de l'Ajuntament per guanyar credibilitat. Els objectius del servei de vigilància de marca són:

- La detecció, eliminació i monitorització de contingut genèric fraudulent que fan ús de la marca corporativa (clic-frau, malware genèric, ofertes de treball i promocions falses, etc.).
- La detecció, eliminació i monitorització de campanyes de fraus específics que fan ús de la marca corporativa (depenent de la indústria).

- La vigilància de les activitats de registre de noms de domini amb l'objectiu de detectar la suplantació de l'organització a Internet.
- La vigilància de les activitats de creació de perfils en les xarxes socials més populars amb l'objectiu de detectar perfils falsos i no oficials.

El servei realitzarà la monitorització, detecció i alerta precoç de riscos de marca: evolució, ús no autoritzat de marca, usurpació de dominis, continguts fraudulents i control continu de detecció de desplaçament a les webs externes de l'Ajuntament.

El servei facilitarà una gestió completa del cicle de vida de les amenaces detectades, contemplant des de la recopilació i emmagatzematge centralitzat de les dades privades i públics obtinguts, el processament intel·ligent dels mateixos, la seva classificació i avaluació, la generació d'alertes i informes, fins les propostes per mitigació i / o eliminació de l'amenaça.

L'esforç contemplat per aquests serveis són:

1. **Servei de ciberintel·ligència** – valoració d'un servei de ciberintel·ligència orientat a protegir els següents actius:
    a. Protecció de marca - 1 marca
    b. Monitorització de Personal VIP – 10 persones
    c. Dominis Internet - El dominis principals que suposen el 90% de les visites, que estarien al voltant de 5.
    d. Perfils de xarxes socials – 12

    També realitzarà les remediacions de deteccions i alertes que correspongui actuar, considerant-se **que com màxim poden ser la meitat de les volumetries que necessitin actuacions de remediació.**

Volumetries servei ciberintel.ligència	**Quantitat**
Servei de ciberintel·ligència (amb meitat de remediacions)	30 assets i màxim 13 remediacions anuals.

Es valoraran positivament les propostes dels licitadors que millorin les volumetries mínimes requerides, en cas de millora per part de l'adjudicatari serà aquesta la que prevaldrà.

2. **Servei de monitorització de la publicació de vulnerabilitats associades a les tecnologies desplegades per l'IMI.**

    a. **Estimar la presència d'unes 100 tecnologies**

    S'entén que aquest apartat contempla la comunicació i reporting de les vulnerabilitats i suport, però queda fora la gestió del cicle de vida de les vulnerabilitats que es farà amb apartat corresponent de Gestió de vulnerabilitats d'aquest plec.

4.1.2. MONITORITZACIÓ I DETECCIÓ D'INCIDENTS

La volumetria prevista pel Servei de monitorització i detecció d'incidents és la següent:

Volumetries de Monitorització i reacció	**Quantitat**
Eps (esdeveniments per segon)	4.000 events per segon
Casos d'ús	40 casos d'ús inicials (migrats)
Increment de casos d'ús els següents anys	10 casos d'ús anuals.
Gestió d'alertes no crítiques mensual: 900. (es considera que en una ratio d'events / alertes de 1000 events per segon es gestionen 300 alertes mes.	1.200 mensuals
Gestió d'alertes crítiques: il.limitat.	Il·limitat

Els serveis que haurà de cobrir-se amb aquesta volumetria es detallen a continuació.

4.1.2.1. Monitorització de seguretat, detecció primerenca d'incidents i amenaces, i correlació d'esdeveniments en temps real

L'adjudicatari prestarà el servei de monitorització en modalitat 24x7x365 a través de la plataforma SIEM, suport i gestió de les alertes generades, incloent la integració amb la plataforma de ticketing de seguretat per a la gestió del cicle de vida d'alertes de seguretat i la gestió dels *playbooks* (pautes d'actuació de ciberseguretat adequats per actuar en les alertes i incidents detectats) , amb els següents requeriments:

- Centre de trucades operatiu 24x7x365 per a la notificació d'alertes i incidents.
- Monitorització 24x7x365 de la plataforma SIEM i generació d'alertes automàtiques.
- Gestió i creació de tiquets a la plataforma de *ticketing* corporatiu (no s'han de gestionar les alertes dins la plataforma SIEM) del Departament de Seguretat de l'IMI. Ha d'incloure tant les alertes de seguretat generades pel SIEM així com

les alertes i/o incidències rebudes pels altres canals que ha de proporcionar l'adjudicatari, es pot automatitzar el servei.

- El sistema de tiquets de l'adjudicatari caldrà integrar-lo amb el corporatiu que proposi el Departament de Seguretat de l'IMI. Aquest sistema ha de permetre entre d'altres conèixer en qualsevol moment el nombre de tiquets gestionats i el seu estat.
- Integrar-se i si cal fer la ingesta dels sistemes de registre i notificació d'incidents corporatius i amb la notificacions externes a què l'Ajuntament estigui subjecte per llei (ENS, RGPD) o que es considerin oportunes per *due diligence* per la cooperació a la gestió i detecció d'incidents amb altres organitzacions i CSIRT, com pot ser CESICAT o LUCIA CCN-CERT.
- Integració d'alertes i informació al servei de monitorització que es requereixi per detectar amenaces de fonts d'intel·ligència i del servei de gestió de vulnerabilitats pròpies del servei o fonts externes (públiques o privades), que es considerin necessàries per millorar la detecció i visibilitat de les amenaces externes que intenten atacar una vulnerabilitat.
- IOCs: En base a la informació d'intel·ligència propis de fabricant del SIEM, propis del SOC, i externes l'adjudicatari determinarà quins IOCs són necessaris incorporar a altres elements de la infraestructura i dispositius de protecció de l'organització. Es requereix una traçabilitat dels IOCs en aquests altres elements, que permeti conèixer quins IOCs s'afegeixen, s'eliminen o es modifiquen diàriament, així com el nombre d'IOCS desplegats en qualsevol moment.

4.1.2.2. Automatitzacions i orquestració

Enriquiment, orquestració i automatització de tasques que es disparen amb les alertes que activa el propi SOC amb les eines de detecció o incidents que es reben pel canal de ticketing IMI o telefònic. Enriquiment de informació associada al ticket a cada nivell d'escalat.

4.1.2.3. Disseny i creació de casos d'ús a mida compatibles amb les tecnologies del IMI

L'adjudicatari realitzarà **el modelat d'amenaces de seguretat** als que estan exposats els sistemes d'informació inclosos a l'abast d'aquest plec. El modelat d'amenaces és una tasca prèvia al disseny i creació de casos d'ús. Aquest modelat es farà d'acord amb les pautes i requeriments establerts per Seguretat de l'IMI. L'objectiu és analitzar el nivell de cobertura davant de diferents amenaces i què es necessita. D'aquest treball s'obtindrà un mapa d'amenaces, prenen com a referència el mapa de MITRE, que permetrà definir un roadmap d'acció amb l'abast de les necessitats específiques

orientat a millorar la cobertura proporcionada pel SIEM i els components tecnològics del client, enfront de l'exposició.

Es requereix de l'adjudicatari els serveis per al desplegament de casos d'ús tècnics, d'intel·ligència i de negoci adaptats a l'IMI, amb una planificació analitzada i que tingui en compte la revisió de l'estat de cobertura de la plataforma SIEM:

- Integració de casos d'ús de negoci i intel·ligència. Disseny i creació del cas d'ús a mida, mentre que els processos d'operacions de seguretat mantenen i executen els *playbooks*.
- El modelat de les amenaces el portem a terme implementant casos d'ús amb objectius de control específics. S'entén per cas d'ús el conjunt de tractaments o operacions que apliquem sobre un conjunt de logs que estan en el SIEM per poder complir amb un requisit específic.

Procediment i ajust de casos d'ús coneguts. Nous casos d'ús.

- Els casos d'ús poden tenir dos orígens:
  - **Peticions específiques per cobrir casos concrets de l'Ajuntament i l'IMI.**
  - **Propostes proactives de l'adjudicatari en base a la seva experiència.**
- Els casos d'ús tindran un procés d'implementació. Es considerarà que s'ha implementat un cas d'ús quan s'han realitzat les següents passos:
  - **Definició:** És l'activitat més crítica perquè és on es defineix quin és l'objectiu del Cas d'Ús. L'objectiu del Cas d'Ús ha de ser específic, a més d'estar clarament delimitat, per evitar falsos positius i errors en la implementació. Aquest procés es desenvolupa normalment en conjunt amb el client.
  - **Anàlisi:** Durant aquesta fase es preveu un estudi dels events generats per les tecnologies involucrades i permet conèixer la visibilitat que el SIEM pugui tenir o no pel que fa a l'abast definit.
  - **Desenvolupament:** En aquesta fase es procedeix al desenvolupament d'aquells continguts que millor puguin complir amb els objectius definits. Els continguts podran ser diferents en nombre i tipus, depenent del Cas d'Ús específic (regles de correlació, informes, *dashboard*, etc.).
  - **Optimització:** Un cop desenvolupat el cas d'ús és fonamental la seva optimització a través dels paràmetres i llindars que caracteritzen els continguts dels que està compost. Així mateix, un altre objectiu principal és reduir la freqüència de falsos positius per optimitzar l'operativitat associada al Cas d'Ús i, més generalment, la gestió de la seguretat. Un cop definit, cada Cas d'Ús serà implementat, provat (si fos possible) i documentat per crear un catàleg de Casos d'Ús, la propietat intel·lectual del qual pertany a l'IMI.

- **Operació:** L'operació del Cas d'Ús comença amb la posada en producció, la documentació, la definició dels processos a executar per part dels operadors del SOC, i els protocols de gestió de la incidència relacionada.

- Els casos d'ús quedaran documentats.
- Es considera que pot arribar a ser necessari configurar un cas d'ús setmanal. Es consideren que s'implementaran 40 casos d'ús anuals, actualment hi ha 30 casos d'ús en producció.

4.1.2.4. Identificació, detecció i categorització d'incidents.

En base a la monitorització i la recepció de les alertes el servei haurà d'identificar i analitzar el possible incident, determinar el seu abast i possible escalat. Per al tractament de la incidència es requereix:

- Recollida i anàlisi de logs.
- Detecció de falsos positius, abans de reportar a següent nivell d'escalat.
- Classificació i tipologia de l'incident. La classificació per tipologia de tots els tiquets gestionats serà d'acord amb la taxonomia estàndard MITRE i NIST.
- Anàlisi de situació i impacte (avaluació).
- Proposta de mesures correctives o de remediació, d'acord amb la criticitat.
- Documentació dels casos tractats.

Per a establir les categoritzacions i tipologies d'incidents prèviament el servei es coordinarà per ajustar-les amb el Servei de la Oficina de Govern, Risc i Compliment (GRC) del Departament de Seguretat de l'IMI.

4.1.2.5. Gestió i comunicació d'incidents. Notificació dels incidents i activitats sospitoses en temps real.

El Departament de Seguretat a través de l'Oficina de GRC manté el registre d'incidents formal de Seguretat de l'Ajuntament i gestiona el cos normatiu de Seguretat. A l'inici del contracte l'adjudicatari revisarà, proposarà, documentarà i implementarà en base a la seva experiència i amb les pautes i supervisió del Departament de Seguretat:

- Document del procediment de Gestió i escalat d'incidents de Seguretat. Actualment hi ha un document en treball.
- Els Plans de Resposta davant incidents, en base a criteris com criticitat, impacte i tipologia de l'incident. Els Plans de Resposta acordats, així com els procediments de gestió i escalat d'incidents, quedaran degudament documentats. Actualment hi ha un document en definició, dins el marc d'aquest plec, que s'haurà d'implementar conjuntament amb el Departament de Seguretat.

- El procediment específic i concret per la identificació i tractament d'incidents MOLT CRÏTICS o d'ALT RISC, amb abast de les tasques, delimitació de responsabilitats, activació del pla comunicació, coordinació de grups, documentació, etc.
- La notificació, gestió dels incidents i registre al "registre d'incidents de Seguretat de l'Ajuntament". Es troba implementat actualment a través de la plataforma Lucia del CCN-CERT.

Es requereix per a la gestió dels incidents:

- Registre i escalat del mateix si escau després de l'avaluació prèvia, atenent al Procediment de gestió i escalat d'incidents que s'acordi amb Seguretat de l'IMI.
- Integració amb els processos de gestió d'incidents de seguretat i TI de IMI: Hi haurà integració amb els models d'operació, eines de *ticketing* i SAU de l'IMI) per a la notificació i report de l'incident.
- S'entén que en la resposta als incidents, les accions proposades de remediació i resposta generalment s'implementaran a través de les àrees operatives de l'IMI i els contractes que aquestes tinguin en el seus serveis.
- En certs casos i si la remediació i contenció està clarament i prèviament identificada, l'adjudicatari realitzarà accions concretes de remediació i contenció. En aquests casos estaran acceptades i acordades pel Departament de Seguretat i s'actuarà sota un procediment.
- Hi haurà un procediment específic per la Gestió d'incidents MOLT CRÍTICS o s'ALT RISC, bàsicament són aquells que afecten als serveis municipals o serveis que dona l'IMI. Aquest procediment ha d'esser 24x7x365.

4.1.3. RESPOSTA A INCIDENTS MOLT CRÍTICS O D'ALT RISC (INCIDENT HANDLING)

Volumetries de Monitorització i reacció	**Quantitat**
Hores Incident Handler 24x7	100 hores anuals

L'adjudicatari prestarà el servei de resposta ràpida a incidents d'alta criticitat o d'alt risc (greus) mitjançant una borsa d'hores estimada de 100 hores anuals ampliables en cas que s'exhaureixin.

El proveïdor indicarà quins perfils contempla com repercutirà les hores en base als diferents perfils que pugui tenir de posar a disposició del servei, donat que no tos els perfils tenen el mateix cost. En aquest sentit, indicarà com comptabilitzarà aquests perfils en relació al consum de les hores d'incident Handler.

L'adjudicatari haurà de proposar un pla de resposta a incidents crítics incloent el protocol d'activació del servei i la fitxa de context de l'IMI.

El servei té els següents requeriments:

- Horaris d'atenció a incidències en format 24x7x365.
- Existència d'un equip específic per a l'atenció que no pot coincidir amb l'equip del SOC.
- Possibilitat d'escalar a perfils de més capacitat i/o expertesa.

Procediment

El procediment de gestió dels incidents crítics es basarà en les millors pràctiques del sector considerant diverses etapes (anàlisi > contenció > erradicació > recuperació). Algunes de les possibles activitats contemplades en cada etapa poden ser:

- Anàlisi: Circumstàncies de l'incident, identificar el tipus i gravetat de l'atac, entrega de la informació que permeti avaluar la sensibilitat d'informació fugada i la protecció de proves existents.
- Contenció: Amb activitats com desactivació de comptes d'usuari, canvis de contrasenya, bastionat de la xarxa o controls del host, desconnexió de sistemes o xarxes compromeses, assessorament en les mesures de mitigació, ús de regles de Firewall per bloquejar vectors d'atac entrants, ús de firewalls/proxies web per bloquejar accessos, ús d'eines de seguretat de la xarxa (IDS/IPS, Netflow...) per detectar comportaments anòmals.
- Erradicació: Execució d'scripts, confirmació de que l'antivirus de la xarxa i del host pot detectar i eliminar el codi maliciós, confirmar que el SO vulnerable està actualitzat o que incorpora el pegat, restauració del trànsit de la xarxa o sistemes afectats, continuació de l'activitat del sistema de logs, conscienciar als usuaris del estat del sistema compromès, assessorar a terceres parts en desenvolupaments que els puguin afectar.
- Recuperació: Recuperació de les plataformes i serveis compromesos, descripció general, lliçons apresses, resum de l'incident, enfoc i cronologia de la investigació, anàlisi detallat de l'incident, detall de les recomanacions tècniques i controls de seguretat.

Es requereixen les següents capacitats en el servei per tal de diversificar la bossa d'hores en cas de necessitat:

- Preparació: anàlisi i diagnòstic de capacitats existents, assessorament, desenvolupament i/o adaptació de documents normatius, actes de formació i conscienciació, desplegament o adequació d'eines de resiliència, automatització de processos.

- Resposta: nivells de resposta disponibles i perfils de cada nivell, capacitats d'orquestració d'altres equips.
- Recuperació: investigació forense, recuperació d'entorns tecnològics, assessorament en la recuperació, destrucció segura d'actius, etc.

La resposta a incidents crítics amb les capacitats demanades a les etapes detallades suposen el treball col·laboratiu de diferents perfils segons la seva àrea d'expertesa i capacitats, considerant que hi haurà flexibilitat en la incorporació d'experts segons la tipologia d'incidents però ja es s'identifiquen unes capacitats mínimes a data d'avui que es relacionen a continuació:

- **Tècnic sènior especialista en SOC** (vegeu *8 Recursos Humans*)**:** Gestor d'emergències (encarregat d'orquestrar les actuacions marcant prioritats)
- **Tècnic sènior especialista en SOC** (vegeu *8 Recursos Humans*)**:** Expert en gestió d'incidents (encarregat de garantir que les activitats planificades es duen a terme) + equip adhoc de recolzament presencial.
- **Tècnic sènior especialista *hacking*, forense i investigació,** i **Especialista en Peritatge Forensic** (vegeu *8 Recursos Humans*)**:** Expert forense digital (encarregat de garantir que les actuacions tècniques del pla d'acció es duen a terme en temps i forma) + equip adhoc de recolzament presencial si calgués (en principi ja cobert per el servei de preventiu fora de l'abast d'aquest plec).
    - Investigacions digitals en servidors i endpoints.
    - Investigacions digitals en smartphones iOS i Android.
    - Investigacions digitals a través de l'anàlisi d'informació en trànsit.
    - Investigacions digitals en sistemes al núvol.
    - Investigacions digitals d'elements com logs, correus o executables.

El servei haurà d'explicitar el consum del servei en unitats de consum per cada perfil posat a disposició d'aquest servei. Dit d'altra manera, les hores contractades, quin pes tindrà cada tipus de perfil requerit per a la resposta a incidents crítics.

4.1.4. ELABORACIÓ D'INFORMES DE PETICIÓ D'EVIDÈNCIES

Aquest servei és complementari a la resposta a incidents la gestió d'evidències i elaboració d'informes que es poden requerir internament o per requeriments judicials.

Aquesta elaboració d'informes té dues vessants que impliquen perfils diferents:

- Tasques d'**informes pericials** amb especialistes en peritatge informàtic i gestió de prova electrònica:

    Peritatges informàtics i formalització de les evidències electròniques obtingudes en la fase d'anàlisi en informes pericials que poden ser utilitzats com a mitjà de prova i ser ratificats en judici pels perits informàtics del contracte.

Al contracte es requereix un informe pericial amb capacitats d'ampliació si es consumeix: en el marc del contracte l'adjudicatari haurà de realitzar com a mínim una anàlisi forense en què es requereixi serveis d'experts pericials amb personal certificat i la presentació de l'anàlisi/informe a l'Ajuntament o en un judici com a l'IMI de part. Aquest peritatge es requereix com a reserva per necessitats d'urgència que l'Ajuntament o IMI puguin necessitar per la defensa dels seus interessos.

- Tasques de **prova electrònica o informàtica forense**

El servei disposarà de **capacitats pericials** per a processos en què es requereixi donar garanties de cadena de custòdia d'actes administratius o d'evidències amb requeriments de tècniques d'anàlisi forense pericial (tecnologies de forense exhaustives amb cadenes de custòdia).

Prova electrònica

Aquest servei requereix d'alta especialització per personal certificat CHFI, Pèrit Judicial Forense. Es preveu un forense amb requeriments judicials.

informació digital iniciant cadenes de custòdia amb totes les garanties tècniques i legals per poder aportar, si fes falta a posteriori, documents electrònics en processos judicials garantint la seva integritat i autenticitat.

Informàtica forense: Localització i extracció d'informació rellevant per al seu cas emmagatzemada en dispositius electrònics com ordinadors, portàtils, telèfons mòbils o servidors, així com de pàgines web, fòrums d'internet o correu electrònic, respectant el marc legal existent i els drets fonamentals de les persones implicades. També recuperar si cal dades esborrades o ocultes.

Aquest servei requereix d'alta especialització per personal certificat CHFI, Pèrit Judicial Forense. En aquest punt (Tasques de **prova electrònica o informàtica forense) n**o es preveu un forense amb requeriments per defensar a l'IMI o Ajuntament amb actes probatòries per a requeriments o defenses en judici. Tan sols es tracta de donar resposta a requeriment judicials o interns requerits.

- Tasques de **gestió de petició d'evidències, recepció i elaboració d'informe sense requeriments pericials experts.**

Són tasques de recepció de la petició, derivar la petició als administradors de sistemes de manera procedimentada, tot indicant com s'ha de fer l'actuació, explotació i elaboració d'informe de resposta. Aquesta tasca es requereix per

poder donar resposta a peticions corporatives d'actuacions que es deriven de l'avaluació d'evidències. Aquestes tasques no tenen requeriments de tecnologies i procediments forenses. També s'inclouen en aquest apartat la resposta a requeriments judicials que no tenen implicacions de investigació pericial amb personal certificat CHFI, on l'Ajuntament no es part implicada directament , és a dir, que tan sols s'ha de indicar qui ha realitzat una acció TIC concreta amb els serveis TIC de l'ajuntament (IPs, accés wifi, etc i que no requereixen realitzar pràctiques exhaustives d'integritat i autenticitat de la prova. Aquest servei requerirà perfil de gestor de tècnic sènior especialista en seguretat preventiva (gestor de vulnerabilitats i elaboració d'informes).

Aquest servei es podrà subcontractar la part més formal a terceres empreses especialitzades. En aquest cas, s'haurà de presentar l'empresa subcontractada al responsable del Departament de Seguretat i recollir la conformitat contractual procedent.

En qualsevol cas, les peticions de forenses sempre la sol·licitarà l'Oficina de GRC, que verificarà la legitimitat del peticionari i la identitat de la petició així com la formalitat i garanties de la cadena de custòdia.

A continuació es presenta una taula de volumetria per aquesta apartat del contracte:

Volumetries del servei de seguretat reactiva	**Quantitat**
Tècniques d'anàlisi **Informe pericial** (tecnologies de forense exhaustives) per a requeriments judicials	2 en 3 anys
Tècniques d'anàlisi **prova electrònica o informàtica forense** (tecnologies de forense exhaustives) per garanties en el procediment administratiu o de l'Administració Municipal	3 anuals
Tasques de gestió de petició d'evidències, recepció i elaboració d'informe	12 informes anuals

Es valoraran les propostes dels licitadors que millorin el nombre mínim de Seguretat reactiva de forenses i tasques d'investigació i petició d'evidències a realitzar anualment.

4.1.5. ADMINISTRACIÓ DE LA PLATAFORMA DE GESTIÓ I CORRELACIÓ D'EVENTS DE SEGURETAT (SIEM) I LOGS CENTRALITZATS

L'adjudicatari serà responsable d'**operar, administrar i evolucionar les eines i plataformes de seguretat,** SIEM i logs centralitzats, de forma totalment transparent a l'IMI, incloent la integració de fonts dins de l'abast, regles de correlació i alertes de seguretat.

Es requereix per a la cobertura del servei d'administració cobertura 24x7x365 per gestionar incidències fora d'aquest horari.

Les tasques d'administració es detallen a continuació:

Gestió d'accés

- Gestió de comptes d'usuari
- Definició i implantació de rols i privilegis
- Revisió periòdica de l'estat i activitat dels usuaris

Gestió de la configuració

- Definició i implantació de polítiques de seguretat
- Definició i implantació de polítiques de retenció de dades
- Establiment de llindars de rendiment
- Definició i implantació d'altres paràmetres d'operació
- Revisió de les fonts integrades

Monitorització

- Monitorització i estat de sistema (disponibilitat de el servei) i integració amb els serveis de Nivell 1 de l'IMI.
- Comprovació de l'estat dels recol·lectors i altres elements
- Volumetria de les capacitats del dispositiu
- Correcció d'errors o events que puguin afectar el servei que ofereix el dispositiu.
- Assegurar una correcta configuració de resiliència del dispositiu

Gestió de logs

- Revisió periòdica de logs (registres d'activitat del dispositiu)
- Detecció d'errors
- Health-checking
- Rendiment del dispositiu

Gestió del canvi

- Actualització a noves versions estables
- Instal·lació de pegats
- Manteniment i escalat a fabricant, quan sigui necessari
- Gestió i actualització de bases de dades (signatures o altres)

- Revisió del correcte funcionament de les regles

Administració de les Plataformes. Remarquem les tasques d'administració de la plataforma SIEM i logs centralitzats com són:

- Tasques vinculades a la instal·lació, manteniment i operació bàsica del producte com són:
  - Monitorització i estat de sistema (disponibilitat de el servei).
  - Backups de el servei
  - Instal·lació de pegats i actualitzacions
  - Evolució i escalat de la plataforma en cas de necessitat
- Configuracions base
- Integració de noves fonts en SIEM i en ELK, logs centralitzats, amb el parseig pertinent i filtratge en origen o destí. Això inclou, dins de cada integració.
- Col·laboració en la configuració de la font per a recollida dels logs
- Regles de filtrat previ per evitar EPS que no aportin informació útil
- Configuració de regles de correlació específiques d'aquesta font ja proporcionades pel fabricant.
- Configuració de casos d'ús específics d'aquesta font ja proporcionats pel fabricant (això no compta com a casos d'ús dels blocs a consumir esmentats de forma prèvia)
- Configuració de quadres de comandament i alertes
- Vigilància / Monitorització que es reben dades d'aquesta font.
- Documentació de les configuracions i integracions
- Identificació i proposta de recomanacions, canvis i altres mesures correctives amb l'evolució del servei, l'aplicació es considerarà a criteri de l'IMI. En general, aportacions a les solucions i serveis desplegats per a la millora contínua del servei.
- L'adjudicatari avaluarà de manera recurrent el grau de protecció proporcionat per la solució SIEM, així com la diferència existent entre el situació actual del SIEM i l'estat objectiu, sempre en base a l'alineament amb els models de riscos del IMI.

4.1.5.1. Posta a punt i configuració SIEM i ELK pels objectius del SOC

Posta a punt i millora de les configuracions i implementacions del SIEM corporatiu, sistema de logs centralitzats i eina d'escaneig de vulnerabilitats internes al servei: anàlisi de l'arquitectura i infraestructura corporativa per tal de posteriorment

personalitzar i implementar les funcionalitats o capacitats necessàries per complir amb els nivells de servei del contracte amb eficàcia i eficiència. Aquesta posta a punt revisió i millora dels eps, per part de l'adjudicatari, inclou ajustar configuracions, definir noves fonts requerides i integrar noves fonts tant al SIEM, als logs centralitzats com al gestor de vulnerabilitats, així com la revisió i migració de Casos d'Ús actualment a Alien Vault.

4.1.5.2. Política de retenció de dades de les plataformes tecnològiques

- Cal disposar d'un mínim de 3 mesos en línia sobre els quals pugui treballar l'eina. A més, es retindrà un històric mínim de 12 mesos. Les dades històriques, davant d'una necessitat, han de poder ser ingestades a l'eina per a una operació "en línia".
- L'adjudicatari haurà de descriure el tractament de les dades que realitza l'eina, indicant el període de retenció de dades online.
- Tot l'emmagatzematge necessari (online i històric) per a la retenció de dades serà proporcionat les infraestructures de l'IMI. **No es permeten dependències d'infraestructura de l'adjudicatari per a l'emmagatzematge de dades.**
- La solució ha d'estar dimensionada per a l'emmagatzematge històric de totes les dades. No obstant això, ha d'oferir la possibilitat de decidir quines fonts es volen emmagatzemar en mode històric i quins no.
- La solució ha d'evitar la pèrdua d'esdeveniments davant pics que superen la llicència en moments puntuals.
- La solució ha d'oferir a través de components propis (sense comptar amb la configuració dels orígens de dades) la possibilitat de filtrar els esdeveniments enviats a la plataforma a fi de poder evitar l'enviament de grans quantitats de dades que no aportin valor. Entre altres coses, ha de permetre filtrar el tràfic d'una font concreta en un moment donat sense haver de desactivar els agents d'integració d'aquesta font. També ha de permetre filtrar logs específics dins dels enviats per una font (Per exemple, dins d'una font com pot ser un servidor intermediari de navegació, ha de permetre el filtrat d'esdeveniments d'accessos a URL concretes).
- Els esdeveniments filtrats no han de ser comptabilitzats a nivell de llicència.
- Com a mínim en el cas de les plataformes OnPremise, el filtrat d'esdeveniments es realitzarà en origen, sense que aquests esdeveniments filtrats consumeixin ample de banda.

4.1.6. MILLORES I EVOLUCIÓ DEL SERVEI

- L'adjudicatari disposarà d'un procés de millora contínua amb identificació i proposta de recomanacions sobre les solucions o serveis, canvis i altres

mesures correctives que alimentin l'evolució del servei, l'aplicació es considerarà a criteri de IMI.

- Cyber exercici: Consisteix a realitzar exercicis conjunts de Red Teaming i Blue Teaming perquè els atacs i les deteccions puguin ser contrastades en temps real. atacs i les deteccions puguin ser contrastades en temps real per avaluar la resposta del SOC.
- Modelatge d'amenaces (*thread modeling*) i manteniment de *playbooks* o procediments d'operació.
- Campanyes de malware IOC: Inclòs com a feed de MSSP
- Formalització de la constitució del SOC:

  Definir formalment la constitució de SOC. Aquesta definició ha d'incloure el detall de com els eixos estratègics del negoci es van a cobrir amb els serveis que es presten, un catàleg clar de serveis de SOC amb entrades i sortides definides per a cada un d'ells, un model organitzatiu del SOC que garanteixi la prestació de serveis i estimacions d'esforç amb unitats per a cada servei
- Definir un Pla Estratègic per al desenvolupament i l'evolució del SOC:

  Avaluació de l'estat de maduresa dels Serveis d'Operacions de Seguretat, creant un marc de control modular per serveis, per a l'avaluació i definició de roadmaps a llarg termini que permetin augmentar la maduresa.

  Per aquest objectiu s'avaluaran els següents dominis:

  - **Negoci** del SOC, incloent impulsors (*drivers*) de negoci, clients, interfícies, documents de constitució del SOC, gestió de costos, externalització, privacitat i gestió de crisi.
  - **Persones**, incloent empleats, rols i jerarquia, gestió de personal, programes de formació.
  - **Processos**, incloent avaluació de la qualitat, estandardització TI, recursos i instal·lacions, canvis de torn, taxonomia d'amenaces, gestió del coneixement, classificació i compartició d'informació, procés d'informe i quadres de comandament.
  - **Tecnologies** utilitzades pel SOC, incloent la infraestructura de seguretat, plataformes de revisió de salut, SIEM, Data Lake, sistema de *ticketing*, SOAR i Plataformes de compartició d'intel·ligència.
  - **Serveis** que proporciona el SOC, incloent la millora contínua i assessoria, enduriment de la infraestructura, Red Team, Pentesting, Gestió de *logs*, gestió d'esdeveniments, monitorització i triatge, gestió d'incidents, Ciberintel·ligència, Threat Hunting, forenses i Cyberwargaming.

4.1.7. COORDINACIÓ AMB ALTRES ÀREES OPERATIVES

Integració amb el servei de Preventiu de l'IMI (Ciberintel•ligència, escanejos automàtics, Hacking ètics, Gestió de Vulnerabilitats) que te l'IMI. **Automatització de processos del Servei de Preventiu.**

Coordinació amb els altres serveis de Seguretat (Oficina GRC, Serveis de Projectes i Arquitectures, Signatura digital i Certificats, Serveis de Preventiu i Servei d'identitats i accessos).

Coordinació amb les àrees Operatives i tecnològiques de l'IMI (que implementen, administres i operen) i que han d'implantar els serveis amb seguretat.

4.1.7.1. Ubicació geogràfica del SOC

SOC localitzat en territori de la Unió Europea. Les alertes i ticketings i altres solucions i serveis que se sustentin fora de l'IMI i en el servei, hauran de residir a un DataCenter en la Unió Europea per assegurar tenir les garanties de seguretat que ens aporta el compliment de la legislació vigent.

4.1.7.2. Idioma

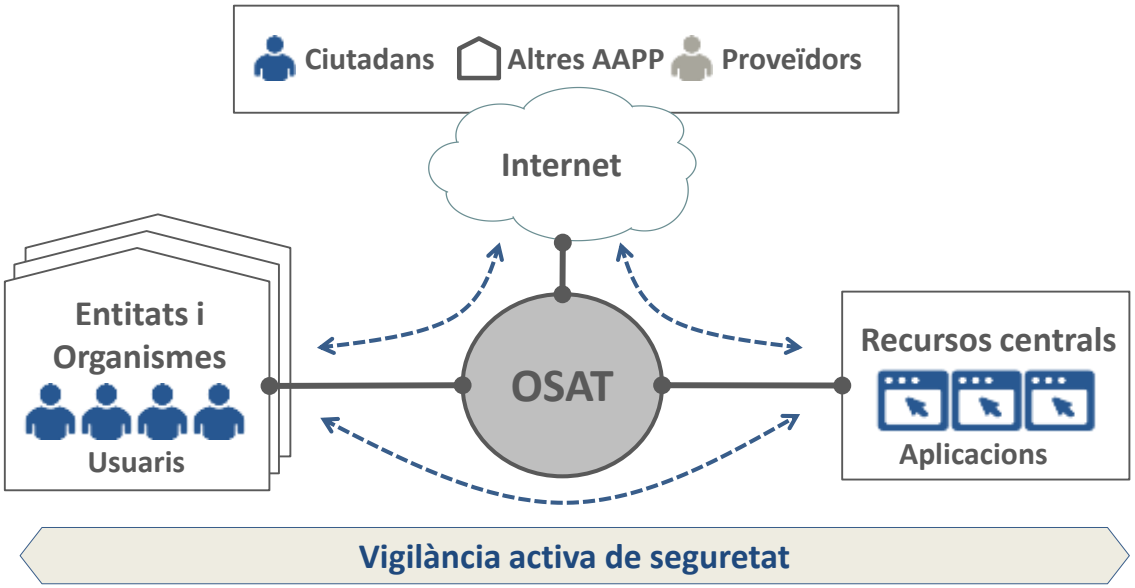
Obligatòriament l'adjudicatari desenvoluparà els sistemes i interfícies d'usuari externes en català.

Això inclou també la documentació de gestió i documentació tècnica requerida i lliurada durant l'execució del projecte.

4.2. SERVEIS OSAT

4.2.1. NUS de COMUNICACIONS

Entenem com a nus de comunicacions l'arquitectura del node de xarxa que proporciona els següents serveis:



Il·lustració 1: Model OSAT

- Serveis d'interconnexió als proveïdors i adjudicataris de serveis diversos
- Serveis d'interconnexió a altres entitats, organismes i empreses amb què l'IMI manté relacions
- Connexió segura a Internet dels usuaris i sistemes d'informació de l'IMI
- Serveis de connexió remota a l'IMI
- Funcionalitats de xarxa a les plataformes d'execució i servidors web en entorns Intranet i Internet com balancejadors, tallafocs, conformadors de tràfics, DNS, NTP, elements de navegació
- Sistemes d'informació i sistemes de gestió associats a la gestió de seguretat i gestió dels serveis del propi nus
- Plataforma de comunicacions wireless centralitzada (Controladores Wifi) i serveis que es presten sobre aquesta
- Serveis associats a la vigilància activa de seguretat
- Serveis de consultoria de solucions de connectivitat i seguretat.

Als apartats següents es descriuen amb més detall els diferents components del nus, objecte del present contracte.

Actualment el nus de comunicacions de l'IMI està distribuït en dos CPDs, Interconnectats entre ells, on es poden observar entorns clarament diferenciats:

- CPD 1

- És el CPD principal del nus de comunicacions i és on s'ubiquen els equips més importants. És en aquest CPD on existeix únicament la sortida a internet.

- CPD 2:
  - És un CPD de nova creació objecte d'un altre concurs públic que s'està desplegant amb l'objectiu de ser el CPD principal de l'organització i ha d'evolucionar fins a ser el CPD principal de l'IMI.

Aquests dos CPDs (Glòries i Via Favència) treballen en alta disponibilitat i configuracions tant d'actiu-actiu com d'actiu-passiu pels serveis de comunicacions i pels sistemes d'informació.

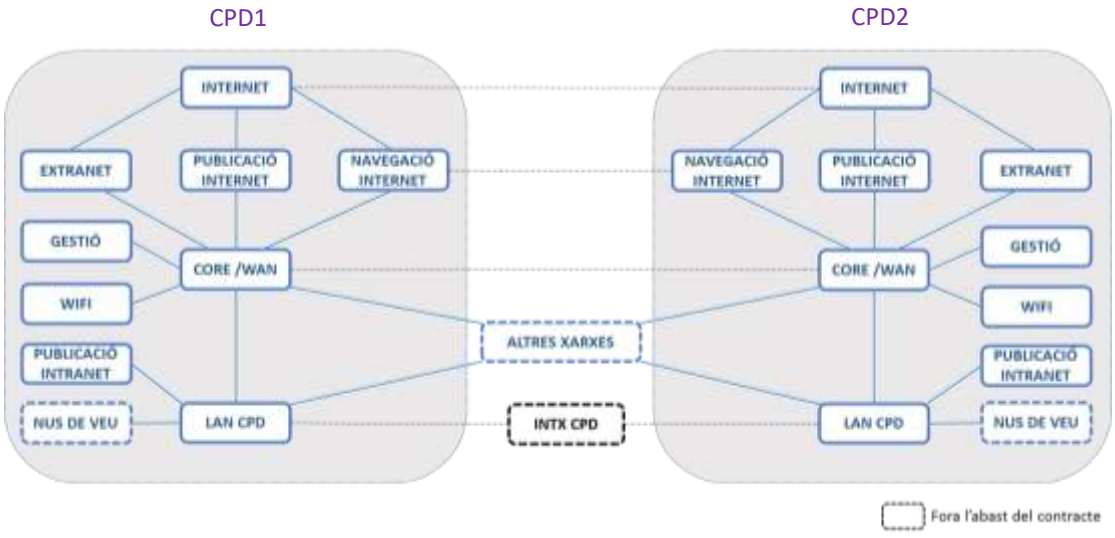
Les volumetries aproximades que es contemplen són d'aproximadament uns 70 elements entre comunicacions i seguretat ubicats als CPDs actuals de l'IMI, amb els elements de gestió associats.

Cal tenir en compte, que durant la vigència del contracte, és probable que es traslladin els elements ubicats al CPD 1 a una nova ubicació, al centre de la ciutat. El proveïdor haurà d'assumir dins les tasques pròpies del Servei, i sense cost addicional, aquelles activitats derivades del trasllat. Habitualment, aquestes tasques es realitzaran fora d'horari laboral.

4.2.1.1. Arquitectura del Nus

L'objectiu d'aquest apartat és la descripció de l'arquitectura dels blocs que conformen el nus de comunicacions.

Les funcionalitats específiques de cada bloc es defineixen a continuació. En l'inventari del plec del concurs es pot consultar la relació entre els equips inventariats i els blocs funcionals.



Il·lustració 2: Blocs funcionals

Bloc Core / WAN

Els equipaments que formen el CORE, són el nucli de comunicacions dels CPDs. Aquests són el punt d'unió entre els diferents blocs. Realitzen funcions d'enrutat dinàmic entre les diferents xarxes. Es fa servir el protocol de routing OSFP i està format per equips 4500X (VSS) amb configuracions en alta disponibilitat. Aquest bloc Core té les capacitats d'enrutament Unicast i Multicast amb diferents Routers virtuals associats (VRF).

La funció de transport de dades entre les diferents seus de l'Ajuntament s'ha adjudicat en un altre concurs, proveint les funcions d'interconnexió en aquest bloc.

Bloc Internet

Aquest bloc dóna connectivitat a Internet (connectivitat amb un adjudicatari d'accés a Internet) i permet definir diferents reserves d'ampla de banda d'Internet. L'Ajuntament, tot i tenir direccionalitat pública, enruta el seu tràfic cap a un proveïdor que gestiona la publicació de l'AS cap al món. En el bloc d'Internet, l'Ajuntament rep el tràfic mitjançant uns equips Cisco Catalyst C3850-12XS en alta disponibilitat, previ pas als elements d'IPS / IDS.

Bloc LAN CPD

Està format per tots els elements que donen connectivitat LAN als sistemes d'informació ubicats als CPDs de l'Ajuntament de Barcelona. Actualment aquests elements estan formats per equipament Cisco Nexus y Catalyst. La gestió d'aquest equipament recau en OSAT. L'inventari d'aquests elements s'entregarà sota petició.

Bloc Publicació Internet

Està format per tots els elements que donen serveis de seguretat, balanceig, accessibilitat, resolució de noms i connexió a Internet als servidors que donen servei a Internet. Els elements destacables són:

- Firewalls perimetrals externs
- Balancejadors externs
- DNS externs

Bloc Publicació Intranet

Està format per tots els elements que donen serveis de seguretat, balanceig, accessibilitat i resolució de noms als servidors de les capes no publicades a Internet. El composen:

- Firewalls perimetrals interns
- Balancejadors interns
- DNS interns

Bloc Gestió

Aquest bloc està format per totes les eines de gestió i monitorització necessàries per poder portar un control acurat del servei en tot moment i així poder optimitzar els recursos existents. En aquest bloc trobem totes les eines i servidors que composen la gestió dels elements del nus.

Bloc Extranet

Aquest bloc està format pels equips necessaris per donar connectivitat i accés remot a la xarxa de l'IMI a través de VPNs, túnels IPSec i línies dedicades de terceres empreses, altres organismes i usuaris corporatius. Formen part d'aquesta funció, les diferents solucions que estan enfocades a obrir connexions remotes a l'Ajuntament. La composen diversos elements:

- Concentradors enfocats a fer VPN IPSEC
- Concentradors VPN-SSL
- Firewalls amb client VPN
- Diversos Routers dedicats a obrir túnels per realitzar un transport transparent

Bloc Navegació Internet

Aquest bloc està format per tots els elements de comunicacions i seguretat que permeten la sortida a Internet dels usuaris de l'IMI i serveis auxiliars. En aquest bloc tenim els elements que fan la funció de proxy de navegació i altres equips tipus NGFW. La navegació està filtrada i assegurada amb diferents perfils en funció del rol de navegació d'usuaris.

Bloc Wifi

Aquest bloc està format per tots els elements de seguretat i controladores que permeten gestionar la infraestructura wifi a las seus de l'Ajuntament, on s'irradien diferents SSID amb diferents perfils de connectivitat i seguretat. Els principals elements d'aquest bloc són:

- Controladores wifi
- Servidors Radius d'intranet i d'extranet
- Firewalls perimetrals.

Bloc Interconnexió de CPD (OTV)

Aquest bloc està format per tots els elements de comunicacions que donen connectivitat entre els actuals CPDs. Es basa en una solució d'OTV i VDC. Per poder mantenir l'aïllament, l'extensió de VLANs es realitza amb fibres dedicades.

Bloc Altres Xarxes

El servei comporta la connectivitat de dades entre les diferents seus de les Anelles o altres xarxes municipals com la xarxa Mesh.

En l'inventari del nus, es pot trobar un mapeig entre l'equipament i el bloc (o blocs) funcionals, on desenvolupa més funcions.

4.2.2. SERVEIS A PRESTAR PER L'ADJUDICATARI DE L'ÀMBIT DE LES TELECOMUNICACIONS I SEGURETAT

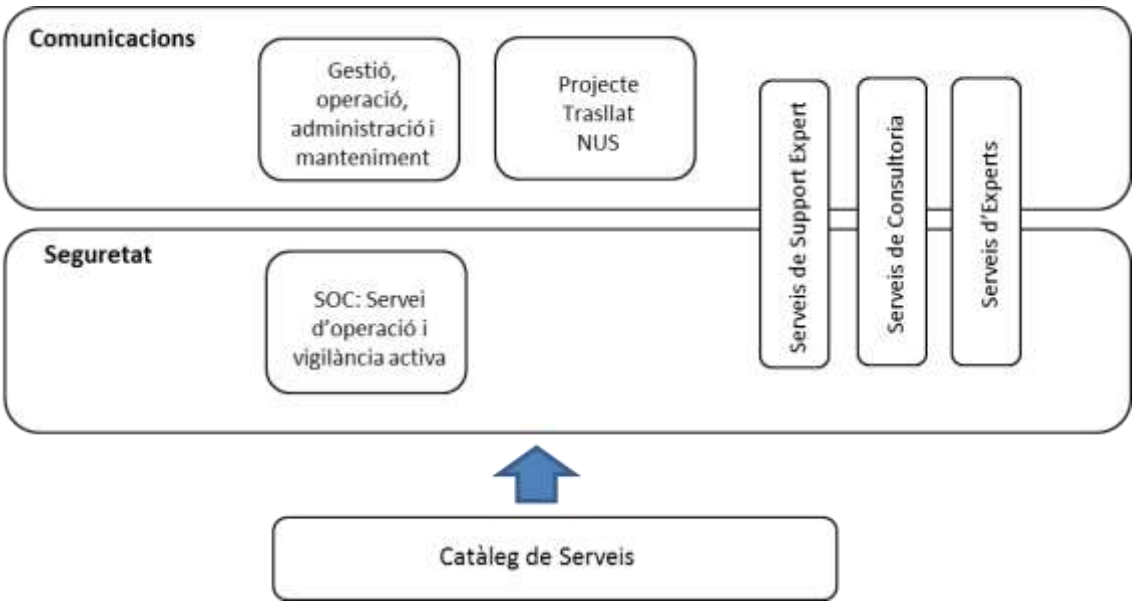
El model de govern de l'OSAT i els serveis prestats per l'oficina hauran de complir les especificacions del model de governança descrit a l'apartat **7. Model de Prestació del Servei** del present document.

Els serveis de telecomunicacions objecte del present contracte s'articulen en sis grups:

- Serveis a prestar compresos en el Catàleg de serveis corporatius.
- Gestió, operació, administració i manteniment de l'equipament del nus de comunicacions, així com dels **nous equipaments que es vagin incorporant pels projectes o renovacions** durant tot el període que cobreix aquest plec, **garantint en tot moment la disponibilitat del servei mantenint el nivell de seguretat determinat**.

- Suport expert en aspectes de comunicacions i seguretat en referència en l'àmbit d'actuació
- Serveis de consultoria del nus
- Serveis d'activitats/actuacions especials
- Serveis de suport a projectes

En el present capítol es detallen les condicions de prestació dels serveis per a cadascun dels grups.



Il·lustració 3: Blocs de serveis a prestar

Els següents apartats detallen, primerament una descripció del catàleg de serveis inicial, que el proveïdor haurà de revisar i actualitzar a l'inici del contracte, agrupats d'acord amb els àmbits de serveis.

A continuació es descriuen les activitats de gestió, operació, administració i manteniment emmarcats dins de les fases d'estratègia, disseny, transició, l'operació i la millora contínua del servei del model ITIL.

Seguidament es detallen els serveis a prestar dins de l'àmbit de l'operació i la vigilància activa de seguretat, tant en seguretat preventiva com reactiva.

Els serveis addicionals de suport i consultoria també formen part dels serveis a prestar i es descriuen abans d'abordar l'últim apartat, dedicat als projectes de transformació identificats per a desenvolupar-se al llarg del contracte, amb el calendari estimat de transformació i la metodologia a utilitzar.

4.2.2.1. SERVEIS A PRESTAR COMPRESOS EN EL CATÀLEG DE SERVEIS CORPORATIUS

Les tasques a realitzar per l'OSAT es realitzaran a partir d'un catàleg de serveis corporatius existent que el propi adjudicatari haurà de revisar (i completar, si calgués) a l'inici de la prestació dels serveis.

Dins el catàleg de serveis podem categoritzar els serveis en dos tipus:

- Serveis finalistes: és el proveïdor qui ha d'informar dels indicadors de disponibilitat de servei.
- Serveis o components base, on típicament presten serveis a altres elements superiors.

En la fase inicial del contracte, serà obligació de l'adjudicatari revisar i completar, si calgués, el catàleg de serveis. El catàleg haurà d'estar molt clar i ser concret, i caldrà, per a cadascun dels serveis del catàleg, redactar un document de provisió i operació pel mateix. Els mínims que aquest document haurà de contenir són:

- Descripció tècnica del servei (ANS's, indicadors del servei, com s'implementa tècnicament, funcionalitats i HW necessaris)
- Descripció detallada del servei, amb un esquema del mateix en format Microsoft Visio.
- Descripció dels paràmetres/variables del servei
- Procediment d'implantació del servei (guia pas a pas amb cada comanda implicada, i descripció amb els paràmetres implicats, perquè un operari de nivell 1 pugui implantar el servei, o en un futur una eina automàtica pugui ser programada a partir d'aquest document)
- Procediments addicionals d'operació del servei que permetin (sempre en el format del més baix nivell, tipus guia): donar de baixa el servei, modificacions sobre el servei (p.ex. afegir ports d'accés, afegir regles de Firewall, donar de baixa una reserva d'ample de banda d'una aplicació)
- Procediments de troubleshooting (comandes, explicacions i baix nivell per a permetre el troubleshooting del servei)
- Estimació de costos del servei durant el cicle de vida del mateix

Serà obligació de l'adjudicatari la creació d'un document en doble format, doc + xls, on constarà el catàleg de serveis, essent més detallat el format doc i essent una eina de referència global amb tots els serveis inclosos l'xls associat, que també contindrà tota la informació de parametritzacions necessàries.

A nivell d'inventari, l'adjudicatari haurà de crear un inventari en format xls (o similar) per tal de mantenir una BBDD de tots els serveis contractats, amb les dades de

parametritzacions necessàries associades a cada servei, permetent evitar el solapament de dades essencials com VLANs, adreçament IP.

Cada nou servei en el catàleg s'haurà d'implantar en un format Pilot, és a dir, totalment operatiu, però sense un servei real al darrere. La validació del servei serà en 2 fases: fase 1 d'implantació (verificació i redacció de la documentació), fase 2 (s'haurà d'implementar de nou el servei seguint el procediment creat per al mateix, comprovant així el correcte redactat i la coherència del mateix).

Als punts que hi ha a continuació es relacionen els serveis identificats inicialment.

4.2.2.1.1. Serveis de navegació

El nus de comunicacions és l'element a partir del qual tots els usuaris accedeixen, de forma segura, a Internet, mitjançant els següents serveis:

- Servei de navegació segura a Internet
  - Mitjançant proxy
  - Sense proxy
- Servei de navegació de cortesia amb enviament SMS amb passarel·la de tercers
- Servei d'anàlisi de la navegació per detecció d'anomalies
- Servei de reserva / limitació d'ample de banda

Dins d'aquests serveis tenim diversos tipus d'usuaris:

- Usuaris de PCs corporatius
- Usuaris de PCs no corporatius
- Usuaris amb dispositius mòbils

4.2.2.1.2. Serveis de connexió de col·laboradors externs

El nus de comunicacions actua com a element neutre central d'interconnexió entre els diferents serveis i proveïdors de l'IMI (comunicacions, CPDs, empreses desenvolupadores, altres organismes). En aquest àmbit es defineixen els següents serveis:

- Serveis de connexió segura al nus
- Servei de gestió i configuració de router per projectes
- Servei de creació de tallafocs virtual
- Aplicació de regles i polítiques definides per GRC als dispositius perimetrals de seguretat
- Monitorització del rendiment de les connexions

- Realització d'informes detallats de l'estat dels elements i l'aplicació de les polítiques.

4.2.2.1.3. Serveis de comunicacions de sistemes d'informació

El nus de comunicacions permet el balanceig de càrrega per servidors ubicats en els CPDs a nivell 4 (balanceig en funció de l'IP i port TCP o UDP), tant per accessos des d'internet com d'intranet, així com el balanceig de càrrega i modificacions de nivell 7 (reescriptura d'URLs, redirecció d'URLs) per servidors ubicats en els CPDs, tant per accessos des d'internet com d'intranet. Dins d'aquest àmbit es defineixen els següents serveis:

- Servei de tallafocs amb eliminació malware nivell 7
- Servei de reserva / limitació d'ample de banda nivell 4 i nivell 7
- Servei de publicació segura de webs
- Servei de balanceig de serveis extern i intern de nivell 4 i nivell 7

4.2.2.1.4. Serveis de connectivitat remota

El nus de comunicacions proporciona el servei finalista de connectivitat remota als usuaris, tant des d'estacions fixes com des de dispositius mòbils, assegurant tant la connectivitat com la seguretat en les comunicacions.

- Serveis de connectivitat remota VPN estacions fixes
- Serveis de connectivitat remota VPN mòbils per telèfons i tablets.

4.2.2.1.5. Serveis de Wireless

Dins de la xarxa municipal podem trobar actualment dues tecnologies (una basada en wifi i l'altra basada en xarxes de dades mòbils), incloses dins l'abast de la gestió, administració i operació.

En aquests punts els elements centrals ubicats als nusos de comunicacions són els dispositius objecte d'administració. Els elements són els següents:

- Controladores Wireless i programaris de gestió associats a tal efecte.
- Elements d'autenticació radius de suport al servei d'APN privat sobre xarxa mòbil d'operadors.

El desplegament físic dels punts d'accés wireless no es gestiona dins l'abast d'OSAT. Tot i això la governança dels serveis, la creació de nous serveis, la gestió dels elements centrals, l'homologació dels serveis i l'evolució de la millora dels serveis wireless és responsabilitat del nus de comunicacions.

L'OSAT és l'element central que proporciona els serveis Wireless de l'IMI. Per tant, dins de les seves tasques haurà d'encarregar-se de gestionar els següents serveis:

- Wireless de convidats desplegats a les dependències municipals
- Wireless corporativa amb autenticació 802.1x basat en solució NPS de Microsoft
- Wireless enfocada als dispositius Mòbils
- Servei de reporting d'ús del wifi
- Serveis de localització sobre wifi indoor
- Servei d'autenticació Radius sobre APN privat propi de l'Ajuntament de Barcelona
- Servei de reporting i anàlisi de servei sobre la infraestructura Wireless corporativa
- Servei de creació de mapes de cobertura wireless

4.2.2.1.6. Serveis de gestió d'adreçament IP Públic i Privat

A la xarxa IP interna de l'IMI s'utilitza adreçament IP privat, que serà gestionat per l'adjudicatari i de forma acordada amb procediments pactats per l'IMI.

En quant l'adreçament públic, l'IMI és LIR (Local Internet Registry) i per tant disposa d'adreçament públic propi i que haurà de ser gestionat per l'adjudicatari amb les eines IPAM de l'Ajuntament.

L'OSAT serà responsable de la gestió dels DNS i DHCP de l'Ajuntament amb el manteniment i vigilància dels elements implicats.

4.2.2.1.7. Serveis de Seguretat perimetral

Dins del nus de comunicacions, es defineixen un conjunt de zones amb diferents nivells de seguretat. Aquestes zones s'organitzen en funció del tipus de serveis que hi resideixen. Els accessos permesos o denegats entre els equipaments de cadascuna d'aquestes zones es regulen mitjançant diversos entorns de tallafocs que limiten el perímetre de les zones i implementen el que es coneix com "seguretat perimetral".

Les diferents zones de seguretat definides són les següents:

- ***Zona Internet:*** correspon a la part més externa de la xarxa que connecta directament a Internet. Les adreces públiques dels serveis de l'IMI es troben en aquesta zona. El nivell de seguretat en aquesta zona és baix ja que no es troba protegida d'Internet.
- ***Zona publicació Internet (DMZ):*** en aquesta zona es troben els servidors que són visibles des d'Internet, que habitualment formen part de la capa de presentació dels sistemes d'informació publicats a Internet. El nivell de seguretat d'aquesta zona és mig ja que els serveis que es publiquen poden ser

accedits des d'Internet, però la resta de serveis dels equipaments es troben protegits per l'entorn de tallafocs.

- ***Zona Extranet o VPN:*** a aquesta zona arriben les connexions d'usuaris remots i de terceres empreses i adjudicataris externs amb què treballa l'IMI, ja sigui mitjançant VPN o línies dedicades. Des d'aquesta zona, es pot anar cap a la zona d'Internet per accedir als serveis públics de l'IMI o cap a la zona d'Intranet per accedir als serveis interns. L'accés des d'aquesta zona cap al nus es regula mitjançant els tallafocs d'extranet. Cada adjudicatari o empresa externa és responsable de protegir-se de la resta de connexions que es troben en aquesta zona.
- ***Zona publicació Intranet (Xarxa VIP):*** en aquesta zona hi trobem els servidors corporatius interns accessibles des de totes les zones menys des d'Internet. És on s'implementa la capa de presentació dels sistemes d'informació corporatius accessibles des d'Intranet i les capes de servidors d'aplicació i bases de dades de tots els sistemes d'informació en general
- ***Zona recepció de proveïdors:*** En aquesta capa és on es reben els proveïdors amb diferents elements de comunicacions i es passen per les diverses capes de seguretat i interconnexió.
- ***Zona WAN Interna:*** en aquesta zona hi ha les xarxes de client dels departaments i organismes públics de l'Ajuntament. Dins d'aquesta zona hi ha el que es coneix per àmbits de confiança. Cadascun dels àmbits de confiança corresponen a un conjunt de xarxes departamentals i d'organismes que es poden "veure" entre elles sense haver de passar a través de cap dispositiu de seguretat. L'accés entre àmbits de confiança es regula mitjançant els tallafocs virtuals corresponents a cadascun dels àmbits

4.2.2.1.8. Serveis de generació de certificats

Tot i que els sistemes de certificats digitals per a la terminació de les sessions xifrades des d'Internet és responsabilitat de l'àrea de Seguretat de l'IMI, l'OSAT participa de la creació dels certificats de lloc. Si aquests són públics i s'han d'instal·lar al sistema de balanceig gestionat per OSAT, l'adjudicatari s'encarregarà de la generació del CSR, així com de la instal·lació del certificat.

Quan el certificat de lloc ha de ser generat amb la PKI pròpia de l'IMI imiCA, aquest certificat serà creat per l'OSAT.

4.2.2.1.9. Serveis de control d'accés a la xarxa corporativa

Es preveu que durant el 2022 es posi en marxa el servei de control d'accés a la xarxa corporativa (NAC). L'adjudicatari s'haurà d'encarregar de la gestió, operació i manteniment una vegada entregat el projecte.

4.2.2.1.10. Monitorització dels elements de comunicacions i seguretat

Tots els elements gestionats per l´adjudicatari han de ser monitoritzats de forma constant. Aquesta monitorització també inclou que la vigilància de totes les connexions entre els elements gestionats per OSAT amb altres elements o entre si, per tal que no superin un llindar de ample de banda consumit i d´aquesta manera evitar la saturació de l´enllaç.

Aquesta monitorització també inclou a les Aplicacions de depenguin de l´adjudicatari.

4.2.2.2. GESTIÓ, OPERACIÓ, ADMINISTRACIÓ I MANTENIMENT

L'adjudicatari serà el responsable de la gestió, administració, manteniment i recolzament en l'evolució de tots els components de servei.

L'IMI treballa en un model de gestió basat en ITIL, per tant, es requereix que l'adjudicatari realitzi totes les funcions pròpies del servei amb aquesta orientació, aportant una millora substancial en quant a processos, procediments i orientació a servei.

En els següents subapartats es detallen les principals activitats a desenvolupar d'acord amb aquest marc de gestió. Aquestes activitats s'estructuren d'acord amb els 5 grans blocs de gestió definits en ITIL: estratègia, disseny, transició, operació i millora contínua.

4.2.2.2.1. Estratègia del servei

Les funcions a desenvolupar a la capa d'estratègia del servei seran compartides entre l'equip de l'IMI i l'adjudicatari, però es requereix d'una aportació de valor per part del proveïdor per a mantenir el servei alineat amb les necessitats de l'organització.

Dins d'aquesta capa es requerirà com a mínim la realització de les següents activitats:

- Elaboració de propostes d'evolució dels serveis a partir de l'experiència de l'adjudicatari en projectes similars i tenint en compte el context de l'IMI
- Gestió financera dels serveis i dels projectes d'actualització que estiguin inclosos en aquest contracte, aportant transparència en el rendiment de comptes
- Gestió del contracte d'acord amb el model de relació acordat, especificada en l'apartat **7: Model de Prestació del Servei**.

- Anàlisi de costos dels serveis prestats de forma quantificable i per client

4.2.2.2.2. Disseny del servei

Dins de la capa de **disseny del servei** caldrà que l'adjudicatari posi especial èmfasi en assegurar la disponibilitat, capacitat i continuïtat dels serveis prestats, així com en l'actualització i manteniment d'un catàleg de serveis complert.

Dins d'aquesta capa es requerirà com a mínim la realització de les següents activitats:

- Manteniment de les versions dels elements dels nus actualitzades almenys un cop cada any en casos de switchos i Routers i de 6 mesos en casos de tallafocs i balancejadors. En cas d'indefinició s'actualitzaran amb una periodicitat mínima d'un cop cada 6 mesos
- Documentació i realització de proves de continuïtat dels serveis almenys un cop cada any
- Anàlisi d'evolució de la capacitat de tots els elements gestionats (CPU, memòria, tràfic, sessions concurrents), indicant alertes de capacitat a partir de la superació de llindars establerts per l'IMI (o els recomanats per l'adjudicatari en cas d'indefinició).
- Definició de nous serveis sobre les infraestructures gestionades des del nus
- Proves anuals en la validació de la seguretat i continuïtat en la prestació del servei, alineades amb les polítiques internes de l'organització
- Revisió del catàleg de serveis del nus del comunicacions amb costos associats, mantenint al dia el serveis prestats
- Modificació/actualització de serveis existents en el catàleg d'accessos remots
- Elaboració de guies de disseny i prescripció de requeriments de comunicacions i seguretat, principalment per a Lloc de Treball, Telecomunicacions i CPD
- Identificació dels indicadors de servei per cada procés en base a ITIL
- Suport a proves de concepte que es realitzen a l'IMI
- Suport en el disseny de solucions tècniques que impliquen elements gestionats
- Disseny del sistema de traces del servei, elaborant i mantenint el "Document Mestre de Traces" que identifiqui les evidències necessàries, protecció i ubicació.
- Identificació de *bugs* als elements de xarxa del NUS i actualització de les IOS sense cap cost per a l´IMI.

Per tal d'assegurar el suport del fabricant, l'adjudicatari haurà de lliurar certificats emesos pel fabricant dels dispositius gestionats on es reflecteixi el pagament del manteniment vigent fins la data de finalització del contracte.

L'adjudicatari serà el responsable de generar tota la documentació necessària pel correcte funcionament i evolució del servei i aquesta documentació del servei s'ubicarà en els repositoris designats per l'IMI. Mentre no es disposi d'aquests repositoris l'adjudicatari haurà de mantenir i actualitzar aquesta documentació en repositoris accessibles en tot moment pel personal de l'IMI.

La documentació a generar haurà d'incloure com a mínim:

- Catàleg de serveis amb ANS i metodologia per mesurar-los associats als serveis
- Pla de proves actualitzat de les solucions
- Pla d'escalat
- Relació d'equips instal·lats, amb número de sèrie i llicencies associades
- Relació de components de cadascun dels equips (cas d'equips modulars)
- Configuracions finals de cada equip
- Esquema físic de connectivitat
- Esquema lògic de connectivitat
- Document d'arquitectura
- Documents de diagnòstics d'errors bàsic de la solució
- Document d'operacions de la solució: actualització/modificació del reporting dels serveis
- Pla de contingència.

Aquesta documentació s'haurà de revisar de forma proactiva com a mínim un cop l'any per garantir la vigència del contingut.

4.2.2.2.3. Transició del servei

En referència a la capa de **transició del servei**, l'adjudicatari haurà de posar especial rellevància a la gestió dels canvis, ja que l'entorn és crític per a tots els serveis TIC de l'Ajuntament, així com en el manteniment de la documentació i configuració de tots els elements dels serveis.

Dins d'aquesta capa es requerirà com a mínim la realització de les següents activitats:

- Planificació i execució de canvis i RFCs, incloent la generació de la documentació prèvia, la participació en els comitès d'aprovació de canvis, la gestió d'excepcions i urgències i la utilització de les eines de gestió que correspongui

- Publicació de nous serveis definits per l'OSAT
- Definició de mecanismes de diagnòstics i escalats de nivell 1 o 2 pel servei de SAU de l'IMI
- Manteniment i actualització de tota la documentació dels serveis a mesura que s'apliquen canvis sobre els mateixos (actualització mapes de xarxa, inventaris de regles de FW, memòries dels serveis...)
- Ajuda activa en la proposició de mesures i solucions tècniques per identificar de forma àgil els errors en l'organització

4.2.2.2.4. Operació del servei

En la capa d'**operació del servei** l'adjudicatari haurà d'assegurar disposar de tots els mecanismes per assegurar el compliment dels nivells de servei marcats així com proporcionar la informació suficient per a la resta de capes de gestió.

Dins d'aquesta capa es requerirà com a mínim la realització de les següents activitats:

- Gestió, monitorització proactiva (24x7), operació, evolució i administració tècnica de la infraestructura i dels serveis finalistes d'OSAT d'acord amb els processos descrits a la Governança de serveis TIC de l'IMI
- Gestió d'alertes d'infraestructura (gestió traps SNMP). L'adjudicatari tractarà les alertes en funció de la criticitat i impacte, de la forma més eficaç i ràpida, procedint segons procediments establerts
- Sistema de tècnics de guàrdia en format 24x7, on sempre hi haurà com a mínim un tècnic de guàrdia disponible per atendre els següents àmbits d'actuació dels elements que gestiona OSAT:
  - Gestió d'incidències
  - Gestió d'excepcions
  - Gestió de canvis programats amb afectació de servei
- Manteniment i operació de nou equipament i gestió dels nous serveis prestats per aquest nou equipament.
- Realització de còpies de seguretat dels elements gestionats per l'OSAT i extracció d'aquestes còpies a ubicacions externes. A l'inici del contracte es detallaran els períodes de retenció i còpia per tal de garantir la normativa de backups de l'IMI i assegurar els SLA de servei. En cas d'indefinició, s'assumirà un backup diari.
- Administració i operació d'equips de Wireless centralitzats

- Manteniment de les garanties esteses de fabricant de tot l'equipament dintre de l'abast, aportant els certificats de fabricant que assegurin que amb els temps de reposició de material contractat es poden complir els ANS establerts, Apartat **6: Acords de Nivell de Servei**.
- Manteniment i evolució de les eines de gestió i de les infraestructures on resideixen aquestes eines que siguin gestionades per OSAT d'acord amb la normativa establerta per l'IMI (versionat, polítiques de seguretat)
- Interacció amb els diferents adjudicataris i tercers (fabricants, proveïdors externs, altres àrees de l'ajuntament, etc.) per a la gestió del servei de comunicacions extrem a extrem, així com per garantir la resolució d'incidències dins de l'àmbit d'activitat, fent ús de les eines de governança comunes
- Realització d'informes de servei amb els camps rellevants per la prestació del servei amb una periodicitat mínima mensual, així com informes puntuals en cas d'incident
- Gestió de la infraestructura
  - Actualitzacions del software base (canvis de firmware, aplicació de pegats)
  - Peticions de nous certificats de servidor que es trobin en les infraestructures abast del servei
  - Configuracions de la infraestructura del nus responent a peticions de projectes
  - Evolució de les versions i configuracions per adaptar-les a les noves necessitats existents
- Suport puntual a les xarxes locals de les seus corporatives per a la proposta de configuracions complexes o resolució de problemes multi proveïdor
- Gestió dels elements associats a serveis singulars de telecomunicacions i que involucren un nivell de gestió tècnic important
- Gestió de peticions de Projectes específiques de noves connectivitats
- Gestió de LOGS de totes les alertes de seguretat en una eina centralitzada i custòdia dels mateixos durant un període mínim de 3 anys, coordinadament amb el SOC.
- Suport a la implantació de nous projectes i actualitzacions d'aquests quan, per la seva importància i complexitat, requereixen actuacions coordinades especials puntuals per part d'OSAT (com ara redireccions de tràfic o canvis de registres DNS durant una migració). Aquestes actuacions solen efectuar-se fora d'horari d'oficina.
- Proposar tasques, canvis i/o plans que cregui necessari per optimitzar el servei i així fer que el volum d'incidències baixi. Es valorarà positivament l'automatització

de tasques, majoritàriament mitjançant programació. Qualsevol proposta per part de l'adjudicatari haurà de ser validada per l'IMI, que determinarà la seva execució.

4.2.2.2.5. Manteniment de les garanties esteses de fabricant

L'adjudicatari serà el responsable de la contractació de les garanties de fabricant de tot l'equipament inclòs a l'abast del contracte a partir de l'1 de gener del 2023, aportant els certificats de fabricant que assegurin que amb els temps de reposició del material contractat, es poden complir els ANS establerts. L'adjudicatari ha d'informar a l'IMI dels codis de llicències i els períodes de cobertura de tots els productes que tingui en nom de l'IMI.

S'inclouran els següents serveis:

- Subministraments d'actualitzacions de programari durant tot el període de garantia, incloent totes les releases menor i major
- Consultes a fabricant sobre les funcionalitats actuals o futures dels equipaments
- Gestió de l'escalat i tractament d'incidències tant de programari com de maquinari incloent suport online de fabricant durant tot el període de garantia en horari 24x7
- Gestió i enviament d'equips i/o parts d'equips avariats (RMA) durant tot el període de garantia. La disponibilitat horària i el temps de resposta per a la gestió o reposició variarà segons el tipus d'equip i els elements i/o necessitats requerits. Al respecte, s'estableixen dos modalitats:
  - Modalitat "Next Business day" (NBD): en horari de 8x5, pels elements d'equips en estoc, elements no productius i/o elements productius amb equipament en stock
  - Modalitat 24x7x4: en horari 24x7 amb 4 hores de reposició

Alguns equips tenen garanties de fabricant contractades. L'adjudicatari haurà de contractar la garantia un cop finalitzi aquesta, i mentre duri l'anterior s'establiran uns procediments entre els dos proveïdors per la gestió de les garanties.

A l'Inventari del nus es podrà consultar la data de finalització del suport de l'equipament a l'actual nus de comunicacions prèvia sol·licitud segons els canals establerts a la licitació. Si es realitza un canvi d'equipament per condicions de prestació del Servei s'hauran de transformar les garanties al nou equipament per part de l'adjudicatari, sense cost addicional per l'IMI.

Aquest inventari pot patir modificacions al llarg de la durada del contracte. Aquestes modificacions es poden deure, per exemple, a la implantació de nous serveis, ja siguin aquests previs a l'entrada en vigor del contracte o posteriors al mateix.

Per aquest motiu, l'adjudicatari realitzarà una revisió inicial de l'inventari, serà obligació seva la posta al dia dels manteniments amb fabricants, si es donés el cas, i acceptarà sense cost addicional un increment màxim del 10% en el servei de manteniment dels equips durant la vigència del contracte, incloent la garantia de fabricant de l'inventari valorat.

D'aquest equipament, l'adjudicatari haurà de proporcionar les garanties del fabricant durant el període de prestació del servei, cada any l'IMI decidirà quins equipaments continuaran en manteniment i quins quedaran fora del manteniment donada la seva obsolescència.

4.2.2.2.6. Millora contínua del servei

Finalment, caldrà realitzar una tasca de millora contínua del servei a partir de la pro activitat de l'adjudicatari i de la presentació dels informes corresponents.

Dins d'aquesta capa es requerirà com a mínim la realització de les següents activitats:

- Elaboració d'informes de seguiment del servei i dels projectes d'acord amb l'establert a l'ANNEX 2: Informes específics del nus

Presentació de propostes de millora i evolució dels serveis prestats d'acord amb l'experiència de l'adjudicatari en serveis similars i a l'evolució del mercat

- Millora dels procediments operatius i de les instruccions operatives associades a cada procés.
- Millores de les eines de suport al procés.

L'adjudicatari haurà d'entendre i utilitzar aquest procés i les tècniques de millora corresponents, com a marc de treball per a:

- Augmentar els paràmetres de qualitat del servei.
- Reduir-ne els costos d'operació.
- Definir noves mètriques.
- Elaborar informes de millora en el rendiment.

En les tasques de gestió cal identificar totes les tasques associades a les possibles evolucions i millores dels serveis, i que l'adjudicatari serà el responsable, com per exemple:

- Estudi de noves funcionalitats realitzant informes de la viabilitat, necessitats i implicacions de les noves funcionalitats o requeriments del servei a petició de l'IMI.
- Implantació, gestió i monitoratge de noves funcionalitats sobre els equipaments gestionats del Nus de comunicacions.

- Instal·lació, gestió i monitoratge de nou maquinari per ampliacions de servei o per noves funcionalitats segons necessitats de l'IMI
    - Aquest nou Maquinari pot estar subministrat per l'adjudicatari i/o per altres plecs de subministrament.
- Migracions de funcionalitats a nou equipament per obsolescència de l'equipament actual. Per exemple:
    - Migració d'usuaris del Steel Belted Radius

    - L'IMI disposa d'un *Steel-Belted Radius* amb el que presta servei a usuaris que disposen d'un dispositiu (PDA, tablets...) amb una SIM corporativa (APN privat corporatiu). Aquest radius assigna actualment una IP dins d'un *pool* a un usuari quan s'autentica.
    - Aquest dispositiu està fora de suport i el que es planteja en aquest punt és migrar els usuaris actuals que té aquesta plataforma a un altre radius (ClearPass d'Aruba) propietat de l'IMI.
    - Per tal de simplificar el comportament, i tenint en compte que aquesta funcionalitat d'assignar IP d'un *pool* concret no és present a la majoria de radius actuals, els usuaris a migrar s'integrarien al ClearPass configurant una IP fixa per usuari, sense tenir en compte cap *pool* addicional.
    - El ClearPass al qual caldria migrar els usuaris disposa de les llicències necessàries per absorbir els usuaris del Steel-Belted Radius que està fora de suport. Per tant, aquesta tasca consistiria només en la migració d'usuaris entre plataformes Radius.
    - Respecte els usuaris, comentar que existeixen actualment uns 12 grups d'usuaris diferenciats, que sumen (en brut) uns 2.550 usuaris.

- Nous i altres CPDs:
    - Instal·lació, gestió i monitoratge del nou maquinari per ampliacions de servei o per noves funcionalitats en nous o altres CPDs segons necessitats de l'IMI.
    - Trasllat, transformació i/o migració d'algun dels CPDs cap a nous CPDs que puguin sorgir durant el contracte o d'altres ja existents.
        - Per exemple, tal com es descriu a l'***apartat 4.2.4: Subministraments i implantació de la solució*** i ***Apartat 4.2.5: Pla d'instal·lació i implantació de la solució,*** actualment es disposa de dos CPDs físics, però la infraestructura que està al CPD 1 haurà de ser traslladada al CPD 3. Serà obligació del contractista la planificació, gestió i execució de les tasques adients per tal de portar a terme aquest trasllat acordat amb l'IMI.

- Entorn de laboratori.

4.2.2.3. SERVEIS DE SUPORT EXPERT EN COMUNICACIONS I SEGURETAT

L'OSAT, com a servei que administra el nus de comunicacions de l'Ajuntament de Barcelona, ha de proporcionar suport expert a la resta d'iniciatives, projectes i serveis TIC de l'IMI.

A continuació es detallen els tipus de serveis a prestar per l'adjudicatari dins d'aquest àmbit d'actuació:

- Anàlisi de solució tècnica davant una demanda d'un projecte, amb expert de cada sub-servei per a la implantació de la solució
- Serveis de seguretat de solucions
- Servei de suport a incidències i peticions
- Servei de suport a l'execució de projectes de mitigació de riscos, renovació tecnològica i evolucions
- Servei d'auditoria de xarxa
- Servei de resolució de problemes complexos

Durant la vigència del contracte l'IMI adoptarà una transició cap a la externalització en tecnologia Cloud. S'espera de l'adjudicatari una actitud oberta a aquesta evolució, i amb participació envers la mateixa, proporcionant el feedback oportú, alhora que aportant solucions a problemes i riscos identificats.

En aquest aspecte l'OSAT realitzarà les següents tasques:

- Participació en reunions tècniques de disseny de les solucions
- Realització de propostes tècniques de solucions i ajuda a la transformació dels serveis
- Elaboració de guies de disseny, plantilles i normatives de comunicacions i seguretat per altres contractes de l'IMI
- Creació de procediments de suport posterior per al servei
- Aprovació dels documents tècnics de serveis previ a la implantació del servei per part dels adjudicataris d'altres contractes de l'IMI
- Seguiment de les tasques de provisió i millora relaciones amb l'àmbit de les comunicacions i seguretat dels adjudicataris externs
- Implantació/modificació de les configuracions dels elements que es gestionen per adaptar-se a les necessitats dels serveis

4.2.2.4. SERVEIS DE CONSULTORIA DEL NUS

OSAT proporcionarà durant el contracte serveis de consultoria orientats al desenvolupament de projectes de transformació que inclouran com a mínim les següents tasques:

- Consultoria de solucions per a realitzar els processos de documentació d'informació
- Consultoria sobre la vigència dels equipaments i la seva evolució. Es realitzarà anualment. Aquesta consultoria inclourà un inventari detallat de l'equipament del nus
- Consultoria tècnica per a redefinir el nus de comunicacions i realitzar la planificació del procés de transformació
- Servei de consultoria a arquitectura de projectes amb una persona de nivell 3 destinada a donar suport presencial a totes les reunions de planificació de projectes on OSAT estigui involucrat, per tal de poder plantejar solucions i alternatives i que els projectes es realitzin amb les màximes garanties
- Serveis de consultoria especialitzada per a la realització de millores del nus
- Serveis de consultoria per realitzar un inventari exhaustiu dels elements i mòduls

4.2.2.5. SERVEIS D'ACTIVITATS/ACTUACIONS ESPECIALS

És necessari cobrir els aspectes de connectivitat i seguretat per a esdeveniments especials realitzats per l'Ajuntament amb col·laboració de l'IMI. Per exemple, eleccions, congressos organitzats per l'Ajuntament, fires al carrer. Aquests esdeveniments, requereixen els serveis TIC de seguretat i connectivitat que presta l'IMI i que durant el mateix esdeveniment són de vital importància que estiguin 100% operatius. Així, es requereix que l'adjudicatari realitzi les següents tasques:

- Muntatge de l'escenari de connectivitat, si s'escau.
- Desmuntatge de l'escenari, si s'escau.
- Serveis de vigilància remota dels serveis que es presta.
- Tècnic de servei in situ en cas necessari.

Aquests esdeveniments tenen una duració de 2-3 dies, amb una extensió d'un edifici petit amb el servei de connexió a internet i vigilància de la seguretat, o bé, es podran realitzar en espais oberts acotats a l'aire lliure.

També es contemplen actuacions especials quan, degut a necessitats d'aplicacions/projectes de l'organització considerats importants, requereixin de modificacions i/o tenir especial cura de les comunicacions fora d'hores d'oficina en fites puntuals, com ara la sortida a producció o d'altres que es puguin considerar.

Aquest tipus d'actuacions són molt puntuals. Podem considerar que, entre activitats i actuacions especials, no seran més de 12 anuals. Es valorarà de manera positiva el fet que l'adjudicatari presenti un número major d'actuacions anuals, tal i com s'indica en els criteris de valoració.

4.2.2.6. SERVEIS DE SUPORT A PROJECTES

L'OSAT proporciona una gran quantitat de serveis transversals a tota l'organització, donant suport i participant, a més, dels projectes de tercers on cal tenir en compte les comunicacions i les particularitats que cadascun d'aquests projectes pugui presentar.

Aquest fet, sumat a les noves iniciatives que de forma paral·lela puguin sorgir des de la pròpia OSAT conjuntament amb l'IMI (modificant i/o transformant algun servei, o creant-ne algun de nou, per exemple), pot fer que en certes situacions es vegi incrementada la càrrega de feina de l'equip. En aquest cas, es podria activar, sota demanda i, per tant, sempre amb el vistiplau de l'IMI, aquest servei de suport a projectes.

Serà l'IMI qui, en cada cas, determinarà el grau d'implicació de l'adjudicatari en cadascun d'aquests projectes a desenvolupar.

Dintre d'aquest servei de suport a projectes hi podem trobar dels següents tipus:

- Desplegament de nous serveis i/o infraestructures.
- Modificacions/transformacions de serveis existents i/o infraestructures.
- Servei de suport a projectes externs.

Les tasques principals que s'hauran de dur a terme en cada projectes són:

- Assignació de recursos necessaris i adients.
- Assistència a totes les reunions necessàries del projecte, per tal d'identificar clarament els requeriments, finalitat i abast del projecte.
- Reunions periòdiques amb l'IMI o les persones que assigni, per fer un seguiment de l'estat de tots els projectes de suport i poder solucionar possibles dubtes / entrebancs.
- Execució de les tasques que es requereixin (dins l'horari establert per les mateixes).
- Coordinació de tasques amb tercers, si s'escau.
- Creació de tota la documentació del projecte , en la que ha d'aparèixer tota la informació referent a aquest (com a mínim: acta d'inici, requeriments, riscos, accions a realitzar, durada i fitxa de tancament).
- Creació de nous procediments i Instruccions Operatives en el cas que fos necessari.

- Creació / modificació de la documentació necessària.

El licitador haurà de definir a la seva proposta la metodologia que utilitzarà per abordar aquest tipus de suport, puntualitzant clarament com a mínim:

- Equip dedicat (recursos) a aquestes tasques indicant:
  - Organització de l'equip
  - Nombre de personal (i percentatge/estimació de dedicació)
  - Perfils assignats
- Metodologia:
  - Documentació a presentar
  - Seguiment del projecte
  - Reunions planificades (la periodicitat de les mateixes haurà de ser aprovada per l'IMI)
- Nombre de projectes assumibles en paral·lel

L'IMI, per raons de negoci, es reserva el dret de poder modificar, temporal o definitivament, alguns dels aspectes abans descrits (com per exemple la documentació a presentar i la priorització dels projectes).

L'adjudicatari s'haurà d'adaptar a les possibles modificacions establertes per l'IMI.

4.2.2.7. SERVEIS DE SUPORT A SOC

- **Executar operatives procedimentades des de l'àrea de seguretat**
  - . Per exemple:

- Atendre i revisar la bústia operativa de seguretat
- Revisió processos de validació de signatures
- Autoritzacions de sortida d'informació i execució no planificada de scripts/batch en producció.
- Supervisar la custòdia de certificats Digitals de l'Ajuntament, fent entre d'altres tasques l'inventari, alerta de caducitats, procés de petició / revocació, custòdia.
- Revisar la caducitat de certificats corporatius (d'aplicatiu, de servidor, de xifrat).
- Mantenir i conèixer els procediments establers per Seguretat.

- Recuperació dels logs de forma periòdica per assegurar el correcte funcionament dels sistemes de traçada.

- **Generar Informes d'indicadors pel quadre de comandament de la DQS-Seguretat.** Participar en la revisió i implementació de millores de l'Informe segons directrius de l'Àrea de Seguretat-DQS.
- **Suport a l'àrea de seguretat en la seguretat preventiva**: zero-days, resolució de consultes, comunicació de vulnerabilitats noves així com de seguretat de noves tecnologies, estudi de noves contramesures (la seguretat preventiva recau en primera instància en l'àrea de seguretat).

Suport a l'àrea de seguretat en la definició del procés de resposta a incidents: definició del procés i construcció de l'Equip de Resposta a Incidents de seguretat (la construcció d'equips de resposta a incidents es realitzarà des de l'àrea de seguretat-DQS)

4.2.3. EINES

L'abast dels serveis són totes les eines de l'àmbit del nus, tant les actuals, descrites en el fitxer d'inventari a disposició del licitador segons recull l'Annex 12.1, com les futures que l'IMI decideixi incorporar durant el temps de vigència del contracte.

Així mateix, serà obligació de l'adjudicatari aportar totes les eines bàsiques necessàries per realitzar la prestació de tots els serveis sol·licitats de la forma més eficaç. En concret, eines de monitorització, supervisió, throubleshooting i còpies de seguretat dels equips de l'inventari aportat, a més de les eines de vigilància i prevenció de la seguretat.

L'adjudicatari es compromet a mantenir l'equip format en les eines de l'àmbit del nus.

L'objectiu és obtenir un alt rendiment de les eines del nus, buscant sempre tant el benefici directe que proporciona l'eina, com l'indirecte en la seva integració amb la resta d'eines del servei.

L'adjudicatari detallarà les eines especifiques a utilitzar per la gestió de la infraestructura.

Actualment l'IMI disposa d'una sèrie d'eines que posarà a disposició de l'adjudicatari per la prestació del servei, si ho estima adient. Aquestes eines són dels següents tipus:

- Consoles de gestió d'equipament
  - Tallafocs
  - Balancejadors
  - Electrònica de xarxa
- Software i Servidors de còpies i llicències associades.

- Servidors d'autenticació de gestió
- Consoles de gestió d'equips via IP
- Software i servidors Syslog
- Servidor mesura ample de banda
- Equips IPAM
- Equip descobriment de ports
- Equips de monitorització
- Equips de gestió d'infraestructura
- Eina d'autenticació centralitzada d'usuaris (per usuaris gestió OSAT)
- Eines de gestió Wifi
- Eines de gestió de navegació internet convidats
- Eina d'automatització diagrames de xarxa
- Eina de gestió de log cetralitzats

La relació d'eines actuals i fabricants es troba detallada en l'inventari que s'haurà de sol·licitar d'acord amb l'establert en l'Annex 12.1 d'aquest PPT.

- Per altra banda, els licitadors podran aportar les eines que considerin més adients per la prestació dels serveis objecte del contracte.
- Aquestes eines s'han de poder utilitzar des de la xarxa municipal, tant si les implanten en equips corporatius, com si estan implantades a les seves dependències.
- Les eines que aporti l'adjudicatari, no han d'implicar cap cost addicional ni utilització de recursos de maquinari ni humans de l'IMI.
- L'adjudicatari estarà obligat a aportar el maquinari necessari i les llicències que calgui per a la implantació de les eines que proposi, així com l'explotació de l'eina i l'anàlisi dels resultats.
- En concret, el tipus i característiques de les eines que es tindrà en compte per la seva valoració en la puntuació segons el PCAP, es detallen en els següents punts.
- D'aquestes eines optatives puntuables, les que s'hagin proposat per l'adjudicatari, hauran d'estar disponibles durant els primers sis mesos un cop adjudicat el contracte, considerant-se una falta lleu en cas que no estiguin disponibles en aquest període.

4.2.3.1. Llicències per automatitzar processos

- En l'actualitat, l'IMI disposa de 10 llicències (perpètues, per a 10 nodes) de la plataforma Tower de RedHat, amb les que té automatitzada l'operativa dels proxies de navegació amb Ansible. Aquestes tasques automatitzades inclouen, per exemple:
  - Modificació i sincronització de les configuracions
  - Tasques de monitorització i reinici del serveis
  - Accions sobre autenticació d'usuaris
- Amb la finalitat d'estendre aquest tipus d'automatitzacions a d'altres tasques i altres elements gestionats per OSAT, i que, per tant, l'adjudicatari pugui simplificar d'altres processos i estalviar temps, es valora que l'adjudicatari aporti llicències d'aquesta plataforma per a 100 hosts més per tal d'ampliar els processos a automatitzar. Aquestes llicències, si són aportades i valorades amb la corresponent puntuació, caldrà mantenir-les durant el la vigència de tot el contracte (possibles pròrrogues incloses).
- Aquestes noves automatitzacions s'acordaran entre l'IMI i l'adjudicatari, així com el seu calendari, i entrarien dins de les tasques de millora dels processos que aporta OSAT.

4.2.3.2. Eina que doni visibilitat dels entorns cloud i kubernetes

- Donat l'augment d'aplicacions que fan servir entorns de cloud públic, l'IMI requereix una solució que permeti gestionar la postura de seguretat al cloud de la infraestructura pròpia de l'Ajuntament, així com dels possibles clouds privats basats en kubernetes. Aquesta eina ha de proporcionar visibilitat, control i compliment dels actius, de tal forma que pugui aportar valor al control que es pugui fer des d'OSAT d'aquests entorns.
- La solució ha de permetre l'administració de la seguretat i el compliment dels entorns de núvol públic a qualsevol escala a Amazon Web Services, Microsoft Azure, Google Cloud Platform i entorns Kubernetes (com ara Open-Shift).
- Aquesta eina ha de permetre la visualització i avaluació de la postura de seguretat, detecció de configuracions errònies i l'aplicació activa de les polítiques que es decideixin, així com la capacitat de detecció d'intrusions al núvol.
- Així, aquesta solució hauria de cobrir els següents casos d'ús:
  - Visualització d'actius
  - Avaluació de la postura de seguretat
  - Detecció de configuracions incorrectes

- Compliment d'estàndards normatius (com ara GDPR o NIST CSF) i polítiques corporatives personalitzades
- Capacitat de detecció d'intrusions al núvol
- Visualització del tràfic de xarxa en temps real
- Anàlisi d'activitats d'usuari
- Integració de controls i proteccions en eines de CI/CD

- Algunes característiques que ha de complir aquesta eina:
  - Integració sense software que instal·lar ni agents que administrar per entorns dels principals cloud públics
  - Integració amb els comptes del servei cloud per recopilar informació de seguretat, sense compartir claus ni credencials
  - Possibilitat de revisar el compliment de normatives i estàndards de la indústria, com ara GDPR o NIST CSF
  - Descobriment i remediació d'usuaris o roles amb privilegis massa permissius
  - Mecanismes per monitoritzar canvis no autoritzats sobre la política de seguretat corporativa
  - Alertes per activitats potencialment malicioses
- En l'actualitat, la infraestructura més nombrosa que té l'IMI encara és interna. Per tant, el nombre d'actius a afegir d'entrada a aquesta eina no seria massa elevat. Estimem que 100 actius serien suficients.
- Aquesta eina amb les seves respectives llicències, si és aportada i valorada amb la corresponent puntuació, caldrà mantenir-les durant el la vigència de tot el contracte (possibles pròrrogues incloses).

4.2.3.3. Eina de gestió de la configuració i canvis

Actualment disposem de l'eina Tufin amb:

- 1 x SecureTrack Server base component (one per installation, centralized or distributed)
- 1 x SecureTrack per Firewall Cluster (Check Point, Cisco, Juniper Networks, Fortinet, Palo Alto Networks)
- 4 x SecureTrack per Virtual Firewall Cluster (Check Point, Cisco, Juniper Networks, Fortinet, Palo Alto Networks)

Es valorarà positivament la proposta que proporcioni una ampliació en el nombre de firewalls físics a gestionar amb la eina.

4.2.3.4. Eina d'Inventari

Característiques mínimes de l'eina:

- L'eina ha de donar suport per defecte als següents fabricants mínims (fabricants del nus):
    - Cisco, Checkpoint, Palo Alto, Infoblox, F5, Juniper i Vmware.
- Eina per inventari automàtic de tot l'equipament de Nus
    - L'eina s'ha de connectar a tots els equipaments periòdicament i actualitzar l'inventari Hardware (incloent mòduls) i software automàticament
- Capacitat per executar comandes massives i multi fabricant, podent-se automatitzar i planificar periòdicament.
- Capacitat per informar del cicle de vida dels dispositius (End of suport i end of life)
- Capacitat de reporting de tota la informació requerida
- Informació de vulnerabilitats conegudes dels equipaments (principalment Cisco)
- Capacitat de connexió cap a la BBDD de cisco per informar dels estats de manteniments (Cisco SMART)

4.2.3.5. Eina Sondes Artificials

Eina amb consola central i dispositius remots

Característiques mínimes dels dispositius remots

- Equip tipus appliance i mida reduïda (no superior a 40 cm)
- Capacitat per realitzar proves sintètiques per verificar la disponibilitat i el rendiment de les aplicacions/serveis, independentment del lloc on es trobin. Simulant automàticament i de forma rutinària les accions reals de l'usuari, provant la xarxa, les aplicacions i els serveis, fins i tot quan no hi ha usuaris en el sistema.
- Capacitat de fer test entre diferents dispositius.
- Capacitat per test de ToIP i videoconferència.
- Capacitat per provar les aplicacions, amb introducció d'usuari i contrasenya i execució de workflow de l'aplicació.

- Capacitat per vitalitzar el dispositiu.
- Capacitat per cada dispositiu per realitzat fins a 20 test simultanis diferents.

Característiques mínimes de la consola central:

- Capacitat per gestionar de forma centralitzada tots els dispositius remots.
- Capacitat per visualitzar tota la informació dels dispositius remots.
- Capacitat per crear una àmplia gamma de gràfics i visualitzacions dels resultats dels dispositius remots.
- Capacitat per crear taules de comandament integren múltiples gràfics, vistes i informes i panells reutilitzables. Capacitat per realitzar i personalitzar ràpidament quadres de comandament per a analistes de gestió, negocis o de seguretat, auditors, desenvolupadors i equips d'operacions.
- Capacitat per crear informes en temps real o programats per executar-se en qualsevol interval, usat en taulers de control o desats i compartits en formats segurs i de només lectura, com ara informes PDF.

4.2.4. SUBMINISTRAMENTS I IMPLANTACIÓ DE LA SOLUCIÓ

Les tasques incloses dins d'aquest apartat són:

- Subministrament de l'equipament demanat
- Provisió, configuració, migració instal·lació i documentació dels diferents elements oferts

A continuació es realitzarà una descripció de cada apartat.

4.2.4.1. Subministraments de l'equipament

Per motius d'obsolescència tecnològica, ampliació de capacitat i millores de seguretat cal renovar part de l'actual maquinari del nus de comunicacions. Per la descripció del maquinari aquest s'ha dividit segons els dos conceptes anteriors.

Els CPDs actuals afectats per aquesta ampliació són:

- Cpd 1
- Cpd 2

L'equipament a subministrar cobreix 2 objectius:

- Obsolescència: Subministrament de nous equipaments per obsolescència tecnològica dels equipaments actuals.
- Capacitat: Subministrament de nous equipaments per manca de capacitat dels equipaments actuals.

4.2.4.2. DDI (DNS, DHCP, IPAM)

- ***Plataforma actual:***
- La solució DDI que té l'IMI actualment per la gestió de la xarxa interna està basada en la solució SolidSever d'EfficientIP. L'arquitectura actual disposa de dos nodes SolidServer-1100 dedicats a donar servei (DNS/DHCP/NTP) i dos nodes SolidServer-1100 dedicats a la gestió i inventariat (IPAM), tenint així les dues parts en alta disponibilitat.
- Els 2 nodes que donen servei no cal actualitzar-los, doncs no han arribat ni a la meitat de la seva vida útil. En canvi, els 2 nodes de gestió i inventariat són els que es troben molt a prop d'estar fora de suport, i és per això que es planteja fer una actualització d'aquests equips a unes noves màquines. Per tal de minimitzar costos de la solució complerta, les noves màquines haurien de ser compatibles amb els equips actuals de l'IMI, i integrables en la solució d'Efficient IP que està prestant aquest servei.
- ***Noves necessitats:***
  - Nous equips pels nodes de gestió integrables a la solució actual, garantint la continuïtat del servei, sense impacte ni afectació en l'arquitectura ni en els equips actualment en producció.
  - Equipament amb alta disponibilitat amb 2 elements independents.
  - Suport associat als equips durant tota la vigència del contracte. es valorarà positivament l'ampliació de la garantia de fabricant
  - Instal·lació i migració dels equips actuals als nous.
  - Actualització de tota la solució a la última versió recomanada pel fabricant.
- Degut a la criticitat d'aquests equips pel funcionament de la xarxa de comunicacions a tot l'Ajuntament, no es consideren viables solucions que no incloguin un fabricant de prestigi de solucions DDI.
- Les migracions es realitzaran en horari no laboral i nocturn (pactat amb la resta d'agents afectats), per impactar el mínim possible en els serveis de producció de tota l'organització.

4.2.4.3. Equip amb capacitats per establir VPN site-to-site

- Actualment l'IMI disposa d'un dispositiu que permet establir i gestionar els accessos VPN site-to-site amb d'altres entitats que tenen relació amb l'Ajuntament de Barcelona i que requereixen d'aquest tipus de connectivitat.
- Aquest equip que s'està fent servir a l'actualitat queda obsolet i es requereix fer un canvi d'equipament per tal de portar a terme aquesta funcionalitat.
- A més a més aquest element es vol fer servir com a VPN Gateway contra els diferents clouds públics.
- Així, les noves necessitats que es requereixen que compleixi aquest equipament són:
  - Equipament amb alta disponibilitat amb un mínim de 2 elements independents
  - Disposar de doble font d'alimentació. Les dobles fonts han de ser subministrades de manera obligatòria
  - Com a mínim interfícies de 2 x 10GE SFP+. s'han de proporcionar les òptiques corresponents per a que el servei funcioni. Aquests equips es connectaran a uns equips cisco del nus de comunicacions
  - Suportar al menys 20 Gbps de throughtput IPsec VPN
  - Suportar al menys 2.000 tunels IPSEC GW to GW
  - Imprescindible suport de connectors cloud per AWS, Azure, Google
  - Disposar de funcionalitats SD-WAN
  - Disposar de interfície gràfica per fer la gestió i operació
- Manteniment / garantia de fabricant de 3 anys. Es valorarà positivament l'ampliació d'aquest període.
- S'inclouen els serveis de migració dels serveis actuals, aproximadament 80 lan to lan, a la nova eina.

4.2.4.4. Servidors i Cabines d'OSAT

Estat actual:

Actualment es disposa de la següent infraestructura de virtualització a OSAT.

- CPD 1

Software:

Llicència de vmware essential plus.

Aquesta llicència permet gestionar tres servidors físics amb dos CPUs. La llicència no disposa de la funcionalitat de backup, però si permet la rèplica de VM entre vCenters.

Servidors:

A GL hi ha tres servidors, el tercer servidor està ja fora de suport, només té la consola d'ALLOT. Les característiques de CPU i memòria son les següents:

- Servidor 1: 2 CPUs de 10 Cores i 192 GB de RAM
- Servidor 2: 2 CPUs de 16 Cores i 256 GB de RAM
- Servidor 3: 2 CPU de 4 Cores i 64GB de RAM.

Aquest servidors reben l'espai d'una cabina d'emmagatzemament que hi ha al mateix site mitjançant ports a 10G i protocol iSCSI.

Storage:

Hi ha una cabina model Huawei OceanStor 2200 V3 on es disposa de 3 Pools de disc actualment:

- Pool 1 i Pool 3: Pool SAS amb 15 discs a 10K proporcionant una capacitat de 12 TB
- Pool 2: El Pool 2 disposa d'un total de 8 disc NL-SAS amb una capacitat de 28 TB

Entorn Virtual: es disposa d'un total de 19 màquines virtuals, les quants tenen en el moment de l'edició del document una ocupació de:

- Total vCPU: 132
- Total RAM: 473 GB
- Total disc: 22TB

- CPD 2

Software:

- Llicència de vmware essential plus.

  Aquesta llicència permet gestionar tres servidors físics amb dos CPUs. La llicència no disposa de la funcionalitat de backup, però si permet la rèplica de VM entre vCenters.

Servidors:

Al CPD 2 hi ha dos servidors. Les característiques de CPU i memòria son les següents:

2 servidors:

- Servidor 1: 2 CPUs de 10 Cores i 160 GB de RAM
- Servidor 2: 2 CPUs de 16 Cores i 256 GB de RAM

Aquests servidors reben l'espai d'una cabina d'emmagatzemament que hi ha al mateix site mitjançant ports a 10G i protocol iSCSI.

Storage:

Hi ha una cabina model Huawei OceanStor 2200 V3 on es disposa de 3 Pools de disc actualment:

- Pool 1 i Pool 3: Pool SAS amb 14 discs a 10K proporcionant una capacitat de 10 TB
- Pool 2: El Pool 2 disposa d'un total de 10 discs NL-SAS amb una capacitat de 17 TB

Entorn Virtual: es disposa d'un total de 21 màquines virtuals, les quants tenen en el moment de l'edició del document una ocupació de:

- Total vCPU: 126
- Total RAM: 331 GB
- Total disc: 16.5 TB

Noves necessitats

Es fa necessari renovar els servidors ja que arriben al final del cicle de vida de suport Tècnic o EoS (End of Service) sent aquest suport indispensable davant de qualsevol tipus d'incidència que es pogues generar durant el decurs del servei. En previsió de creixement de noves VM, es necessita ampliar memòria i el número de cores per a mantenir al relació vCPU/Core.

Per dur a terme aquesta renovació es fa necessari el següent equipament i llicenciament.

- Renovació de suports de les llicències VMware durant la vigència del contracte incloses les possibles pròrrogues.
- Renovació dels equips de còmput per 4 nous que han de complir com a mínim amb les següents característiques tècniques.

    - El Xassís ha de disposar de 8 slots per discs 2.5'', per si fossin necessaris per a futures transformacions del servidor.
    - CPU: 2 x Solució Intel Xeon d'última generació de 24 nuclis a 2,2 GHZ, amb 35,75 MB de caché...
    - Ram: 512 GB de RAM configurats per utilitzar el màxim nombre de canals de comunicació amb la CPU, i que permetin tenir el màxim d'slots disponibles per a futures ampliacions. La memòria Ram ha de ser de tipus DDR4 a 2933 MHZ en DIMMS de 32 GB.
    - HD: Doble disc de tipus Enterprise, amb capacitat de 32 GB i en configuració RAID 1 per hardware, no essent vàlides solucions que utilitzin disc de tipus targes SD.

- Xarxa: 2 Ports de tipus elèctric a 1 G i 2 ports de tipus òptic a 10 G integrats a la placa base per no utilitzar slots PCI.
- El servidor no ha d'ocupar un espai superior a 1 RU.
- Font d'alimentació de Doble font d'alimentació de tipus Hot SWAP, de 550W i nivell d'eficiència Platinum.
- Suport: 5 anys de suport en modalitat 24x7.
- Guies de Rack

- Ampliació a cabines on:
  - S'afegiran 6 discs de 3,84TB. Aquests discs aniran destinats a millorar el rendiment del Pool SAS on hi haurien d'estar totes les màquines virtuals.
  - S'afegiran discs de tipus NL-SAS (7,2K RPM) per:
    - Ampliar la capacitat actual fins als 45-50 TB.
    - Ampliar la capacitat de la cabina del CPD 1 addicional a l'anterior ampliació, amb espai destinat per al Pool de Backup amb 22 TB útils per aguantar el Backup de la plataforma actual amb polítiques de Backup durant 5 anys. La idea és que la cabina de Glòries tingui el Backup de les màquines virtuals de Via Favència.
    - Ampliar la capacitat de la cabina del CPD 2 addicional a l'anterior ampliació, amb espai destinat per al Pool de Backup amb 31 TB útils per aguantar el Backup de la plataforma actual amb polítiques de Backup durant 5 anys. La idea és que la cabina de Via Favència tingui el Backup de les màquines virtuals de Glòries.
  - Instal·lació de 2 targes PCI (1 per controladora) a cadascuna de les 2 cabines, per dotar a aquestes amb connectivitat 10G.
  - Cables tipus TWINAX per als ports 10G.
  - Les ampliacions han de permetre mantenir les actuals garanties de fabricant així com ampliar-les en el temps durant la vigència del contracte.

- Instal·lació de la solució de Backup, disposant de 2 servidors virtuals, 1 per CPD.
  - Possibilitat de gestionar entorns Vmware, HyperV, AHV Nutanix, sistemes físics Windows/ Linux, NAS, workstations i O365 des d'una única consola web.
  - Suport 24x7.
  - Llicenciament per sockets i TeraBytes a copiar.
  - Suport per el seguiment de blocs modificats sense agent per a VMWare, HyperV i AHV Nutanix des de la mateixa consola.
  - Incrementals infinits, només una còpia completa a l'inici.
  - De duplicació global i en origen amb compressió i encriptació que permeti la protecció de les dades.

- Configuració de les hores i dies que es realitzarà la replicació així com l'ample de banda utilitzat.
- Recuperar un servidor virtual en un altre hipervisor o servei físic.
- Recuperació instantània de màquines a partir del repositori on es guarden les còpies de seguretat. Aquesta funcionalitat permet arrancar màquines virtuals a partir de còpies sense utilitzar capacitat d'emmagatzematge addicional (disponible tant en entorn HyperV com Vmware).

Tots els serveis d'instal·lació i configuració i petit material necessaris per dur a terme aquestes ampliacions han d'estar inclosos.

4.2.4.5. SFP's 10G per equipament gestionat per OSAT

Els actuals balancejadors es troben connectats als equips del nus de comunicacions amb enllaços 1G. Cal ampliar aquests enllaços amb òptiques de 10G.

En concret, cal subministrar:

8 unitats de F5-UPG-SFP+-R (OPT-0016-00) - 10GBase-SR (Short Range) 10G Ethernet Transceiver with DDM Support

- Laser emitter: 850 nm (multi-mode)
- Connector type: LC
- Operating distances and cable specification/requirements:
  - 26 meters maximum for type FDDI grade 160MHz-km 62.5 µm core multi-mode fiber (MMF)
  - 33 meters maximum for type OM1 200MHz-km 62.5 µm core multi-mode fiber (MMF)
  - 66 meters maximum for type FDDI grade 400MHz-km 50.0 µm core multi-mode fiber (MMF)
  - 82 meters maximum for type OM2 500MHz-km 50.0 µm core multi-mode fiber (MMF)
  - 300 meters maximum for type OM3 2000MHz-km 50.0 µm multi-mode fiber (MMF)
  - 400 meters maximum for type OM4 4700MHz-km 50.0 µm multi-mode fiber (MMF)
- Supported platforms:

- 2000s/2200s, 4000s/4200v, 5000s/5200v, 7000s/7200v, 8900, 8950, 10000s/10200v, 11000, and 11050 platforms

  Note: The 2000s/2200s and4000s/4200v series platforms do not support the Digital Diagnostic Monitoring feature (DDM).

- VIPRION B2100/B2150, B4100 (PB100), B4200 (PB200), and B4300 blades
- BIG-IP i2600, i2800, i4600, i4800, i5600, i5800, i7600, i7800, i10600, and i10800 platforms
- Herculon i2800, i5800, and i10800 platforms

- 8 unitats de sfps 10 Gbps SR per la banda d'equipament cisco del nus de comunicacions.

4.2.5. PLA D'INSTAL·LACIÓ I IMPLANTACIÓ DE LA SOLUCIÓ

4.2.5.1. Fase d'instal·lació

Aquesta fase inclourà totes les tasques necessàries per a la correcta recepció de l'equipament, la instal·lació del mateix als espais tècnics habilitats, les proves d'acceptació i la posada en marxa de tots els components de la solució que permetin que la xarxa estigui operativa per començar a proveir serveis incloent tots els serveis de monitorització, reporting, gestió i backups que es requereixin.

Entre les tasques a realitzar caldria destacar:

- Definició i creació de les plantilles de monitorització i de les sondes de servei així com la col·laboració en la definició de les alertes de monitoratge.
- Definició i creació de polítiques de còpies de configuracions.
- Definició i creació de polítiques de repositori de logs
- Accés a tots els equips i creació d'usuaris tant de lectura com escriptura per qui determini l'IMI
- Definició i implantació del reporting segons necessitats.
- Creació de tota la documentació associada (tota la documentació haurà d'ésser validada per l'IMI):

4.2.5.2. Tasques d'implantació

Durant tot el temps que duri la fase d'implantació l'equip de l'adjudicatari haurà de realitzar totes les tasques associades a l'administració de la nova infraestructura.

Dintre de les tasques a realitzar cal destacar:

- Migració dels serveis
- Documentació a generar per l'adjudicatari i posar accessible
- Reporting

5. FASES DE LA PESTACIÓ DEL SERVEI

Es descriuen a continuació les fases de la prestació del servei i la seva durada aproximada.

- **Transició**: és el període que va entre l'entrada en vigor del contracte i el moment d'aplicació dels ANS acordats en aquest document.

  Atenent a la diferent data de finalització dels actuals contractes dels quals el nou adjudicatari haurà de fer-se càrrec, la fase de Transició s'haurà d'executar en dos trams diferents, condicionats a la data en què cada servei entri a formar part d'aquest nou contracte.

  El primer tram inclou:

  - Tots els serveis de l'OSAT (apartat 4.2)
  - Primer grup de serveis del SOC:
    - Monitorització i detecció d'incidents (Apartat 4.1.2)
    - Resposta a incidents molt crítics o d'alt risc (incident handling) (Apartat 4.1.3)
    - Administració de la Plataforma de gestió i correlació d'events de seguretat (SIEM) i logs centralitzats (Apartat 4.1.5)
    - Millores i evolució del servei (Apartat 4.1.6)
    - Coordinació amb altres àrees operatives (Apartat 4.1.7)
    - Servei preventiu (només els serveis vinculats a la identificació i gestió de les vulnerabilitats del contenidors productius i de les imatges Dockers productives i al servei d'escaneig de vulnerabilitats internes descrits a l'apartat 4.1.1.

  El segon tram inclou:

  - Segon grup de serveis del SOC:
    - Servei de preventiu (gestió de vulnerabilitats, auditories tècniques i hacking ètic i servei de ciberintel·ligència) Apartat 4.1.1 a excepció dels indicats en el primer Tram.
    - Elaboració d'informes de petició d'evidències (Apartat 4.1.4).

El nou adjudicatari estarà obligat a presentar i desplegar el seu pla de transició considerant que el primer tram s'haurà d'executar a partir de l'endemà de la formalització del contracte i el segon tram s'iniciarà en data 2 d'abril 2022. Aquesta segona data pot variar depenent de la proposta de l'adjudicatari.

Cada un dels trams de la transició tindrà un període màxim de 2 mesos, a comptar des de l'inici de cada un d'ells.

Durant la transició es duran a terme les següents activitats:

- *Transferència*: El nou adjudicatari rebrà la informació que actualment disposa l'IMI i l'actual adjudicatari, els quals facilitaran i col·laboraran en el traspàs de coneixement així com en l'habilitació de l'operació. En aquest moment, l'adjudicatari actual continua realitzant la prestació del servei i assolint els ANS actuals. Aquesta fase tindrà una duració màxima de 30 dies naturals.
- *Prestació en transició:* El nou adjudicatari comença a prestar el servei amb els seus propis mitjans. Durant la mateixa, el nou adjudicatari serà l'únic responsable de la prestació del servei. Tindrà una duració màxima de 30 dies naturals o fins a completar els 2 mesos previstos a nivell general per l'etapa de transició. El nou adjudicatari haurà d'assolir els valors objectius requerits en els indicadors, tot i que el model de penalitzacions no serà aplicat en el transcurs d'aquesta fase.

Durant els 2 mesos de cada tram de la fase de transició (transferència i prestació en transició), l'adjudicatari començarà a facturar els serveis vinculats a cada tram, parcialment; el primer mes un 30% i el segon més un 70% .

- **Execució**: un cop finalitzi cada tram de la fase de transició, l'adjudicatari prestarà els serveis en les condicions que s'especifiquen en aquest document.

- **Devolució**: inclou les accions necessàries per tal de traspassar el servei al nou proveïdor a la finalització del contracte.

En la fase d'execució del servei i a l'acabament del contracte, l'adjudicatari queda obligat a prestar la màxima col·laboració per a la realització del traspàs del servei al nou prestatari que se'n pugui fer càrrec, o a l'IMI directament en els casos de no existir un nou prestatari o be extinció o supressió del servei. El licitadors hauran de desenvolupar un pla de devolució del servei detallat d'acord als requeriments especificats a **l'apartat 5.3**.

5.1. FASE DE TRANSICIÓ

La fase de transició es durà a terme en dos trams segons hem especificat en l'apartat anterior. La durada màxima de cada tram serà de dos (2) mesos a comptar des de l'inici de cada un d'ells, durant els quals es seguiran aplicant els ANS actuals.

En aquesta fase l'adjudicatari rebrà totes les infraestructures i contractes de manteniment així com els compromisos de serveis amb els ANS associats.

Durant aquesta fase el nou adjudicatari rebrà suport de l'adjudicatari actual, que facilitarà i col·laborarà en el traspàs de coneixement. En aquest moment, l'adjudicatari actual continua realitzant la prestació del servei i assolint els ANS actuals.

Finalitzada la transferència de coneixement entre l'adjudicatari cedent i el nou adjudicatari aquest darrer comença a prestar el servei amb els seus propis mitjans, encara que els ANS segueixen sent els de la prestació actual. Durant aquesta fase el nou adjudicatari serà l'únic responsable de la prestació del servei.

El nou adjudicatari haurà d'assolir els valors objectius requerits en els indicadors, tot i que el model de penalitzacions no serà aplicat en el transcurs d'aquesta fase.

L'adjudicatari haurà de presentar un **pla de transició** que descrigui les tasques a dur a terme per cada un dels trams, per assegurar la correcte assumpció del servei.

El pla de transició haurà de contemplar, com a mínim, els següents punts per cada un dels dos trams descrits:

- Pla de transferència del coneixement, indicant detalladament les activitats que s'hauran de dur a terme durant el procés.
- Pla d'implantació dels processos, procediments i normativa tècnica.
- Descripció de la metodologia que el nou adjudicatari preveu aplicar.
- Model de relació, governança i reporting definint per cada servei el grau de participació de l'adjudicatari sortint i de l'IMI i el tipus de col·laboració que es requerirà.
- Pla d'implantació dels nous ANS.
- Pla d'activació del servei, incloent com a mínim els següents aspectes:
  - Seqüència d'activitats a realitzar per assolir el control efectiu del servei.
  - Planificació d'incorporació de recursos, definint actors, rols, responsabilitats per cada servei.
  - Pla de riscos de la transició.
  - Pla de contingència que garanteixi la continuïtat dels serveis.
- Descripció dels recursos tècnics i humans que es posaran a disposició de l'execució del pla.
- Pla de fites principals.

El pla de transició haurà de complir amb els següents principis:

- Cada un dels trams del pla de transició, no excedirà, en cap cas, el termini màxim de 2 mesos des de la data d'inici descrita per cada un d'ells. El pla de transició ha de garantir que no hi haurà cap interrupció del servei i que es realitzarà una transferència de coneixement adequada.
- En cas de no poder completar la transició d'un servei en el temps definit, l'IMI es reserva el dret de resoldre el contracte de serveis o perllongar el període de transició del servei en qüestió. En aquest darrer cas, l'adjudicatari assumirà les despeses necessàries per a la continuïtat del servei per part de l'actual contractista fins a la correcta transició.
- A la finalització de cada un dels trams de la fase de transició, i no més enllà del període fixat per aquests, entraran en vigor els nous ANS definits així com el model de penalitzacions establert.
- Addicionalment, en cada tram de la fase de transició, l'adjudicatari haurà de realitzar Revisar (i completar, si calgués) el catàleg de serveis tal i com s'ha descrit a l'apartat corresponent dels serveis a prestar per l'adjudicatari
- En el pla de transició l'adjudicatari haurà de descriure amb detall el conjunt d'activitats a realitzar així com el suport que requereixi per part de l'adjudicatari actual i/o de l'IMI per a completar-les, així com identificar les fites i calendari compromès per a acomplir-les.

L'abast contempla:

- Revisió de la situació actual de l'equipament i de les capacitats per a realitzar el contracte amb la infraestructura disponible
- Realització d'una consultoria tècnica per a la realització del document de disseny d'alt nivell del contracte
- Adquisicions i ampliacions temporals d'infraestructura necessàries per al contracte
- Adaptació dels elements actuals per a la creació de models estàndards per a poder prestar el servei de forma escalable, minimitzant els costos d'operacions i els costos d'implantació
- Adaptació de la infraestructura per a la integració de forma adient les noves tecnologies de cloud i els nous mecanismes d'orquestració. Veure annex 12.1.

Durant aquesta fase, si així ho considera l'IMI, el 100% (o el percentatge que l'IMI consideri) dels recursos treballaran en les oficines de l'IMI, donat l'alt grau d'adaptació necessari.

5.1.1. Fites i calendari

Les fites principals de la transició han d'incloure, almenys, per a cadascuna de les tasques a dur a terme en el procés de transició, les dates d'inici i fi de cadascuna d'elles, la distribució de responsabilitats, els criteris aplicables d'acceptació i qualsevol altre detall addicional que s'estimi pertinent.

5.1.2. Transferència del Servei

La transferència de serveis entre proveïdors serà responsabilitat del proveïdor entrant, tot i que el proveïdor sortint col·laborarà perquè, en cap cas, aquesta transferència afecti el funcionament del servei. Per garantir aquesta col·laboració, l'IMI supervisarà els processos de transferència.

El procés de transferència del coneixement ha d'incloure, almenys:

- Formació específica i formal per a l'assumpció del servei. Aquesta formació serà proporcionada pel proveïdor sortint segons les condicions que hagi acordat amb el proveïdor adjudicatari del servei i sota la supervisió de l'IMI.
- Documentació necessària per a l'assumpció del servei a ser proporcionada pel proveïdor sortint. És responsabilitat del proveïdor adjudicatari identificar i recopilar tota la informació necessària per a la correcta prestació del servei. En aquells casos en què no hi hagi documentació prèvia necessària per prestar el servei, el proveïdor adjudicatari haurà de planificar i executar la seva elaboració, d'acord amb l'IMI i sense cost addicional per a l'IMI.

A l'inici de cada tram de la fase de transferència, el proveïdor entrant haurà de realitzar les següents tasques:

- Coordinació amb el proveïdor sortint del procés de transferència del coneixement i de la formació formal que hagi considerat necessària.
- Presentació d'un pla de contingència, per assegurar la continuïtat del servei.
- Qualsevol altre condicionant necessari per a l'execució del procés de transferència del coneixement i de la transferència de responsabilitat.

De manera addicional, el proveïdor entrant ha de comunicar a l'IMI l'organització amb què proporcionarà el servei, així com l'assignació de recursos i confirmació de rols, tasques i responsabilitats necessàries per a la prestació del servei.

La transferència del servei tindrà associada una fase de presa de contacte i una fase de desenvolupament de la transferència.

5.1.3. Presa de contacte

L'objectiu d'aquesta fase és assegurar que existeixen les condicions adequades per a l'èxit de la transferència del servei, així com introduir les modificacions que es considerin convenients al que s'estableixi en el pla de transició, si així l'aprova l'IMI.

Es tracta d'una fase de durada curta que no ha d'excedir els 5 dies hàbils per cada tram de transició i que només es podrà perllongar en casos excepcionals (per exemple per limitacions temporals en la implantació d'infraestructura o altres temes logístics).

En aquest cas, es solaparà amb la fase de desenvolupament de la transferència, encara que sempre haurà de finalitzar abans de la transferència de responsabilitat. El proveïdor entrant haurà d'agilitzar, en aquest cas, la realització de totes les tasques associades per assegurar la consecució en temps de les fites planificades.

5.1.4. Desenvolupament de la transferència

L'objectiu d'aquesta fase és el traspàs dels elements bàsics i imprescindibles per a la prestació del servei entre el proveïdor sortint i l'entrant. Durant la mateixa, el proveïdor sortint segueix prestant servei a l'IMI i el proveïdor entrant executa el pla de transició amb totes les activitats que li permetin preparar-se per assumir la responsabilitat del servei, que es produirà a la finalització.

Addicionalment, la prestació de serveis per a la transferència del coneixement per part del proveïdor sortint es realitzaran de manera independent de la prestació del servei regular.

Aquesta fase s'executarà d'acord al pla de transició realitzat pel proveïdor i aprovat per l'IMI.

El proveïdor entrant té l'obligació de documentar totes les activitats del procés de transició i lliurar aquesta documentació a l'IMI quan acabi el procés de transició.

La dedicació per part del nou adjudicatari a la presa de coneixements mitjançant les reunions seran sense cost per l'IMI.

5.1.5. Prestació en Transició

Un cop finalitzada la transferència, el proveïdor sortint finalitza les seves responsabilitats i el proveïdor entrant serà l'únic responsable del servei a tots els efectes.

Si bé el nou adjudicatari haurà d'assolir els valors objectiu d'ANS establerts en aquest plec, el model de penalitzacions no s'aplicarà durant aquest període.

5.1.6. Garantia de nivell de servei durant la transició

El proveïdor entrant és responsable de les tasques i treballs que estiguin iniciats o pendents d'inici en el moment que assumeixi la responsabilitat del servei.

Un cop acabats cada un dels trams de la transferència del servei, el proveïdor entrant és responsable d'oferir els serveis que es detallen en aquest document.

5.2. FASE D'EXECUCIÓ

La fase d'execució s'inicia a la finalització de cada un dels trams de la fase de transició i s'estén fins a la devolució.

Durant aquesta fase l'adjudicatari portarà a terme tots els serveis descrits dins l'abast del contracte, amb aplicació dels ANS i resta de requeriments definits en el present plec.

Tal i com es descriu en la clàusula model de prestació del servei, l'adjudicatari haurà de funcionar en base a aquest model.

Addicionalment l'adjudicatari haurà de presentar mecanismes que permetin assegurar l'evolució dels serveis tant des del punt de vista dels preus, com tecnològic, de governança o d'incorporació de noves funcionalitats i serveis.

Els mecanismes d'evolució han d'incloure informació detallada sobre les pautes d'activació, instruments de seguiment, integració de les necessitats dels usuaris de forma reactiva o pro activament per part del licitador, compromisos temporals d'implantació.

A banda dels criteris generals, els mecanismes d'evolució han de tenir en compte la incorporació de noves funcionalitats que no s'hagin previst inicialment o que l'evolució del mercat i de la demanada facin que l'IMI decideixi incorporar-les (p. ex. nous serveis de xarxa, nous serveis sense fils, nous serveis de ciberintel·ligència)

Durant aquesta fase, l'IMI decidirà quin percentatge dels recursos del servei treballaran a les oficines de l'IMI, podent modificar-lo en tot moment. Donat l'alt grau d'adaptació necessari, aquest percentatge pot arribar a ser del 100%, si així ho considera l'IMI. No hi haurà cap cost addicional relacionat al percentatge de recursos treballant a les oficines de l'IMI.

5.3. FASE DE DEVOLUCIÓ

L'adjudicatari inclourà en la seva proposta un **Pla de Devolució** del servei detallat que descrigui les obligacions i tasques que hauran de ser desenvolupades per cadascuna de les parts en relació amb la devolució del servei motivat per la finalització del contracte i/o de les seves prorrogues i que inclogui els termes i condicions en què es realitzarà aquesta reversió.

El disseny d'aquest Pla de Devolució és una obligació inherent al contracte, per tant es realitzarà sense càrrec a l'IMI, i estarà basat en la seva proposta presentada en la fase de licitació. L'adjudicatari presentarà el pla de devolució del servei que millor aprofiti la feina implementada i menys disruptiu sigui per l'IMI.

El Pla de Devolució haurà de complir amb els següents principis i continguts:

- L'adjudicatari haurà de dur a terme el Pla de Devolució en el termini de dos mesos, a comptar des de l'endemà de la notificació oficial d'expiració o cancel·lació, total o

parcial, del contracte. L'IMI podrà modificar el termini de la fase de devolució si es posa en risc el servei o considera insuficient el període perquè el nou adjudicatari assumeixi el servei amb plenes garanties de continuïtat.

- El traspàs es realitzarà durant l'horari de prestació del servei definit i a les oficines de l'IMI i a les diferents dependències de l'Ajuntament.
- Inclourà tota la documentació referent al contracte, serveis i maquinari relacionats, degudament actualitzada fins la data de finalització del contracte.
- Inclourà la metodologia de traspàs de coneixement dels aspectes fonamentals d'operacions i projectes en curs i que, com a mínim, descriurà:
  - L'assistència, la formació i la documentació sobre els procediments dels serveis i sistemes de l'IMI al nou adjudicatari.
  - L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat per l'adjudicatari o l'IMI en la provisió del servei.
  - La formació pràctica tutelada, en la qual el personal designat per l'IMI realitzi els treballs propis de cada procés o funcionalitat, tutelats pel personal de l'adjudicatari.
- A la finalització del contracte, l'adjudicatari haurà de lliurar el maquinari, programari i/o llicències d'ús de la seva propietat que hagin estat adquirides durant l'execució del contracte i que l'adjudicatari hagi emprat en la prestació del servei.
- L'IMI podrà subscriure un contracte de llicència d'ús sobre els sistemes de l'adjudicatari que fossin necessaris per a assegurar la continuïtat del servei.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència a l'IMI, o a terceres parts anomenades per ell mateix, de serveis subcontractats, garanties o contractes de manteniment existents fins al moment de la terminació en els mateixos termes pactats amb els adjudicataris d'aquest.
- L'adjudicatari haurà d'oferir un pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, l'IMI i/o altres adjudicataris
  - Durant el període de la devolució del servei, l'adjudicatari ha de complir els acords de nivell de servei. El pla de devolució no ha de causar cap discontinuïtat en el servei. En aquest sentit l'adjudicatari sortint, proveirà al contracte l'equip necessari per l'acompliment del servei demanat.
- Descripció detallada dels recursos tècnics i humans que participaran en el pla, així com uns planificació de les activitats i tasques que es proposen realitzar.

- Especificar si es disposarà de un suport addicional post-execució del pla de devolució envers al nou adjudicatari i al propi IMI. En cas afirmatiu caldrà especificar la seva durada que en cap cas podrà ser inferior a 30 dies naturals.
- L'IMI haurà d'assumir la mínima dedicació possible de recursos propis en les activitats de devolució

Durant aquesta fase, si així ho considera l'IMI, un mínim del 50% dels recursos del servei treballaran en les oficines de l'IMI, donat l'alt grau d'adaptació necessari. Aquest percentatge podrà variar en funció de l'efectivitat de la feina en remot i de la càrrega de les reunions presencials dels projectes a executar.

6. ACORDS DE NIVELL DE SERVEI

Per a la gestió i seguiment dels serveis prestats per a l'adjudicatari, es defineixen una sèrie d'Acords de Nivell de Servei (ANS) que els licitadors poden complementar i/o millorar. Aquests permeten monitoritzar i avaluar la qualitat, així com la gestió dels serveis a través d'indicadors que parametritzen el grau de consecució acordat per a cada servei.

L'objectiu de l'IMI és obtenir un servei de qualitat, així com un alt grau de satisfacció per part dels usuaris. Per això, la definició dels ANS busquen:

- L'establiment d'indicadors del servei prestat, de forma que tant l'IMI com l'adjudicatari tinguin una base objectiva amb la que avaluar el servei, i aixecar possibles punts de millora o eventuals deficiències en la prestació del servei.
- L'establiment d'indicadors que permetin mesurar el grau de satisfacció dels usuaris del servei
- Establir un model de elements que permetin relacionar la qualitat de la prestació del servei amb la facturació establint mecanismes de penalitzacions o altres compensacions que es puguin definir per tal de millorar el servei.

6.1. DEFINICIÓ DELS ANS

Els indicadors tindran la següent estructura en comú:

- **Indicador:** Codi de l'indicador.
- **Descripció:** Definició de l'indicador i objecte de mesura.
- **Càlcul:** Explicació del càlcul de l'indicador.
- **Periodicitat:** Període de temps entre càlcul d'ANS.
- **Llindar ANS:** Llindar d'aplicació a l'indicador.
- **Penalització màxima:** Import màxim a descomptar de la factura mensual de la part d'OSAT i del SOC en el cas d'incompliment de l'ANS.

El compliment dels ANS ha de ser revisat de manera mensual. En el comitè de direcció del contracte i en el Comitè de seguiment dels serveis s'haurà de realitzar una presentació de l'estat de compliment dels ANS, així com de les desviacions ocorregudes.

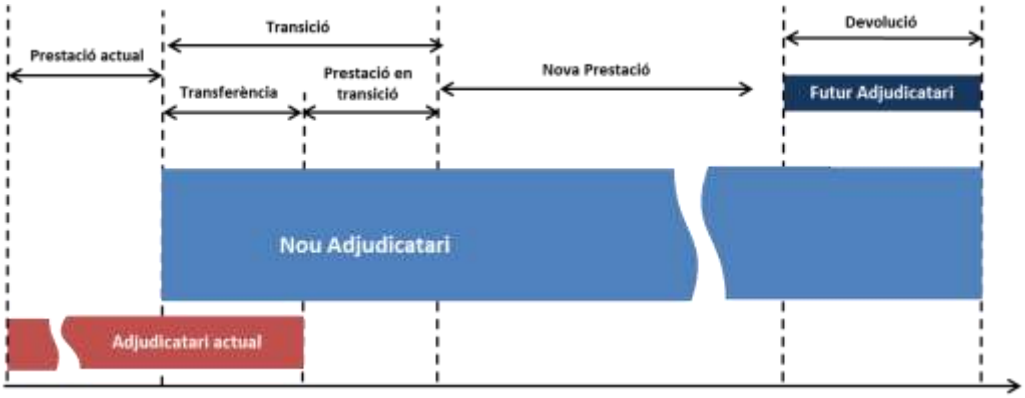
Per tal d'assegurar la fiabilitat i l'automatització de l'extracció dels ANS del servei, es podrà fer servir, en els casos que sigui possible, l'enviament d'informació des de les diferents eines de registres, ja sigui de l'organització o de l'adjudicatari, i dels equips propis gestionats per OSAT, a través de les APIS o altres funcionalitats que puguin proveir. L'IMI es reserva el dret de fer servir un altre sistema per extreure la informació que permeti fer el seguiment del contracte i dels ANS.

L'adjudicatari enviarà la informació requerida i prèviament pactada amb l'IMI.

6.2. APLICACIÓ DELS ANS

Els Acords de Nivell de Servei definits per a cada servei seran d'obligat compliment al llarg del contracte.

Per a cada servei, l'adjudicatari ha de complir plenament els Acords de Nivell de Servei definits una vegada **finalitzada la fase de transició** definida per cadascun dels serveis.



S'estableixen els següents condicionants:

- En l'etapa de Transferència i prestació en transició del servei, s'aplicaran per part de l'adjudicatari actual els ANS definits a la fase de prestació actual.
- Durant l'etapa de Transició, l'adjudicatari podrà sol·licitar a l'IMI la revisió temporal dels indicadors o ANS que cregui necessaris. L'IMI estudiarà la seva viabilitat o aplicació.

6.3. ANS EXIGITS

Els següents apartats mostren els nivells de servei exigits per l'IMI. Amb caràcter general i per a tots els serveis, es consideren com a part dels acords de nivell de servei, la disponibilitat dels serveis prestats d'acord a la taula següent:

Serveis	**% Disponibilitat**	**Horari del servei**
Preventiu. *Ciberintel·ligència*	99,99%	24x7
Monitorització i detecció d'incidents	99,99%	24x7
Resposta a incidents molt crítics o d'alt risc (Incident Handling)	99,99%	24x7
Administració de la plataforma de gestió i correlació d'events de seguretat (SIEM) i logs centralitzats	99,99%	24x7
Resta serveis SOC	99,99%	8x5
Gestió dels Serveis OSAT	98%	24x7
Gestió, administració, manteniment dels components del servei de telecomunicacions	98%	24x7
Administració, gestió i monitorització de les plataformes de Telecomunicacions	95,0%	24x7
Serveis de consultoria del Nus	98%	8x5
Projectes	98%	8x5

Els serveis prestats s'oferiran amb la disponibilitat descrita, a excepció de les franges establertes per a finestres de manteniment de les eines i plataformes tecnològiques necessàries per a la prestació dels serveis. L'incompliment de la disponibilitat dels serveis prestats podrà constituir una falta greu i serà motiu de penalització.

6.3.1. ANS d'Incidències i Problemes aplicables a serveis OSAT

En aquest grup d'ANS s'ha establert un criteri de **criticitat de la incidència**, diferenciant així entre les considerades **crítiques** i les que no ho són:

- **Incidència *crítica***: la que afecta a un servei que provoca indisponibilitat o interrupció del mateix, implicant així una aturada en l'operativa de funcionament normal del servei.
- **Incidència *no crítica***: la resta d'incidències.

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_INC_1	Temps màxim de resposta per incidències crítiques (Aplica a tots els serveis)	Temps que transcorre des què es notifica fins que es rep resposta	Mensual	30min	1% Facturació Mensual
ANS_INC_2	Temps màxim de resposta per incidències "no crítiques" (Aplica a tots els serveis)	Temps que transcorre des què es notifica fins que es rep resposta	Mensual	90min	1% Facturació Mensual
ANS_INC_3	Temps màxim de resolució per incidències crítiques (Aplica a tots els serveis)	Temps que transcorre des què es notifica fins que es resol	Mensual	120min	0,5% Facturació Mensual
ANS_INC_4	Temps màxim de resolució per incidències "no crítiques" (Aplica a tots els serveis)	Temps que transcorre des què es notifica fins que es resol	Mensual	5h	0,5% Facturació Mensual

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_INC_5	Percentatge màxim d'incidències reobertes responsabilitat de l'adjudicatari (Aplica a tots els serveis)	Percentatge en relació al volum total d'incidències obertes	Mensual	5%	0,1% Facturació Mensual
ANS_INC_6	Temps màxim de lliurament d'informes definitius d'incidències crítiques (Aplica a tots els serveis)	Temps màxim de lliurament d'informes definitius d'incidències crítiques un cop tancada la incidència	Mensual	8h laborables	0,5% Facturació Mensual
ANS_INC_7	Temps màxim de lliurament d'informes definitius d'incidències sota demanda (Aplica a tots els serveis)	Temps màxim de lliurament d'informes definitius d'incidències sota demanda un cop tancada la incidència	Mensual	12h laborables	0,5% Facturació Mensual

6.3.2. ANS de Peticions aplicables a serveis OSAT

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_PTC_1	Percentatge de peticions resoltes en un temps màxim de 4 dies laborables (Aplica a tots els serveis)	Percentatge de peticions resoltes en el temps màxim establert (calculat com el temps que transcorre des què es notifica fins que es resol)	Mensual	>95%	1% Facturació mensual
ANS_PTC_2	Percentatge de peticions prioritzades per l'IMI resoltes en un temps màxim de 10 hores laborables (Aplica a tots els serveis)	Percentatge de peticions resoltes en el temps màxim establert (calculat com el temps que transcorre des què es notifica fins que es resol)	Mensual	>95%	1% Facturació mensual
ANS_PTC_3	Percentatge màxim de peticions reobertes responsabilitat de l'adjudicatari (Aplica a tots els serveis)	Percentatge en relació al volum total de peticions obertes	Mensual	<5%	0,5% Facturació mensual

6.3.3. ANS de Disponibilitat, Continuïtat i Capacitat aplicables a serveis OSAT

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_DCC_1	Disponibilitat per servei	Percentatge del temps en el que el servei es troba plenament operatiu en relació al temps total	Mensual	>99,9%	≥ 99,5 → 1% Facturació mensual ≥ 99,0 → 2% Facturació mensual <99,0 → 4% Facturació mensual
ANS_DCC_2	Temps de recuperació del servei (RTO) en cas de desastre	Temps màxim de 2 hores per assolir com a mínim el 50% del servei	Puntual	L'establert al DRP (Disaster Recovery Plan)	1% Facturació mensual
ANS_DCC_3	Notificació de la superació dels llindars definits de la capacitat dels equipaments i infraestructura gestionats per OSAT (Aplica a tots els serveis)	Percentatge d'alarmes de superació de llindars de capacitat notificats a l'IMI abans de 60 minuts	Mensual	>95%	0,2% Facturació mensual

6.3.4. ANS de Gestió del Servei aplicables a serveis SOC i OSAT

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_GS_1	Temps de solapament de tècnics quan es produeix una substitució	Dies que treballen de forma conjunta el tècnic que marxa i el de nova incorporació	Puntual	>15 dies	1% Facturació mensual
ANS_GS_2	Temps de substitució d'una baixa imprevista d'un tècnic	Dies que transcorren des què es produeix una baixa imprevista i es substitueix	Puntual	<7 dies	1% Facturació mensual
ANS_GS_3	Temps màxim d'aprovisionament de recursos addicionals per projectes específics	Dies que transcorren des què es sol·licita el recurs per un projecte concret i aquest recurs està disponible	Puntual	<15 dies	1% Facturació mensual
ANS_GS_4	Temps màxim d'entrega de l'informe setmanal sobre l'estat dels serveis operats per OSAT	Data límit d'entrega de l'informe setmanal serà el dimarts de la següent setmana	Mensual	Dimarts	0,2% Facturació mensual
ANS_GS_5	Temps màxim d'entrega de l'informe mensual sobre l'estat dels serveis operats per OSAT	Data límit d'entrega de l'informe mensual serà el dia 10 de cada mes	Mensual	Dia 10 de cada mes	0,2% Facturació mensual
ANS_GS_6	Percentatge de rotacions del personal adscrit al servei	Percentatge de Rotacions (R) respecte el número de Persones adscrites al contracte (P): Càlcul = R / P	Anual	<40%	4% Facturació anual

6.3.5. ANS de Gestió de Versions aplicables a OSAT

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_GV_1	Periodicitat mínima per actualitzacions de versió per equip (Aplica a tots els serveis)	Temps que transcorre entre actualitzacions per equip	Anual	12 mesos	1% Facturació anual
ANS_GV_2	Temps màxim d'execució de canvi de versió per equip des de la petició expressa des de l'IMI (Aplica a tots els serveis)	Temps que transcorre des què es notifica expressament des de l'IMI fins que s'executa	Puntual	15 dies	1% Facturació mensual
ANS_GV_3	Correcció de vulnerabilitats de la infraestructura gestionada per OSAT	Temps que transcorre des de la publicació de vulnerabilitats crítiques/molt crítiques d'equipament gestionat per OSAT fins que s'actualitza a una versió que corregeix aquesta vulnerabilitat	Trimestral	<7 dies	1% Facturació mensual

6.3.6. ANS de Serveis Transversals

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_ST_1	Temps que transcorre entre la comunicació d'una substitució i la sortida del treballador/a.	Pre Subs = Data sortida del treballador/a - data comunicació de la substitució		Pre Subs >= 10 dies laborables	1.000 € per substitució que incompleixi l'ANS

(*) En el cas de que al finalitzar el mes el treballador/a no s'hagi incorporat, s'utilitzarà pel càlcul de l'ANS mensual, com a "Data d'incorporació real al contracte del treballador/a" el darrer dia laborable del mes. Aquest càlcul es continuarà realitzant cada mes, per calcular l'ANS, fins que s'incorpori el treballador/a.

6.3.1. ANS específics SOC

Per als següents ANS, es consideraran les següents prioritats per als incidents de seguretat:

Crítica quan es confirma que la xarxa es troba sota atac prolongat i/o l'Ajuntament està sent compromès pels atacants i/o es troba sota un atac de virus a gran escala i/o s'ha identificat una bretxa de seguretat a gran escala que impactarà immediatament a la reputació de l'Ajuntament (incloent la fugida de documents confidencials i crítics de l'Ajuntament).

Alta quan es confirma que la xarxa es troba sota atac continuat i/o múltiples sistemes s'han vist compromesos per un virus i/o s'ha identificat una fuita d'informació que no suposi un impacte immediat a la reputació de l'Ajuntament i/o un atac imminent reportat als mitjans de comunicació contra l'Ajuntament.

Mitjana quan un servidor s'ha vist compromès per malware o compromès per un altre mitjà, s'han exposat unes úniques credencials d'usuari mitjançant malware o hacking i/o algun informe de qualsevol tipus d'amenaça que afecti a l'Ajuntament.

Baixa alerta sense impacte.

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_SO_1	**Preventiu** Temps transcorregut entre la identificació d'una vulnerabilitat i la proposta de pla d'acció de mitigació	Data límit entrega proposta pla de mitigació	mensual	5 dies laborables	0,5% Facturació Mensual
ANS_SO_2	**Auditoria Tècnica** Temps transcorregut entre la sol·licitud d'una auditoria tècnica i l'inici de la mateixa	Data límit inici auditoria tècnica	mensual	5 dies laborables	0,5% Facturació Mensual

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_SO_3	**Monitorització i detecció d'incidents de seguretat. Prioritat baixa** Temps transcorregut entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com *baixa* i es notifica per al seu tractament.	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a baixa i es notifica per al seu tractament.	mensual	8 hores	0,3% Facturació Mensual
ANS_SO_4	**Monitorització i detecció d'incidents de seguretat Prioritat mitja** Temps transcorregut entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com *mitja* i es notifica per al seu tractament.	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a mitja i es notifica per al seu tractament.	mensual	4 hores	0,5% Facturació Mensual
ANS_SO_5	**Monitorització i detecció d'incidents de seguretat Prioritat alta** Temps transcorregut entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com *alta* i es notifica per al seu tractament.	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a alta i es notifica per al seu tractament.	mensual	1 hora	1% Facturació Mensual

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_SO_6	**Monitorització i detecció d'incidents de seguretat Prioritat crítica** Temps transcorregut entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com *crítica* i es notifica per al seu tractament.	Temps entre que s'origina una alerta al sistema SIEM, es processa (verifica i categoritza) com a crítica i es notifica per al seu tractament.	mensual	30 minuts	2% Facturació Mensual
ANS_SO_7	**Monitorització i detecció d'incidents** Percentatge d'incident crítics reportats directament per personal del client al servei de SOC	Nombre d'incidents crítics no reportades en el període * 100 / nombre d'incidents crítics en el període	mensual	< 1%	2% Facturació Mensual
ANS_SO_8	**Incident Handling** Temps de updates (reports) d'investigacions per incidents crítics	Temps màxim transcorregut entre actualitzacions de reports d'investigacions	mensual	4 hores	1% Facturació Mensual
ANS_SO_9	**Incident Handling** Temps límit d'entrega d'informe final d'impacte per incidents crítics	Temps transcorregut entre la notificació del incident i l'entrega de l'informe.	mensual	24 hores	1% Facturació Mensual
ANS_SO_10	**Evidències** Temps d'entrega d'informe d'evidències	Data límit entrega d'informe d'evidències	mensual	7 dies laborables	0,5% Facturació Mensual

CODI	Descripció ANS	CÀLCUL	PERIODICITAT	LLINDAR ANS	PENALITZACIÓ MÀXIMA
ANS_SO_11	**Administració palataformes** Disponibilitat de la plataforma	Tdispon= (Ttot-Tnodisp)/Ttot * 100 (%)	mensual	>= 95%	0,5% Facturació Mensual

6.4. MODEL DE PENALITZACIONS

Tal i com s'ha descrit a l'apartat **6.3: ANS Exigits**, a cada definició d'ANS s'introdueix la penalització màxima sobre la facturació de la part d'OSAT que s'aplicarà.

A més, al Plec de Clàusules Administratives Particulars d'aquest contracte s'especifiquen clàusules de penalitzacions addicionals per situacions relacionades amb els ANS descrits, i segons es consideren faltes lleus, greus o molt greus.

6.5. MODIFICACIÓ DELS INDICADORS

Al llarg de la prestació del servei, davant qualsevol modificació dels indicadors i nivells de servei amb l'objectiu de donar un millor servei, l'IMI, conjuntament amb l'adjudicatari, consensuaran i planificaran la seva introducció, així com el model de penalitzacions, si fos el cas.

Algunes de les causes que poden comportar aquestes modificacions són, per exemple: les variacions d'entorn tecnològic, d'entorn funcional i de condicions de negoci, els canvis d'abast i volum, així com les innovacions tecnològiques.

6.6. MILLORA DEL ANS

Durant l'execució del servei, l'IMI pretén obtenir una millora del nivell de servei prestat per l'adjudicatari. Aquestes millores seran assolides com a conseqüència de l'execució de les activitats de millora contínua del servei, aplicades per l'adjudicatari.

Aquestes millores seran objectivades, definides i consensuades com a evolucions en el temps dels valors dels llindars assignats a un indicador de mesura o mètrica.

7. MODEL DE PRESTACIÓ DEL SERVEI

El model de relació defineix les funcions i responsabilitats del adjudicatari i de l'IMI en un marc d'actuació comú, per assegurar el compliment de les obligacions de cadascuna de les parts. És un marc de relació que permet acordar el contingut i nivell de la prestació dels serveis, així com el seguiment de la prestació real en els aspectes estratègics, contractuals, tàctics i operatius.

L'adjudicatari pot ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb l'IMI, així com els mecanismes de control propis de cada servei i funció transversal. L'equip de treball dels adjudicataris, haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les tasques assignades.

El model de relació se sustenta en una estructura de competències i funcions que recauen sobre un esquelet de responsables de l'adjudicatari, els quals es relacionaran amb l'IMI en base a 3 àmbits: Estratègic, tàctic i operatiu.

L'adjudicatari designarà el responsable del contracte que serà l'interlocutor i representant principal entre l'empresa adjudicatària i l'IMI.

Addicionalment comunicarà a l'IMI els responsables que sostindran el Model de Relació. L'equip de responsables haurà de disposar igualment del dimensionament, la formació i els mitjans adequats per desenvolupar les funcions i responsabilitats assignades.

7.1. ÒRGANS DE GOVERN DEL SERVEI

Per la correcta prestació dels serveis i la consecució de l'èxit en qualitat, terminis i homogeneïtat del treball a realitzar, s'estableix que el contracte estarà governat pels següents comitès:

- Comitè Directiu a nivell estratègic
- Comitè de Seguiment a nivell tàctic
    - Comitè de Seguiment d'OSAT
    - Comitè de Seguiment del SOC
- Operació dels serveis a nivell operatiu
    - Operació servei OSAT
    - Operació servei SOC
- Reunió de seguiment del servei amb l'Oficina Tècnica d'Explotació (OTE)

Tant l'adjudicatari com l'IMI es comprometen a què les decisions preses en un àmbit flueixin a l'àmbit posterior o anterior.

El responsable dels serveis del Contracte per part de l'adjudicatari assistirà a les reunions d'aquest comitè sempre i serà el responsable de l'elaboració de la documentació de seguiment del servei necessària per a tal fi i també d'aixecar l'acta de les reunions de les reunions.

L'acta de cada comitè/reunió haurà de ser enviada a l'IMI abans de 3 dies laborables després de la seva realització.

7.1.1. Comitè Directiu

A l'àmbit estratègic l'IMI i els adjudicataris tindran un intercanvi d'experiències i visions sobre l'estat dels serveis d'OSAT i SOC per vetllar i supervisar la marxa del contracte i la presa de decisions que afecten a l'objectiu i abast del mateix.

Les principals activitat d'aquest comitè seran:

- Control de l'execució del contracte
- Seguiment i avaluació del servei prestat. Anàlisi de les necessitats del servei en base als informes del Comitè de Seguiment (ampliacions / reduccions)

- Validar l'abast general, objectius i resultats esperats dels serveis
- Validar la planificació de les tasques previstes a realitzar
- Verificar el compliment de les especificacions sol·licitades
- Proposta de modificacions / ampliacions dels Acords de nivell de servei (ANS)
- Seguiment econòmic del contracte
- Resolució dels conflictes que puguin sorgir en l'execució del contracte
- Comunicació de les faltes i penalitzacions i afectació en la propera facturació si s'escau
- Gestió de riscos i oportunitats
- Seguiment global d'expectatives i feedback de l'IMI a l'adjudicatari.

Els assistents per part de l'adjudicatari als comitès d'aquest àmbit hauran de tenir capacitat decisòria sobre els compromisos de serveis i visió global dels mateixos.

L'àmbit estratègic és el nivell màxim de seguiment del contracte i la prestació del servei. Des d'aquest àmbit s'elevarà a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.

Aquest comitè es celebrarà amb una periodicitat trimestral, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

En formen part:

- Directora de Operacions i Sistemes de l'IMI
- Directora de Qualitat i Seguretat per part de l'IMI.
- Cap del Departament de Seguretat de l'IMI
- Responsable departament de Telecomunicacions de l'IMI
- Responsable global del servei de l'IMI
- Responsable del compte per part de l'adjudicatari
- Responsable del servei per part de l'adjudicatari

Puntualment poden assistir-hi aquelles persones, integrants o no del contracte, que es consideri necessari en funció dels temes a tractar, tant per part de l'IMI com per part de l'adjudicatari.

7.1.2. Comitè de Seguiment

En aquest àmbit es farà un seguiment exhaustiu de l'execució dels serveis a través del comitè de seguiment dels serveis d'OSAT i el SOC. Inicialment es plantejaran aquestes reunions de manera independent, quedant a potestat de l'IMI modificar, si escau, la organització d'aquests comitès de

seguiment. S'elevaran a l'àmbit estratègic aquells aspectes que puguin originar la modificació del contracte.

Aquests comitès es celebraran amb una periodicitat mensual, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

7.1.2.1. COMITÈ DE SEGUIMENT DE L'OSAT

La finalitat d'aquestes reunions mensuals serà exposar l'estat del servei, les principals incidències operatives, la situació dels projectes en curs i el calendari previst.

Les principals activitats d'aquest comitè seran:

- Revisió de les incidències en curs i el seu pas a problema si així es considera per l'IMI.
- Validació de les tasques de control de la explotació i implantació dels serveis
- Aprovació de la execució de projectes i nous serveis
- Seguiment dels ANS
- Resolució de conflictes
- Anàlisi i priorització de tasques
- Validació dels procediments de millora per part del responsable de servei
- Anàlisi i control de la ocupació dels perfils assignats per l'assoliment del servei
- Totes aquelles que li atribueixi el present plec.

En formen part d'aquest comitè:

- Directora de Operacions i Sistemes de l'IMI
- Responsable departament de Telecomunicacions de l'IMI
- Responsable global del servei de l'IMI
- Responsable del servei OSAT de l'IMI
- Responsable del contracte per part de l'adjudicatari
- Responsable del servei OSAT per part de l'adjudicatari
- Responsable del servei del SOC per part de l'IMI i de l'adjudicatari, si es considera necessari.

Puntualment poden assistir-hi aquelles persones, integrants o no del contracte, que es consideri necessari en funció dels temes a tractar, tant per part de l'IMI com per part de l'adjudicatari.

7.1.2.2. COMITÈ DE SEGUIMENT DEL SOC

En línies generals, en aquest comitè es revisarà l'estat i l'evolució de cadascun dels serveis del SOC amb els indicadors corresponents, posant en el focus la mitigació i eliminació dels riscos d'acord amb els objectius de seguretat.

En formen part:

- Directora de Qualitat i Seguretat per part de l'IMI.
- Cap del Departament de Seguretat de l'IMI/Responsable de Seguretat de l'IMI.
- Responsable global del servei de l'IMI
- Responsable del servei SOC de l'IMI
- Responsable del contracte per part de l'adjudicatari
- Responsable del servei SOC per part de l'adjudicatari
- Responsable del servei de l'OSAT per part de l'IMI i de l'adjudicatari, si es considera necessari.

Puntualment poden assistir-hi aquelles persones, integrants o no del contracte, que es consideri necessari en funció dels temes a tractar, tant per part de l'IMI com per part de l'adjudicatari.

7.1.2.3. Operació del serveis

Aquest àmbit té com a objectiu l'operació diària del servei segons els procediments desenvolupats i tractar les problemàtiques específiques que afectin al servei prestat.

Es tractaran en seguiments separats el servei d'OSAT i el del SOC

Òrgan de Gestió	Periodicitat aproximada	Participants
Operació Servei OSAT	Setmanals / Ad-hoc	• Responsable del servei d'OSAT de l'IMI • Responsable del servei per part de l'adjudicatari • Equip tècnic de l'adjudicatari
Operació Servei SOC	Setmanals / Ad-hoc	• Responsable del servei del SOC de l'IMI • Responsable del servei per part de l'adjudicatari • Equip tècnic de l'adjudicatari

7.1.2.4. Reunió de seguiment del servei amb l'OTE

Es podrà reunir amb caràcter mensual per cadascú dels serveis definits (OSAT i SOC) encara que es podrà convocar també amb caràcter extraordinari sempre que es consideri necessari.

Les seves funcions són les d'informar de la marxa del servei a l'equip de l'OTE que supervisa el bon funcionament dels serveis TIC contractats i compliment d'ANS pactats.

En formen part:

- Coordinació de l'OTE
- Responsables de servei de l'IMI
- Responsable del contracte de l'adjudicatari

Es tractarà el reporting de l'estat de cada servei d'aplicació amb el detall de l'evolució de les incidències (obertes, gestionades i en curs) i la planificació i priorització de les peticions de cada servei.

Li correspon al Responsable del contracte de l'empresa adjudicatària la preparació de la documentació necessària per a la realització de la reunió i aixecar acta dels temes i acords de la reunió.

En aquest cas, l'IMI és l'encarregat de fer les convocatòries.

7.2. RELACIÓ AMB ALTRES PROVEÏDORS (SERVEIS DE NEGOCI)

Dins dels serveis de negoci és necessari definir les funcions i responsabilitats de l'adjudicatari vers altres proveïdors per tal d'assegurar el compromís d'acompliment de les respectives obligacions.

OSAT té un alt grau d'interacció amb altres proveïdors, permetent a l'adjudicatari tenir una visió global de tots els servei TIC que ofereix l'IMI a l'Ajuntament de Barcelona.

Per aquest motiu, és fonamental que l'adjudicatari assumeixi un rol important en la coordinació i en el suport i validació tècnica de les solucions proposades per la resta de proveïdors, assegurant així, la coherència tècnica de la xarxa de l'Ajuntament i dels serveis que s'hi ofereixen a sobre.

Les relacions més importants, que no les úniques, que tindrà l'adjudicatari amb els altres proveïdors de l'IMI són:

Proveïdors dels CPD dels Sistemes d'Informació:

Aquests proveïdors són els encarregats de subministrar maquinari i programari, administració i gestió de la infraestructura i prestació dels serveis dels sistemes d'informació dels CPDs.

Les tasques més importants a realitzar per l'adjudicatari en relació amb aquests proveïdors són:

- Assignació d'adreçament IP (IPv6 i IPv4) per a cada un dels CPDs dels sistemes d'informació
- Validació tècnica de la connexió dels CPDs a la xarxa de l'Ajuntament

- Validació tècnica dels projectes de trasllat i transformació dels sistemes d'informació de CPD
- Realització de les tasques necessàries durant els trasllats i transformacions dels sistemes d'informació per assegurar la seva correcta execució
- Validació tècnica i suport durant l'execució de les proves d'estrès i alta disponibilitat dels sistemes d'informació
- Suport tècnic per troubleshootings i resolució d'incidències a la xarxa
- Suport i col·laboració amb tots els implicats durant les migracions de sistemes d'informació cap els nous CPDs
- Suport i col·laboració en tots els nous projectes dels sistemes d'informació de CPD
- Presència en totes les reunions que siguin necessàries per les migracions i posades en marxa de nous projectes de sistemes d'informació.

Proveïdor del GIX (Gestió Integrada de Xarxes):

Aquest proveïdor és l'encarregat de gestionar, operar i evolucionar tota la infraestructura de Fibra Òptica Municipal així com la electrònica de xarxa associada per proveir la connectivitat a les dependències municipals. Les tasques més importants a realitzar per l'adjudicatari amb relació amb aquests proveïdors són:

- Assignació de rangs de direccionament IP perquè GIX faci la seva gestió
- Validació tècnica de la interconnexió de xarxes gestionades pel GIX amb el nus de comunicacions
- Validació tècnica i suport durant l'execució de les proves d'estrès i alta disponibilitat dels sistemes d'informació
- Suport tècnic per troubleshootings i resolució d'incidències a la xarxa
- Presència en totes les reunions que siguin necessàries per validar arquitectures de comunicacions.

Proveïdor gestió LAN i WLAN:

Aquest proveïdor és l'encarregat de la gestió, operació i manteniment dels switchos i access points indoor de les dependències municipals amb xarxa corporativa.

Les tasques més importants a realitzar per l'adjudicatari en relació amb aquest proveïdor són:

- Assignació d'adreçament IP (assignació d'adreçament IP IPv6 i IPv4) per les xarxes LAN i WLAN de les dependències municipals
- Validació tècnica de les arquitectures LAN i WLAN
- Suport i col·laboració en els troubleshootings de la xarxa LAN i WLAN

- Realització de les tasques necessàries durant les transformacions de les LANs per assegurar la seva correcta execució.

Proveïdor de Lot4 acord marc de Telecomunicacions:

Aquest proveïdor és l'encarregat de proporcionar la sortida a Internet de manera centralitzada a tot l'Ajuntament i el servei de Anti DDoS. Les tasques més importants a realitzar per l'adjudicatari en relació amb aquest proveïdor són:

- Assignació d'adreçament IP pels equips del proveïdor
- Gestió, operació i monitorització de router ASR100 que interconnecta amb punt neutre de CATNIX per realitzar l'intercanvi de rutes per sortir a internet.
- Validació tècnica de la connexió d'aquest proveïdor al Nus de comunicacions
- Validació i suport per la configuració del gestor d'ample de banda
- Coordinació i suport tècnic en cas de necessitat d'utilització del servei Anti DDoS.
- Validació i suport per les proves d'estrès i d'alta disponibilitat dels equips de connectivitat
- Realització de les tasques necessàries durant les transformacions de les solucions de connectivitat per assegurar la seva correcta execució
- Suport tècnic per la resolució d'incidències de connectivitat.

Proveïdor del Lot1 acord marc de Telecomunicacions:

Aquest proveïdor és l'encarregat de proporcionar els serveis i sistemes de comunicacions de veu fixa i serveis de xarxa de banda ampla. Les tasques més importants a realitzar per l'adjudicatari en relació amb aquest proveïdor són:

- Assignació d'adreçament IP per les solucions d'aquest lot
- Validació tècnica de la connexió d'aquest proveïdor a la xarxa corporativa
- Validació tècnica de les arquitectures de comunicacions i seguretat que es puguin desplegar en aquest lot
- Validació i suport per les proves d'estrès i d'alta disponibilitat dels equips d'aquest proveïdor
- Realització de les tasques necessàries durant les transformacions de les solucions d'aquest proveïdor per assegurar la seva correcta execució
- Suport tècnic per la resolució d'incidències.

Proveïdor del Lot2 acord marc de Telecomunicacions:

Aquest proveïdor és l'encarregat de proporcionar servei de comunicacions mòbils de l'Ajuntament. Les tasques més importants a realitzar per l'adjudicatari en relació amb aquest proveïdor són:

- Assignació d'adreçament IP
- Validació tècnica de la connexió d'aquest proveïdor a la xarxa de l'Ajuntament
- Validació i suport per les proves d'estrès i d'alta disponibilitat dels equips d'aquest proveïdor
- Realització de les tasques necessàries durant les transformacions de les solucions de mobilitat per assegurar la seva correcta execució
- Suport tècnic per la resolució d'incidències.

8. RECURSOS HUMANS

Es requereix que l'adjudicatari disposi d'una estructura organitzativa mínima que respongui als requeriments establerts en el present document.

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos humans propis de l'adjudicatari (o subcontractistes autoritzats) amb la qualificació necessària per a la prestació del servei en el seu estat actual i que pugui aconsellar, guiar i acompanyar la seva evolució futura.

Tal i com s'especifica en aquest document, per cadascuna de les fases que es detallen s'indica el percentatge de l'estructura organitzava que ha de prestar serveis en modalitat in-situ. L'IMI es reserva el dret de modificar aquest llindar (ampliant-lo o disminuint-lo) segons necessitats del servei i polítiques de l'organització.

Durant el contracte, l'IMI podrà revisar conjuntament amb l'adjudicatari l'estructura organitzativa, proposant els canvis adients per tal d'adaptar-ser als requeriments funcionals.

L'apartat **8.1: Funcions per Perfil**, mostra els diferents perfils que l'IMI considera que poden o han de formar part de l'estructura organitzativa del contracte, així com el número mínim de FTE que es considera per cadascun dels perfils més crítics[1].

[1] Aquells perfils que no tenen cap número de FTE assignat, l'IMI deixa llibertat a l'empresa adjudicatària perquè els assigni segons consideri per tal de donar el millor servei.

Servei	Perfil	Num mínim de FTEs
	Responsable de contracte	-
OSAT	Responsable del servei	1
	Tècnic de nivell 3 / Arquitecte	1
	Tècnic de nivell 2	3
	Tècnic de nivell 1	- -
	Cap de projecte	-
	Programador	-
	Tècnic especialista	-
SOC	Responsasble del servei	-
	Tècnic de nivell 2	2
	Tècnic de nivell 1	-
	Tècnic especialista	-
	Tècnic administrador plataformes	-
	Gestor incidents	-

Taula 1: Perfils i FTEs

Es requereix que l'empresa licitadora presenti la descripció i el dimensionament de l'estructura organitzativa que es mantindrà durant la durada del contracte, tenint en compte els mínims que l'IMI considera necessaris.

Així, el licitador haurà de valorar el nombre d'FTEs necessaris per a cada perfil, proposant ampliacions o enfocaments diferents, i que assegurin el compliment i la qualitat dels serveis descrits en el present plec. Aquesta proposta d'ampliacions serà valorada positivament. Com a mínim l'equip haurà de comptar amb tècnics certificats amb els següents certificats: CCNP Routing, Checkpoint CCSA, CCNA Wireless, F5 LTM, Palo Alto CNSE, ITIL V3 Foundation, -, CISSP, -o similars.

Per a l'elaboració de l'estructura organitzativa s'han de tenir en compte els requeriments del model de relació establerts en l'aparta 7 MODEL DE PRESTACIÓ DEL SERVEI, descrit en el present PPT, així com els perfils professionals requerits.

8.1. FUNCIONS PER PERFILS

Els següents apartats descriuen els perfils professionals i, de forma il·lustrativa, les principals funcions que hauran de desenvolupar, que no les úniques.

8.1.1. Gestió del Compte

Perfil	Responsabilitat
Responsable del Contracte	El responsable del compte serà la figura de referència del contracte amb l'IMI i el darrer responsable de la prestació del conjunt de serveis i projectes. Assegurarà el compliment de les següents funcions: • Aquesta figura és única per tot el contracte i es mantindrà durant tota la durada del contracte incloses les prorrogues si fossin d'aplicació. • Ha de tenir capacitat decisòria sobre el servei. • Gestió de la qualitat dels mecanismes de relació dins la seva organització per portar a terme els acords presos amb l'IMI. • Gestió del contracte: en cas que es produeixin canvis en l'abast o el cost dels serveis que impliquin una modificació contractual, és el responsable de vehicular-la.

8.1.2. Perfils OSAT

8.1.2.1. Gestió del servei

Perfil	Responsabilitat
Cap de Servei OSAT	El responsable del servei serà el màxim interlocutor de la gestió del servei amb l'IMI i executarà, com a mínim, les següents funcions: • Direcció Tècnica de projectes d'evolució i execució parcial del servei • La gestió i seguiment diari del servei, així com la resolució de conflictes i redimensionament temporal o permanent del mateix. • Seguiment dels indicadors de servei i evolució dels mateixos per a posteriorment poder elaborar els informes de servei i justificar el compliment dels ANS. • Gestió dels processos de suport i canvis sobre eines • Definició i gestió del catàleg de serveis • Aplicació de bones pràctiques en la gestió de serveis TIC • Gestió de la configuració i l'inventari

	• Gestió de la continuïtat • Millora dels processos d'operació i administració • Gestió dels riscos detectats, així com la presentació del pla de mitigació dels mateixos • Seguiment i control dels recursos assignats al/s servei/s • Analitzaran qualsevol desviació i situacions de gravetat dins la qualitat, terminis o abast del servei.
Cap de Projecte OSAT	El cap de projecte és una figura que es contempla a l'OSAT com a suport a les tasques que pot fer el responsable del servei, i més orientat a projectes i/o tasques puntuals que puguin requerir de més dedicació per part dels membres de l'OSAT. El cap de projecte hauria de donar suport a la direcció tècnica de projectes que es puguin requerir, control de la documentació, seguiment de problemes o incidències complexes que puguin sorgir, així com diferents tasques de gestió que se li puguin delegar en moments puntuals. La necessitat que es preveu per aquest perfil, d'entrada, és d'un percentatge petit d'un FTE, per superar moments puntuals que es requereixen tasques de seguiment, de gestió i de suport als nous projectes, tant propis de l'OSAT com de l'organització. Les tasques mínimes que hauria de realitzar aquest perfil són: • Actuar com a interlocutor entre els diferents actors que poden estar involucrats en el projecte/tasca assignada • Assistir a les reunions relacionades amb les seves tasques assignades, traslladant als membres de l'OSAT i l'IMI els compromisos o necessitats resultants • Gestionar els riscos que puguin anar sorgint • Vetllar per la qualitat del projecte en tot moment • Assegurar la disponibilitat i actualització de la documentació associada al projecte/tasca • Garantir el traspàs a explotació un cop finalitzat el projecte / tasca.

8.1.2.2. Arquitectura, administració i gestió de Comunicacions / Seguretat

Perfil	Responsabilitat
Tècnic Arquitectura, administració i gestió de Comunicacions/Seguretat OSAT nivell 3 (N3)	El rol de tècnic de nivell 3 de Comunicacions i Seguretat serà el de responsable tècnic de l'administració i operació de les plataformes de comunicacions i Seguretat així com el responsable de l'evolució de l'arquitectura d'OSAT. Haurà de garantir com a mínim les següents funcions: • Integració noves plataformes i evolució de les actuals • Gestió de la demanda i capacitat de les eines • Gestió de la continuïtat • Millora dels processos d'operació i administració • Consultoria de nous projectes • Aportació/disseny de noves solucions (a nivell tecnològic) que permetin cobrir les necessitats que vagin apareixent • Aportació/proposició de millores a nivell d'arquitectura que impliquin beneficis als serveis prestats • Realització dels següents informes: - Anàlisi d'obsolescència del maquinari. - Anàlisi de les versions existents i relació de les versions a implementar, amb els pros i contres de les mateixes. - Guia de "Bones Pràctiques" adaptades al servei que s'està prestant. - Anàlisi de les alertes de seguretat. - Anàlisi dels missatges que apareixen en els logs. - Evolució dels equipaments i serveis del Nus OSAT Assistència a les reunions de l´IMI on es vegi involucrat el projecte OSAT, així com la supervisió de les possibles solucions presentades per altres grups i que puguin tenir un impacte en el servei del Nus.
Tècnic Especialista OSAT	El rol de tècnic especialista entraria dintre les funcions de consultoria d'OSAT, i allà on el tècnic de nivell 3 o arquitecte pugui requerir suport perquè no sigui la seva àrea d'experiència. Podria ser, per exemple, un tècnic especialista en temes d'arquitectura cloud que doni suport puntual quan l'IMI requereixi d'aquest coneixement.

	Així, haurà de garantir com a mínim les següents funcions: • Tenir coneixements profunds en un tema dins l'àmbit d'OSAT. • Donar suport a l'IMI i al tècnic de nivell 3/Arquitecte quan es consideri necessari pels projectes d'evolució i/o transformació que es puguin plantejar dins el contracte. • Implementació de les solucions que es considerin oportunes dins el seu àmbit de coneixement. • Suport a la resolució d'incidències complexes.

8.1.2.3. Operació i monitorització

Perfil	Responsabilitat
Tècnic Operació i Monitorització OSAT nivell 2 (N2)	El rol de tècnic de nivell 2 executarà com a mínim les següents funcions: • Gestió, administració i operació plataformes de seguretat i comunicacions OSAT • Definició i evolució de l'arquitectura d'OSAT • Integració de noves plataformes i evolució de les actuals • Gestió de la demanda i capacitat de les eines • Gestió de la continuïtat • Integració entre les eines de monitorització i seguretat • Millora dels processos d'operació i administració • Suport en l'assistència a les reunions i grups de treball on es vegi involucrat el projecte OSAT • Desenvolupar i/o mantenir, amb revisions periòdiques, els manuals de procediment d'actuació i de manteniment preventiu i correctiu dels equips que formen part d'OSAT • Procedimentar tots els canvis i incidències per traspassar a nivell 1 d'operació de l'IMI • Evolució i automatització[2] de procediments, amb l'objectiu d'automatitzar les configuracions i l'aprovisionament de nous serveis i/o modificacions dels actuals

[2] Aquesta tasca requerirà, amb molta probabilitat, de programació, donada l'evolució de la pròpia tecnologia; per això es planteja també com a tasca per a un programador que pugui ajudar en aquest tipus d'automatitzacions.

Programador OSAT	El rol de programador a l'OSAT neix com a necessita pròpia de l'evolució del mercat i el servei. La majoria de dispositius (per no dir la totalitat) presenten avui dia interfícies que permeten la configuració i/o el control, si més no, de part de les funcionalitats que es presten. Aquest fet ajuda a l'automatització de tasques que permeten prestar el servei amb garanties i evitant així l'acció manual i les possibles errades humanes. La necessitat que es preveu per aquest perfil, d'entrada, és d'un percentatge petit d'un FTE, implementant automatitzacions de les tasques que es vagin detectant com possibles i recomanables. Aquestes tasques podria realitzar-les un membre propi de l'equip de l'OSAT amb coneixements de programació, tot i que entenem que poden pertànyer a perfils diferents i que pot ser més eficient si les realitza un programador. Les tasques mínimes que hauria de realitzar aquest perfil són: • Consultoria: determinar si les taques que els membres de l'OSAT i/o l'IMI plantegen són efectivament automatitzables o no, i quin seria el millor mecanisme per fer-ho (plataforma, llenguatge...) • Implementació de les solucions que s'acordin • Manteniment evolutiu d'aquestes implementacions • Mantenir control de les versions implementades i fer servir el repositori pel codi generat que determini l'IMI • Documentació del codi generat, fent esment de l'entorn de desenvolupament emprat, versions utilitzades, procés de compilació i/o generació de l'executable (si fos el cas), procés d'instal·lació, repositori, control de versions, etc.
Tècnic OSAT nivell 1 (N1)	El rol de tècnic de nivell 1 executarà com a mínim les següents funcions: • Operació i monitorització de les plataformes de seguretat i comunicacions d'OSAT • Gestió de la configuració i l'inventari • Gestió d'incidències, problemes, peticions i canvis • Gestió de la continuïtat • Millora dels processos d'operació i administració • Revisió diària de les tasques programades

8.1.3. Perfils SOC

8.1.3.1. Gestió del Servei

Perfil	Responsabilitat
Cap de Servei SOC	És el màxim responsable de dur el Servei del SOC a bon port. Per tant serà responsable de la gestió del Servei del SOC en les condicions descrites en aquest plec. Les seves principals tasques són: • Coordinació amb el Cap del Contracte • Dedicació plena al contracte. • Interlocutor principal del servei del SOC amb el Departament de Seguretat de l'IMI. • Portarà la gestió i coordinació dels equips tècnics del SOC. Actuarà com a Coordinador del Servei del SOC, tant de la part preventiva (ciberintel.ligència, Gestió de vulnerabilitats i Hacking ètic), com de la monitorització i detecció d'alertes i en la Gestió d'incidents de Ciberseguretat i evidències forensics. Coordinació entre equips de diferents disciplines dins del servei del SOC per tal d'obtenir un servei integral i que aprofiti be les sinergies. • Capacitat de direcció i gestió de personal. Controlar i gestionar els recursos del Servei del SOC. • Capacitat de planificació de treballs, realitzant el fixat de dates de lliurament. • Elaboració i presentació d'entregables dirigits tant a personal executiu com a tècnic. Especial atenció la qualitat dels informes i documents forenses. • Garantir que tot el personal del SOC segueix els procediments existents, que tots estiguin documentats i posats a disposició del IMI. • Assegurar el suport tècnic als tècnics i serveis operatius de l'IMI per la integració de fonts de dades i esdeveniments de seguretat amb el SIEM. • Assegurar i gestionar la coordinació dels serveis tècnics i operatius de l'IMI amb el servei de gestió de vulnerabilitats del SOC. • Gestió del pla del servei del SOC: – Presentacions de l'estat del servei / desplegament del SOC. Realitzar i actualitzar en cada fase o iteració el Pla del Servei. Especialment: calendari, riscos, tasques, recursos i implicació dels

	participants. – Definició del full de ruta d'evolució del Servei del SOC. Proposar i donar suport al Departament de Seguretat de la Informació de l'IMI – Monitorar el pla del Servei • Assegurament el compliment del Pla de Qualitat del servei del SOC. • Tasques de control i priorització • Gestionar emergències • Gestionar problemes i incidències en les operacions de seguretat que puguin comprometre al servei i garantirà que es gestionin correctament. Gestionar accions correctives a les incidències. • Gestionar els canvis. • Proporcionar les següents mètriques de seguiment a IMI associats al servei prestat: – Reunions de seguiment. Presentacions d'informes del servei mensuals – Quadres de comandament estàndard del servei. – Informe de seguiment mensual: Mapa d'atacs, Volum i productivitat. • Avaluació de l'acompliment i revisió de SLA • Anàlisi de millores i elaboració de recomanacions a lliurar al client, gràcies a les quals es permet incrementar l'eficiència dels treballs duts a terme per aquests.

8.1.3.2. Operació i Monitorització

Perfil	Responsabilitat
Tècnic Operador SOC nivell 1 (N1)	24x7 d'operació Monitorització dels esdeveniments i detecció d'incidents de seguretat. Haurà de realitzar les següents tasques: • Capacitats d'identificar, categoritzar i d'analitzar les incidències detectades, podent solucionar les mateixes o escalar-a el personal corresponent. • Gestionar tickets del SOC i bústies de correu de comunicacions d'esdeveniments de seguretat ja sigui d'entitats externes com de usuaris de l'Ajuntament o de l'IMI.

	• Realitzar investigació inicial d'incidents. • Realitzar tasques de ciberintel·ligència i vigilància activa sobre informació d'amenaces emergents, d'alertes externes, findings o d'intel·ligència d'amenaces, • Processament d'alertes generades per les diverses solucions de seguretat, aplicant les metodologies i procediments pertinents per assegurar la resolució de les mateixes. • Monitorització de l'estat de la plataforma i atendre els problemes detectats en base als procediments de correcció existents. • Extracció de la informació en brut necessària per a l'elaboració dels informes, ja sigui en forma de llistats, taules, gràfiques, etc. • Habilitats de comunicació per assistència a el públic.
Tècnic Operador SOC nivell 2 (N2)	2 persones 8x5 de suport amb guàrdies a la resta de serveis. Tasques d'analista de seguretat especialista en el anàlisis, classificació i avaluació de l'impacte i proposta de pla d'actuació: • Executar la remediació d'un l'incident segons procediments establerts. • Documentar i registrar informes resultats de la investigació i resolució d'un incident i fer el tancament de l'incident (en base al procediment de l'IMI de Registre d'incidents de Seguretat corporatiu). • Escalar els incidents que no es puguin resoldre amb aquest nivell al Servei especial de Gestió d'incidents crítics (Incident Handler). • Capacitats per a la realització de ciber simulacions que permetin identificar punts vulnerables d'una infraestructura tecnològica, permetent solucionar-los. • Elaboració de procediments de correcció d'errors, per solucionar qualsevol tipus d'incidència del servei deguda a problemes de la plataforma. • Capacitats de processament d'alertes generades per les diverses solucions de seguretat, aplicant les metodologies i procediments pertinents per assegurar la resolució de les mateixes. • Extreure la informació en brut necessària per a l'elaboració dels informes tècnics pertinents, ja sigui en forma de llistats, taules, gràfiques, etc. • Gestió del pool de tècnics del nivell 1. • Exercir de pont entre la operativa de l'IMI i del Nivell 1 del SOC. Coneixement de la organització operativa de l'IMI. • Experiència en assistència al públic.

8.1.3.3. Implantació i evolució del SOC

Perfil	Responsabilitat
Tècnic sènior especialista en SOC	• Arquitecte especialista en la implantació del SOC i evolució tecnològica, desplegament d'eines, processos i tecnologies. • Automatitzar la càrrega de logs. • Crear i provar els casos d'us de modelat de comportaments anòmals i probables incidents i gestionar la implantació. Desplegament de casos d'ús tècnics, d'intel·ligència i de negoci. • Definir i comunicar els processos i procediments del SOC. • Dissenyar i mantenir el ecosistema de eines que aporten control al SOC ja siguin de l'IMI o es troben en el servei del licitador (Ticketing, CMDB, Portal de Mando del SOC, etc.) • Enriquiment, orquestració i automatització de tasques que es disparen amb les alertes o incidents que es reben pel canal de ticketing o telefònic. Enriquiment de informació associada al tiquet a determinats nivells d'escalat. • Identificació, detecció i categorització d'incidents. Anàlisi de situació i impacte (avaluació). Proposta de mesures correctives, de remediació i contenció, d'acord amb la criticitat. Documentació dels casos tractats. Proposta de mesures correctives o de remediació, d'acord amb la criticitat. Documentació dels casos tractats. • Noves fonts i gestió de la detecció d'amenaces incipients. • Donar Suport tècnic als tècnics i serveis operatius de l'IMI per la integració de fonts de dades i esdeveniments de seguretat amb el SIEM.

8.1.3.4. Administració plataformes tecnològiques (SIEM i logs centralitzats)

Perfil	Responsabilitat
Tècnic Administrador plataformes tecnològiques (SIEM i Logs Centralitzats)	• Administració de dispositius implantats a les xarxes i garantir la connectivitat amb els mateixos. • Realització del manteniment de l'arquitectura i gestió de les actualitzacions necessàries, tant de programari com de regles. • Coneixements en el desenvolupament de controls per a solucions SIEM QRADAR i ELASTIC ELK.

	• Coneixement dels detalls de l'operació de la solució SIEM QRADAR i ELASTIC ELK. • Implantació de regles de correlació. • Instal·lació, prova i desplegament de solucions de SIEM. • Creació i configuració de quadres de comandament i informes. • Capacitats de processament d'alertes generades per les diverses solucions de seguretat, aplicant les metodologies i procediments pertinents per assegurar la resolució de les mateixes. • Extreure la informació en brut necessària per a l'elaboració dels informes tècnics pertinents.

8.1.3.5. Gestor incidents (Incident handler)

Perfil	Responsabilitat

Gestor Incidents (Incident Handler)	Modalitat del Servei 24x7x365
	
	Enginyers de Seguretat TIC experts en la resolució i mitigació d'incidents:
	
	• Gestor d'emergències (encarregat d'orquestrar les actuacions marcant prioritats)
	• Expert en gestió d'incidents (encarregat de garantir que les activitats planificades es duen a terme).
	• Expert forense digital (encarregat de garantir que les actuacions tècniques del pla d'acció es duen a terme en temps i forma)
	• Recolzament dels d'experts d'investigació:
	  ○ Investigacions digitals en servidors i endpoints
	  ○ Investigacions digitals en smartphones iOS i Android
	  ○ Investigacions digitals a través de l'anàlisi d'informació en trànsit
	  ○ Investigacions digitals en sistemes al núvol
	  ○ Investigacions digitals d'elements com logs, correus o executables
	
	Realitzarà les següents tasques:
	
	• Resolució i/o mitigació d'incidents que no puguin ser resolts amb el Nivell 2 del SOC.
	• Anàlisi amb profunditat dels incidents escalats recollint i analitzant la informació holística que envolta al incident (vulnerabilitats, ciber amenaces, esdeveniments del SIEM, hackings, informació CERTS, etc.).

	• Anàlisi d'impacte de l'incident, amb actius afectats. • Executar si cal procediments de mitigació. • Informar CERTs. • Documentar i Registrar incident i tancar. • Participar en les reunions de gestió de l'incident estratègiques de presa de decisions pels incidents de gran impacte. • Col·laborar amb el pla de comunicació corporatiu en cas d'incidents de gran impacte.

8.1.3.6. Servei forense i investigació interna

Tècnic especialista de Forense i investigació interna	• Modalitat del Servei és en Horari Laboral • Capacitats de respondre a peticions d'evidències: investigació d'una actuació a posteriori, determinar com fer vehicular de forma procedimentada les peticions d'informació d'evidències a àrees operatives IMI, i elaborar informes dels resultats dels forenses. • Les peticions poden venir de peticions de requeriments judicials, per peticions internes de sectors de l'Ajuntament, o requeriments per deixar constància d'actes administratius. Són peticions que es requereixen a l'IMI/Ajuntament. • Coordinació amb l'Oficina de GRC del departament de Seguretat de l'IMI per determinar la fiabilitat de la petició i el peticionari així com entrega a l'Oficina de GRC de l'Informe resultant per la seva supervisió i entrega. • Recepció de peticions d'evidències i derivar la petició si s'escau amb instruccions documentades a les àrees operatives de l'IMI o contractes de clouds públics, recollir resultats i elaboració d'informe Tècnic. • Garantir que les actuacions tècniques per a es duen a terme en temps i forma. • 2 informes anuals requeriran tècniques pericials i/o de cadena de custòdia. Poden requerir-se informes de cadena de custòdia quan es requereixi o experts d'investigacions digitals varies per poder donar resposta a requeriments judicials, interns o administratius en la volumetria indicada en el plec. • Tècniques d'anàlisi forense pericial.

8.1.3.7. Seguretat preventiva

Perfil	Responsabilitat
Tècnic sènior especialista en seguretat preventiva	Especialistes en la realització d'escanejos de vulnerabilitats i realització de hackings ètics i tests d'intrusió, recepció i gestió de vulnerabilitats de o-days i comunicats de CERTs i fonts externes, de ciberintel·ligència i gestió de les vulnerabilitats detectades. Gestió de les vulnerabilitats, Servei de ciberintel·ligència, Hacking ètics: • Anàlisi de riscos de seguretat de la informació (atacs massius d'Internet, problemes potencials a la seguretat pública, amenaces físiques, financeres, de pèrdua de negoci, reputació o confiança de la ciutadania, i pèrdua de danys en les dades, entre altres) i de l'impacte dels mateixos en les diferents comunitats d'usuaris. • Gestionar les vulnerabilitats i debilitats tècniques més freqüents, així com la seva mitigació. Això inclou les alertes de ciberintel·ligència, alerta temprana, vulnerabilitats d'infraestructures, findings de hackings ètics i auditories tècniques etc. • Gestió, configuració i us d'eines de gestió de vulnerabilitats i processos d'automatització i millora de la gestió del cicle de vida de les vulnerabilitats. Obertura de ticketing i interlocució amb les parts per la seva gestió. • Revisions d'arquitectures de seguretat, tant a nivell de xarxes de comunicacions, desenvolupaments i gestió de Sistemes d'informació. • Revisió d'eines de seguretat (IPS, Tallafocs, filtratge de contingut, polítiques de seguretat de informació, bastionatge de servidors,...) • Relacions amb els operadors del SOC per la coordinació i alineament d'estratègies operatives conjuntes. • Supervisió de la gestió, optimització i incorporació d'esdeveniments en SIEM relacionats amb el servei de preventiu i altres consoles centralitzades d'esdeveniments (Checkpoint Fw SmartEvent/Smart Log, etc.). • Coordinació / Supervisió dels sistemes d'evidències , propostes de noves incorporacions als logs centralitzats, mantenir inventari d'evidències, vetllar per la estratègia d'evidències establerta i per la implementació a la organització de la política d'evidències i proposar anualment millores del sistema d'evidències corporatives. Mantenir inventari i polítiques d'evidències i retencions. • Registrar i informar/documentar al "Registre d'incidents corporatiu"

	incidents de seguretat que es derivin de les tasques del servei de gestió de vulnerabilitats. • Gestió dels findings o alertes detectades pel servei de ciberintel·ligència. • Tècnic sènior especialista per de Hacking**:** – Realització de auditories tècniques de seguretat, escanejos de de xarxa interna o externa de vulnerabilitats, anàlisi de codi i tests d'intrusió. – Revisions de vulnerabilitats derivades de falles de disseny en arquitectures de xarxa, sistema o desenvolupament

8.2. CARACTERÍSTIQUES PROFESSIONALS

L'experiència professional que s'exigeix per a cada perfil és la següent:

Perfil	Experiència/Coneixements
Responsable del contracte	• Coneixements de comptabilitat analítica i financera. • Coneixements amb 3 anys d'experiència en gestió de costos de projectes similars.

8.2.1. Servei OSAT

Perfil	Experiència/Coneixements
Responsable del servei / **Cap de projecte**	**Experiència professional mínima:** Cal que acrediti una experiència mínima de 3 anys en el món del suport a client, resolució d'incidències, gestió administrativa de peticions i incidències i funcionament d'eines de gestió de tiquets **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI **Formació:** Ha de tenir alguna de les certificacions següents: • De Comunicacions: CCNA o equivalent • Formació en Gestió de Projectes i/o Serveis: Certificacions en ITIL, PMP, PRINCE2 o equivalents. Es valorarà que en tingui dues certificacions addicionals.
Tècnic nivell 3	**Experiència professional mínima:** Cal que acrediti una experiència mínima de 3 anys en el món de les infraestructures de comunicacions i la seguretat informàtica **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI **Formació:** • Certificacions dels productes que són objecte d'aquest contracte. • Certificacions de sistemes de comunicacions i seguretat, com ara Checkpoint , Palo Alto i F5 • Es valorarà que tingui una de cada tipus de les següents certificacions: ◦ Cisco Certified Specialist - Enterprise Core (400-101) 000 ◦ Cisco Certified Specialist - Data Center Design (300 -160)
Tècnic especialista	**Experiència professional mínima:** Cal que acrediti una experiència mínima de 3 anys en el seu àmbit d'experiència. **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI **Formació:** • Certificacions en el seu àmbit de coneixement relacionat amb alguna de les àrees d'OSAT

Perfil	Experiència/Coneixements
Tècnic nivell 2	**Experiència professional mínima:** Cal que acrediti una experiència mínima de 3 anys en administració d'infraestructures de comunicacions i d'eines de gestió de la seguretat informàtica **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI **Formació:** • Es requereix un perfil amb CCNP en R&S o altres disciplines del CCNP com security. • Nivell alt o mig d'anglès, que li permeti: - Llegir i interpretar correctament manuals, informes, estudis, etc. - Comunicar-se en aquesta llengua (per exemple amb serveis tècnics de fabricants) • Amb alguna de les certificacions a nivell de comunicacions, seguretat, marcs metodològics i dels productes que són objecte d'aquest contracte, com ara: - Certificació SANS SEC-503, SEC-504, SEC-511 o similarF5-CA: Fonaments d'administració - CCSA: Check Point Certified Security Administrator - Accredited Configuration Engineer (ACE): Palo Alto - CCNP Security - CCNP Routing & Switching Es valorarà que en tingui dues certificacions addicionals a la mínima requerida.

Perfil	Experiència/Coneixements
Programador	**Experiència professional mínima:** Cal que acrediti una experiència com a programador en l'àmbit de l'automatització de tasques amb equips de comunicacions i/o seguretat. Experiència en arquitectures de software REST, Python, Ansible, entorns XML/JSON, SNMP... mínima de 3 anys en administració d'infraestructures de comunicacions i d'eines de gestió de la seguretat informàtica **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI **Formació:** • Python • Ansible • XML/JSON • SNMP
Tècnic nivell 1	**Experiència professional mínima:** Cal que acrediti una experiència mínima de 3 anys en el món de la seguretat informàtica i/o comunicacions: • Serveis de monitorització i gestió d'alertes, • Administració d'infraestructures de comunicacions i/o d'eines de gestió de la seguretat informàtica. **Titulacions:** Enginyeria en informàtica, telecomunicacions o similar en l'àmbit TI. **Formació:** • Es requereix un perfil amb CCNA en R&S, o altres disciplines del CCNA com wireless.

8.2.2. Servei SOC

Perfil	Experiència/Coneixements
Cap de Servei SOC	**Experiència professional mínima:** Cal que acrediti, durant els darrers 6 anys, una experiència mínima de 3 anys d'experiència en lideratge i responsabilitat d'un SOC o com a cap d'operacions de Seguretat. Ha de tenir amplis coneixements i experiència en solucions tecnològiques i eines de seguretat relatives a plataformes SIEM QRADAR i ELASTIC ELK i serveis del SOC. **Titulacions:** Enginyeria Informàtica, Telecomunicacions, Enginyeria. Preferiblement Informàtica i Telecomunicacions. **Formació:** Ha de tenir alguna de les certificacions següents: • De Seguretat: CISM de ISACA, CISSP de ISC2 • Formació en Gestió de Projectes i/o Serveis: Certificacions en ITIL Expert, PMP, PRINCE2 o equivalents. Es valorarà que en tingui una certificació addicional de cada tipus.
Tècnic Operador SOC N1	**Experiència professional mínima:** Cal que acrediti mínim 1 any d'experiència demostrable en: • Operació i manteniment de plataformes de SIEM, anàlisi de logs i gestió d'esdeveniments de xarxes, servidors, i infraestructures de seguretat perimetral • O experiència en operació d'eines de seguretat com són tallafocs, proxies, IPS/IDS, antivirus, entre d'altres. Ha de tenir coneixements de ciber amenaces, malware, phishing, atacs DDoS, entre d'altres. **Titulacions:** Formació professional de grau superior d'administració de Sistemes informàtics de xarxa o altres de formació professional de grau superior relacionada amb tecnologies de la informació i de les comunicacions, o titulació Universitària d'Enginyeria Informàtica, Telecomunicacions. **Formació:** Requerit Nivell d'anglès B2 o equivalent. Certificacions recomanades: – Alguna certificació de fabricants de solucions de seguretat (Palo Alto, CISCO, IBM, Checkpoint, etc.).

Tècnic Operador SOC N2	**Experiència professional mínima:** Cal que acrediti 2 anys d'experiència en: • Administració de plataformes de seguretat SIEM, de casos d'ús, anàlisi de logs de seguretat, detecció d'amenaces, gestió d'incidents de seguretat i de elaboració de plans de mitigació, • O experiència en disseny i administració d'infraestructures de eines de seguretat com son tallafocs, proxies, IPS/IDS, antivirus, entre d'altres. **Titulacions:** Formació professional de grau superior d'administració de Sistemes informàtics de xarxa o altres de formació professional de grau superior relacionada amb tecnologies de la informació i de les comunicacions o titulació Universitària de Enginyeria Informàtica, Telecomunicacions. **Formació:** Requerit: Nivell d'anglès B2 o equivalent. Certificacions recomanades: – Comptia Security + o similar – Alguna certificació de fabricants de solucions de seguretat (Palo Alto, CISCO, IBM, Checkpoint, etc.).
Tècnic sènior especialista en SOC	**Experiència professional mínima:** Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC com arquitecte de seguretat en relació al disseny i operació de sistemes SIEM, de sistemes de seguretat perimetral, tallafocs, proxies, Detecció i prevenció d'intrusions, etc. **Titulació**: Universitària d'Enginyeria Informàtica, Telecomunicacions. **Formació:** Cal que tingui alguna de les següents certificacions: • CEH, CSX, OCSP, CISA, CSIH, CISSP Es valorarà que tingui dues certificacions addicionals a la requerida.
Tècnic Administrador plataformes tecnològiques	**Experiència professional mínima:** Cal que acrediti, durant els darrers 3 anys, 2 anys d'experiència mínima en administració de les solucions SIEM QRADAR y ELASTIC ELK. **Titulació**: Formació professional de grau superior d'administració de Sistemes informàtics de xarxa o altres de formació professional de grau superior relacionada amb tecnologies de la informació i de les comunicacions o titulació Universitària d'Enginyeria Informàtica, Telecomunicacions.

	Formació: Requerit Nivell d'anglès B2 o equivalent. Certificacions recomanades: • Certificacions recomanades en tecnologies SIEM • Alguna certificació de fabricants de solucions de seguretat (Palo Alto, CISCO, IBM, Checkpoint, etc.).
Gestor Incidents (Incident Handler)	**Experiència professional mínima:** Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència mínima correlació avançada d'esdeveniments i logs de seguretat i en anàlisi, mitigació i plans d'acció de resposta d'incidents complexes. Ha de tenir experiència en tasques de prevenció com són la gestió de vulnerabilitats i detecció d'amenaces **Titulació**: Universitària d'Enginyeria Informàtica, Telecomunicacions. **Formació:** Cal que tingui alguna de les certificacions indicades: • CEH, CSX, OCSP, CISA, CSIH, CISSP, CHFI.
Tècnic especialista de Forense i investigació interna	**Experiència professional mínima:** Cal que acrediti, durant els darrers 5 anys, 3 anys en elaboració d'informes per requeriments d'evidències i gestió de la petició d'evidències a les àrees operatives i tècniques dels servei de l'IMI per donar resposta a requeriments externs o interns. La majoria són informes sense requeriments d'especialistes en peritatge informàtic estrictes, i 2 anuals han de ser amb **informes pericials** amb especialistes en peritatge informàtic i gestió de prova electrònica**.** **Titulació**: Universitària d'Enginyeria Informàtica, Telecomunicacions. **Formació:** Cal que tingui alguna de les certificacions indicades : • CEH, CSX, OCSP, CISA, CSIH, CISSP, CHFI. Pels 2 informes anuals i un perit judicial que s'exigeix en el contracte amb requeriments d'**informes pericials** amb especialistes en peritatge informàtic i gestió de prova electrònica **es requereix la certificació de** CHFI.

Tècnic sènior especialista en seguretat preventiva	**Experiència professional mínima** Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC amb experiència en tècniques en la gestió de les vulnerabilitats i findings detectats per diverses fonts internes del SOC o fonts externes (CERTs i publicacions). **Titulació**: Universitària d'Enginyeria Informàtica, Telecomunicacions. **Formació:** Cal que tingui alguna de les certificacions indicades: • CISSP (Certified Information Systems Security Professional), • CEH (certifie Ethical Hacker – EC-Council), • CSX (Cubersecurity Fundamentals Certificate . ISACA), • OCSP (Offensive Security Certified Professional – Offensive Security), • CSIH • Certificacions de fabricants de Vulnerabilitats com són Nessus o Qualys. Es valorarà que tingui dues certificacions addicionals a la requerida.

9. CONDICIONS D'EXECUCIÓ

9.1. DURADA DEL CONTRACTE

El contracte tindrà una durada de 3 anys des del dia següent al de la seva formalització. I tindrà l'opció de pròrroga de fins un màxim de 2 anys addicionals.

9.2. LLOC DE PRESTACIÓ DEL SERVEI

Degut a què està previst que part de l'estructura organitzativa proposada presti els serveis en remot des de les instal·lacions de l'adjudicatari[3], aquest estarà obligat a realitzar la connexió entre les dependències de l'IMI i el seu centre o centres de treball per tal de poder prestar els serveis de forma remota.

[3] *Com ja s'ha anat explicant, el percentatge de l'estructura organitzativa que prestarà serveis in-situ/remot podrà variar segons la fase del contracte, i també segons les necessitats a nivell de servei que pugui decidir l'IMI, i tenint sempre present les pròpies polítiques que pugui anar incorporant l'IMI com a organització respecte aquest assumpte.*

Aquesta connexió no representarà cap cost addicional a l'IMI i com a mínim ha de ser una línia dedicada d'un ample de banda mínim de 100 Mbps. Així mateix, l'adjudicatari haurà de proveir una connexió alternativa per garantir la redundància de la mateixa[4].

La no prestació del servei per manca de connexió es considerarà una falta greu.

Al llarg del contracte es podria requerir un canvi en la ubicació dels professionals entre els centres operatius de l'IMI, d'acord amb les necessitats dels serveis i l'organització d'equips de treball. En cap cas la ubicació dels professionals suposarà un increment dels costos vinculats a la prestació dels serveis.

En qualsevol moment durant l'execució del contracte, l'IMI es reserva el dret de sol·licitar a l'adjudicatari la realització de la prestació del servei de forma presencial en les instal·lacions de l'IMI i en els percentatge dels recursos que consideri. L'adjudicatari s'haurà d'adaptar a aquests canvis consensuats en el termini pactat.

En aquesta situació, l'IMI serà responsable de proveir del mobiliari i serveis generals d'oficina.

Els licitadors també hauran d'incloure en la seva oferta la provisió d'instal·lacions de contingència tal i com es detalla en **l'apartat 11.8**,relatiu a la contingència i continuïtat del servei.

9.3. SERVEIS EN REMOT

Donat que part de l'estructura organitzativa de l'adjudicatari haurà de poder operar en remot, aquest haurà d'assegurar l'eficiència del recursos en tots els processos d'administració i d'operació. Per tant, l' adjudicatari haurà de valorar i detallar un model de relació que permeti abordar d'una manera òptima les tasques a realitzar.

Per a poder prestar serveis en remot l'adjudicatari haurà de contractar 1 circuit amb redundància amb un cabdal de 100 Mbps simètrics i establir un circuit privat amb l'IMI. Tots els costos d'aquest circuit aniran a càrrec de l'adjudicatari:

- 1 circuit es finalitzarà al CPD 1 o CPD 3[5]
- i l'altre al CPD 2

Els servei en remot ofert per l'adjudicatari haurà d'incloure, entre d'altres, les següents característiques:

- Capacitat d'absorció de càrrega de treball variable

[4] *Tal i com s'ha detallat a l'apartat 9.3 Serveis en remot.*

[4] *Tal i com s'ha detallat a l'apartat 9.3 Serveis en remot.*

[5] *Durant la primera part del contracte, el CPD operatiu serà el CPD 1. Entrat en el contracte, i també com a tasques d'OSAT, caldrà traslladar el CPD operatiu del CPD 1 al CPD 3.*

- Capacitat d'adaptació a noves necessitats: equip multidisciplinari i certificat amb els principals fabricants de l'IMI
- Disponibilitat de recursos experts
- Procediment de pla de contingència i garanties del servei
- Possibilitat d'introduir un sistema de monitorització amb valor afegit
- Capacitat de fer totes les tasques operatives de forma remota
- Capacitat de fer auditoria i gestió de la seguretat de forma remota
- Equip de treball especialitzat i rigorosament en línia amb l'estructura de l'IMI i els serveis
  - Els serveis remots hauran de prestar el nucli del servei i disposar de grups especialitzats i dedicats. Cadascun d'aquests grups disposarà d'enginyers N-I i N-II amb la finalitat d'optimitzar la resolució de les incidències en funció de la gravetat i afectació al servei de les mateixes, així com optimitzar la realització de canvis en la infraestructura segons la complexitat de la mateixa o del canvi
  - En el cas d'incidències o canvis que requereixin un elevat coneixement tecnològic de la solució, es formaria un grup de treball en què s'inclourien enginyers N-III
- Tots els serveis proporcionats en remot hauran d'estar liderats per el Cap de Servei, qui, entre d'altres tasques, es responsabilitzarà d'assegurar un intens i productiu procés de comunicació amb l'IMI, així com una evolució i optimització constant del servei. El Cap de Servei mantindrà i fomentarà l'estreta relació amb l'IMI.

9.4. ESTRUCTURA ORGANITZATIVA I RECURSOS HUMANS

La prestació dels serveis ha de poder ser proporcionada en la seva totalitat amb els recursos humans propis de l'adjudicatari (o subcontractistes autoritzats en un únic nivell de subcontractació) amb la qualificació necessària i adequada per a la prestació del servei.

Els mitjans personals necessaris per a la prestació dels serveis descrits i detallats en **l'Apartat 8: Recursos Humans,** han de ser els adequats per realitzar amb garantia les tasques definides i han de mostrar les habilitats necessàries per tal d'integrar-se en un equip d'alt rendiment, entre les quals es podrien determinar a efectes enunciatius les següents:

- Professionalitat, bona actitud i respecte per a la feina realitzada i pels demés.
- Destresa comunicativa i interpersonal.
- Capacitat de treballar en equip.
- Habilitat per identificar, analitzar i resoldre problemes.
- Capacitat de treball sota pressió.

- Coneixement de català, castellà i anglès, parlat i escrit.
- Ampli coneixement tecnològic i de negoci de seguretat informàtica.

Els licitadors hauran d'incloure en la seva proposta l'organigrama i esquemes organitzatius dels equips de treball proposats per tal de donar resposta a les necessitats expressades en aquest plec i permeti mantenir un model de relació fluid amb la resta d'equips i personal de l'IMI.

Tal i com es mostra a la *Taula 1*, l'IMI considera que existeixen diversos perfils que tenen cabuda dins l'equip de servei. La mateixa taula mostra també el número mínim de FTEs considerats per alguns dels perfils considerats més crítics.

L'IMI tindrà dret a exigir justificadament a l'adjudicatari el canvi d'un recurs que d'ell depengui, quan així ho justifiqui l'execució dels treballs, quan no s'acompleixin els requisits demanats per a l'equip humà indicats en el present capítol o per tal de garantir la correcta prestació, dimensionament i organització dels serveis. Aquesta substitució s'haurà de fer efectiva en el termini de 15 dies a partir de la recepció de la comunicació per part de l'adjudicatari. L'adjudicatari haurà de presentar en un termini màxim de 10 dies a partir de la comunicació de sol·licitud de substitució, el pla d'acció previst per resoldre les causes que han determinat la sol·licitud de substitució.

9.5. HORARI DE PRESTACIÓ DEL SERVEI

Es descriuen a continuació els horaris d'execució de les tasques que l'adjudicatari haurà de realitzar durant la durada del contracte. l'IMI pot variar els horaris i les tasques per adaptar-se a les necessitats que puguin sorgir durant la vigència del contracte.

Tasques	Horari	Observacions
Tasques de monitoració**., gestió d'incidències i operació i vigilància de seguretat**	24x7 365 dies l'any	
Tasques de gestió de peticions i problemes	DL a DV: 8 a 18h	Excepte festius en calendari AjBCN
Tasques de canvis diversos[6]	A pactar segons impacte i criticitat	Típicament fora d'horari laboral (festius i/o nocturns)
Projectes	DL a DJ: 9 a 18h DV: 8 a 15h	

[6] *Aquests canvis poden ser deguts a equips/serveis directament gestionats per OSAT, o també com a suport de fites de projectes importants que requereixin un desplegament, tasques i/o tractament especial.*

Tots els canvis es gestionaran de forma coordinada amb el procés de gestió del Canvi de l'IMI.

Si durant l'execució del contracte l'IMI o l'adjudicatari detecten la necessitat de modificar l'horari de servei d'algun dels processos o serveis descrits en aquest contracte, l'IMI i l'adjudicatari consensuaran de forma conjunta la modificació.

És d'obligatori acompliment la cobertura per vacances, malaltia o altres motius dels professionals que realitzen la prestació del servei, amb un període de transició mínim d'una setmana. En cas d'incompliment, es considerarà una falta lleu per cada setmana que no es cobreixi el perfil indicat.

9.6. EINES I EQUIPAMENT PERSONAL PER A LA PRESTACIÓ DEL SERVEI

Quan l'adjudicatari es trobi en les instal·lacions del IMI, **l'IMI proveirà** a les persones que prestin els serveis:

- Ubicació física adequada per al desenvolupament i prestació dels serveis ubicats a les instal·lacions de l'IMI.
- Infraestructura per al suport de les eines corporatives (servidors) i xarxa de comunicacions necessàries per la prestació del servei a les instal·lacions escollides per l'IMI.
- Telefonia fixa a les instal·lacions del servei.
- Accés a Internet a través de la xarxa d'àrea local, restringit als llocs de treball que ho requereixin així com a les adreces o pàgines web que siguin necessàries per al desenvolupament del servei.

L'IMI no proveirà:

- Ordinadors de sobretaula amb sistema operatiu i programari habitual d'oficina.
- Línies o terminals de telefonia mòbil personals o per activitats professionals no vinculades a la prestació de serveis de l'IMI.
- Ordinadors portàtils (PCs), ordinadors de mà (PDAs).
- Accés a Internet via xarxes de telefonia mòbil (5G, 4G...).
- Cap altre recurs no especificat explícitament.

En conseqüència, l'adjudicatari haurà de:

- Subministrar tots elements de maquinari, programari i serveis i el seu manteniment durant la durada del contracte, que siguin necessaris per complir amb els requeriments d'aquest capítol. Aquests elements seran d'ús exclusiu pels serveis prestats a l'IMI i es requerirà l'esborrat complet dels mateixos quan es deixi de prestar el servei de manera individual o de part de l'adjudicatari a la finalització del contracte.
- Acceptar i respectar les polítiques de seguretat establertes per l'Àrea de Seguretat de l'IMI i la instrucció de personal Municipal.

- Permetre l'administració, maquetat, esborrat i supervisió dels equips per part de l'equip tècnic que designi l'IMI.

S'ha de realitzar una proposta homogènia de maquinari, programari i de tots aquells accessoris i equipaments auxiliars que siguin necessaris per què els treballadors puguin executar les seves funcions amb eficàcia, disposant d'un entorn adaptat a les necessitats de cada tipus d'usuari. Els equips hauran de seguir les especificacions donades per l'equip que designi l'IMI per garantir la compatibilitat amb el sistema de maquetat i per reduir al mínim el nombre de maquetes necessàries pel servei de Suport al Lloc de Treball.

L'IMI es troba en un procés de transformació i millora contínua que pot implicar la realització de canvis importants en el referent a les eines que s'hauran d'utilitzar per dur a terme l'execució del servei.

Per aquest motiu és imprescindible que l'adjudicatari tingui presents les següents consideracions en el referent a les eines de gestió durant l'execució del contracte:

- L'IMI decidirà la utilització de qualsevol tecnologia nova o evolució de les existents, relacionades amb la prestació del servei.
- L'IMI decidirà la forma d'implantar qualsevol d'aquests nous sistemes, planificar els projectes corresponents i el seu calendari, així com la transició des dels sistemes existents cap als nous.
- Els adjudicataris es comprometen a assumir i adaptar-se a aquestes noves tecnologies i sistemes per donar el servei de suport, així com participar activament en el procés de transició, formant i preparant el seu personal en aquestes noves tecnologies i sistemes implantats sense cost addicional per l'IMI.

9.7. SEGURETAT CORPORATIVA

Tant l'empresa adjudicatària com el personal de l'adjudicatari s'hauran de sotmetre a les polítiques i regulacions internes que estableix l'àrea de Seguretat Corporativa en matèria de seguretat de la informació, com a mínim i no limitant-se a:

- Permetre i facilitar la realització d'auditories de compliment de les normatives establertes per el Departament de Seguretat, internes o externes, sobre els sistemes d'informació vinculats a la prestació del servei, i garantir la possibilitat de traçabilitat de les accions fetes per l'auditor per facilitar el seguiment d'aquestes i els seus possibles impactes no desitjats.
- Facilitar l'accés en qualsevol moment als equips i mitjans tècnics emprats pel personal de l'adjudicatari en les oficines de l'IMI (sigui o no per l'exercici de la seva funció).
- Acceptar les normes i polítiques que estableix l'àrea de Seguretat tant en el moment de la seva incorporació com després de cada canvi important de les polítiques, normes o regulacions.
- Permetre l'administració i gestió dels equips i mitjans tècnics emprats per l'exercici de les seves funcions per part de l'equip que designi l'IMI per fer el desplegament de polítiques i

controls de seguretat, actualització d'eines i manteniment d'aplicacions autoritzades i permisos d'accés a la informació.

- La custòdia per part de l'IMI dels equips, així com la informació resident dels mateixos.
- Donar compliment a totes les normes, polítiques i marcs reguladors vigents durant el període del contracte (LOPDGDD i LSSI).

A la finalització del contracte, l'adjudicatari quedarà obligat a l'entrega o destrucció en cas de ser sol·licitada, de qualsevol informació obtinguda o generada com a conseqüència de la prestació del servei.

9.8. CONTINGÈNCIA I CONTINUÏTAT DEL SERVEI

L'adjudicatari haurà de proveir un pla de continuïtat dels Serveis objecte d'aquest plec.

Aquest pla inclourà dues parts:

- Pla de continuïtat per a cadascun dels serveis del catàleg de serveis: es detallaran les propostes tècniques de modificació i/o transformació del servei, si s'escau, per tal de garantir l'alta disponibilitat del mateix. L'adjudicatari haurà d'elaborar aquest pla dintre dels 6 primers mesos de vigència del contracte.
- Pla de continuïtat en la prestació dels serveis de gestió, monitorització i operació: es detallaran les mesures que aplicarà l'adjudicatari per tal de garantir la continuïtat dels serveis de gestió, operació, i monitorització, de forma que es puguin prestar sense interrupció, ja sigui des de les dependències de l'IMI com des d'altres dependències de l'adjudicatari. Aquest Pla haurà d'estar operatiu al finalitzar la fase de transició.

El Pla de contingència o DRP (*Disaster Recovery Plan*) ha d'establir l'estratègia proposada tant d'accés i comunicació com dels diferents plataformes i elements que composen el serveis d'aquest plec segons la criticitat del Servei.

Pel què fa als centres de gestió, contemplarà com a mínim que la gestió del Servei tracti els aspectes:

- Estacions de treball amb el programari adequat per realitzar les tasques descrites
- Comunicacions d'accés a les aplicacions informàtiques
- Telefonia fixa a les instal·lacions del servei
- Accés a Internet a través de la xarxa d'àrea local
- Espai suficient per allotjar en condicions de treball òptimes:
  - El personal necessari de l'adjudicatari per realitzar el servei i
  - Personal de l'IMI o de terceres parts determinades per aquest

La continuïtat del Servei es definirà en base a la governança de la continuïtat establerta a l'apartat **11.8 Governança de la continuïtat i disponibilitat**.

Els serveis del catàleg es classificaran en el moment de l'inici del contracte, però per la tipologia de serveis de Seguretat i comunicacions, s'anticipa que molts serveis tindran RTO (*Recovery Time Objective*) entre 0 i 2 hores.

9.9. PLA DE FORMACIÓ

Els licitadors hauran de presentar la seva proposta del Pla de formació detallat, tant pel personal del SAU, com pel personal tècnic de l'IMI responsable del servei per donar-los a conèixer les característiques i funcionament dels serveis i els processos de gestió. El pla de formació haurà d'incloure com a mínim:

- Metodologia
- Calendari
- Continguts:
  - Manuals d'usuari del servei amb informació detallada de les prestacions i funcionalitats.
  - Accés a entorns de proves o de simulació.
  - Documentació de processos, base de dades de coneixement.
  - Disponibilitat contínua via web.

El Pla de formació al personal tècnic de l'IMI podrà incloure els següents continguts específics:

- Tallafocs i gestió de checkpoint
- Balancejadors F5
- Wifi CCNP CISCO
- Palo Alto CNSE
- Antispam TrendMicro
- Concentradors Pulse/Cisco/Fortinet
- Gestió de logs Splunk, ELK
- SIEM
- DDI (DNS, DHCP, IPAM)
- Ciberseguretat
- Resposta a incidents, forenses i preventiu
- Altres temaris que es considerin adients en la prestació del servei
- Per cada nou projecte implantat, formació específica d'acord a la certificació corresponent

La formació constarà d'un mínim de 100 hores anuals, que tractarà sobre els temes anteriorment mencionats.

El licitador haurà de presentar un pla de formació en seguretat de la informació per als responsables de l'IMI dels serveis; aquest pla de formació es mantindrà actualitzat i es realitzaran sessions presencials en funció de les necessitats. La formació es podrà derivar a centres especialitzats en formació sobre les temàtiques indicades. En el cas de realitzar la formació a les instal·lacions municipals, és contemplarà un mínim d'assistència de 4 persones.

Tot el material que es faci servir a les sessions de formació es lliurarà a l'IMI a la seva finalització.

9.10. PLA DE QUALITAT

L'adjudicatari haurà de definir i documentar, durant el primer mes de la vigència del contracte, segons els punts que s'indiquen a continuació, un Pla de Qualitat específic que asseguri la qualitat dels serveis oferts.

El Pla de Qualitat inclourà tots els requisits definits en el present plec per part de l'IMI.

L'OSAT serà responsable de la implantació, seguiment i compliment dels estàndards de qualitat que contempla el present contracte. Per tal d'assegurar aquest compliment, els licitadors s'hauran de comprometre a contractar una auditoria interna amb periodicitat biennal per tal d'auditar que tots els procediments contemplats dins la norma ISO20000 i la certificació ITIL v3 són vigents i s'implanten d'acord als estàndards.

Els punts que s'indiquen a continuació seran els índexs que, com a mínim, ha d'emplenar l'adjudicatari:

- Cicle de Vida d'un servei:
  - Checkpoints.
  - Rols responsables de cada tasca o activitat.
- Gestió de la Configuració: Assegura que els canvis no afecten els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- Control de la documentació:
  - Procediments que assegurin que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Gestió de la documentació i dels requeriments del servei.
- Regles i procediments que garanteixin la millora contínua del servei.
- Planificació de les auditories internes que asseguren l'adequada documentació dels resultats i accions dutes a terme.
- Mètriques i indicadors.
- Pla de validació de la qualitat.
- Gestió de les responsabilitats relatives a l'actualització del Pla de Qualitat.

- Gestió de riscos que possibiliti una reducció o eliminació dels possibles impactes en el servei.
- Plans de continuïtat del servei que garanteixin que el servei podrà ser restaurat en cas de produir incidències en el mateix.
- Pla de formació que cobreixi les necessitats dels rols implicats en el servei.

Els rols responsables de l'execució de les activitats detallades en el Pla de Qualitat, l'Assegurament de la Qualitat i Auditories internes han d'estar reflectits en l'apartat corresponent a recursos.

Els licitadors han de presentar aquest Pla de Qualitat en el conjunt de documentació tècnica que es detalla al punt "Proposta Tècnica", amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa.

9.11. QUALITAT DEL SERVEI I TREBALLS REALITZATS

Li correspon a l'adjudicatari establir les mesures que consideri adients per lliurar les tasques del contracte amb els nivells mínims de qualitat que li són exigits.

En aquest sentit, l'IMI exigirà l'acompliment dels nivells de servei descrits al següent punt

L'IMI procedirà a l'avaluació d'aquesta qualitat mitjançant:

1. El rebuig o no acceptació de les tasques determinades en l'ordre de treball que no hagin acreditat l'entrega de la documentació associada.
2. Auditories aleatòries en el temps que per si mateix o realitzades per empreses especialitzades es facin sobre el conjunt de les tasques o en algunes fases d'aquest conjunt tant des de l'òptica tècnica com des de l'òptica d'acompliment de la metodologia.

9.11.1. Auditories

9.11.1.1. Introducció

L'IMI en funció del desenvolupament del contracte pot exigir la realització, sense càrrec per l'IMI, d'auditories sobre el conjunt del seu treball des de la vesant de qualitat.

L'auditoria en cas que s'exigeixi ha de complir els següents requisits:

- Periodicitat: semestral
- Abast: totalitat del servei
- Serveis a auditar: compliment del contracte amb la qualitat desitjada.
- Equip: Empresa externa i independent.
- Resultat: informe d'auditoria.

9.11.1.2. Objectiu de les Auditories

L'objectiu de les Auditories i Revisions de Qualitat dels Serveis Contractats és proporcionar visibilitat i control a la Direcció de l'IMI, sobre el grau de compliment dels adjudicataris amb els aspectes formals del servei.

Els aspectes més rellevants a verificar des del punt de vista d'Auditoria són:

- Verificació del compliment del Pla de Qualitat de Servei, de les condicions contractuals i dels procediments de treball establerts.
- Pla de Qualitat del Servei: fent especial èmfasi en els mecanismes d'assegurament de la qualitat proposats per l'adjudicatari per a les seves pròpies activitats (controls, revisions, proves, auditories internes de l'adjudicatari, etc.).
- Condicions contractuals: verificant, entre altres aspectes, el compliment dels requisits d'infraestructura (entorns, eines, comunicacions, etc.), Requisits de personal i requisits de seguretat inclosos en el contracte.
- Procediments de treball: verificant el compliment del Model Operatiu i els procediments definits per a la prestació del servei (activitats, i lliurables).

Els aspectes més rellevants a verificar des del punt de vista d'una revisió són:

- Revisió del compliment i execució del Pla d'Acció proposat per a la seva esmena.

9.11.1.3. Procediment d'Auditoria

L'adjudicatari cooperarà en l'auditoria, responent immediatament a les informacions demanades per a l'execució de mateixa, i auxiliant als auditors en el que considerin necessari.

Tota informació addicional o canvis de conducció d'un procés o com a resultat d'auditoria, serà considerada informació confidencial, segons els termes i condicions del Contracte.

La realització de l'auditoria en cap moment no eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis d'acord amb els termes inclosos en aquest Plec.

Els costos dels mitjans emprats per l'adjudicatari associats a les auditories no podran ser repercutits en cap cas a l'IMI.

9.11.1.4. Resultats de l'Auditoria

L'auditoria es realitzarà mitjançant revisions dels diferents aspectes que es contemplen en aquest plec, en el pla de qualitat del servei, , formació, model de prestació del servei , així com qualsevol altre pla detallat en aquest plec. L'equip auditor buscarà la conformitat amb els aspectes establerts en aquests documents. Per a cada aspecte revisat existiran quatre possibles valoracions:

- **Conformitat**: si es compleix completament amb el que indica aquests documents.

- **No Conformitat Major**: si hi ha evidències d'incompliment de requisits relacionats amb la metodologia o els models de governança que incideixen directament en la prestació del servei (Documentació i Lliurables, Gestió de la Configuració, Traçabilitat, Gestió de Riscos i Problemes, Seguretat Físic-Lògica, etc.)
- **No Conformitat Menor**: si hi ha evidències d'incompliment de requisits no relacionats amb la metodologia o els models de governança i els procediments vigents en el moment d'execució de l'auditoria relatius als serveis d'aquest plec que incideixin directament en la qualitat del servei (organigrama, Responsabilitats, Rols, pla de recursos, Temes Laborals i Subcontractacions, Certificacions, Acords de Confidencialitat, Auditories internes de l'adjudicatari, comunicacions, etc.)
- **Observació**: addicionalment, s'inclouran com "observació" aquells fets identificats que afectin o puguin afectar, segons el parer de l'equip auditor, a la qualitat del servei, però que no suposin un incompliment formal dels compromisos establerts. Les observacions identificades en un informe d'Auditoria podrien derivar a No Conformitats en futures auditories si no s'esmenen.

A la finalització de l'auditoria les parts revisaran les desviacions i/o observacions detectades respecte a l'acordat en el contracte. L'adjudicatari haurà d'establir un pla d'acció amb:

- Accions per assegurar que les desviacions i / o observacions detectades es corregeixin.
- Identificació de responsables i dates límit per l'execució de les accions.

L'adjudicatari haurà de presentar a l'IMI el pla d'acció en el termini d'un mes des de la comunicació dels resultats finals de l'auditoria. Serà responsabilitat de l'adjudicatari la realització de les accions en els terminis establertes en el pla d'acció.

9.11.1.5. Resultats de la Revisió

Alternativament a les auditories completes, l'IMI podrà realitzar una revisió de l'execució del pla d'acció proposat després dels resultats de l'auditoria del període anterior.

El mètode consistirà en la revisió del pla d'acció de cadascuna de les No Conformitats detectades i també es revisaran algunes de les observacions.

S'avaluarà amb una valoració entre 0 i 5 l'estat de l'acció corresponent, si l'acció s'obté un valor de 3 o més, es donarà com a vàlid el pla d'acció i per tant "tancada la No Conformitat".

9.12. GESTIÓ DE COSTOS

L'adjudicatari del present contracte, dins el marc TIC de l'Ajuntament, ha de disposar d'un marc de costos analítics que permeti a l'IMI obtenir informació de costos dels serveis per centre de cost. La informació necessària, ha de contenir com a mínim:

- Indicadors de costos de serveis.
- Usuaris donats alta al servei.
- Usuaris que fan servir el servei per setmana / dia.
- Desglossament de les partides de cada factura per a poder fer-ne seguiment.

Donada la vida dinàmica del contracte, i durant la fase d'execució de contracte, amb una periodicitat mínima de 6 mesos s'analitzaran els costos unitaris de cada ítem associat als diferents Projectes o serveis prestats a l'Ajuntament.

9.13. GESTIÓ DE LA DOCUMENTACIÓ

El Servei, dins el marc de treball, posarà a disposició tots els documents de treball i consulta a través d'eines de treball col·laboratiu. Igualment s'haurà de traslladar aquesta documentació als diferents departaments de l'IMI que la puguin sol·licitar. Durant els primers 3 mesos de l'execució del contracte l'adjudicatari haurà de presentar una proposta al respecte.

10. PROPOSTA TÈCNICA

Els licitadors presentaran la seva oferta tècnica de realització del contracte tant per fer comprensible la seva proposta com per facilitar i fer possible la seva valoració d'acord amb els criteris d'adjudicació assenyalats en el plec de clàusules administratives particulars que regeixen per aquesta contractació.

Els licitadors hauran de presentar la seva oferta en format electrònic. A l'oferta tots els arxius han d'estar en qualsevol dels formats admesos per la Plataforma de Contractació Electrònica d'acord amb els requeriments assenyalats en el plec de clàusules administratives particulars, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.

Els licitadors podran adjuntar tota la informació complementària que considerin d'interès, sempre que es presentin els continguts mínims. Aquests hauran d'estructurar-se de la següent forma:

Es presentaran dos sobres electrònics:

- **Sobre electrònic B**: En el sobre electrònic B s'inclourà la documentació indicada en el punt 10.1.

- **Sobre electrònic C:** En el sobre electrònic C s'inclourà la documentació indicada en el punt 10.2.

A l'interior de cada sobre s'ha d'incorporar una relació, en full independent, dels documents que hi conté ordenats numèricament, especialment en el sobre B, ja que aquest ha de respondre a les explicacions i compromisos sobre tots i cadascun dels criteris de valoració subjectius definits.

10.1. CONTINGUT SOBRE ELECTRÒNIC B

En el sobre electrònic B s'inclourà la següent documentació indexada de manera que faciliti la seva localització. Per a cada apartat, s'indica entre parèntesi el nombre màxim de pàgines.

Resumen executiu (10 pàgines)

Un resumen executiu de la proposta, indicant com el licitador planteja assolir els objectius definits. En aquesta secció el licitant ha d'exposar el seu enteniment del contracte, els serveis i les línies principals de la seva estratègia per afrontar-lo tenint en compte els requeriments exposats en el plec de prescripcions tècniques. El licitador presentarà els diagrames i esquemes que cregui necessaris i que ajudin a visualitzar el grau de comprensió del contracte i el servei demanat. Es valorarà un plantejament que demostri la millora dels mínims requerits descrits al Plec de Prescripcions Tècniques, en els apartats corresponents a l'objecte, abast, descripció i metodologia del servei.

Model de relació (màxim 5 pàgines)

En aquesta secció el licitant ha d'exposar el seu enteniment i la seva proposta de models de gestió del risc descrit a l'apartat Model de Relació IMI/Adjudicatari d'aquest plec de prescripcions tècniques a generar per al servei als diferents destinataris. També es descriurà el model de relació dels serveis OSAT i SOC.

Solució proposada pels serveis (màxim 60 pàgines)

Un document que defineixi en detall la informació que es sol·licita i que contindrà com a mínim, els capítols que es detallen a continuació:

a) Plantejament general i tècnic del contracte (màxim 6 pàgines).
b) Servei de Preventiu (màxim 5 pàgines).
c) Monitorització i Detecció d'Incidents (màxim 5 pàgines).
d) Resposta a incidents molt crítics o Alt risc (màxim 5 pàgines).
e) Model de reporting d'indicadors del servei (5 pagines).
f) Millores i Evolució del Servei (màxim 4 pàgines).
g) Aportació eines addicionals (màxim 2 pàgines)
h) Catàleg de Serveis (màxim 4 pàgines).
i) Gestió, operació, administració i manteniment (màxim 3 pàgines).
j) Estructura organitzativa servei OSAT (màxim 3 pagines)

k) Serveis de suport expert en comunicacions i seguretat (màxim 4 pàgines).

l) Serveis de consultoria (màxim 3 pàgines).

m) Proposta de gestió de projectes (màxim 5 pàgines).

1. Equip dedicat (recursos) a aquestes tasques indicant:
   (1) Organització de l'equip
   (2) Nombre de personal (i percentatge/estimació de dedicació)
   (3) Perfils assignats
2. Metodologia:
   (1) Documentació a presentar
   (2) Seguiment del projecte
   (3) Reunions planificades (la periodicitat de les mateixes haurà de ser aprovada per l'IMI)

n) Pla d'activitats i actuacions especials (màxim 4 pàgines).

o) Proposta d'altres millores (màxim 2 pàgines).

<u>Pla de Formació (màxim 4 pàgines)</u>

Els licitadors hauran de presentar la seva proposta del Pla de formació detallat, tant pel personal del SAU, com pel personal tècnic de l'IMI responsable del servei per donar-los a conèixer les característiques i funcionament dels serveis, els processos de gestió i els continguts tècnics específics. Hauran d'especificar com a mínim:

- Equip dedicat (recursos) a aquestes tasques indicant:
  - Organització de l'equip
  - Nombre de personal (i percentatge/estimació de dedicació)
  - Perfils assignats
- Metodologia:
  - Documentació a presentar
  - Seguiment del projecte
  - Reunions planificades (la periodicitat de les mateixes haurà de ser aprovada per l'IMI)

10.2. CONTINGUT SOBRE ELECTRÒNIC C

En el sobre electrònic C s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars que regeixen per aquesta contractació.

Proposta econòmica dels serveis i subministraments

El proveïdor haurà de detallar una proposta econòmica dels subministraments i serveis següents:

Adquisicions, instal·lacions, configuracions i posada en marxa segons descrit al punt 4.2.10:

Oferta econòmica total sense IVA per a l'adquisició, instal·lació, configuració i posada en marxa i amb el següent desglossament d'aquest dels elements que el conformen a preu unitari:

Concepte	Tipus	Import unitari sense iva
DDI (DNS, DHCP, IPAM)	Maquinari	
Equip amb capacitats per establir VPN site-to-site	Maquinari	
Servidors i Cabines d'OSAT	Maquinari	
SFP's 10G per equipament gestionat per OSAT	Maquinari	
Import total sense IVA		

Oferta econòmica sense IVA per la prestació dels projectes:

Concepte	Hores/perfil	Import unitari sense iva
Projecte Complexitat ALTA - 1 mes	# hores Perfil N2/ cost hora # hores Perfil N3 / cost hora # hores cap projectes/ cost hora	
Projecte Complexitat Baixa - 1 mes	# hores Perfil N2/ cost hora # hores Perfil N3 / cost hora # hores cap projectes/ cost hora	
Import total sense IVA		

Oferta econòmica total sense IVA pel cost de manteniment de les garanties dels fabricants desglossat pels anys de vigència del contracte i amb el següent desglossament d'aquest:

Concepte Manteniment i llicenciament a 1 any	Descripció	Import unitari sense iva
Manteniment Cisco ASA		
Manteniment F5		
Manteniment Palo Alto Networks		
Manteniment Pulse Secure		
Manteniment Fortinet		
Manteniment Aruba Networks		
Manteniment Efficient IP		
Manteniment Trendmicro		
Manteniment Fluke		
Manteniment Infoblox		
Manteniment equipament Cabines VMWARE		
Manteniment Checkpoint		
Manteniment equipament CISCO		
Manteniment Alienvault		
Manteniment Tuffin		
Import total sense IVA		

Oferta econòmica total sense IVA per la prestació dels serveis de suport expert i operacions i amb el següent desglossament:

Concepte	Cost	Import unitari sense iva
Cost de la prestació dels serveis - **Serveis de suport expert** - **Serveis d'operacions**		

- **Serveis de SOC**		
- **Servei de Preventiu**		
Import total sense IVA		

Oferta econòmica sense IVA per la prestació del servei incident handling

Concepte	Import unitari perfil/h sense iva
- **Servei incident handling**	

Addicionalment, aportarà:

a) Propostes d'ampliacions de les garanties dels subministraments oferts

11. CLÀUSULES GENERALS DE SEGURETAT

11.1. SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU.

L'IMI ha adoptat com a marc de referència per a la Seguretat dels Sistemes d'Informació el conjunt de bones pràctiques internacionalment reconegudes que desenvolupa la norma ISO-27002:2013.

L'IMI, com a Organisme Autònom de caràcter administratiu de l'Administració Local depenent de l'Ajuntament de Barcelona, es troba subjecte al Principi de Legalitat i posa especial èmfasi en el compliment de les obligacions legals que es deriven de la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia de Drets Digitals, de la Llei 39/2015 en tot allò que fa referència a l'accés dels ciutadans als serveis públics, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 3/2010 de 8 de gener pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

Les empreses licitadores s'obliguen a vetllar pel compliment de la legislació vigent aplicable a l'objecte del contracte i especialment pel què fa referència a la protecció de dades de caràcter personal.

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i IMI indistintament. De conformitat als seus estatuts s'ha d'entendre que

l'IMI actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les que no sigui directament titular.

11.1.1. Compliment normatiu

L'adjudicatari haurà d'aplicar totes les normatives i procediments de Seguretat que li siguin d'aplicació segons l'abast del seu servei, havent de contribuir igualment en la millora i revisió de la documentació existent del cos normatiu. Tanmateix, qualsevol procediment del servei susceptible a ser incorporat al Cos Normatiu de Seguretat de la Informació (CNSI) s'haurà de documentar i estructurar com a part d'aquest.

L'adjudicatari haurà de lliurar a l'IMI, la seva Política de Seguretat de la Informació i l'aplicació d'aquesta en els serveis oferts a l'IMI.

L'adjudicatari vetllarà pel compliment dels estàndards de l'IMI i podrà serà auditat de forma anual per valorar el grau de compliment i identificar riscos de seguretat.

L'adjudicatari haurà de garantir l'accés del personal autoritzat de l'IMI a la informació de seguretat. Tota la informació de seguretat haurà d'estar sempre disponible per a aquest personal, autoritzat i prèviament identificat. L'IMI i l'adjudicatari establiran conjuntament els mecanismes per facilitar l'accés del personal autoritzat de l'IMI a aquesta informació, establint els controls de seguretat mínims.

11.1.1.1. Control del compliment normatiu

- Qualsevol canvi en un entorn productiu que afecti tant a infraestructura com a programari base, o de nous serveis, anirà precedit d'una comprovació de l'adequació al cos normatiu de l'IMI. En cas que no s'adeqüi, l'adjudicatari haurà d'adaptar-se a les normatives i pot demanar assessorament a l'àrea de Seguretat per analitzar les viabilitats per a l'adequació.
- L'adjudicatari haurà de tractar les excepcions amb l'àrea de Seguretat i establir una planificació de resolució de les excepcions autoritzades.
- En els casos que es determinin, s'instal·laran agents de eines automàtiques, per auditar el grau de compliment normatiu de manera contínua i automàtica

11.1.2. Responsable de seguretat

L'adjudicatari nomenarà un Responsable de Seguretat, el qual haurà de vetllar pel compliment dels següents requeriments:

- Actuar d'interlocutor únic per a tots els aspectes de seguretat del contracte.

- Garantir que tots els serveis prestats pel proveïdor a l'Ajuntament es realitzen d'acord al model i requeriments de seguretat establerts per l'IMI i seguint la normativa de seguretat vigent.
- Garantir i liderar dins la seva organització la correcta implantació dels nivells de seguretat i les seves corresponents mesures (tècniques, organitzatives i jurídiques), així com les directrius en matèria de seguretat establertes per l'IMI.
- Assegurar que tot el personal de l'adjudicatari que prestarà serveis a l'Ajuntament, passi per un pla de conscienciació i formació en matèria de seguretat.
- Informar al seu personal qualsevol obligació a què l'empresa estigui sotmesa per contracte, formar al seu personal en les polítiques i instruccions de l'Administració Municipal en cas que els sigui d'aplicació i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.
- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

11.2. CLÀUSULA DE PROPIETAT INTEL·LECTUAL

L'accés a informació i/o productes protegits per la propietat intel·lectual, propietat de l'Ajuntament de Barcelona, necessaris per al desenvolupament del producte o servei contractat no pressuposa en cap cas la cessió de la mateixa ni el seu ús sense autorització expressa.

11.3. CONFIDENCIALITAT

L'adjudicatari s'obliga a no difondre i a guardar el més absolut secret de tota la informació a la qual tingui accés en compliment del present contracte i a subministrar-la només al personal autoritzat per l'Ajuntament.

L'adjudicatari queda expressament obligat a mantenir absoluta confidencialitat i reserva sobre qualsevol dada que pogués conèixer com a conseqüència de la participació en la present licitació, o, amb ocasió del compliment del contracte, especialment els de caràcter personal, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

Quan l'objecte del contracte sigui la construcció i/o el manteniment de Sistemes d'Informació i/o Infraestructures Tecnològiques, el deure de secret inclou els components tecnològics i mesures de seguretat tècniques implantades en els mateixos.

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir

l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

Un cop finalitzat el present contracte, l'adjudicatari es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Ajuntament, així com qualsevol altre producte obtingut com a resultat del present contracte.

11.4. CLÀUSULA PER A LA PROTECCIÓ DE DADES DE CARACTER PERSONAL

L'adjudicatari resta obligat al compliment del que estableixen la Llei Orgànica 3/2018 de Protecció de Dades Personals i Garantia de Drets Digitals (LOPDGDD) i el Reglament Europeu de Protecció de Dades (RGPD).

L'adjudicatari es considera, a efectes d'aquest contracte, encarregat del tractament en els termes establerts per la vigent normativa de protecció de dades personals.

L'adjudicatari s'obliga a tractar les dades de caràcter personal a les quals tingui accés en virtut de l'execució del contracte, d'acord amb les instruccions dictades per l'Ajuntament de Barcelona.

L'adjudicatari no podrà aplicar ni utilitzar les dades de caràcter personal a les quals tingui accés amb finalitats diferents a les de l'objecte del contracte i necessàries per a la seva execució. Tampoc podrà comunicar-les a tercers, ni tan sols per a la seva conservació.

Les dades personals a les que, per motiu d'aquest contracte, tingui accés l'adjudicatari no podran sortir de l'àmbit municipal.

En cas que haguessin de sortir dades de l'entorn municipal caldrà un acord entre el departament de Seguretat de l'IMI i el responsable de seguretat del contracte, sotmès a les condicions que s'indiquin i amb garanties de destrucció dels originals i les còpies o backups existents a la finalització del contracte.

Correspon a l'Ajuntament de Barcelona, la resolució dels procediments d'exercici dels drets d'accés, rectificació, cancel·lació i oposició que puguin exercir els titulars de dades de caràcter personal.

1.- L'adjudicatari està obligat a guardar secret en relació a les dades de caràcter personal a les quals tingui accés en virtut d'aquest contracte, obligació que subsistirà, fins i tot després de la finalització de la relació contractual.

Així mateix, l'adjudicatari ha de guardar reserva respecte de les dades o antecedents dels quals hagi tingut coneixement en ocasió del present contracte i que corresponguin, o bé a dades de caràcter personal o a dades identificades com a confidencials per motius de seguretat.

En tot cas, i sens perjudici d'altres mesures a adoptar d'acord amb la normativa vigent en matèria de protecció de dades personals, només podran accedir a les esmentades dades, informacions i documentació, les persones estrictament imprescindibles per al desenvolupament de les tasques inherents al propi encàrrec, que hauran d'estar informades del caràcter confidencial i reservat de les dades, i l'obligació de secret als quals estan sotmeses, i l'adjudicatari serà responsable del compliment d'aquestes obligacions per part del seu personal. Així mateix, s'obliga a realitzar la

formació necessària al personal al seu càrrec que tingui accés a les dades personals, garantint el compliment de les obligacions derivades de la normativa de protecció de dades.

2.- El contractista està obligat a implantar les mesures de caràcter tècnic i organitzatiu necessàries per garantir la seguretat de les dades de caràcter personal a les quals tindrà accés per l'execució del contracte, i haurà de garantir que no es produeixin alteracions, pèrdues, tractaments o accessos no autoritzats, tenint en compte I' estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a que estan exposades, i en estricte compliment de la normativa vigent en matèria de protecció de dades de caràcter personal.

Les mesures de seguretat a implantar són d'aplicació als fitxers, centres de tractament, locals, equips, sistemes, programes i persones que intervinguin en el tractament de les dades en els termes que estableix la Llei Orgànica 3/2018 de protecció de dades de caràcter personal i garantia dels drets digitals, el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes dades, la Llei 11/2007 d'Accés dels Ciutadans als Serveis Públics i la resta de l'ordenament jurídic que en sigui d'aplicació. En cas que la normativa estableixi noves mesures de seguretat, el contractista i estarà obligat a la seva implantació.

L'adjudicatari tindrà a disposició dels tècnics municipals còpia de les mesures de seguretat aplicades (document de seguretat de l'adjudicatari).

L'adjudicatari té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa.

L'adjudicatari ha de posar en coneixement de l'òrgan de contractació, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de les dades de caràcter personal.

3.- L'Ajuntament de Barcelona podrà verificar que l'adjudicatari té implantades les mesures necessàries per garantir la seguretat de les dades de caràcter personal.

4.- Durant la vigència del contracte l'adjudicatari haurà de conservar qualsevol dada objecte de tractament, llevat que rebi indicacions en sentit contrari de l'Ajuntament de Barcelona.

5.- Una vegada executat el contracte, l'adjudicatari haurà de destruir o retornar a l'Ajuntament de Barcelona, d'acord amb allò que s'estableixi legalment o les indicacions que en aquell moment li transmeti aquest Ajuntament, les dades de caràcter personal que hagin estat objecte de tractament per part d'aquell durant la seva vigència, juntament amb els suports o documents en que consti alguna dada de caràcter personal. El retorn de les dades es durà a terme en el format i els suports utilitzats per l'adjudicatari per al seu emmagatzematge.

En el cas que alguna previsió legal exigeixi la conservació de les dades, o de part d'elles, l'adjudicatari haurà de conservar-les, degudament bloquejades, per impedir-ne l'accés i el tractament en tant en quant puguin derivar-se responsabilitats de la seva relació amb l'Ajuntament de Barcelona.

6. L'incompliment del que s'estableix en els apartats anteriors pot donar lloc a l'empresa contractista sigui considerada responsable del tractament, als efectes d'aplicar el règim sancionador i de responsabilitats previst a la normativa de protecció de dades

L'adjudicatari s'obliga a demanar autorització a l'Ajuntament de Barcelona respecte de quins treballs seran objecte de subcontractació i quines seran les empreses que els realitzaran.

Per tal que aquestes tasques puguin ésser realment subcontractades, l'Ajuntament de Barcelona haurà d'haver donat permís exprés i escrit. Només llavors, actuant en nom i representació d'aquest Ajuntament, l'empresa contractada formalitzarà el corresponent contracte amb la empresa o empreses subcontractades que, als efectes de l'aplicació de la normativa de protecció de dades, tindran la consideració d'encarregats de tractament de l'Ajuntament de Barcelona. Aquests contractes s'afegiran com annex al contracte administratiu que formalitza aquesta adjudicació.

El tractament de dades realitzat per part del subcontractista haurà de complir amb la normativa vigent en matèria de protecció de dades de caràcter personal, i s'ajustarà així mateix a les obligacions assumides pel contractista i a les instruccions específiques que li doni l'Ajuntament de Barcelona al respecte.

11.5. CLÀUSULA PROGRAMARI DE L'AJUNTAMENT

L'empresa contractada, disposarà del programari necessari i farà servir la metodologia implantada pel Institut Municipal d'Informàtica (IMI) per al desenvolupament dels serveis contractats.

Si l'Administració Municipal ho considera necessari, es podrà instal·lar programari en els equips de l'empresa contractada, sempre sota la responsabilitat de l'empresa contractada, amb la finalitat d'obtenir una correcta prestació dels serveis contractats. Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

L'Administració Municipal continuarà essent la propietària o, en el seu cas, titular dels drets de propietat intel·lectual que el corresponen sobre el programari i bases de dades instal·lat en les màquines de l'empresa contractada, sense que la corresponent llicència d'ús suposi transferència o cessió, total o parcial de la titularitat, ni autorització per la seva utilització amb una finalitat diferent a la definida en el contracte de prestació de serveis.

L'empresa contractada donarà a conèixer a tot el personal adscrit a la prestació dels serveis, el contingut d'aquesta clàusula respecte al programari, sistemes operatius i bases de dades cedides per l'Administració Municipal, la seva obligació respecte a:

No reproduir-los.

No transmetre'ls a un altre sistema.

No modificar, adaptar, cedir, ni realitzar qualsevol altre activitat sobre el programari cedit, sense l'autorització de l'Administració Municipal.

No divulgar, publicar, ni posar a disposició d'altres persones diferents a les autoritzades.

Fer ús única i exclusivament per les tasques encomanades, incloses en els serveis contractats.

11.6. ACCÉS A SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT

11.6.1. Auditoria

L'IMI auditarà que l'adjudicatari vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

- Auditoria de seguretat periòdica/planificada: l'IMI podrà realitzar auditories de seguretat planificades per verificar el compliment dels requeriments de seguretat, de l'oferta de l'adjudicatari.
- Auditoria sobrevinguda: addicionalment l'IMI podrà efectuar més auditories que les planificades respecte el servei que s'està prestant.

En tots aquells casos en què l'IMI decideixi la realització d'una auditoria des de les instal·lacions de l'adjudicatari, aquest haurà de garantir a l'IMI l'accés necessari, incondicional i irrevocable als documents existents que estiguin relacionats amb l'abast de l'auditoria.

L'adjudicatari proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per l'IMI.

La realització de l'auditoria en cap moment eximirà l'adjudicatari del compliment dels compromisos derivats de la prestació dels serveis.

A la finalització de l'auditoria, es revisaran els resultats i s'elaborarà un pla d'acció per corregir les desviacions i/o observacions detectades. El conjunt del resultat serà signat per ambdues parts.

L'adjudicatari, d'acord amb el calendari establert al pla d'acció, es compromet a portar a terme les activitats establertes en el pla d'acció. L'IMI podrà verificar que el pla d'acció s'ha implementat correctament.

11.6.2. Gestió d'Incidents

Les persones adscrites a la prestació del servei hauran d'informar diligentment seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona qualsevol incident de seguretat del qual tinguin constància, ja sigui a través del servei o com a usuaris de sistemes de l'Ajuntament.

Davant qualsevol esdeveniment de seguretat tipificat com de nivell Alt, Molt Alt o Crític, haurà de ser comunicat al departament de Seguretat del IMI per a la seva revisió.

11.6.3. Registre d'activitat dels usuaris

Com a responsables de la gestió dels registres d'activitat dels usuaris, l'adjudicatari serà encarregat de:

- Determinar el període de retenció dels registres

- Garantir la seva data i hora
- Garantir la integritat dels mateixos
- Garantir que en cas d'existir còpies de seguretat, aquestes compleixen els mateixos requisits.

Sense considerar aquest llistat exclusiu, alguns dels possibles tipus d'activitats a registrar són:

- Activitats sospitoses
- Intents d'accés no autoritzat
- Excepcions i altres activitats no usuals
- Connexions establertes amb èxit
- Intents de connexió denegats i rebutjats
- Inicis de sessió vàlids i erronis
- Missatges d'error i alertes
- Temps de connexió elevats
- Ús concurrent d'identificadors d'usuari duplicats
- Accés remot de proveïdors
- Activitat del tallafocs
- Activitat dels administradors
- Inici i apagat dels sistemes
- Accés fallit a fitxers u objectes
- Canvis en la política de seguretat
- Canvis en els fitxers de registre o del sistema
- Còpies de seguretat i restauració de les mateixes
- Activitat de l'antivirus o altre software de detecció/prevenció

11.6.4. Sistema de mètriques

S'hauran de recopilar les dades dels sistemes administrats dins l'abast del present plec que permetin determinar el nivell de compliment de les mesures de seguretat del disposat per l'ENS a l'Annex II, prestant especial atenció a controls com:

- [op.acc.1] – Control d'accessos
- [op.acc.7] – Accés remot
- [op.exp.3] – Gestió de la configuració
- [op.exp.6] – Protecció front codi nociu
- [op.mon.1] – Detecció d'intrusions

Addicionalment, s'han de recollir dades per tal de valorar el sistema de gestió d'incidents, permetent obtenir:

- Número d'incidents de seguretat gestionats i tipificats segons els procediments interns.
- Temps destinat per solucionar el 50% dels incidents

- Temps destinat per solucionar el 90% dels incidents

11.6.5. Dimensionament/gestió de capacitats

El proveïdor disposarà del personal necessari amb les qualificacions professionals adients, per a la prestació del servei de forma adequada.

11.6.6. Accés a la informació

Si l'accés a les dades es fa als locals de l'Ajuntament de Barcelona, o si es fa de forma remota exclusivament a suports o sistemes d'informació de l'Ajuntament, l'adjudicatari té prohibit incorporar les dades a d'altres sistemes o suports sense autorització expressa i haurà de complir amb les mesures de seguretat establertes per l'IMI.

11.6.7. Control d'accés

11.6.7.1. Accés local

L'adjudicatari haurà de protegir les estacions de treball amb les quals prestarà el servei i es compromet a complir les següents condicions:

- La informació revelada a qui intenta accedir ha de ser la mínima imprescindible. Els diàlegs d'accés proporcionaran únicament la informació indispensable.
- El nombre d'intents permesos serà limitat, bloquejant l'oportunitat d'accés una vegada efectuats un cert nombre de fallades consecutives.
- Es registraran els accessos amb èxit, i els fallits.
- El sistema informarà a l'usuari de les seves obligacions immediatament després d'obtenir l'accés.
- S'informarà a l'usuari de l'últim accés efectuat amb la seva identitat.

11.6.7.2. Accés remot

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Ajuntament, sent els costos de connexió a càrrec de l'empresa adjudicatària.

La connexió remota als sistemes de l'Ajuntament es realitzarà seguint els protocols establerts per l'IMI per als sistemes de l'Ajuntament.

11.6.7.3. Segregació de funcions i tasques

L'adjudicatari s'encarregarà de que el sistema de control d'accés s'organitzi de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.

En concret, se separaran almenys les següents funcions:

- Desenvolupament d'operació. Garantint, com a mínim, que els desenvolupadors únicament disposin d'accés a l'entorn de preproducció i desenvolupament. La configuració dels entorns productius l'haurà de realitzar persones o equips diferents.
- Configuració i manteniment del sistema d'operació.
- Auditoria o supervisió de qualsevol altra funció.

11.6.7.4. Accés de perfils administradors

Respecte l'accés dels usuaris administrador dels sistemes objecte del plec, aquests hauran de complir amb les polítiques internes d'usuaris administradors definides per l'IMI, on entre d'altres:

- Hauran d'autenticar-se sempre com usuaris no privilegiats del sistema i només amb fins d'administració podran autenticar-se com administradors del mateix.
- Han de comptar amb el mínim de privilegis necessaris per a la situació que requereix l'ús de credencials d'administració.
- Els sistemes emprats al servei han d'estar adscrits a la política de contrasenyes de l'IMI.
- Qualsevol accés amb credencials d'administració haurà de comptar amb un doble factor d'autenticació que protegeixi el sistema.
- En cas de comptar amb un sistema de gestió de contrasenyes, el seu ús ha de restar degudament procedimentat i tots els usuaris adscrit al recollit en aquest.
- S'hauran de registrar totes les accions dutes a terme amb credencials d'administració
- L'adjudicatari haurà de validar els usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades.
- L'IMI haurà de tenir accés a les eines de gestió d'identitats dels administradors dels serveis que continguin informació de la l'Ajuntament de Barcelona en mode consulta per poder fer les revisions que es considerin pertinents.

11.6.8. Gestió del Personal

11.6.8.1. Deures i obligacions del personal

El Cap del servei de l'empresa adjudicatària durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.

L'empresa adjudicatària està obligada a implantar i donar a conèixer al seu personal els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat, integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

El Cap del servei de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte i formar al seu personal en la política i instruccions de l'Ajuntament que els sigui d'aplicació.

El Cap del servei haurà d'informar a tothom que presti serveis dins del marc del contracte, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat de la informació i protecció de dades de caràcter personal, especificant les mesures disciplinàries al fet que pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El Cap del Servei de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Ajuntament, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al Cap del servei de l'Ajuntament, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

Es contemplarà el deure de confidencialitat respecte de les dades a les que tingui accés, tant durant el període de duració del contracte, com posteriorment a la seva terminació.

L'empresa adjudicatària haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

11.6.8.2. Formació i conscienciació

L'adjudicatari realitzarà les accions necessàries per conscienciar regularment al personal sobre el seu paper i responsabilitat respecte a la seguretat dels sistemes. Es recordarà regularment:

- Normatives sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona.

- Normativa de seguretat relativa al bon ús dels sistemes.

- Normativa d'identificació i comunicació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat.

L'adjudicatari haurà de formar regularment al personal en aquelles matèries que requereixin per a l'acompliment de les seves funcions, en particular en relació a configuració de sistemes, detecció i reacció a incidents, i gestió de la informació i dades personals en qualsevol tipus de suport.

L'Ajuntament podrà demanar evidències de les diferents accions de formació i conscienciació que l'adjudicatari ha realitzat sobre el personal assignat a l'execució del contracte.

11.6.9. Clàusula de comunicacions externes

L'adjudicatari disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'adjudicatari serà el responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús del certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

11.6.10. Protecció del lloc de treball

11.6.10.1. Lloc de treball buit

L'adjudicatari haurà d'establir una política de "taules netes" respecte a la documentació de l'Ajuntament. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

El material haurà de quedar guardat en un espai tancat quan no s'estigui utilitzant.

11.6.10.2. Bloqueig del lloc de treball

L'adjudicatari garantirà que els seus equips es bloquejaran al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de l'usuari per reprendre l'activitat.

11.6.10.3. Protecció d'equips

L'adjudicatari es compromet a que els equips que surtin, o puguin sortir de l'empresa adjudicatària, estaran protegits adequadament contra accessos no autoritzats en cas de pèrdua o robatori.

Sense perjudici de les mesures generals que els afectin, es requereix a l'adjudicatari que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Els usuaris hauran de disposar d'un canal de de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a l'IMI.

S'evitarà, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que habilitin un accés a altres equips de l'organització, o unes altres de naturalesa anàloga.

Addicionalment, els equips hauran de disposar:

- Solució antivirus actualitzada a la última versió i configurada per a que realitzi anàlisis regulars de l'equip.
- Política d'actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant aquelles actualitzacions crítiques.
- *Firewall* habilitat restringint el tràfic entrant a l'equip al mínim necessari.

11.6.10.4. Medis alternatius

L'adjudicatari garantirà l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius hauran d'estar subjectes a les mateixes garanties de protecció. Igualment, s'haurà d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

11.6.11. Protecció dels Suports Informàtics

L'adjudicatari haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

11.6.11.1. Etiquetat

L'adjudicatari es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

11.6.11.2. Criptografia

Qualsevol informació corporativa que requereixi ser xifrada a la seva ubicació d'emmagatzemament, en particular a tots els dispositius extraïbles del tipus CD, DVD, discos USB,

o uns altres de naturalesa anàloga, han de seguir els estàndards de seguretat, custòdia i protecció de les claus establerts per IMI-Seguretat.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'adjudicatari haurà de presentar-les per ser validades per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

11.6.11.3. Transport

L'adjudicatari garantirà que els dispositius romanen baix control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'adjudicatari garantirà que es segueix el procediment de transport, de manera que s'haurà de disposar d'un registre de sortida que identifiqui al transportista que rep el suport per al seu trasllat i d'un registre d'entrada que identifiqui al transportista que el lliura, conjuntament amb un procediment rutinari que quadri les sortides amb les arribades i elevi les alarmes pertinents quan es detecti algun incident.

11.6.11.4. Esborrat i destrucció

L'adjudicatari haurà de seguir els estàndards i normes de l'IMI respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut. S'hauran de destruir de forma segura els suports en cas de que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, fent us dels productes certificats per l'IMI.

Periòdicament i segons les necessitats de recurrència d'aquestes activitats, s'haurà d'informar i lliurar al responsable del contracte el certificat de destrucció corresponent, on quedarà especificat com a mínim, el identificador dels actius, el mètode d'esborrat i/o destrucció emprat, la data de l'activitat i el destí dels actius.

11.6.12. Protecció de la Informació

11.6.12.1. Neteja de documents

L'adjudicatari disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura serà especialment rellevant quan el document es difongui àmpliament, com quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

11.6.12.2. Protecció del correu electrònic

L'adjudicatari resta obligat a l'ús del correu electrònic corporatiu pel tractament d'informació i desenvolupament de les seves funcions dins l'Ajuntament.

En el cas de que sota alguna circumstància específica l'adjudicatari faci ús del seu correu electrònic corporatiu per gestionar informació de l'Ajuntament, l'haurà protegir enfront d'amenaces que li són pròpies:

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'adjudicatari.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:
    - Correu no sol·licitat (*spam*)
    - Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
    - Codi mòbil de tipus *applet*.

L'adjudicatari establirà polítiques d'ús del correu electrònic que inclourà com a mínim:

- Limitacions a l'ús com a suport de comunicacions privades.
- Realitzar activitats de conscienciació i formació relatives a l'ús del correu electrònic per al seu personal, per exemple per detectar casos de *malware* o *phishing*.

Si l'Ajuntament considera que la informació tractada pel contracte és prou sensible, facilitarà a l'adjudicatari un correu electrònic de l'Ajuntament el qual es convertirà en la via de comunicació entre l'adjudicatari i l'Ajuntament.

11.6.13. Protecció de les instal·lacions

Les instal·lacions de l'adjudicatari hauran de disposar de certes condicions de seguretat física:

- En cas de emmagatzemar informació de l'Ajuntament de Barcelona, disposar de les mesures de seguretat pertinents per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació.
- Garantir que la informació de l'Ajuntament de Barcelona no pugui ser visible i/o audible des de l'exterior de les instal·lacions.

11.6.14. Gestió d'excepcions

Qualsevol excepció als anteriors apartats no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials a IMI-Seguretat per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

11.7. CLÀUSULES DE SEGURETAT PER A LA IMPLANTACIÓ I ADMINISTRACIÓ DE PRODUCTES

11.7.1. Gestió d'identitats, autenticació d'usuaris

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuaris, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants.

L'empresa proveïdora haurà de validar i revisar accessos dels usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades. Els comptes d'usuari estaran integrats amb l'eina que l'IMI posa a disposició.

11.7.1.1. Autenticació interna

Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el repositori central per a l'autenticació dels usuaris. La solució d'autenticació corporativa utilitzada per l'IMI és l'Oracle Access Manager (OAM) que proveeix el Single Sign On corporatiu.

La integració amb l'OAM es podrà fer mitjançant les següents opcions:

- Integració mitjançant capçaleres.
- Integració mitjançant l'estàndard SAML 2.0.
- Integració mitjançant l'estàndard OAuth 2.0.

11.7.1.2. Autenticació externa

Els usuaris externs (fora de l'àmbit municipal, empreses i altres persones físiques - clients de l'aplicatiu) hauran d'autenticar-se mitjançant la solució corporativa (Mòdul Comú d'Autenticació).

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació, requerint així una verificació de la identitat de l'usuari que sol·licita accés. Actualment, la solució implantada al IMI fa ús de Google Authenticator.

11.7.2. Autorització dels usuaris als sistemes

L'IMI disposa d'un mecanisme d'autorització d'usuaris corporatiu basat en el producte Oracle Unified Directory (OUD). L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en el repositori central d'autorització (OUD).

En cas que l'adjudicatari no pugui delegar l'autorització per impediments greus del sistema, com a mínim, hauran d'integrar-se amb GID (eina de gestió d'identitats corporativa basada en Oracle Identity Manager) per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els funcionals definits a GID (capa de negoci).

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats. El temps dedicat normalment a integrar un connector estàndard amb una BBDD Oracle és aproximadament 80 hores d'un tècnic.

11.7.2.1. Perfilat d'usuaris

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i per IMI-Seguretat.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
- Mínim privilegi, els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir les seves obligacions.
- Necessitat de Conèixer, els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.
- Capacitat d'autorització, només i exclusivament el personal amb competència d'autorització, podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.

La gestió de permisos haurà de ser en base a perfils i rols, podent un usuari tenir múltiples perfils. Els usuaris només podran accedir a aquelles funcions que tinguin expressament autoritzades. La implementació ha de permetre la implementació de matrius de segregació de funcions i l'agilitat en l'administració d'aquests permisos.

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant perfils (rols) de seguretat. Entenent com a perfil o rol una entitat que dona accés a una sèrie d'operacions.

Sota la premissa d'aquests criteris generals, l'adjudicatari haurà de dissenyar el joc de permisos i autoritzacions requerits pels sistemes d'informació implementats, en base al document 'Pla d'Autoritzacions'. Aquest document serà revisat i actualitzat per l'adjudicatari per incloure nous punts a tractar o adaptacions dels punts existents.

11.7.3. Protecció de les aplicacions i serveis web

L'adjudicatari garantirà que els subsistemes dedicats a la publicació de la informació hauran de ser protegits front a les amenaces que li siguin pròpies:

- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
    - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
    - Es previndran atacs de manipulació de URL.
    - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pagina web a traves del seu navegador, a petició del servidor de la pagina, conegut en la terminologia anglesa com a "cookies".
    - Es previndran atacs d'injecció de codi.
- Es previndran intents d'escalat de privilegis.
- Es previndran atacs de "cross site scripting".
- Es faran servir certificats d'autentificació de llocs web d'acord amb les polítiques establertes per IMI-Seguretat.

11.7.4. Acceptació i posta en servei

L'adjudicatari ha de comprovar el correcte funcionament de qualsevol sistema i/o aplicació que implementi, per tal de garantir que:

- Es compleixen els criteris d'acceptació en la matèria de seguretat.
- No es deteriora la seguretat d'altres components del servei.

Addicionalment, l'adjudicatari realitzarà les següents inspeccions prèvies a l'entrada en servei:

- Anàlisis de vulnerabilitats.
- Test de penetració.

11.7.5. Dades de proves

L'adjudicatari es compromet a assumir tota la responsabilitat en la creació de dades de proves per testejar els serveis. En cap cas s'utilitzaran dades de l'entorn de producció per fer proves.

En cas que sigui necessari copiar dades de l'entorn productiu, aquestes seran les mínimes necessàries i hauran de ser sotmeses a un procés d'ofuscació. L'adjudicatari es farà càrrec del desenvolupament dels procediments de tractament de dades (ofuscació, truncament, etc.) en cas que fossin necessaris.

Tota manipulació de dades de l'entorn de producció haurà de ser informada i aprovada pel propietari de les mateixes.

En cas que s'hagi de realitzar una migració de dades entre sistemes, l'adjudicatari haurà de presentar un pla de migració de les dades on es detallin les operacions necessàries.

Aquest pla de migració s'adequarà al procediment establert per seguretat per tal de minimitzar l'exposició de les dades productives.

11.7.6. Xifratge de dades

Qualsevol informació corporativa que requereixi ser xifrada en la seva ubicació d'emmagatzemament (i per tant, queda exclòs l'encriptació per transit en les comunicacions) ha de seguir els estàndards de seguretat, custòdia i protecció de les claus que estableix IMI-Seguretat. IMI-Seguretat ha de assegurar la disponibilitat de la informació als propietaris d'aquesta dins de l'Ajuntament. IMI-Seguretat custodiarà les claus de xifratge.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser validades per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

11.7.7. Signatura electrònica

Qualsevol requeriment de signatures digitals que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser valides per IMI-Seguretat i/o seguir els estàndards i normes de l'IMI.

Per la signatura electrònica s'empraran els mecanismes aprovats per l'IMI, en cas que hagin de ser uns altres, s'haurà de justificar, documentar tècnicament i haurà d'estar validat per IMI-Seguretat. En tot cas s'ha de complir la política de signatura electrònica de l'ajuntament de Barcelona.

11.7.8. Certificats

L'IMI-Seguretat serà el responsable de la custòdia i protecció dels certificats digitals emesos en nom de l'Ajuntament de Barcelona a través de l'IMI-Seguretat. S'entén per certificats digitals corporatius: els de servidor segur, els d'aplicatiu per autenticació o signatura digital, de signatura de codi, de xifratge, etc.

Tots els certificats hauran de ser sol·licitats a través del procediment establert en l'IMI-Seguretat per al seu control i gestió.

El proveïdor haurà de seguir l'estàndard establert per la protecció i custòdia dels certificats digitals a l'hora d'incorporar el certificat pel seu ús.

11.7.9. Inventari d'actius

L'adjudicatari haurà de mantenir un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa i identificant al seu responsable; és a dir, la persona que és responsable de les decisions relatives al mateix.

11.7.10. Explotació

11.7.10.1. Configuració de seguretat

L'adjudicatari haurà de configurar els equips prèviament a la seva entrada en operació, de manera que:

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
  - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.
  - No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
  - S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.
- S'aplicarà la regla de "seguretat per defecte":
  - Les mesures de seguretat seran respectuoses amb l'usuari i protegiran a aquest, tret que s'exposi conscientment a un risc.
  - Per reduir la seguretat, l'usuari ha de realitzar accions conscients.
  - L'ús natural, en els casos que l'usuari no ha consultat el manual, serà un ús segur.

11.7.10.2. Gestió de la configuració

L'adjudicatari s'encarregarà de gestionar de forma continua la configuració dels components del sistema de manera que:

- Es mantingui a tot moment la regla de "funcionalitat mínima".
- Es mantingui a tot moment la regla de "seguretat per defecte".
- El sistema s'adapti a les noves necessitats, prèviament autoritzades.
- El sistema reaccioni a vulnerabilitats reportades.
- El sistema reaccioni a incidents.

11.7.10.3. Gestió de canvis

L'adjudicatari s'encarregarà de mantenir un control continu de canvis realitzats en el sistema, de manera que:

- Tots els canvis anunciats pel fabricant o proveïdor seran analitzats per determinar la seva conveniència per ser incorporats, o no.
- Abans de posar en producció una nova versió o una versió amb un pegat, es comprovarà en un equip que no estigui en producció, que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per al treball diari. L'equip de proves serà equivalent al de producció en els aspectes que es comproven.
- Els canvis es planificaran per reduir l'impacte sobre la prestació dels serveis afectats.
- Mitjançant anàlisi de riscos es determinarà si els canvis són rellevants per a la seguretat del sistema. Aquells canvis que impliquin una situació de risc de nivell alt seran aprovats explícitament de forma prèvia a la seva implantació.

11.7.10.4. Protecció de claus criptogràfiques

- L'adjudicatari utilitzarà programes avaluats o dispositius criptogràfics certificats.
- S'empraran algoritmes acreditats pel "Centre Criptològic Nacional".

11.7.11. Manteniment

L'adjudicatari haurà de mantenir l'equipament físic i lògic que constitueix el sistema i/o infraestructura administrada, incloent tots els elements de comunicació dels quals sigui responsable de la seva administració.

La política d'actualitzacions està basada en el nivell de criticitat de la vulnerabilitat valorada segons l'última versió publicada de l'estàndard públic CVSS (Common Vulnerability Scoring System). Segons el nivell de CVSS, les actualitzacions per la correcció de vulnerabilitats s'hauran de produir dins d'uns terminis específics (en funció del nivell d'exposició i la criticitat de la vulnerabilitat), detallats en la taula següent:

		Nivell d'exposició	
		Exposat a internet	No exposat a internet
Criticitat vulnerabilitat	CVSS <=3	20 dies[7]	40 dies
	3 < CVSS <= 6	5 dies	20 dies

[7] *Tots els dies indicats en la taula són dies laborables.*

	6 < CVSS <=8	1 dia	5 dies
	CVSS > 8	1 dia	1 dia

Prèviament a la seva implementació, l'adjudicatari haurà de dur a terme les comprovacions pertinents (com l'aplicació en entorns alternatius) per verificar que el pegat no suposa cap risc de seguretat. Tanmateix, haurà de rebre l'aprovació formal del propietari de l'actiu per procedir a la seva implementació.

El proveïdor s'haurà d'involucrar en tot el cicle de vida de les vulnerabilitats, des de la seva detecció fins a la mitigació d'aquesta. Haurà de tenir un seguiment proactiu de les vulnerabilitats que es puguin produir amb un seguiment continu del anunci de defectes, mantenint el contacte amb els fabricants per tenir coneixement de les possibles solucions que aquest proposin per corregir-les.

11.7.12. Protecció dels serveis

11.7.12.1. Protecció enfront de la denegació de servei

L'adjudicatari establirà mesures preventives i reactives enfront d'atacs de denegació de servei (DoS Denial of Service). Per tal de garantir-ho:

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.
- Es desplegaran tecnologies per prevenir els atacs coneguts.

11.8. GOVERNANÇA DE LA CONTINUÏTAT I DISPONIBILITAT

La finalitat de la governança de la continuïtat i la disponibilitat es centra, principalment, en garantir la continuïtat dels serveis i processos davant de qualsevol situació adversa, evitant un impacte significatiu en l'organització.

Els objectius que es persegueixen són:

- Disposar de Plans de Continuïtat que permetin gestionar de forma eficient una situació d'emergència.
- Garantir la continuïtat dels processos i serveis considerats crítics.
- Provar els Plans de Continuïtat com a mesura de garantia de la seva efectivitat davant una situació real de contingència.
- Focalitzar l'esforç en la mitigació de riscos rellevants.
- Coordinar a totes les persones clau per fer front a una situació de contingència.
- Complir amb els requeriments legals / regulatoris en matèria de continuïtat de negoci.
- Alinear-se amb les bones pràctiques del mercat (ISO 27002, ISO22301, ITIL)

L'adjudicatari haurà de lliurar a l'IMI un Pla de Continuïtat i Recuperació davant Desastres (en endavant, PRD) **per garantir els nivells de servei establerts**. El PRD haurà de permetre recuperar tots els serveis objecte del contracte d'acord als requeriments fixats pel negoci (RTO, RPO). S'hauran de proveir solucions tecnològiques que permetin assolir els objectius fixats, essent aquestes certificades mitjançant proves de recuperació periòdiques. Tota la informació del PRD haurà d'estar sempre disponible per al personal de l'IMI autoritzat i prèviament identificat. S'establiran els mecanismes per facilitar l'accés del personal autoritzat de l'IMI a aquesta informació, establint els controls de seguretat mínims exigits per l'àrea de Seguretat. L'adjudicatari haurà de mantenir actualitzat el PRD. L'adjudicatari haurà de documentar, desenvolupar i implantar les mesures de disponibilitat necessàries per cobrir els indicadors de nivell de servei de disponibilitat. Aquesta documentació s'haurà de lliurar a l'IMI. L'adjudicatari participarà en les proves de recuperació i alta disponibilitat que l'IMI planifiqui, elaborant un pla de proves i executant-lo el dia de la prova, coordinadament amb els equips que realitzen les proves de continuïtat de l'Ajuntament.

Les activitats de governança de la continuïtat i disponibilitat seran executades segons s'especifica a la següent matriu RACI:

Activitats de Governança de la Continuïtat i Disponibilitat	**IMI**	**Adjudicatari**	**Negoci**
Identificació dels requeriments de continuïtat de negoci	A, R		R
Implantació de solucions que garanteixin els requeriments de continuïtat i disponibilitat	A	R	I
Execució de Proves de Continuïtat i Disponibilitat	A, R	R	I, R
Validació dels resultats de les proves	A, R	R	I
Auditoria de compliment dels requeriments fixats per l'IMI	A, r	R	I

11.8.1. Pla de continuïtat de negoci de l'adjudicatari

L'adjudicatari haurà de desenvolupar i implantar un pla de continuïtat per al seu personal i per a les instal·lacions des de les quals opera. Aquest pla haurà:

- D'alinear-se amb els millors pràctiques del sector per desenvolupar plans de continuïtat

- Incloure la ubicació alternativa, els llocs de treball i l'equipament necessari per garantir la prestació del servei des d'un lloc alternatiu compliment amb els nivells de servei fixats per l'IMI.

L'IMI podrà participar en totes les proves d'aquest pla de continuïtat de negoci de l'adjudicatari que consideri convenients.

L'adjudicatari haurà de mantenir-ho actualitzat, i posar a disposició de l'IMI la documentació associada:

Els procediments i plans hauran de complir en tot moment amb legislació de protecció de dades i els estàndards de seguretat de l'IMI. L'adjudicatari haurà de presentar el seu pla a l'IMI per revisió i aprovació.

11.8.2. Plans de Continuïtat de Negoci de l'Ajuntament

L'adjudicatari participarà, quan s'escaigui, en les proves de continuïtat de negoci de l'Ajuntament coordinades des de l'IMI i que poden implicar la participació de diversos adjudicataris.

11.8.3. Plans i Procediments

- Plans de recuperació tecnològics de cada sistema/servei
    - L'adjudicatari haurà de desenvolupar els plans de recuperació tecnològics de cada servei/sistema d'informació coordinat amb cada responsable del servei.
    - Els procediments tecnològics desenvolupats hauran de permetre l'assoliment dels objectius de recuperació de sistemes i d'informació pactats amb l'IMI.
- Els plans de recuperació tecnològics s'hauran d'alinear amb els plans de continuïtat de l'àrea de Seguretat i de l'Ajuntament de Barcelona.

11.8.4. Execució de Proves de Recuperació

- Per als serveis que disposin d'alta disponibilitat en dos CPDs, executar un cop a l'any una prova de recuperació total d'aquests serveis, balancejant-los cap al CPD alternatiu demostrant així la seva continuïtat en situació de desastre.
- Execució de Proves de recuperació del servei/sistema d'informació:
    - Elaborar un pla de proves parcials anual que haurà de ser aprovat per l'àrea de Seguretat.
    - Executar proves de recuperació, donant prioritat als serveis classificats com a molt crítics.
    - Tota aplicació classificada com a molt crítica podrà ser sotmesa a una prova de recuperació anual. En els serveis classificats com de Nivell mig o baix, es farà anualment una selecció d'aquells que han de ser sotmesos a una prova de recuperació.

11.9. SEGURETAT DEL CPD

Si el servei se sustenta amb infraestructura que resideix en un CPD del proveïdor, aquest CPD haurà de garantir el compliment dels controls del nivell TIER 3 de la TIA-942, o TIER2 segons el nivell de RTO pactat.

Un cop a l'any, l'adjudicatari haurà de sotmetre's a una auditoria externa de seguretat (a càrrec de l'adjudicatari) per avaluar el nivell de compliment dels controls de seguretat de la instal·lació des d'on es presta el servei.

11.9.1.1. Documentació

Tota la documentació generada per garantir la continuïtat i recuperació dels serveis haurà d'estar disponible per al personal de l'IMI autoritzat.

Aquest plec de prescripcions tècniques ha estat emès en data 30 de juliol de 2021 per la Sra. Sònia Càrdenas Monroy i el Sr. José Manuel Velilla Balaguer, tècnics responsables del contracte, adscrits a la Direcció d'Operacions i Sistemes, amb el vistiplau de:

Amparo Rodríguez Rodríguez
Directora d'Operacions i Sistemes

12. ANNEXOS.

12.1. ANNEX 1: DOCUMENTS A DISPOSICIÓ DEL LICITADOR

A continuació s'enumeren els documents que es proporcionaran sota demanda, mitjançant correu electrònic a l'adreça indicada per a consultes (veure l'Annex 12.4), i amb la prèvia signatura del corresponent Acord de confidencialitat adjunt, com annex, al PCAP.

1. L'inventari detallat dels elements del NUS-OSAT
2. Ubicació dels 2 CPDs de l'IMI

12.2. ANNEX 2: INFORMES ESPECÍFICS DEL NUS

L'adjudicatari està obligat a la realització d'un conjunt d'informes que inclouran les mètriques del servei per tal que l'IMI disposi d'una visió global i es puguin determinar fàcilment actuacions de millora contínua sobre el servei.

Tots els informes s'ubicaran en servidors facilitats per l'IMI i estaran en tot moment disponibles pel personal de l'IMI.

El format detallat dels informes es pactarà entre l'adjudicatari i l'IMI durant la fase de planificació inicial. Tot i això, l'adjudicatari presentarà a la seva oferta els models d'informes.

L'adjudicatari configurarà l'eina (facilitada per l'IMI o proporcionada per l'adjudicatari) accessible via web per (Cacti o similar) la consulta en temps real de tots els informes de:

- Disponibilitat
- Capacitat
- ANS tecnològics
- ANS de gestió (si és possible)

A part dels informes accessibles via web s'hauran de generar els informes periòdics següents:

- **Informe diari:** resum de l'activitat del dia anterior i de l'activitat programada pel dia següent en referència a l'operació dels serveis
- **Informe mensual** amb la següent informació mínima
  - Informes amb la proposta de valor d'ANS i la penalització associada si escau
  - Informe d'explotació indicant les mètriques de gestió dels serveis
  - Evolució de la disponibilitat i capacitat de la infraestructura i els serveis, d'acord amb els paràmetres i llindars establerts per l'IMI

- Recull d'informes ad-hoc generats per incidències greus
- Resum dels projectes de transformació indicant-ne l'estat, actualització de la planificació i riscos més importants

- **Informe mensual amb indicadors de seguretat**. Han de tenir com a mínim la següent informació:
  - Registre de Seguretat (Peticions/Incidents)
  - Indicadors tècnics de seguretat: (Correu, Firewalls, IPS – Intrusions, Signatura electrònica, Usuaris)
  - Temes a ressaltar que s'han produït durant el mes
  - Canvis respecte a les regles de seguretat perimetral
  - Incidències rellevants produïdes. Indicar quines s'han registrar al registre d'incidències
  - Caducitat de Llicències de productes de seguretat en període de 2 mesos
  - Mesures pel què fa a l'ús del servei
  - Riscos vigents

Tot i que existeixi una periodicitat inicial pactada per al lliurament de cada tipus d'informe, l'IMI es reserva el dret de sol·licitar els informes o modificar algun dels existents, en casos puntuals, de forma immediata, podent limitar el número de sistemes, serveis, ubicacions o període d'observació. L'adjudicatari automatitzarà el màxim possible l'elaboració d'aquests informes, per tal de poder donar resposta immediata a sol·licituds d'informes fora de la planificació inicial establerta.

Els informes es lliuraran en format electrònic imprimible i tractable posteriorment per l'IMI, i s'emmagatzemaran de forma centralitzada a on l'IMI determini.

L'IMI podrà sol·licitar, durant la vigència del contracte i sense cost addicional, canvis en els formats i informació continguda en qualsevol dels informes.

Informe resum de l'activitat i rendiment del dia anterior

L'adjudicatari elaborarà un informe diari que contindrà un resum dels trets més destacats de la jornada de treball del dia anterior. Aquests informes cobriran les 24 hores del dia anterior i es lliuraran abans de les 10:00 del matí de cada dia.

L'informe diari inclourà com a mínim:

- Taula resum de les activitats d'explotació del dia anterior: per a cada activitat es detallarà el nombre total de sol·licituds i tiquets rebuts, tancats, pendents de tancar per causes imputables i pendents de tancar per causes no imputables. Les activitats a reflectir en l'informe són: o Incidències per criticitat.

- Nombre de sol·licituds o tiquets rebutjats i els motius.
- Relació d'incidències massives produïdes el dia anterior, indicant el número i tipus de serveis afectats i el temps de resolució.
- Relació d'incidències sobre equips molt crítics tancades el dia anterior.
- Detall de les execucions del canvis planificats amb ris de tall fetes el dia anterior.
- Relació dels equips amb alarmes per capacitat el dia anterior.
- Relació dels enllaços de dades que han superat el 80% de la seva capacitat, ordenats de major a menor grau d'utilització.
- Informe d'anàlisi dels backups amb explicació de les còpies de seguretat que hagin fallat.
- Informe d'anàlisi de logs, identificant els logs anòmals detectats.

Tots els informes hauran d'estar categoritzats per a cada sistema i servei gestionat durant el període d'observació.

Informe de gestió de capacitat i disponibilitat

L'adjudicatari disposarà en l'eina web tots els informes de disponibilitat i capacitats de tots els serveis i els equips implicats en els serveis.

Els informes inclouran, com a mínim:

- Informes de disponibilitat dels sistemes i/o serveis gestionats
- Informació estadística de tots els equips de rendiment amb establiment de llindars de criticitat
- Informes de rendiment dels equips: CPU, memòria, errors interfícies o Informes de volum de tràfics totals per interfície de l'equip
- Informes de rendiment en determinats períodes de temps (busy hour, horaris laborals)
- Informació de taxa de pèrdua de paquets, jitter i latència de la xarxa per cada equip
- Informes de capacitat per tecnologies
  - Tallafocs:
    - Informes de nombre de connexions en els equips.
    - Informes de nombre de NATs establerts.
    - Informes d'utilització de disc.
    - Informes de paquets acceptats, rebutjats i denegats.

- Balancejadors (N4, N7):
  - Informes de nombre de connexions per IPs virtuals, servidors reals i ports.
  - Informes de nombre de connexions encriptades SSL per IPs virtuals.

- DNS
  - Informes de volum de peticions per segon
  - Informes de volum de peticions per tipus, per dominis i per IP.

- VPN
  - Informes de connexions IPSEC establertes
  - Informes de connexions SSL VPN establertes
  - Informes de connexions L2L establertes

- Troncals
  - Informes d'instàncies de routing creades (VRFs)
  - Informes d'instàncies VPLS/MPLS creades (VPN N2, VPN N3)
  - Informes sobre les VLANs de nivell 2.

L'adjudicatari elaborarà informes resum de rendiment tràfic i rendiment dels equips i serveis gestionats amb periodicitat mensual o sota demanda de l'IMI.

Els informes de tràfic i rendiment elaborats han de permetre disposar d'informació actualitzada i real de l'ús dels serveis gestionats, així com identificar de forma preventiva possibles problemes i recomanacions d'accions de millora contínua.

Els informes resum inclouran per dispositiu, com a mínim:

- Informació detallada per sistema i/o servei gestionat del rendiment i ús dels mateixos en les franges horàries de màxim ús o superació dels llindars establerts
- Correlació històrica dels informes de tràfic i rendiment, identificant l'evolució d'ús i rendiment dels equips i serveis. La correlació històrica ha de permetre identificar tendències i preveure noves necessitats (ampliacions, canvis, re configuracions) per tal de no assolir degradacions en la qualitat dels serveis oferts

- Identificació de rendiments anòmals destacables dels equips i serveis coneguts, deguts a incidències i problemes. Correlació amb les actuacions realitzades per a la resolució de les incidències i problemes
- Identificació de rendiments i tràfics anòmals destacables dels equips i serveis coneguts, deguts a aturades de servei programats per part de l'adjudicatari (sobre la infraestructura pública o de l'IMI). Correlació amb les actuacions realitzades en aturades programades dels serveis
- Identificació de fets rellevants esdevinguts durant el període d'observació, que justifiquin un ús anòmal dels equips i serveis
- Identificació i proposta d'accions de millora de la infraestructura operativa, per garantir la disponibilitat, capacitat i continuïtat dels serveis gestionats
- Grau d'utilització (alt / mig / baix) de cada dispositiu

Tots els informes hauran d'estar categoritzats per a cada sistema i servei gestionat, durant el període d'observació.

12.3. ANNEX 3: VOLUMETRIES INCIDÈNCIES, PETICIONS I CANVIS

OSAT	CRITICITAT		
	Alta	Mitja	Baixa
PETICIONS	60	135	90
INCIDÈNCIES	45	160	140
CANVIS	15	40	15

12.4. INFORMACIÓ ADDICIONAL / ACLARIMENTS

L'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: nbellavista@bcn.cat ; scardenasm@bcn.cat

En l'assumpte del correu indicar:

Contracte: [Número d'expedient del contracte]

En cas de no obtenir resposta, contactar amb el telèfon 93 291 83 65.

S'atendran les sol·licituds d'informació fins a 3 dies laborables abans de la data límit de presentació d'ofertes.

La sessió informativa presencial, on es dona resposta a totes les consultes recepcionades per correu electrònic, podrà resultar anul·lada, amb motiu de les mesures organitzatives que se n'adoptin a causa de la COVID-19, determinades pel Comitè de Seguiment de l'Ajuntament de Barcelona en coordinació amb l'Agència de Salut Pública de Barcelona.

En cas que es pugui convocar aquesta sessió informativa, aquesta sessió es celebrarà a partir dels 5 dies hàbils posteriors al dia següent de la data de publicació de l'anunci de licitació a la plataforma de contractació pública del perfil del contractant. El lloc, el dia i l'hora d'aquesta sessió es publicarà a l'anunci de licitació en el perfil del contractant.

https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903