Ajuntament de Barcelona

Institut Municipal d'Informàtica
Direcció de Qualitat i Seguretat

C/ Tànger, 98, p 11
08018 - Barcelona
Telèfon 93 291 81 00
www.bcn.cat

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

Plec de prescripcions tècniques per a la contractació dels serveis de Preventiu-Seguretat TIC de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

ÍNDEX

1. INTRODUCCIÓ 4

2. OBJECTE 7

PROCEDIMENT DE CONTRACTACIÓ 8

3. ABAST 9

4. DESCRIPCIÓ DELS SERVEIS 9

SERVEI DE CIBERINTEL·LIGÈNCIA ____ 9

SERVEI D'AUDITORIES DE SEGURETAT I GESTIÓ DE VULNERABILITATS ____ 10

ANÀLISI D'INCIDENTS DE SEGURETAT A POSTERIORI I ELABORACIÓ DE FORENSES JUDICIALS ____ 10

4.1. SERVEI DE CIBERINTEL·LIGÈNCIA ____ 10

4.2. SERVEI DE GESTIÓ DE VULNERABILITATS ____ 12

4.3. ANÀLISI D'INCIDENTS DE SEGURETAT A POSTERIORI I ELABORACIÓ DE FORENSES JUDICIALS O INTERNS ____ 18

5. MODEL DE PRESTACIÓ DEL SERVEI 20

5.1. MODEL DE RELACIÓ IMI/ADJUDICATARI 20

5.2. SEGUIMENT DEL SERVEI 23

5.3. PLA DE SERVEI 25

5.4. PLA DE QUALITAT 25

6. ORGANITZACIÓ I PERFILS REQUERITS 26

RECURSOS HUMANS ____ 26

7. CONDICIONS D'EXECUCIÓ 30

7.1. LLOC DE PRESTACIÓ DEL CONTRACTE 30

7.1. HORARI DE PRESTACIÓ DEL SERVEI 31

7.3. IDIOMA I TRADUCCIONS 32

7.4. INFRAESTRUCTURA NECESSÀRIA PER A LA PRESTACIÓ DEL SERVEI. 32

8. PRESSUPOST, OFERTA ECONÒMICA I FACTURACIÓ 33

9. PROPOSTA TÈCNICA 33

10. CONDICIONS GENERALS D'EXECUCIÓ 35

SEGURETAT DELS SISTEMES D'INFORMACIÓ, PROTECCIÓ DE DADES I COMPLIMENT NORMATIU ____ 35

CLÀUSULA DE PROPIETAT INTEL·LECTUAL ____ 36

CONFIDENCIALITAT ____ 36

PROTECCIÓ DE DADES DE CARÀCTER PERSONAL ____ 36

CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT ____ 39

CLÀUSULA DE COMUNICACIONS EXTERNES ____ 39

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

CLÀUSULA DE SEGURETAT DELS EQUIPS, PROGRAMES I INFORMACIÓ ____ 39
CLÀUSULA DE PERSONAL EXTERN ____ 40
GESTIÓ D'INCIDENTS ____ 40
ANÀLISIS FORENSES ____ 40
ANNEX I: VOLUMETRIA DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT 41
ANNEX II: INFORMACIÓ ADDCIONAL I/O ACLARIMENTS..... 42

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

1. INTRODUCCIÓ

L'Ajuntament de Barcelona gestiona una ciutat d'1,6 milions de ciutadans, unes 200.000 empreses i un teixit associatiu format per més de 10.000 entitats. Disposa d'una oferta de serveis molt àmplia, emmarcada en diferents àmbits: serveis socials, mobilitat, educació, salut, cultura i oci, promoció econòmica, etc. sempre amb la vocació de servir a la ciutadania i a realitzar la gestió de la ciutat que té encomanada de forma òptima, àgil i eficient.

Aquests serveis, s'han d'oferir amb garanties i seguretat TIC pel ciutadà i per la pròpia ciutat, i això suposa, des de protegir la informació personal del ciutadà, garantir els serveis i protegir la pròpia gestió de la ciutat i de l'Administració Municipal.

La informació relativa a aquests serveis, es troba disgregada en un gran nombre de sistemes d'informació i fitxers legals diferents la qual cosa porta a la necessitat de disposar de serveis de identificació, protecció, prevenció i reacció davant amenaces a què es troben exposades els sistemes d'informació i les infraestructures TIC i així reduir i minimitzar els riscos d'incidents de seguretat i ciberatacs.

A més, en un escenari en què el concepte i continguts de seguretat lògica o ciberseguretat avança i es troba en contínua i ràpida evolució, els serveis de ciberseguretat que requereix l'Ajuntament han de ser confiables i àgils, així com configurats amb la flexibilitat suficient per poder estar fent front als riscos que es presenten, sovint impredictibles.

L'Institut Municipal d'Informàtica (en endavant, IMI) té delegades les funcions de Seguretat en les Tecnologies de la Informació i Comunicació de l'Ajuntament de Barcelona, i exerceix de Responsable de Seguretat TIC, en funció de la seva organització interna, d'acord amb els preceptes, estàndards internacionals en matèria de seguretat TIC i en especial, amb els requeriments que l'Esquema Nacional de Seguretat (ENS) i la normativa de Protecció de Dades Personals estableix en els entorns automatitzats.

Dins d'aquest escenari, l'IMI ha definit **un Model de Gestió de la Seguretat** on s'hi desenvolupen els programes de Seguretat Corporatius del mandat. El marc hi encabeix el model de seguretat del NIST framework de Ciberseguretat (Identificar, Protegir, Detectar, Respondre i Recuperar) així com el de l'SGSI ISO 27001 i la seva interpretació en l'administració espanyola amb l'Esquema Nacional de Seguretat.

Aquest Marc de Seguretat estableix la base per definir el pla de seguretat que ha de desenvolupar el mandat, és a dir, les línies d'actuació, projectes i serveis a executar per donar resposta i sortida, en l'àmbit de protecció i seguretat, a les estratègies i plans d'actuació de l'Ajuntament, amb l'objectiu de:

- Incrementar els Serveis de seguretat TIC
- Dotar a l'Ajuntament d'una estructura que asseguri el compliment de la seguretat i la minimització dels riscos de Seguretat TIC corporatius.
- Assegurar un Marc Normatiu de referència per l'Ajuntament
- Garantir el compliment de la legalitat (ENS, RGPD, eIDAS, LPACAP,...)
- Implantar Projectes de Seguretat per donar resposta a les necessitats TIC en matèria de seguretat i protecció
- Securitzar els projectes del pla de digitalització: Establir en base als riscos els requeriments de seguretat dels projectes del Pla de transformació digital. Establir, implementar i governar el model i les condicions de seguretat per a tots projectes i iniciatives que se'n deriven del Pla de transformació Digital de l'Ajuntament de Barcelona.
- Tenir Govern dels accessos TIC en base als principis de mínim privilegi i necessitat de saber per tal de poder conèixer qui fa què i quan dins dels sistemes d'informació i infraestructures TIC de l'Ajuntament.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Disposar de vigilància activa, reactiva i preventiva de la seguretat

Així dons, l'IMI desenvolupa la funció de la seguretat dins d'un model de Gestió de la Seguretat a tres nivells o línies de defensa: Estratègic, Tàctic i Operatiu, i estableix 5 línies d'actuació sobre les que es desenvolupen els programes de seguretat del mandat.

Funció Seguretat Informació en tres linees de defensa



Marc de Seguretat : línies d'actuació



- **Govern de la seguretat de la informació:** Establiment d'una estructura i un model organitzatiu sòlid en l'àmbit de la seguretat, amb capacitat per a controlar i prendre decisions en totes aquelles accions que així ho requereixin
- **Control i divulgació de la normativa:** Disposar d'un marc normatiu actualitzat i alineat a l'estratègia de seguretat i exercir un control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat
- **Protecció dels sistemes d'informació**: Aplicació de mesures de seguretat per tal de mitigar els riscos que se'n puguin derivar com possibles fallides o atacs intencionats així com gestionar de manera ràpida i efectiva tots aquells incidents que es produeixin
- **Seguiment de la identitat digital:** Gestió de les seves credencials i control de la manera de compartir i accedir a la informació, tant a l'organització com al propi usuari i del ciutadà per tal de garantir la confidencialitat, l'autenticitat, l'autenticació, la integritat i el no repudi de la informació i les accions que realitzi.
- **Detecció, reacció i reducció d'amenaces:** Identificar les amenaces més rellevants per als sistemes d'informació de l'organització, sigui pel seu número o per l'impacte que puguin produir.
- **Millora de la resiliència de l'activitat:** Cal valorar el nivell de resistència dels sistemes d'informació en situacions adverses i detectar millores i mesures per augmentar o assegurar la capacitat per mantenir els sistemes en funcionament.

Les línies d'actuació donen cobertura a 4 de les 5 funcions del framework del NIST de Ciberseguretat: Identificar (Govern), Protegir (Arquitectura de Seguretat), Detectar i Respondre (operació de la seguretat). Deixant la funció de "Recuperar" en un marc d'actuació global més gran de l'organització fora de la seguretat.

Així doncs, l'IMI, per exercir aquesta funció delegada de la Seguretat Corporativa TIC i en la seva vocació d'oferir els millors serveis TIC a l'Ajuntament de Barcelona i al ciutadà, ha establert conjunt de serveis de seguretat TIC per cobrir els requeriments identificats i de futur en aquesta matèria:

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

En l'àmbit del **Govern de la Seguretat**:



- **Govern de la seguretat de la informació**: Establiment d'una estructura i un model organitzatiu sòlid en l'àmbit de la seguretat, amb capacitat per a controlar i prendre decisions en totes aquelles accions que així ho requereixin
- **Control i divulgació de la normativa**: Disposar d'un marc normatiu actualitzat i alineat a l'estratègia de seguretat i exercir un control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat

Estableix els serveis següents:

- **Serveis de GRC** (Govern Risc i Compliment). El servei engloba tota la Gestió i iniciatives de l'SGSi de Seguretat per garantir el tractament dels Riscos de seguretat identificats amb l'objectiu de donar cobertura a la missió estratègica del govern de la seguretat.

En l'àmbit **d'Arquitectura de Seguretat**:



- **Protecció dels sistemes d'informació**: Aplicació de mesures de seguretat per tal de mitigar els riscos que se'n puguin derivar com possibles fallides o atacs intencionats així com gestionar de manera ràpida i efectiva tots aquells incidents que es produeixin

Estableix els serveis següents:

- **Serveis d'arquitectura i Projectes** Servei que ofereix solucions àgils i arquitectures enfront a noves tecnologies i reptes i que permetin mantenir i evolucionar de manera contínua el nivell de protecció dels actius d'informació de l'Ajuntament enfront a canvis en els mateixos o en les amenaces. Aquest Servei serà l'únic punt d'entrada de la resta d'equips de Projectes de l'IMI i de l'Ajuntament, i gestionarà la cartera de participació de seguretat en els projectes i coordinarà la participació dels altres equips de Seguretat.

En l'àmbit de **Seguretat Operativa** en relació a les identitats i accessos:



- **Seguiment de la identitat digital**: Gestió de les seves credencials i control de la manera de compartir i accedir a la informació, tant a l'organització com al propi usuari i del ciutadà per tal de garantir la confidencialitat, l'autenticitat, l'autenticació, la integritat i el no repudi de la informació i les accions que realitzi.

Estableix els serveis següents:

- **Serveis de Identitats i accessos**: Control Autenticació, autoritzacions i Control d'Accés (CAAA). Aquest servei ha d'operar els processos d'identitats, credencials, autoritzacions i accessos de tot l'Ajuntament, amb l'objectiu de garantir la protecció requerida i proporcional de la informació i serveis TIC corporatius.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

En l'àmbit de **Seguretat Operativa** en relació a la ciberseguretat:



- **Detecció, reacció i reducció d'amenaces:** Identificar les amenaces més rellevants per als sistemes d'informació de l'organització, sigui pel seu número o per l'impacte que puguin produir.

Estableix els serveis següents:

- **Serveis de Preventiu.** El servei de seguretat preventiva ha de disposar i ingestar múltiples fonts de ciberintel·ligència i realitzar proves d'intrusió d'infraestructures i serveis amb la finalitat de garantir que les infraestructures o serveis siguin segurs i de realitzar la gestió complerta del cicle de vida de les vulnerabilitats i posterior revisió. També ha d'assessorar en la definició de les arquitectures dels sistemes i tecnologies que té actualment l'IMI, que dintre de la seva funció de donar servei informàtic a l'Ajuntament de Barcelona, necessita per donar el correcte i segur servei, analitzant les millores que es poden implantar relacionat amb les novetats tecnològiques del mercat i els nous paradigmes d'atacs informàtics que es poden patir.

- **Serveis de Vigilància, detecció i Reactiu (SOC i Resposta a incidents).** Aquest servei inclou El Centre d'Operacions de Seguretat, per la vigilància i monitorització dels esdeveniments de la seguretat, i el CSIRT, Centre de Seguretat de Resposta d'incidents, per el ràpid anàlisi i gestió de l'incident per tal de reduir o minimitzar l'impacte que pugui produir i establir les mesures preses per tal que no es torni a produir, es coordinarà amb el servei de preventiu per millorar, si fos el cas, la infraestructura de seguretat fent les propostes pertinents.

I per tal de donar un pas endavant, s'estableix en aquest contracte la licitació dels serveis de Preventiu, serveis que cobreixen una part dels serveis requerits en la línia d'actuació de Serveis Operatius de Detecció, reacció, mitigació i reducció d'amenaces.

2. OBJECTE

El contracte té per objecte la prestació dels serveis de seguretat preventiva de l'Ajuntament de Barcelona, en tant a serveis de ciberintel·ligència, detecció de vulnerabilitats i alerta primerenca, anàlisi de hacking ètic i els serveis associats de gestió del cicle de vida de les vulnerabilitats detectades. D'igual manera, aquest servei atendrà els anàlisis forenses judicials formals, així com les peticions d'informació d'actuacions internes adreçades a l'Ajuntament de Barcelona o de requeriments d'informació judicials.

Pel què fa a la gestió del cicle de vida de les vulnerabilitats, cal remarcar que aquest servei implica que l'IMI té diversos proveïdors i contractes de suport tècnic i operatiu que el contracte haurà de tenir en compte per la comunicació i gestió de l'aplicació de la vulnerabilitat, i per altra banda haurà d'automatitzar el màxim de processos ja sigui col·laborant en procedimentar sobre l'eina de ticketing actuacions, així com participant i integrant la detecció automàtica de vulnerabilitats del SIEM que han d'implementar els serveis i/o proveïdors.

Per portar a terme aquest objectiu, els licitadors hauran d'entendre que les especificacions dels serveis i processos són els requeriments mínims a desenvolupar, d'acord amb la situació actual i les millors pràctiques de gestió de la provisió i suport dels serveis TIC:

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Funcionalment, mitjançant la revisió i millora dels procediments de gestió actuals, o amb la seva definició en el cas que no existeixin.
- Orgànicament, mitjançant la dotació d'un equip tècnic qualificat i un equip de gestió del servei, que permeti assolir el nivell de servei descrit en aquest plec mitjançant la total integració amb les diferents unitats estructurals de l'IMI.
- Tecnològicament, utilitzant les eines de gestió pròpies de l'IMI havent d'implantar els seus procediments sobre aquestes, tot i que les podrà personalitzar i adaptar al seu model de gestió. No obstant, si ho creuen convenient, les empreses licitadores podran incloure una proposta d'eines diferent que permetin una evolució futura, sota la supervisió de l'IMI.

PROCEDIMENT DE CONTRACTACIÓ

La contractació es realitzarà pel procediment obert harmonitzat amb publicitat tot entenent que es garanteix la màxima concurrència i competitivitat.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

3. ABAST

L'abast dels serveis inclou tots els sistemes d'informació i components de l'Ajuntament de Barcelona gestionats per l'IMI i/o connectats a la xarxa corporativa a través dels seus serveis. Això inclou serveis on-premise, en el Cloud públic i en clouds privats.

Es pot trobar més informació sobre la volumetria dels sistemes d'informació gestionats per l'IMI a l'Annex I d'aquest plec.

També forma part de l'abast d'aquest contracte l'assessorament puntual a l'Ajuntament en matèria de seguretat TIC de sistemes no gestionats per l'IMI contractats directament per l'Ajuntament.

Actualment, l'IMI està immers en la revisió i evolució dels processos operatius i de gestió dels serveis. Aquesta revisió està tenint com a resultat la re definició 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 re alimentació oportuna, alhora que aportant solucions a problemes i riscos identificats.

Concretament, l'abast del contracte inclou tots els Sistemes d'Informació de l'Ajuntament de Barcelona i organització Municipal classificats i gestionats per l'IMI i tota la infraestructura i serveis que donen suport als sistemes d'informació, tant si estan ubicats a l'IMI com si estan sota contractes de Serveis TIC realitzats per l'IMI basats en Cloud o on premise, així com eines de suport al treball del personal corporatiu com són les estacions de treball, dispositius de mobilitat, correu corporatiu, eines de col·laboració, gestors documentals, etc.

En definitiva les volumetries de la infraestructura i serveis amb què ha d'actuar aquest servei es relaciona en l'Annex 1.

També formen part de l'abast totes les tecnologies i eines o components que ofereixen protecció i milloren aspectes concrets de la seguretat i la seva governança i que anomenarem en aquest plec "competències tècniques específiques de Seguretat".

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

4. DESCRIPCIÓ DELS SERVEIS

Els serveis que s'han de proporcionar amb contracte són serveis de Ciberintel·ligència, Auditories tècniques de seguretat i Hacking ètic, de Gestió de vulnerabilitats i d'Anàlisis i gestió d'incidents de seguretat:

SERVEI DE CIBERINTEL·LIGÈNCIA

- Servei de Ciberintel·ligència

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Servei de monitorització i report als serveis/departaments afectats de la publicació de vulnerabilitats associades a les tecnologies desplegades per l'IMI.

SERVEI D'AUDITORIES DE SEGURETAT I GESTIÓ DE VULNERABILITATS

- Auditories tècniques de seguretat i Hacking ètic
  - Escanejos periòdics de vulnerabilitats
  - Auditories Tècniques de seguretat de dispositius de seguretat
  - Test d'intrusió a aplicacions o webs
- Gestió de Vulnerabilitats

ANÀLISI D'INCIDENTS DE SEGURETAT A POSTERIORI I ELABORACIÓ DE FORENSES JUDICIALS

Donat que el món de ciberseguretat va evolucionant recurrentment a mesura que apareixen nous atacs, els serveis que es descriuen a continuació, estaran subjectes a revisió semestral per incorporar propostes d'evolució i adaptació del servei per donar cobertura a les amenaces emergents i vulnerabilitats atòpiques.

4.1. SERVEI DE CIBERINTEL·LIGÈNCIA

L'objectiu de la ciberintel·ligència és ajudar els equips interns de l'IMI a anticipar la detecció de possibles amenaces contra l'organització Municipal amb l'objectiu de poder prendre mesures preventives sobre els sistemes d'informació de l'Ajuntament que protegeixin davant d'aquestes amenaces, evitar i prevenir incidents de ciberseguretat. Per això, l'adjudicatari ha d'executar les següents tasques:

• **Vigilància d'amenaces.** La preparació i planificació de ciberatacs contra una organització pot deixar algun rastre en Internet superficial, la Deep Web i també en 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. Monitorització i detecció primerenca d'alertes de seguretat** de la informació fora de l'Ajuntament (fuites d'informació de l'Ajuntament de Barcelona, atacs DDoS, activisme i hacktivisme, vulneració de mecanismes de seguretat, conductes perilloses, suplantacions d'identitat, robatori de credencials, espionatge, monitorització d'amenaces en 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.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

Notificació ràpida d'amenaces publicades a Internet, de forma genèrica que 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 l'avís de vulnerabilitats conegudes relacionades amb el programari i maquinari identificats en el conjunt d'actius i sistemes de l'Ajuntament. L'emissió 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.

Les volumetries contemplades 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

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

c. Dominis Internet - 5 dominis principals que suposen el 90% de les visites

d. Perfils de xarxes socials – 10

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.**

Taula 1 - Volumetries servei ciberintel.ligència	**Quantitat**
Servei de ciberintel·ligència (amb meitat de remediacions)	26 assets i màxim 13 remediacions

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 el servei del perfil requerit dins d'aquest plec.

4.2. SERVEI DE GESTIÓ DE VULNERABILITATS

L'objectiu de la detecció i gestió de vulnerabilitats és gestionar la informació necessària perquè el servei pugui prendre les mesures adients per preveure i mitigar l'aparició de les amenaces rebudes (externament o les obtingudes del propi servei que es materialitzin en incidents de seguretat).

Aquest objectiu es materialitza en l'ajuda als equips interns i de serveis de l'IMI a anticipar la identificació de vulnerabilitats presents en els seus sistemes d'informació i donar un seguiment i suport fins a la resolució de les mateixes.

Per això, l'adjudicatari ha d'executar les següents tasques:

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
- Auditories Tècniques de seguretat.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- 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.
- Auditories codi Font.
- Exercicis de phishing/ enginyeria social

L'adjudicatari del servei haurà d'establir un pla d'auditories tècniques d'ofici per a la detecció de vulnerabilitats en les infraestructures corporatives on-premise o en el núvol, en el que, com a mínim, s'inclouran les auditories indicades a continuació amb la volumetria que es detalla per a cada una d'elles:

Servei d'Escanejos periòdics de vulnerabilitats	**Quantitat**
Escanejos de vulnerabilitats sobre 800 IPs públiques	1 per any

Es valoraran les propostes dels licitadors que millorin el nombre mínim d'un escaneig anual a 800 IPs públiques (aprox.) a realitzar anualment sigui:

- en la freqüència
- com en un servei de vigilància activa de vulnerabilitats que pugui aplicar-se de forma puntual en algun actiu o en aspectes puntuals a fer seguiment
- possibilitat de realització d'escaneig de vulnerabilitats a noves de infraestructures a la zona publicada a internet o intranet.

En cas de millora oferta per part de l'adjudicatari en la seva oferta, serà aquesta la que prevaldrà.

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

A priori a la xarxa interna es disposa d'eines i processos per la realització d'escanejos de vulnerabilitats i per tant no es requerirà d'aquests, si bé el servei de gestió de vulnerabilitats haurà de vetllar perquè els processos de remediació d'aquestes vulnerabilitats detectades es gestionin. Tot i això, en el cas que internament no es puguin emprar aquestes eines d'escanejos de la xarxa interna per alguna infraestructura especial, el servei haurà de proveir les eines/serveis per a realitzar-los.

Taula 2 - Volumetria d'auditories tècniques	**Quantitat**
Test Intrusió extern/Intern – Caixa negra - Hacking ètic – 30 IPs	1
Auditoria tècnica de sistemes i configuracions de dispositius de seguretat: DNS, IPS i proxies corporatius (elements de comunicacions), wifis, End Point, MDM, SIEM, WAF, NGFW, AntiSpam, IDS,Serveis IOT,NAC, etc.	3
Auditoria d'aplicatius web/Serveis: aplicatius web, apps mòbils, productes (Serveis), de complexitat mitjana	3
Auditories d'intrusió i revisions de codi (línies per any)	100 k línies/any

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

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.

Es valoraran les propostes dels licitadors que millorin el nombre mínim d'auditories a realitzar anualment. En cas de millora oferta per part de l'adjudicatari, serà aquesta la que prevaldrà.

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 bon plantejament de com enfocaran i plantejaran elaborar aquest pla d'auditories. 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 falles 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.

Gestió de Vulnerabilitats

L'adjudicatari ha de gestionar el cicle de vida de les vulnerabilitats detectades en els apartats anteriors, 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 a 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 (SOC i / o Operació de Sistemes i Suports Tècnics Operatius):
    - Priorització
    - 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

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Realització de propostes d'evolució i adaptació del servei per donar cobertura a les amenaces emergents i vulnerabilitats atòpiques.

El servei ha de ser acurat i tenir la qualitat requerida. Per això durà a terme les tasques que s'indiquen a continuació:

- Vetllar perquè no es proporcionen falsos positius, amb verificacions manuals.
- Vetllar perquè 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 estaran filtrades i lliures de falsos positius i repeticions.
- Re certificació de vulnerabilitats per a l'assegurament de la seva resolució.
- Realitzar informes mensuals per Direcció, destinats a la Gerència de l'IMI/Ajuntament 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, 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 operatius de gestió de infraestructures i programaris o serveis de Suport tècnic, d'administració i operació de sistemes informació i en especial amb el SOC de l'IMI 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 viu anualment i trimestralment proporcionarà els avenços.

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.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

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. Actualment es preveu que el contracte haurà de donar resposta i supervisar les implementacions de:

- Servei Clare a la Pipeline de DEVSECOPS, definir polítiques de pipeline i fer suport puntual a les vulnerabilitats complexes
- Servei de vulnerabilitats i processos operatius de kubernates a IBM Cloud PRIVATE pel control de les vulnerabilitats productives al propi ICP i a les imatges productives
- Projecte operatiu del SOC de Migrar de SIEM actual a QRADAR els escanejos de vulnerabilitats i processos implementats al SOC de control de vulnerabilitats a les xarxes dels grans proveïdors de clouds privats de l'IMI i xarxes de lloc de treball.
- Revisar i complementar si cal els processos i/o les eines de escaneig de vulnerabilitats del servei que administra i opera les infraestructures i plataformes de web municipals (serveis Hosting WEB del Departament de Canals Digitals de l'IMI).
- Establir alertes de notificació centralitzada de les eines de escaneig

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

- Eina escaneig de vulnerabilitats
- Eina de gestió de vulnerabilitats

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.

Una eines/solució d'escaneig de vulnerabilitats que compleixi amb els següents requisits:

- Per als escanejos dels sistemes exposats a Internet, el proveïdor haurà de proveir l'eina d'escaneig de vulnerabilitats. Aquesta eina el proveïdor haurà de justificar la seva efectivitat indicant 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.

- Per als escanejos dels sistemes ubicats a les xarxes internes de l'Ajuntament, el proveïdor en principi no haurà de proveir l'eina d'escanejos de vulnerabilitats tot i que haurà de gestionar i millorar la implementació de l'eina i processos actuals que es troben desplegats al SOC i altres àrees operatives de l'IMI. Tot i que no es preveu que es requereixi que el proveïdor proporcioni sondes d'escaneig en la xarxa interna, si mai es requerís per algun punt concret de la xarxa, el proveïdor haurà de desplegar una sonda a la xarxa interna. Si fos el cas, l'IMI proporcionarà la

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

infraestructura necessària (maquinari, processament i sistema operatiu) per desplegar aquesta llicència o les connectivitats per realitzar-se en remot.

Una eina/solució per la gestió de vulnerabilitats, amb una interfície web accessible per a l'Ajuntament, que ha de permetre la gestió eficaç, com pot ser, per exemple:

- Perfils d'accés a la mateixa.
- 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.

Un repositori únic en què bolcar 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.

Elaboració de Quadres de comandament de seguiment 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 una visió general de seguretat ràpida i general actualitzada.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

4.3. ANÀLISI D'INCIDENTS DE SEGURETAT A POSTERIORI I ELABORACIÓ DE FORENSES JUDICIALS O INTERNS

Aquest Servei contempla la capacitat anàlisi del servei en front a un incident de seguretat a posteriori.

Aquest servei no és el servei que es troba als serveis operatius del SOC, es un servei a posteriori per l'anàlisi de causa arrel d'incidents i per la gestió d'evidències i elaboració d'informes ja sigui per requeriments interns o per peticions de informació de requeriment judicials per actuacions de tercers.

El contracte haurà de contemplar durant el contracte una anàlisi forense en què es requereixi serveis d'experts pericials amb personal certificat i disposició de presentar l'anàlisi/informe l'Ajuntament o IMI de part en un judici. Aquest peritatge es requereix com a reserva per necessitats d'urgència que l'Ajuntament o IMI puguin necessitar. Es considera que màxim suposarà el cost de 2 auditories tècniques de nivell MIG i es pot subcontractar a empreses especialitzades amb prèvia conformitat del responsable corporatiu del contracte.

El servei Tècniques d'anàlisi forense pericial (tecnologies de forense exhaustives) n'hi haurà un per contracte amb possibilitat d'ampliació, ha d'esser per incorporar evidències en processos judicials que interessi a l'Ajuntament. Aquest servei l'empresa podrà subcontractar a tercers. En aquest cas, s'haurà de presentar l'empresa subcontractada al responsable del contracte de l'IMI.

Les tasques que l'adjudicatari haurà de portar a terme per realitzar els serveis de seguretat reactiva són:

- Anàlisi forense:
    - **Tècniques d'anàlisi forense** d'investigació sobre actuacions per requeriments d'expedients interns o requeriments judicials on es requereixin emprar les tecnologies de forense exhaustives, com són garanties exhaustives d'integritat i autenticitat de la prova. Aquest servei requereix d'alta especialització per personal certificat CHFI, Pèrit Judicial Forense. Aquest forense es pot subcontractar el servei a una empresa especialista sempre que s'acordi amb el responsable de contracte de l'IMI .
    - **Tasques investigació d'actuació o anàlisi incident a posteriori** menys exhaustives en quant a garanties d'integritat i autenticitat de la prova, sobre actuacions internes no crítiques i per la identificació d'un incident. Anàlisi de la causa arrel d'un incident i l'impacte real del mateix a l'IMI. Aquest servei requerirà perfil de tècnic de ciber seguretat i Servei de hacking (RCA anàlisi)
    - **Tasques de gestió de petició d'evidències, recepció i elaboració d'informe**. 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 document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Gestió de les peticions de forenses:
    - Recepció de la petició.
    - Validar la idoneïtat de la persona que sol·licita i a qui s'entregarà informe
    - Sol·licitar i rebre la informació als/dels administradors amb garanties de confidencialitat
    - Classificar si es tracta d'un forense
    - Elaborar informe forense
    - Gestionar la correcta entrega de l'informe tant en contingut com en la forma de l'entrega.

També durà a terme altres funcions, com són:

- Coordinació / Supervisió dels sistemes d'evidències (logs centralitats) que opera el SOC. Proposta de noves incorporacions als logs centralitzats, tant pels sistemes de logs centralitzats de l'IMI com pels sistemes dels clouds.
- Mantenir inventari d'evidències.
- Vetllar per la estratègia d'evidències establerta i per la implementació a la organització de la política d'evidències.
- Proposar anualment millores del sistema d'evidències corporatives.
- Registrar i informar/documentar al "Registre d'incidents corporatiu" incidents de seguretat que es derivin de les tasques d'investigació o Forenses.
- Servei de comprovació de la qualitat de les evidències corporatives per mostreigs. Pla de comprovació de la exactitud i integritat de les evidències mes critiques (accés wifi, navegació, Accés als sistemes, correu, etc.).
- Definir estratègia i Polítiques de les evidències corporatives.
- Planificar i donar suport per la integració noves fonts d'evidències en la eina de logs centralitzats i/O SIEM per tal que ho implementi el suport Tècnic i operatiu del SOC de l'IMI.

L'anàlisi enfront a la causa arrel d'incidents de seguretat requereix d'una evolució constant de les capacitats. En aquest sentit es sol·licita un servei que tingui per objectiu estudiar els actuals procediments, normes i polítiques per a la seva millora contínua, així com la creació d'aquells que se'n derivin del mateix.

En aquest sentit, el servei ha de gestionar de forma regular i proactivament les relacions amb les àrees operatives periòdiques per a tenir una fluida informació i treball coordinat:

- Relacions amb el 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.).
- Relacions amb els serveis operatius dels contractes de l'IMI que fan la gestió de clouds privats i públics corporatius.
- Relacions amb els serveis operatius del SAU de l'IMI.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Coordinació amb el Departament de Canals digitals per el control preventiu de les webs corporatives.
- Qualsevol altra tasca en relació amb el servei que li sigui encomanada pel Departament de Seguretat de l'IMI.

A continuació es presenta una taula de volumetria exhaustiva que es demana en aquest plec pel servei d'auditoria tècnica, tot indicant que no incorpora les tasques o funcions diàries i/o periòdiques regulars, detallades en el paràgraf anterior.

TAULA 3 – Volumetries del servei de seguretat reactiva	**Quantitat**
Tècniques d'anàlisi **forense pericial** (tecnologies de forense exhaustives)	1 per contracte
Tasques investigació d'actuació o anàlisi incident a posteriori (sense tecnologies de forense especialista pericial)	8 per any
Tasques de gestió de petició d'evidències, recepció i elaboració d'informe	20 per any
Presentar una proposta anual de millores del sistema d'evidències corporatives	1 proposta anual
Planificar i coordinar noves integracions als logs centralitzats i/o SIEM	2 any

Es valoraran les propostes dels licitadors que millorin el nombre mínim Seguretat reactiva de forenses i tasques d'investigació i petició d'evidències a realitzar anualment. En cas de millora oferta per part de l'adjudicatari en la seva proposta, serà aquesta la que prevaldrà.

5. MODEL DE PRESTACIÓ DEL SERVEI

5.1. MODEL DE RELACIÓ IMI/ADJUDICATARI

El model de relació defineix les funcions i responsabilitats de l'adjudicatari 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 del licitador i en el seu cas l'adjudicatari, haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les tasques assignades.

L'adjudicatari haurà de plantejar de forma explícita, i el més exhaustiva possible, un model de relació amb l'IMI, dissenyat de manera que s'asseguri el correcte acompliment de les seves funcions.
L'esmentat model de relació haurà de fer explícits els rols i responsabilitats del contracte, els nivells de relació i l'estructura i funcionament dels Comitès de relació i coordinació que siguin precisos per mantenir una interlocució permanent amb els actors involucrats en el procés.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

Model de Relació

El model de relació haurà de fer explícits els rols i responsabilitats del contracte, que com a mínim establirà:

- Relació amb els clients finals (Ajuntament) la gestionarà l'IMI,
- Determinarà el model i figures que actuaran com interlocució i lligam entre l'IMI i l'organització interna del licitador.
- Establirà les figures i determinarà les responsabilitats de responsable del contracte, i establirà responsables de blocs de serveis o agrupacions de serveis en base a la seva dimensió i/o funcionalitat que cobreixin, així com la responsabilitat de transformació del servei cap al model proposat.

Àmbits del Model de Relació

Aquest model de relació ha de determinar com es gestionarà el seguiment del contracte a nivell estratègic, tàctic i operatiu, i com es materialitza aquest seguiment per nivells mitjançant els Òrgans de govern.
Hi haurà d'haver, com a mínim, els següents **òrgans de govern**:

- Comitè de Direcció
- Comitè de Seguiment Operatiu

Òrgans de Gestió (Comitès)

L'empresa adjudicatària anomenarà un responsable del contracte, que serà l'únic interlocutor vàlid entre l'empresa i l'Institut per a tots els temes relacionats amb la gestió i execució del contracte. Les seves funcions i responsabilitats estan detallades en l'apartat 6 d'aquest plec.

Comitè de Direcció

L'Institut anomenarà un Comitè de Direcció que assumirà les funcions de supervisió de l'execució del contracte així com la presa de decisions que afectin a l'objectiu i abast del mateix, especialment per definir i encarregar tasques sota demanda de nous projectes o iniciatives no identificades inicialment. L'àmbit executiu és el nivell màxim de seguiment del contracte i la prestació del servei.

Aquest comitè farà un seguiment exhaustiu de l'execució dels serveis tecnològics i de negoci i del contracte. S'assegura el compliment dels mateixos de control global i s'elevaran a l'àmbit executiu aquells aspectes que puguin originar la modificació del contracte o contractes.

Aquest Comitè es reunirà mensualment, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

Aquest comitè definirà les directius i assumirà els canvis de contractes o resoldrà conflictes contractuals:

- Revisar compromisos de serveis i visió global dels mateixos.
- Des d'aquest àmbit s'elevaran a l'òrgan de contractació les propostes d'actuació en aquells aspectes que puguin originar la modificació del contracte.
- Marcar les directius estratègiques.
- Realitzar el seguiment tàctic de les activitats realitzades i l'assoliment d'objectius plantejats en el Pla de Seguretat del Servei.
- Gestionar i identificar de canvis o modificacions d'objectius o canvis d'abast, modificacions de contracte, condicions econòmiques.
- Definir el catàleg de Serveis.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Proposta del règim sancionador.

El Comitè Executiu estarà format com a mínim per les següents persones:

- Director de Qualitat i Seguretat
- Responsable de Seguretat
- Director d'Operacions i Sistemes
- Responsable de Telecomunicacions
- Responsable del Departament de Canals Digitals
- Responsable del Contracte en l'IMI
- Responsable del contracte empresa adjudicatària

El responsable del contracte de l'empresa adjudicatària assistirà a les reunions d'aquest Comitè sempre que sigui requerit per qualsevol dels seus membres. Quan ho faci serà el responsable de l'elaboració de la documentació de seguiment del projecte necessària per a tal fi i també d'aixecar l'acta de les reunions d'aquest Comitè a les que hi assisteixi.

Comitè de Seguiment Operatiu
L'IMI anomenarà un Comitè de Seguiment Operatiu que s'encarregarà de la gestió del dia a dia de l'execució del contracte. També resoldrà les incidències i conflictes menors que apareguin al llarg de la vida d'aquest contracte.

Aquest comitè es reunirà amb una periodicitat quinzenal.

El Comitè de Seguiment està format com a mínim per:
- Responsable del contracte de l'empresa adjudicatària
- Responsable del contracte per part de l'IMI.

Quan calgui, es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip adscrits al contracte necessaris per a tractar en profunditat determinats temes. El responsable del contracte de l'empresa adjudicatària és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Li correspon al comitè de seguiment les funcions de control de l'execució del contracte

- Validació de la feina
- Verificació operativa de l'acompliment del contracte
- La resolució dels conflictes que puguin sorgir en l'execució del contracte
- Detecció d'incompliments i escalat

L'IMI controlarà, mitjançant la figura d'un Responsable el contracte de l'IMI, el compliment dels terminis acordats, així com la qualitat i l'adequació dels serveis objecte d'aquest contracte i l'execució del contracte segons la metodologia i els estàndards de l'IMI.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Cal que els licitadors detallin a les seves propostes quina és l'organització que proposen per al contracte, tenint en compte que hauran de dotar el personal necessari per assegurar les funcions de governança que són objecte d'aquest contracte i permeti mantenir un model fluid amb els agents que participen en el procés.

5.2. SEGUIMENT DEL SERVEI

L'adjudicatari haurà de presentar un model de seguiment del servei de l'Oficina tècnica objecte d'aquest contracte.

En això, serà obligatori convocar una reunió de Kick-off o llançament de servei amb els principals membres del contracte (Equip de l'adjudicatari i Equip de l'IMI) amb caràcter obligatori.

També s'inclourà un **quadre de comandament** amb un model d'indicadors de compliment dels compromisos associats i un esquema de reporting dels mateixos pel seguiment, control i gestió del servei.

Es valorarà el contingut del quadre de comandament, el detall del seu model d'indicadors i la facilitat d'interpretació de l'esquema de reporting.

Obligatòriament, l'adjudicatari haurà de presentar com a mínim en la temporalitat que s'especifica en cada apartat els següents **informes de comunicació i seguiment**:

Informe de feina en curs i prioritats establertes: (setmanal)

- Estat de cada una de les tasques o serveis que s'estan realitzant. Per cada una d'elles:
  - Estat actual.
  - Passos que s'han realitzat fins la data actual.
  - Passos pendents per tal de finalitzar-ho.
  - Detecció i proposta de resolució de problemes.
  - Revisió segons planificació i dates previstes d'execució.
- Tasques futures previstes.

Informe de seguiment de l'avenç: (mensual)

- Estat general de les tasques o serveis que s'estan realitzant:
  - Estat actual.
  - Passos que s'han realitzat fins la data actual.
  - Passos pendents per tal de finalitzar-ho.
  - Detecció i proposta de resolució de problemes.
  - Revisió segons planificació i dates previstes d'execució.
- Tasques futures previstes.
- Quadre de comandament / Dashboard de gestió del servei.

Tanmateix la composició dels informes es consensuarà amb l'IMI a l'inici del contracte i podrà variar durant la prestació del mateix en funció de les necessitats del gestor del contracte per part de l'IMI.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Es valoraran les propostes que millorin el contingut i estructura dels informes previstos en aquest apartat. I en especial les millores en l'accessibilitat a la informació i el quadre de comandament proposat.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

5.3. PLA DE SERVEI

El servei es desplegarà seguint les següents fases:

Llançament del Servei

Es definiran les tasques necessàries per crear i activar el servei de prevenció de seguretat i

Es validaran amb la Direcció de l'IMI els assistents als comitès del servei i es planificaran els primers comitès.

Es realitzaran les tasques de comunicació interna i externa per informar del pla d'acció del servei i dels actors que hi participaran en la Direcció de Qualitat i Seguretat.

Execució del Servei

Es realitzaran les tasques necessàries per la gestió del servei.

Es planificaran els comitès del servei.

Es continuaran les accions de comunicació interna i externa per informar dels resultats del servei i per comunicar properes passes.

Resolució del Servei

Es definiran les tasques necessàries per realitzar el traspàs del servei exposat a l'IMI o al següent adjudicatari.

Es validarà amb la Direcció de l'IMI la transferència de coneixement dels lliurables, tasques i accions del servei.

Es realitzaran les tasques de comunicació interna i externa per informar dels resultats del servei.

5.4. 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.

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

- Cicle de Vida del servei:
  - Checkpoints.
  - Rols responsables de cada tasca o activitat.
- Gestió de la Configuració: Assegurar que els canvis no afecten els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- 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.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- 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.
- 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 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.

6. ORGANITZACIÓ I PERFILS REQUERITS

RECURSOS HUMANS

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis, i presentarà i detallarà els següents aspectes que es sol·licita que plantegi en la proposta l'empresa licitadora.

Els licitadors hauran de plantejar a les seves propostes de forma genèrica quina és l'organització per al servei, tenint en compte que hauran de dotar el personal necessari per assegurar les funcions que són objecte d'aquest contracte i permeti mantenir un model fluid amb els agents que participen en el procés.

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis i n'assegurarà la seva estabilitat mentre estigui vigent el contracte.

Aquest servei té establerts serveis tancats i alguns executats des de les seves dependències com a serveis tancats: Serveis de ciberintel·ligència, Escanejos de vulnerabilitats, Anàlisis forenses i d'evidències, recepció de CERT externs i reportings d'auditories tècniques alienes al servei.

També contempla la dedicació d'un perfil que gestioni totes les entrades i sortides d'aquests serveis de cibertintel·ligència, actuacions d'escanejos de vulnerabilitats d'infraestructura, d'auditories tècniques i peticions d'anàlisis forenses i evidències, i recepcions d'informes de CERTs i resultats auditories tècniques alienes a aquest contracte. El licitador haurà de plantejar quina part dels seus serveis tancats delega en aquest perfil. Tot i això, es considera que aquest perfil tindrà una dedicació quasi exclusiva al contracte (recomanable 85 % i mínim 75 % del temps setmanal).

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

Fet aquest aclariment, en l'oferta presentada s'indicarà, un compromís d'adscripció en cas de resultar adjudicatari dels recursos inclosos amb especificació de les dedicacions i condicions proposades.

L'adjudicatari haurà de presentar un detall exhaustiu de l'equip que proposarà amb els compromisos de l'oferta detallats amb la concreció i acreditació de l'experiència, certificacions i formació requerides en aquest apartat i que hagin estat proposades pel mateix.

No obstant, l'IMI considera que **es necessiten com a mínim els següents perfils que es detallen a continuació**, i exigirà que aquests hi participin amb les dedicacions que s'expliciten:

- **Funcions per Perfil professional**

D'acord a les volumetries anteriorment descrites, s'estima necessària la implicació d'un equip de 2-3 persones considerant que una persona ha de tenir una dedicació específica i propera a l'IMI i amb dedicació quasi exclusiva (mínim 80% del temps setmanal) per tal de realitzar una bona gestió de totes les necessitats diàries del servei:

A continuació s'identifiquen i es descriuen els perfils a proporcionar per l'adjudicatari, agrupats per àrees:

Perfil	Responsabilitat
Cap d'Oficina (Service Manager)	Màxim responsable de l'equip de l'adjudicatari, i en conseqüència de la provisió en temps i qualitat dels serveis inclosos en aquest contracte. Actuarà com a Coordinador del Servei i donarà Suport a l'Àrea de Seguretat de la Informació de l'IMI en la definició del full de ruta d'evolució del Servei. Màxim interlocutor de l'equip, revisa amb la direcció del contracte per part de l'IMI el correcte avenç de les activitats previstes, l'adequació dels recursos humans, i gestiona riscos, desviacions, peticions fora de l'abast inicial, etc. Tasques: • Participació al Comitè Tècnic del Servei fent reporting de l'evolució del servei als responsables del servei de l'IMI • Definició del catàleg serveis • Aplicació de les bones pràctiques en la gestió de serveis TIC
Tècnic sènior especialista en seguretat preventiva	• 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, vulnerabilitats d'infraestructures, 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

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

	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 el 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. • Registrar i informar/documentar al "Registre d'incidents corporatiu" incidents de seguretat que es derivin de les tasques d'investigació o Forenses. ***Servei de Forense i investigació interna:*** • Elaborar investigacions d'incidents o peticions internes, elaborar informes dels resultats dels forenses formals, fer vehicular de forma procedimentada les peticions d'informació d'evidències ja siguin per peticions a requeriments judicials com per peticions internes regulades de l'Ajuntament. • Avaluar si procedeix el peticionari i la petició i contrastar la fiabilitat de la mateixa. • Realitzar, executar 1 forenses any per presentar proves o actuacions en judicis d'interès per Ajuntament de Barcelona ***Servei de Hacking*** Realització de auditories tècniques de seguretat, escaneijos de vulnerabilitats i tests d'intrusió Revisions de vulnerabilitas derivades de falles de disseny en arquitectures de xarxa, sistema o desenvolupament

Es considera que aquest servei inclourà com a mínim 2-3 FTEs dels perfils indicats que es repartiran en els diferents serveis del contracte.

L'IMI podrà demanar en qualsevol moment a l'adjudicatari el llistat de persones que formen part de l'equip adscrit al contracte.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- **Característiques professionals**

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

L'IMI podrà demanar en qualsevol moment a l'adjudicatari el llistat de persones que formen part de l'equip adscrit al contracte.

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

Perfil	Experiència professional
Cap d'oficina (Service Manager)	Cal que acrediti, durant els darrers 6 anys, 4 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC. Ha de tenir alguna de les certificacions següents: ITIL Expert, PMP, CGEIT, CISA, CISM, CISSP
Tècnic sènior especialista en seguretat preventiva	Cal que acrediti, durant els darrers 3 anys, 2 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC. Cal que tingui alguna de les certificacions indicades per cada grup (o similar): • CISA, CISM, CISSP
Tècnic sènior especialista per de Hacking i _Servei de Forense i investigació interna:	Cal que acrediti, durant els darrers 3 anys, 2 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC. Cal que tingui alguna de les certificacions indicades per cada grup (o similar): • Ha de disposar alguna d'aquestes certificacions: o CICH o EC-Council CEH o Offensive Security OCSP o SANS GIAC GPEN o SANS GIAC GPXN o SANS GIAC GAWN o SANS GMOB o CSX
Especialista en Peritatge Forensic (1 forense cada 2 anys, ampliable)	Cal que acrediti, durant els darrers 3 anys, 2 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC. Cal que tingui alguna de les certificacions indicades per cada grup (o similar): • CHFI, Pèrit Judicial Forense col·legiat pels forenses Judicials i per les investigació interna complexes. (Aquest perfil és exclusiu per executar 1 forense dins del contracte per judicis d'interès per Ajuntament de Barcelona)

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

L'adjudicatari haurà de mantenir format a l' equip de treball. Per tal efecte, l'adjudicatari es compromet a definir un pla de formació anual pel perfil de Gestió de vulnerabilitats i hacking ètic que es concretarà amb el responsable del contracte de l'IMI per cobrir mancances i actualitzar coneixements necessaris que es detectin pel desenvolupament del contracte. Aquesta formació com a mínim serà de 20 hores anuals.

Els licitadors es comprometran a posar a disposició de l'execució del contracte l'equip mínim requerit en la forma que s'indica en el plec de clàusules administratives particulars en cas de resultar adjudicatari.

L'adjudicatari amb caràcter previ a l'adjudicació del contracte haurà de declarar la composició de l'equip de treball que posarà a disposició del contracte, acreditant que tenen l'experiència professional exigida en el quadre anterior.

L'IMI es reserva el dret de verificar les capacitats del personal que participa en el contracte en qualsevol moment i rebutjar-lo en cas que no compleixin amb els requisits exigits. Les despeses que es derivin com a conseqüència de canvis en l'equip adscrit al contracte aniran a càrrec de l'adjudicatari.

L'empresa adjudicatària haurà de mantenir l'equip de treball adscrit al contracte durant tota la vigència d'aquest. En cas que s'hagi de produir la substitució d'algun membre de l'equip, que no sigui per causes de força major, l'adjudicatari ho comunicarà a l'IMI i la substitució s'haurà de fer per un perfil que com a mínim tingui les mateixes característiques professionals i tècniques que les exigides en aquesta clàusula; en cas contrari i sense el consentiment de l'IMI, aquest fet serà susceptible de sanció.

A més, en cas de substituir algun membre de l'equip de treball, s'exigirà el següent:

- un període de formació, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.
- Un període de coexistència, d'un mínim d'un mes, entre la persona que causa baixa i la persona que s'incorpora

A tal objecte, i per donar continuïtat i valor afegit al servei, l'empresa licitadora haurà d'acreditar que disposa d'un mínim de certificacions personals sobre coneixements adquirits així com experiència en projectes similars, indicats en els criteris de solvència.

7. CONDICIONS D'EXECUCIÓ

A continuació es detallen les condicions d'execució del present contracte.

7.1. LLOC DE PRESTACIÓ DEL CONTRACTE

El personal de l'adjudicatari que realitza les tasques de gestió de vulnerabilitats treballarà a les oficines de l'IMI almenys en un 75% restant, quan participin en reunions amb personal de l'IMI o de l'Ajuntament es desplaçaran allà on aquestes es produeixin, i que poden ser en dependències municipals o de tercers involucrats en el contracte.

Pel que fa al suport, formació, i reunions de treball, s'hauran de dur a terme en les dependències que l'IMI indiqui, i que seran dins de la província de Barcelona.

Si cal habilitar una connexió des de les dependències de l'adjudicatari amb la xarxa Per la realització de les activitats de forma remota, és a dir, des de les instal·lacions de l'adjudicatari, s'ha de garantir el compliment dels requisits de:

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Seguretat. Garantint la confidencialitat, integritat i accessibilitat de les activitats a realitzar.
- Infraestructural. Disponibilitat de les comunicacions, hardware i software necessari per garantir les activitats a realitzar.
- Organitzatiu i funcional. Que l'adjudicatari pugui disposar de la logística, processos, procediments i coneixements necessaris per a garantir les activitats a realitzar.

Si cal habilitar una connexió des de les dependències de l'adjudicatari amb la xarxa corporativa municipal o amb l'entorn de desenvolupament i test de l'IMI, el seu cost anirà a càrrec de l'adjudicatari. En el cas de desenvolupament de software, l'adjudicatari haurà d'aportar medis logístics suficients per a la prestació del servei des de les seves instal·lacions.

7.1. HORARI DE PRESTACIÓ DEL SERVEI

L'adjudicatari haurà de cobrir els horaris descrits a continuació, en funció del procés/servei prestat:

L'horari de prestació del servei pel personal que es personarà en les oficines de l'IMI serà aplicable als dies que siguin laborables a la ciutat de Barcelona, de dilluns a divendres de 9:00h a 18:00h.

El servei de Ciberintel·ligència i detecció de vulnerabilitats en la infraestructura i serveis corporatius serà 24x7 i aquest haurà de tenir processos especials de comunicació de vulnerabilitats molt crítiques fora d'horaris laborals per tal que els procediments desenvolupats en l'IMI rebin les notificacions i que els serveis operatius amb els seus SLAs les puguin gestionar. La resta de vulnerabilitats comunicaran i es gestionaran en horaris laborals.

El servei de vulnerabilitats haurà de preveure comunicar 24x7 vulnerabilitats MOLT Crítiques que s'hauran de gestionar mitjançant procediments establerts per aquest servei per tal que els serveis operatius de l'IMI procedeixin a actuar per mitigar o eliminar la vulnerabilitat.

També s'haurà de preveure 4 situacions a l'any d'emergències fora del l'horari laborable indicat per tractament, contenció i remediació de:

- forenses crítics anàlisi d'incidents
- processos d'emergències d'aplicació de vulnerabilitats
- deteccions crítiques dels serveis de ciberintel.ligència

En casos excepcionals i de forma prèviament planificada, es podrà requerir l'execució de determinats serveis fora de l'horari normal, incloent disponibilitat en horari nocturn.

Aquests casos es poden donar, per exemple, per:

- Emergències i/o esdeveniments crítics i/o importants per l'Ajuntament de Barcelona amb requeriments directes als serveis d'aquest contracte.
- En desplegaments crítics que es realitzen fora de l'horari de servei, per tal de minimitzar l'impacte al ciutadà amb necessitats directes dels serveis d'aquest contracte.
- Auditories tècniques i hacking ètics que es requereixi realitzar-se en horaris especials, fora de l'horari de prestació de servei indicat.
- En cas de situacions d'emergència excepcionals que es concretaran dins del servei i que es preveu un màxim d'1 situació semestral.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

En aquests casos, l'adjudicatari haurà d'assumir el cost econòmic com a servei bàsic d'aquest contracte sense que s'incrementi el cost de l'import adjudicat.

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

7.3. IDIOMA I TRADUCCIONS

Les llengües de treball del servei seran, per la mateixa naturalesa de la feina i per l'àmbit en què es relacionen, el català i el castellà.

Serà responsabilitat de l'adjudicatari generar tots els documents i lliurables del servei en català.

7.4. INFRAESTRUCTURA NECESSÀRIA PER A LA PRESTACIÓ DEL SERVEI.

L'adjudicatari haurà d'aportar els medis logístics i tècnics suficients per a la prestació del servei des de les seves instal·lacions.

La connexió remota amb l'Institut Municipal d'Informàtica es podrà fer amb les següents alternatives: En cas de ser factible, mitjançant enllaços propietaris de fibra òptica. L'enllaç a establir serà una connexió Giga bit amb separació i translació d'adreces en el costat de l'adjudicatari. En aquest cas és a càrrec de l'adjudicatari els costos derivats de qualsevol actuació necessària per a la posada en marxa de la connexió: esteses de fibra i electrònica addicional, manipulacions de connexions de fibra a la via pública, etc. A través d'una connexió al servei Metrolan de Telefònica i amb una connexió d'ample de banda suficient per a garantir un adequat rendiment. L'enllaç a establir serà una connexió Ethernet amb separació i translació d'adreces en el costat de l'adjudicatari. És a càrrec de l'adjudicatari els costos derivats de qualsevol adquisició o actuació necessària per a la posada en marxa de la connexió. També serà al seu càrrec la quota mensual de la línia a contractar.

Per últim i de forma preferent, mitjançat solució VPN (lan-to-lan) sobre l'accés a Internet existent a les dependències de l'IMI d'acord amb la normativa establerta per aquest institut per l'accés remot als seus sistemes d'informació. És responsabilitat de l'adjudicatari la contractació i manteniment del seu accés a Internet així com de disposar d'un equip que suporti aquest tipus de connexions i d'un ample de banda suficient en aquesta línia. És responsabilitat de l'adjudicatari disposar del personal tècnic necessari per a la correcta configuració dels equips que acaben del circuit VPN del seu costat i dels seus sistemes de seguretat i translació d'adreces IP (si cal), l'IMI col·laborarà en la seva implantació facilitant els paràmetres de configuració i el certificat per a l'equip que acaba el circuit. Opcionalment podrà oferir un model de configuració tipus si aquest equip final és un router cisco de la sèrie 800.

En cas de dificultats per a l'establiment d'aquest circuit, l'IMI es reserva el dret de comprovar, amb equips de la seva propietat, la causa del problema amb l'objectiu de determinar responsabilitats en la resolució de qualsevol incidència. Per a realitzar les tasques de desenvolupament requerides caldrà realitzar la instal·lació d'un software a les estacions del client (aquest software està garantit sobre plataformes Windows). Aquest software permetrà accedir a unes màquines de desenvolupament remot que estaran a la seu del IMI. El software que serà necessari instal·lar a les màquines de l'adjudicatari serà el client de firewall i l'escriptori remot XP en les estacions. Es responsabilitat de l'adjudicatari aquesta instal·lació i el seu manteniment així com disposar dels equips que suportin aquest software. El firewall cal configurar-lo amb les opcions estàndard que indicarà l'IMI. L'accés a la màquina o màquines de desenvolupament

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

assignades es farà mitjançant un o més noms DNS que l'IMI subministrarà. Per a la resolució d'aquests noms cap a una adreça IP també es facilitarà l'adreça d'un servidor DNS de l'IMI capaç de resoldre correctament els noms d'estació. És responsabilitat de l'adjudicatari configurar les estacions o els servidors DNS interns perquè les peticions puguin arribar fins als servidors de l'IMI.

Cada estació de desenvolupament només admet una connexió remota. És responsabilitat del client garantir que cada usuari utilitzi una màquina diferent de les que l'IMI els ha assignat. Les estacions de desenvolupament estan preparades per permetre la impressió a models d'impressores reconeguts per Windows XP. Si es requereix algun model no reconegut, caldrà notificar-ho a l'IMI perquè s'afegeixin els drivers necessaris. Per poder utilitzar la impressió des de sistemes externs (Host Print o Paris) cal que les impressores tinguin assignada una IP del rang subministrat per l'IMI.

S'ofereix la possibilitat de transferir fitxers entre l'estació de desenvolupament i la de l'usuari, però es recomana fer-ho amb moderació degut a l'alta utilització d'ample de banda que requereix. Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari.

8. PRESSUPOST, OFERTA ECONÒMICA I FACTURACIÓ

L'import de licitació del contracte és de 477.787,84 €, IVA inclòs, dels quals 394.865,98 € corresponen al pressupost net i la resta de 82.921,86 € a l'IVA del 21 %.

Els licitadors presentaran la seva oferta econòmica pel conjunt dels serveis objecte del contracte, d'acord amb el model de proposta econòmica que s'adjunta en el plec de clàusules administratives particulars, detallant l'import de les diferents parts que el composen (separant l'import net, l'IVA i l'import total).

Els licitadors detallaran en les seves ofertes el preu ofert (IVA exclòs) detallant com a partida independent la corresponent a l'IVA aplicable.

Els serveis es facturaran mensualment en atenció als serveis realitzats. Així doncs a la factura hi constarà l'import econòmic corresponent a la part proporcional resultant de dividir l'import d'adjudicació entre el mesos d'execució del contracte.

9. 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.

El licitador haurà de presentar la seva oferta tant en format paper com en format electrònic, ambdós obligatoris. A l'oferta en suport electrònic tots els arxius han d'estar en format **Open Document (odt o odp) i pdf obligatori**, en format no protegit, amb fonts incrustades i que accepti cerques, seleccions i copiat del text.

El licitador pot adjuntar tota la informació complementària que consideri d'interès, tot i això haurà de presentar uns continguts mínims i estar obligatòriament estructurada de la forma següent:

Es presentaran dos sobres tancats, **el sobre B** on s'inclourà la documentació que haurà de ser valorada segons els criteris de judici de valor assenyalats en les clàusules del plec de clàusules administratives

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

particulars, i **el sobre C** que haurà de contenir la documentació que haurà de ser valorada segons els criteris avaluables de forma automàtica assenyalats en les clàusules del plec de clàusules administratives particulars que regeixen per aquesta contractació.

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.

En el **sobre B** s'inclourà la documentació següent indexada de manera que faciliti la seva localització, per a cada apartat i entre parèntesi s'ha indicat en grandària 12 i interlineat simple:

1.- Resum executiu (màxim 3 pàgines)

En aquest apartat s'exposarà un resum per a la direcció dels continguts més significatius de la proposta del projecte.

2.- Plantejament del servei de prevenció (màxim 30 pàgines)

- **Enfoc general de la proposta** on s'exposarà l'enteniment dels serveis i les línies principals de l'estratègia per afrontar-lo, tenint en compte els requeriments exposats en el plec de prescripcions tècniques. Es detallarà tot el que es consideri interessant de caràcter general i integrat dels diferents serveis incidint especialment en aspectes de gestió de la qualitat i eficiència de l'objecte del contracte, que és el de serveis preventius i anàlisi a incidents, i evidències en la seva globalitat, així com i elaboració de forenses judicials.

  Es descriurà amb detall cada servei del plec de manera que es visualitzi com es desplegaran els serveis dins de l'organització.

  També es descriurà com es proposa la implicació i interaccions amb els diferents servei, equips de treball de l'IMI i contractes de serveis de infraestructures i/o operació i suport tècnic (CPD-Datacenter, lloc de treball, proveïdors, Servei operatiu webs corporatives, administradors i operadors, xarxes i telecomunicacions, Suports tècnics verticals com són SAP, sistemes informació Contractació, Decidim Barcelona, etc.). per a la coordinació, comunicació, seguiment i resolució o minimització de les vulnerabilitats a través d'aquests contractes.

- **Proposta de comunicació 24x7 de vulnerabilitats molt crítiques** a l'IMI i desenvolupament de procediments interns per l'escalat d'emergència als diferents serveis i contractes operatius de l'IMI

- **Proposta d'industrialització dels serveis**. Indicar la proposta dels processos i eines per industrialitzar parts dels serveis mitjançant automatització de tasques i generació d'activitats a través de l'eina de ticketing o altres mecanismes.

- **Eines o millores de serveis d'auditories tècniques i gestió de vulnerablitats** a més de les exigides objectivament i descrites al punt 4.2 del plec tècnic, que suposin per l'IMI i l'Ajuntament una millora
- **Eines o millores de serveis de ciberintel·ligència** a més de les exigides objectivament i descrites al punt 4.1 del plec tècnic, que suposin per l'IMI i l'Ajuntament una millora

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

3.- Proposta de quadres de comandament i reporting: detall dels informes de cadascun dels serveis (màxim 5 pàgines)

Detall dels informes operatius de cadascun dels serveis i nivell de detall i profunditat de les recomanacions que es proposen implementar pels diferents equips d'operació i administració de sistemes. S'ha de tenir en compte la diversitat de proveïdors que gestionaran plataformes i serveis de l'IMI, i proporcionar comandament i reporting a nivell estratègic, tàctic i operatiu que permetin tenir coneixement del nivell d'exposició i riscos corporatiu i l'efectivitat i progrés de la gestió del servei objecte d'aquest contracte.

Detall d'informes tàctics i executius destinats a directius de l'Ajuntament i IMI. Indicant el nivell de claredat i reporting estratègic.

4.- Millora del Pla de Qualitat del Servei (màxim 5 pàgines)

El Pla de Qualitat del Servei ha d'explicar, amb suficient nivell de detall, com es garantirà l'execució dels serveis amb la qualitat estipulada i com es gestionaran els possibles riscos i desviaments derivats.

Altra informació que el licitador consideri rellevant per fer més comprensible la seva proposta (màxim 5 pàgines).

En el sobre C s'inclourà la documentació que s'especifica en el plec de clàusules administratives particulars.

10. CONDICIONS GENERALS D'EXECUCIÓ

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.

Els estàndards vigents aprovats i operatius del cos normatiu establerts es troben recollits sota la nomenclatura de "Criteris de Seguretat de la informació i Protecció de Dades" i es troben a disposició dels licitadors. L'adjudicatari haurà d'aplicar aquestes normatives i estàndards que li corresponguin per l'abast del contracte i donar compliment a les modificacions dels estàndards o a aquells de nova creació

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 de Caràcter Personal i del Reglament que la desenvolupa, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, 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 que 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 que fa referència a la protecció de dades de caràcter personal (LOPDGDD).

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

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.

CLÀUSULA DE PROPIETAT INTEL·LECTUAL

La propietat intel·lectual dels treballs realitzats a l'empara d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

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.

L'empresa contractada accepta expressament que els drets d'explotació dels productes derivats d'aquest plec corresponen única i exclusivament a l'Ajuntament de Barcelona. Així doncs, el contractat cedeix, amb caràcter d'exclusivitat, la totalitat dels drets d'explotació dels treballs objecte d'aquest plec, inclosos els drets de comunicació pública, reproducció, transformació o modificació i qualsevol d'altre dret susceptible de cessió en exclusiva, d'acord amb la legislació sobre drets de propietat intel·lectual.

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'IMI.
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 les de caràcter personal, que no podran copiar o utilitzar amb una finalitat diferent a les que la informació té 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 als 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'Administració Municipal, així com qualsevol altra producte obtingut com a resultat del present contracte.

PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

L'adjudicatari, com a encarregat de tractament i tenint en compte l'adequació del nivell de seguretat al risc, tindrà les obligacions següents:

- Utilitzar les dades personals objecte del tractament, o les que reculli per a la seva inclusió, només per a la finalitat objecte d'aquest encàrrec. En cap cas podrà utilitzar-les per a finalitats pròpies.
- Tractar les dades personals seguint únicament les instruccions documentades del responsable.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Portar, per escrit, un registre de totes les categories d'activitats de tractament efectuades per compte del responsable que contingui:
    - El nom i les dades de contacte de l'encarregat o encarregats i de cada responsable per compte del qual actuï l'encarregat.
    - Les categories de tractaments efectuades per compte de cada responsable.
    - Una descripció general de les mesures tècniques i organitzatives de seguretat apropiades que estigui aplicant.
- No comunicar dades a terceres persones, excepte en el cas que compti amb l'autorització expressa del responsable del tractament, o en els supòsits legalment admissibles. Si l'encarregat vol subcontractar, haurà d'informar obligatòriament al responsable i sol·licitar la seva autorització prèvia.
- Mantenir el deure de secret respecte a les dades de caràcter personal a les quals hagi tingut accés en virtut del present encàrrec, inclús després de que finalitzi el contracte.
- Garantir que les persones autoritzades al tractament de dades personals s'hagin compromès, de forma expressa i pe escrit, a respectar la confidencialitat i a complir les mesures de seguretat corresponents, de les quals se les ha d'informar convenientment.
- Mantenir a disposició del responsable la documentació acreditativa del compliment de la obligació establerta a l'apartat anterior.
- Garantir la formació necessària en matèria de protecció de dades personals de les persones autoritzades per a tractar dades de caràcter personal.
- Quan les persones afectades exerceixin els drets reconeguts per la normativa de protecció de dades davant de l'encarregat del tractament (accés, rectificació, supressió, oposició, limitació del tractament i portabilitat de les dades), aquest haurà de comunicar-ho per correu electrònic a l'adreça que indiqui el responsable. La comunicació haurà de fer-se de forma immediata i en cap cas més enllà del dia laborable següent al de la recepció de la sol·licitud, juntament amb altres informacions que puguin ser rellevants per a resoldre la sol·licitud (per valorar la pertinença del seu contingut)
- Assistir al responsable en la seva obligació de respondre a les sol·licituds que tinguin per objecte l'exercici dels drets dels interessats així com també als requeriments de les autoritats de control.
- En allò referent a les notificacions de violacions de la seguretat de les dades:
    - L'encarregat del tractament notificarà al responsable del tractament, de forma immediata i mitjançant l'adreça de correu electrònic facilitada pel responsable, les violacions de la seguretat de les dades personals al seu càrrec de les quals tingui coneixement, juntament amb tota la informació rellevant per a la documentació i comunicació de la incidència.
      Es facilitarà, com a mínim, la informació següent:
        1. Descripció de la naturalesa de la violació de la seguretat de les dades personals, incloent quan sigui possible, les categories i el nombre aproximat d'interessats afectats i les categories i el nombre aproximat de registres de dades personals afectats.
        2. Dades de la persona de contacte per obtenir més informació.
        3. Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals. Descripció de les mesures adoptades o proposades per a posar remei a la violació de la seguretat de les dades personals, incloent si escau, les mesures adoptades per a mitigar els possibles efectes negatius.

      Si no és possible facilitar la informació de forma simultània, la informació s'ha de facilitar de forma gradual i sense dilacions.
    - L'Encarregat, a petició del responsable, comunicarà en el menor temps possible aquestes violacions de la seguretat de les dades als interessats, quan sigui probable que la violació suposi un alt risc pels drets i llibertats de les persones físiques.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

La comunicació ha de fer-se en un llenguatge clar i senzill i haurà d'incloure els elements que en cada cas assenyali el responsable, com a mínim:

1. La naturalesa de la violació de les dades.
2. Dades del punt de contacte del responsable o de l'encarregat on es pugui obtenir més informació.

- Descripció de les possibles conseqüències de la violació de la seguretat de les dades personals.
- Descripció de les mesures adoptades o proposades pel responsable de tractament per a posar remei a la violació de la seguretat de les dades personals, incloent si escau, les mesures adoptades per a mitigar els possibles efectes negatius.
- Posar a disposició del responsable tota la informació necessària per a demostrar el compliment de les seves obligacions, així com per a la realització de les auditories o les inspeccions que realitzi el responsable o un altre auditor autoritzat per ell.

- Permetre i contribuir a la realització d'auditories, incloses inspeccions, per part del responsable o auditor autoritzat per aquest.
- D'acord amb l'art. 32 del RGPD i el nivell de mesures establert per l'Ajuntament de Barcelona, prendrà totes les mesures necessàries per a la seguretat del tractament, incloent entre d'altres, si s'escau:
  - La pseudoanonimització i el xifrat de dades personals.
  - La capacitat de garantir la confidencialitat, integritat, disponibilitat i resiliència permanents dels sistemes i serveis de tractament.
  - La capacitat de restaurar la disponibilitat i l'accés a les dades personals de forma ràpida en cas d'incident físic o tècnic.
  - Un procés de verificació, avaluació i valoració regulars de l'eficàcia de les mesures tècniques i organitzatives per garantir la seguretat del tractament.
- Per tal d'avaluar l'adequació del nivell de seguretat, tindrà particularment en compte els riscos que presenti el tractament de les dades com a conseqüència de la destrucció, pèrdua o alteració accidental o il·lícita de dades personals trameses, conservades o tractades d'altra forma, o la comunicació o accés no autoritzats a les dades esmentades.
- Al finalitzar la prestació dels serveis del tractament d'acord amb les instruccions que rebi de l'Ajuntament de Barcelona, suprimir o tornar totes les dades personals i suprimir les còpies existents (tret que existeixen obligacions legals que requereixin la conservació per un temps definit).
- Si considera que una instrucció del responsable infringeix el RGPD o altres disposicions en matèria de protecció de dades de la Unió o dels Estats membres, l'encarregat informarà immediatament al responsable.
- Si l'encarregat infringeix la normativa de protecció de dades vigent (RGPD, LOPDGDD...) serà considerat responsable del tractament.

En cas que l'encarregat de tractament decideixi recórrer a un altre encarregat (com per exemple, en cas de subcontractació):

- Haurà de comptar amb l'autorització prèvia per escrit de l'Ajuntament de Barcelona.
- Si s'autoritzés recórrer a un altre encarregat i s'hagués de produir algun canvi, s'haurà d'informar a l'Ajuntament de Barcelona, i aquest tindrà la possibilitat d'oposar-se i rescindir el contracte.
- L'altre encarregat tindrà les mateixes obligacions de protecció de dades que les estipulades en el contracte o acte jurídic entre el responsable i l'encarregat i la consideració d'encarregat de tractament de l'Ajuntament de Barcelona.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

- Si l'altre encarregat incompleix les seves obligacions de protecció de dades, l'encarregat inicial seguirà sent plenament responsable davant de l'Ajuntament de Barcelona pel que respecta al compliment de les obligacions de l'altre encarregat.

CLÀUSULA PROGRAMARI I METODOLOGIA DE DESENVOLUPAMENT

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.

CLÀUSULA DE COMUNICACIONS EXTERNES

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'adjudicatari.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establertes 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 subsidiari de l'ús dels certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

La gestió dels certificats es realitzarà d'acord amb l'estàndard per la protecció i custòdia dels certificats digitals establert pel Departament de Seguretat de l'IMI.

CLÀUSULA DE SEGURETAT DELS EQUIPS, PROGRAMES I INFORMACIÓ

L'adjudicatari es compromet a vetllar per la seguretat dels equips on es trobin instal·lats els programes, bases de dades i informació de l'Administració Municipal, així com per la seguretat en els canals de comunicació emprats. Per tant, prestarà els seus serveis guardant estrictament les mesures de seguretat necessàries, amb la finalitat d'evitar la pèrdua d'informació, així com danys, pèrdua o deteriorament dels programes i bases de dades utilitzades i que són propietat de l'Administració Municipal.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

CLÀUSULA DE PERSONAL EXTERN

El Cap responsable del contracte de adjudicatari durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.
L'adjudicatari està obligat a implantar els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat, privacitat, integritat i continuïtat i la disponibilitat de la informació de l'Administració Municipal, i de donar-los a conèixer al seu personal.

El Cap responsable del contracte de l'adjudicatari, 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, formar al seu personal en la política i instruccions de l'Administració Municipal 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.

L'adjudicatari 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.
El Cap responsable del contracte de l'adjudicatari 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'Administració Municipal, 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 responsable del contracte de l'Administració Municipal, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Administració Municipal o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'adjudicatari que haurà de presentar-los quan siguin requerits per l'Administració Municipal.

GESTIÓ D'INCIDENTS

L'adjudicatari informarà a l'IMI-Seguretat de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert en l'IMI.

L'adjudicatari col·laborarà amb el Departament de Seguretat de l'IMI en la resolució de qualsevol incident produït en el seu entorn, proporcionant totes les evidències requerides.

S'han d'establir els mecanismes adients per que, en cas d'incident de seguretat i si es considera necessari, el personal del Departament de Seguretat de l'IMI pugui accedir a les instal·lacions del proveïdor de forma immediata.

ANÀLISIS FORENSES

L'execució d'anàlisis forenses és responsabilitat exclusiva del Departament de Seguretat de l'IMI.

L'adjudicatari haurà de col·laborar proporcionant la informació requerida i el coneixements de les plataformes i tecnològics que facin falta. Les peticions de col·laboració es realitzaran a través dels procediments que s'acordin entre el Departament de Seguretat de l'IMI i l'adjudicatari.

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

ANNEX I: VOLUMETRIA DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT

Relació volumètrica dels sistemes d'informació de l'Ajuntament de Barcelona.

SISTEMES D'INFORMACIÓ	
Seu Electrònica	https://seuelectronica.ajuntament.barcelona.cat Podeu trobar informació general de l'Ajuntament, processos administratius i tràmits.
Núm. de SI	300
Núm. webs	700
Núm. SI Classificats (ENS)	140
Núm. Tractaments de Protecció de dades	400
Protecció de dades personals	A la URL: https://seuelectronica.ajuntament.barcelona.cat/sites/default/files/ApdInSeu.pdf podeu trobar la relació de tractaments de l'Ajuntament de Barcelona. Del total, aproximadament el 90% són gestionats per l'IMI.
Núm. Pcs corporatius	9.000
Núm. Servidors	1.100

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.

ANNEX II: INFORMACIÓ ADDCIONAL I/O ACLARIMENTS

L'IMI entén que la informació proporcionada en el present Plec constitueix una base suficient per a la presentació de les ofertes.

Tot i així, si és de l'interès dels licitadors sol·licitar informació addicional per a la presentació de l'oferta, així com altres consultes o aclariments, l'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: **acolladoc@bcn.cat**

En l'assumpte del correu indicar:

Codi de l'expedient a K0117 – Contracte de serveis de preventiu i seguretat TIC per a l'Ajuntament de Barcelona

En cas de no obtenir resposta, contactar amb el telèfon 93 291 81 00

S'atendran les sol·licituds d'informació fins a 3 dies laborables abans de la data límit de presentació d'ofertes.

Es convocarà una **sessió informativa** per tal d'aclarir als licitadors interessats en presentar oferta, tots els dubtes que els hi puguin sorgir. Aquesta sessió es celebrarà a partir dels 5 dies hàbils posteriors al dia següent de la data de publicació de l'anunci de licitació en el Diari Oficial de la Unió Europea (DOUE). El lloc, el dia i l'hora d'aquesta sessió es publicarà a l'anunci de licitació en la plataforma del perfil del contractant.

Ana Bastida i Vilà
Direcció de Qualitat i Seguretat de l'IMI

Neus Bellavista i Arimany
Responsable del Contracte

Aquest document és una còpia autèntica. L'Ajuntament de Barcelona custodia el document i les signatures originals.

El document original ha estat signat electrònicament per:
Ana Bastida Vila el dia 17/08/2019 a les 18:14, que informa.