Ajuntament de Barcelona

Institut Municipal d'Informàtica

Direcció d'Operacions i Sistemes

PLEC DE PRESCRIPCIONS TÈCNIQUES

PER A LA CONTRACTACIÓ DE SERVEIS ESPECIALITZATS DE SUPORT A LA SEGURETAT OPERATIVA, AMB MESURES DE CONTRACTACIÓ PÚBLICA SOSTENIBLE

ÍNDEX

1. INTRODUCCIÓ

L'institut Municipal d'Informàtica (en endavant IMI) és l'organisme autònom de l'Ajuntament de Barcelona responsable de subministrar tots els serveis de les tecnologies de la informació i comunicació (TIC) a l'Ajuntament de Barcelona i els seus organismes autònoms.

Concretament, l'IMI participa en el disseny i execució de l'estratègia TIC de l'Ajuntament de Barcelona, ofereix assessorament i suport en tots aquells projectes o programes de l'Ajuntament que requereixen una estratègia de sistemes d'informació i telecomunicacions i impulsa i executa projectes tecnològics de diversa índole.

L'IMI, alineat amb la estratègia de l'Ajuntament de Barcelona, ha de liderar el procés de transformació digital, per tal d'oferir serveis més eficients i assequibles a la ciutadania, així com aconseguir un govern més transparent, participatiu i eficaç.

Dins del marc de transformació digital i modernització de l'administració i de les seves infraestructures, des de l'Institut Municipal d'Informàtica de Barcelona s'està treballant en l'adopció d'un model de multi-cloud híbrid que millori l'escalabilitat i la resiliència dels sistemes. Actualment, l'administració es troba davant de diferents reptes, entre d'altres, la creixent evolució de productes cap a una modalitat SaaS, l'increment de la complexitat i perillositat dels ciberatacs, la identitat com a nou perímetre de seguretat, el teletreball i l'accés remot a determinats sistemes corporatius amb estacions de treball corporatives i no corporatives, i l'adopció de noves eines de seguretat que permetin millorar i automatitzar la resposta a ciberincidents minimitzant la detecció de falsos positius.

En aquesta línia, l'any 2021 l'IMI va procedir a la publicació d'una licitació mitjançant un procediment obert per a l'adjudicació dels serveis d'operació de seguretat (SOC) per a la prevenció, detecció i resposta d'incidents i dels serveis informàtics de les oficines de serveis avançats de telecomunicacions (OSAT), que té per objecte el servei especialitzat de seguretat i telecomunicacions encarregat de la implantació, adaptació, gestió, suport i evolució tècnica de la infraestructura tecnològica del nus de comunicacions, dels elements de xarxa i dels CPDs nucli, així com el manteniment de l'equipament amb garanties esteses de fabricant, juntament amb la prevenció, monitorització d'esdeveniments i gestió d'incidents de seguretat emprant les eines que disposa l'IMI de SIEM (QRadar) i de logs centralitzats (ELK), amb l'abast dels sistemes d'informació i serveis TIC de l'Ajuntament de Barcelona.

L'empresa UTE SIRT-SIA va resultar guanyadora del concurs obert, i per tant adjudicatària dels serveis, per un import total de 5.101.344,73 € (IVA inclòs), dels quals 4.215.987,38 € corresponien al preu net, i 885.357,35 € en concepte d'IVA al tipus del 21% vigent a la formalització del contracte, amb càrrec al pressupost de serveis de l'IMI dels anys 2022, 2023, 2024 i 2025.

Aquest contracte (21000130) es va formalitzar el 31/03/22 i es va iniciar l'1/04/22 amb una durada de 35 mesos, és a dir, fins el 28/02/25, amb la possibilitat de pròrroga fins a un màxim de 24 mesos addicionals.

D'altra banda, l'any 2021 l'IMI va impulsar la creació d'un equip de seguretat operativa (SecOps) multidisciplinar, depenent de la Direcció d'Operacions i Sistemes (en endavant DOiS), amb l'objectiu de col·laborar amb el departament de Seguretat i amb els diferents departaments de la DOiS en la millora de les capacitats operatives de resposta de l'IMI davant de qualsevol tipus de ciberincident, així com en la mitigació efectiva i eficient dels riscos i les vulnerabilitats que puguin afectar els actius i els serveis TIC de l'Ajuntament de Barcelona.

La seguretat operativa (SecOps) té com a objectiu maximitzar la col·laboració i l'alineament dels equips de Seguretat i dels equips d'Operacions TIC, per tal d'integrar eines, processos i tecnologia per mantenir segura l'organització, reduint el risc.

Els membres de l'equip de SecOps assumeixen la coresponsabilitat davant de qualsevol incidència que afecti la seguretat operativa, assegurant-se que la seguretat s'inclou a tot el cicle d'operacions. Sovint, els equips d'operacions i de seguretat tenen objectius i eines diferents que en alguns casos poden entrar en conflicte i crear ineficiències. Els primers es focalitzen en configurar els sistemes d'una manera que permeti assolir els objectius de rendiment i disponibilitat, mentre que els segons centren principalment els seus esforços en el compliment dels requisits normatius, en posar en marxa defenses i en respondre als incidents de seguretat. L'inconvenient d'aquest model és que la seguretat de vegades es planteja com una idea a posteriori, de vegades fins i tot com una càrrega que fa alentir les operacions. Però a mesura que les amenaces continuen augmentant i esdevenen més sofisticades, és molt important alinear els equips d'operacions i de seguretat.

L'objectiu del model SecOps és que la seguretat es tingui en compte en tot el procés d'operacions, aplicant els principis bàsics i requisits mínims detallats a l'Esquema Nacional de Seguretat (RD 311/2022, de 3 de maig), per garantir una protecció adient de la informació tractada i dels serveis prestats, amb l'objecte d'assegurar l'accés, la confidencialitat, la integritat, la traçabilitat, l'autenticitat, la disponibilitat i la conservació de les dades, la informació i els serveis oferts per mitjans electrònics.

El model SecOps proposa que els equips de Seguretat i d'Operacions treballin junts de forma més estreta, compartint les prioritats de l'organització pel que fa al manteniment de l'estat productiu i a la seguretat dels sistemes TIC. Amb aquest esforç conjunt proactiu, s'aconsegueix una major visibilitat de les vulnerabilitats de seguretat que afecten a tota l'organització, i la valuosa informació compartida pot ajudar a resoldre problemes de seguretat més ràpidament, alhora que les operacions TIC es mantenen àgils i en funcionament.

Per aquest motiu l'IMI decideix impulsar la contractació de serveis especialitzats de suport a la seguretat operativa per tal d'elaborar el pla de governança de la seguretat operativa, i també perquè l'equip de seguretat operativa disposi d'un assessorament expert en la matèria que permeti millorar la postura de seguretat de l'organització i la seva capacitat de resposta davant de ciberincidents.

2. OBJECTE

L'objecte d'aquest contracte és la prestació de serveis especialitzats de suport a la seguretat operativa per als serveis TIC de l'Ajuntament de Barcelona.

En concret, els objectius d'aquesta licitació són:

- Col·laborar en la confecció dels protocols i procediments operatius de seguretat, identificant dins l'àmbit operatiu els punts forts de l'organització i els punts febles que calgui potenciar, aplicant la normativa i les bones pràctiques nacionals i internacionals.
- Recomanar i oferir suport a l'adopció de noves eines de seguretat operativa que permetin millorar la postura de seguretat i la capacitat de resposta a ciberincidents de l'organització, facilitant la seva integració amb el SIEM i el servidor de logs centralitzats corporatiu.
- Desenvolupar i implementar un pla de formació en resposta a incidents de ciberseguretat específic pels membres de l'equip de seguretat operativa, i pels integrants de l'equip de resposta a incidents de ciberseguretat.
- Oferir suport a l'equip de seguretat operativa en la resposta a ciberincidents, formant part de l'equip de resposta a incidents de ciberseguretat de l'organització, dins i fora d'horari laboral.

La forma de treballar haurà de ser mitjançant metodologia ITIL i metodologies àgils, en concret SCRUM, per tal d'establir les tasques a les quals l'adjudicatari haurà donarà suport. De manera periòdica s'establiran el nous objectius per tal de conformar de nou la llista de tasques (backlog) tal com es coneix en la metodologia SCRUM.

3. ABAST

Els serveis a prestar que apliquen al present procés de contractació pública, són els que s'indiquen a continuació.

- Coordinació transversal a tots els paquets.
  - Serveis de coordinació, planificació i seguiment de les tasques del contracte.
  - Llançament del contracte.
  - Control i seguiment del contracte.
  - Avaluació de riscos.
  - Execució del pla de comunicació.
  - Transició del servei.

- Col·laboració en la confecció dels protocols i procediments operatius de seguretat.
  - Col·laboració en l'actualització i millora del portfoli de protocols i procediments operatius de seguretat (p.e. procediment de reposta a phishing, ransomware, etc).
  - Col·laboració en l'actualització de l'inventari d'actius i serveis crítics de l'organització.
  - Identificació dins l'àmbit de la seguretat operativa dels punts forts i dels punts febles de l'organització, i proposta de millores.
  - Identificació de les necessitats i oportunitats en l'aplicació de la seguretat operativa als serveis TIC de l'Ajuntament de Barcelona.
  - Aplicació de la normativa i de les bones pràctiques nacionals i internacionals.
  - Recomanació i suport en la confecció de procediments operatius de bastionat de sistemes i serveis.

- Recomanació i suport en l'adopció de noves eines de seguretat operativa.
  - Anàlisi de les necessitats de negoci i dels possibles riscos.
  - Identificació i definició de requeriments tecnològics i metodològics.
  - Identificació i recomanació de noves eines que facilitin el govern i la gestió de seguretat operativa.
  - Elaboració d'un pla de governança de la seguretat operativa.
  - Suport a la implementació i desplegament de noves eines de seguretat operativa.
  - Suport a la realització d'avaluacions d'impacte relatives a la protecció de dades de les noves eines de seguretat operativa.

- Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat.
  - Elaboració d'un pla de formació específic pels membres de l'equip de seguretat operativa.
  - Elaboració d'un pla de formació específic pels integrants de l'equip de resposta a incidents de ciberseguretat.
  - Elaboració d'un pla de formació específic per altres col·lectius vinculats a la ciberseguretat.
  - Elaboració de materials de suport:
    - Metodologies i estàndards de treball en l'àmbit de la seguretat operativa.
    - Formació en eines, processos i procediments.

- Suport a l'equip de seguretat operativa en la resposta a ciberincidents.
  - o Anàlisi del model actual de l'equip de seguretat operativa en la resposta a ciberincidents i proposta de millores, si escau.
  - o Col·laboració en la identificació dels rols operatius que han de formar part de l'equip de resposta a ciberincidents.
  - o Disponibilitat per oferir suport i formar part de l'equip de resposta a incidents de ciberseguretat, dins i fora d'horari laboral.
  - o Col·laboració en la realització de ciberexercicis ('tabletop' i 'dry run').

3.1. Serveis inclosos

A continuació es detallen el serveis inclosos, i les activitats o subserveis que els composen.

L'adjudicatari haurà de presentar un informe mensual que detalli les hores dedicades a cadascun dels serveis detallats a continuació, que haurà de ser acceptat i signat pel responsable del contracte. Les hores no consumides s'acumularan a les hores disponibles el mes següent.

3.1.1. Servei de Coordinació

El servei de coordinació, fa referència a les tasques que s'executaran de manera transversal a la resta de serveis, amb l'objectiu d'assegurar el correcte desenvolupament del contracte, tot assegurant la planificació, el govern, la qualitat i la documentació de les tasques realitzades.

El desenvolupament del contracte es farà seguint metodologia SCRUM, on a cada sprint (14 dies) es definirà el conjunt de tasques a realitzar. Aquest servei serà recurrent durant la durada del contracte.

Les activitats contemplades en aquest servei seran:

3.1.1.1. Llançament del contracte

L'activitat de llançament del projecte té com a objectius comunicar als interlocutors clau del contracte els elements més rellevants del projecte (objectius, planificació, recursos, model de govern, riscos etc). Les tasques a realitzar per part de l'adjudicatari inclouran, al menys:

- Definició conjunta, amb la direcció del contracte, de l'abast inicial del projecte
- Coordinació i suport a l'organització i execució de la reunió de llançament del contracte, que ha de permetre compartir amb tots els agents implicats: el context i els objectius a assolir,
- Elaborar, en coordinació amb el responsable del projecte, el document de llançament de contracte que ha de recollir com a mínim tots els punts esmentats anteriorment.

Així mateix l'adjudicatari serà responsable de dotar el contracte amb els recursos necessaris (humans i materials), que permetin el correcte desenvolupament de les tasques que conformen l'abast del servei amb temps i qualitat requerits d'acord amb les condicions d'aquest plec.

3.1.1.2. Control i seguiment del contracte

L'activitat de control i seguiment del contracte té com a objectiu la coordinació del projecte durant tot el seu transcurs. Les tasques a realitzar per part de l'adjudicatari són, com a mínim:

- Control, assegurament i garantia de la coherència de la planificació de les tasques des d'una perspectiva global.
- Vigilància del correcte desenvolupament de les tasques en abast, temps i forma.
- Detecció, anàlisi i aplicació d'accions de contingència i mitigació de tots els riscos que puguin sorgir al llarg del transcurs del contracte.
- Assessorament i suport a la presa de decisions.
- Coordinació dels diferents stakeholders implicats.
- Assegurament de la qualitat del producte final (acompliment dels requeriments tècnics i funcionals i satisfacció dels usuaris).
- Informació sobre l'estat i avenç del projecte als òrgans de govern del projecte i a l'eina de gestió de projectes corporativa de l'IMI.

Trimestralment, l'adjudicatari farà una presentació executiva de l'estat del projecte, que inclourà la relació de tasques realitzades, els resultats de productes/lliurables, la planificació actualitzada, les desviacions de tasques, així com l'avaluació i gestió dels riscos identificats.

3.1.1.3. Avaluació i gestió de riscos

L'empresa adjudicatària haurà de vetllar per la identificació, gestió i mitigació dels riscos presentats en l'execució i planificació dels diferents serveis del contracte.

Una gestió de riscos implica una anàlisi constant dels riscos existents al servei i una proposta de solucions mitigadores, la definició i implantació d'uns indicadors que mesurin i avaluïn com s'estan executant els serveis.

Inicialment, cal fer una identificació i anàlisi dels possibles riscos, planificant la seva mitigació en cas que esdevinguin. Durant l'execució dels serveis del contracte l'adjudicatari haurà de fer la supervisió i control dels riscos i determinant les accions necessàries per mitigar-los o evitar-los.

L'objectiu és oferir una gestió de riscos contínua des de l'inici del servei de transició, fins a la finalització del contracte de manera que l'adjudicatari sigui proactiu i ajudi a la presa de decisions.

3.1.1.4. Execució del pla de comunicació

Aquesta activitat té com a finalitat l'execució del pla de comunicació i dinamització necessari per l'objecte del contracte.

3.1.1.5. Tancament del projecte

El tancament del projecte té com a objectiu la validació i acceptació per part del comitè de direcció del projecte dels productes resultants dels treballs que conformen l'abast del projecte. El resultat inclourà el lliurament de tota la documentació generada i la transferència del coneixement al personal intern.

La documentació haurà d'incloure el llistat d'encerts (per reutilitzar-los en futurs projectes) i errades (per no repetir-les) com a part del *know-how*.

L'adjudicatari haurà de facilitar material comunicatiu de què disposi per què l'IMI pugui fer el comunicat intern adequat donant a conèixer els èxits del projecte.

Aquesta activitat es donarà per finalitzada quan el cap de projecte de l'Ajuntament de Barcelona rebi formalment tots els lliurables que es requereixen i aquest lliurament quedi acreditat.

3.1.1.6. Transició del servei

L'objecte del servei de transició és assegurar que el traspàs d'informació entre adjudicataris a la finalització/inici del contracte, es realitzi correctament, sota els estàndards de qualitat exigibles i assegurant el traspàs d'informació i de coneixement. Tanmateix, s'ha de garantir la continuïtat dels serveis prestats en els termes que s'especifiquen en el present plec.

Li correspon a l'adjudicatari del present contracte (adjudicatari sortint) liderar i assegurar que la devolució del servei es realitza assegurant la qualitat i transparència del procés.

La devolució del servei únicament es farà efectiva quan l'adjudicatari sortint i el nou adjudicatari siguin proveïdors diferents. Quan hi hagi continuïtat de proveïdor, aquesta fase no caldrà executar-la. S'entén que hi ha continuïtat de proveïdor davant els següents supòsits:

- És el mateix proveïdor.
- Forma part d'una unió temporal d'empreses.
- És subcontractat pel proveïdor adjudicatari.
- Es tracta d'una empresa del mateix grup empresarial.

3.1.2. Col·laboració en la confecció de protocols i procediments operatius de seguretat

L'objectiu del servei és col·laborar amb el SOC i amb la resta d'equips operatius en la confecció de protocols i procediments operatius de seguretat per donar compliment a la mesura de seguretat [org.3] detallada a l'Annex II de l'ENS, per tal de disposar d'una sèrie de documents que detallin de forma clara i precisa com operar els elements dels diferents sistemes d'informació:

1. Com dur a terme les tasques habituals.
2. Qui ha de fer cada tasca.
3. Com identificar i reportar comportaments anòmals.
4. Com s'ha de tractar la informació d'acord al seu nivell de seguretat, precisant com fer el control d'accés, l'emmagatzemament, la realització de còpies de seguretat, l'etiquetat dels suports, la transmissió telemàtica, o qualsevol altra activitat relacionada amb aquesta informació.

Les activitats contemplades en aquest servei seran:

3.1.2.1. Col·laboració en l'actualització i millora del portfoli de protocols i procediments operatius de seguretat.

En aquesta activitat, a partir de la recopilació inicial dels protocols i procediments operatius de seguretat documentats, l'adjudicatari elaborarà un portfoli que s'anirà actualitzant i millorant de forma progressiva al llarg del contracte, amb el seu suport.

En base a l'anàlisi d'aquest portfoli, l'adjudicatari proposarà millores als protocols i procediments operatius de seguretat de forma proactiva i també proposarà incorporar-ne de nous, identificant les capacitats necessàries per dur-los a terme, i acordant-los amb el SOC i amb la resta d'equips operatius, abans de ser presentats a l'autoritat competent per a la seva aprovació.

L'objectiu serà proporcionar un benefici, tant per a la organització com per a la millora dels actuals serveis a la ciutadania, així com aixecar riscos en aquest àmbit.

Alguns exemples de protocols i procediments operatius de seguretat són el procediment de gestió d'incidents de phishing, el procediment de gestió d'incidents de ransomware, el procediment de gestió d'una identitat compromesa, el procediment de gestió d'una estació de treball compromesa, etc.

3.1.2.2. Col·laboració en l'actualització de l'inventari d'actius i serveis crítics de l'organització

L'objectiu d'aquesta activitat és, en base a l'anàlisi previ, identificar els actius i els serveis crítics dins de cadascuna de les àrees de l'organització i també els que són transversals, així com les seves dependències.

L'adjudicatari haurà de mantenir actualitzat l'inventari d'actius i serveis crítics al llarg de tot el contracte de servei, facilitant actualitzacions de forma mensual com a mínim.

Aquesta anàlisi també ha de facilitar la identificació de riscos derivats de les vulnerabilitats que puguin afectar els actius i serveis crítics en un moment donat, i l'elaboració del pla de mitigació.

3.1.2.3. Identificació de necessitats i oportunitats dins l'àmbit de la seguretat operativa als serveis TIC de l'Ajuntament de Barcelona

El resultat final d'aquesta activitat serà l'elaboració d'un informe, consensuat amb el responsable del contracte, per tal d'identificar els punts forts i febles de l'organització dins l'àmbit de la seguretat operativa, i establir un pla estratègic, tant d'actuació a curt termini amb actuacions concretes que puguin ser executades en el present contracte, com a mig termini identificant les necessitats i oportunitats en l'aplicació de la seguretat operativa que permetin millorar la qualitat i seguretat dels serveis que l'Ajuntament ofereix al ciutadà, així com processos interns de l'Ajuntament de Barcelona.

3.1.2.4. Aplicació de la normativa i de les bones pràctiques nacionals i internacionals

L'objectiu d'aquesta activitat és oferir suport a l'equip de seguretat operativa en l'adopció i l'aplicació de la normativa i de les bones pràctiques nacionals i internacionals en l'àmbit de la seguretat operativa.

L'adjudicatari elaborarà informes en aquest àmbit en cas que siguin requerits.

3.1.2.5. Recomanació i suport en la confecció de procediments operatius de bastionat de sistemes i serveis

Aquesta activitat té per objectiu recomanar i oferir suport a l'equip de seguretat operativa en la confecció de procediments operatius de bastionat de sistemes i serveis, d'acord a l'ENS, a les recomanacions dels fabricants, a les guies de seguretat CCN-STIC del CCN-CERT, i a les bones pràctiques nacionals i internacionals.

A partir de la recopilació inicial dels procediments operatius de bastionat de sistemes i serveis, l'adjudicatari elaborarà un portfoli que s'anirà actualitzant i millorant de forma progressiva al llarg del contracte, amb el seu suport.

En base a l'anàlisi d'aquest portfoli, l'adjudicatari proposarà millores als procediments operatius de bastionat de sistemes i serveis de forma proactiva i també proposarà incorporar-ne de nous, identificant les capacitats necessàries per dur-los a terme, i acordant-los amb el SOC i amb la resta d'equips operatius, abans de ser presentats a l'autoritat competent per a la seva aprovació.

3.1.3. Recomanació i suport en l'adopció de noves eines de seguretat operativa

L'objectiu d'aquest servei és oferir recomanació i suport a l'organització en l'adopció de noves eines de seguretat operativa, d'acord als requeriments i les directrius de seguretat de l'organització, analitzant el seu impacte a nivell de seguretat i de privacitat, donant suport al SOC i a l'equip de seguretat operativa en les tasques prèvies a la implantació de la nova eina, per tal que estigui correctament dimensionada i integrada amb la resta de serveis corporatius, especialment amb el SIEM corporatiu.

Durant la implantació de les noves eines de seguretat operativa, l'adjudicatari analitzarà l'aplicabilitat de la tecnologia, el seu encaix dins la pila tecnològica actual de l'organització, el cicle de vida dels serveis, així com la identificació de riscos tecnològics i ètics.

Aquest servei tindrà una dedicació determinada, especificada a l'Informe Justificatiu, i serà executat quan es requereixi oferir recomanació i suport en l'adopció de noves eines de seguretat operativa durant l'execució del contracte.

Dins d'aquest servei es contemplen els següents subserveis o activitats:

3.1.3.1. Anàlisi de les necessitats de negoci i dels possibles riscos

En aquesta activitat, a partir de la recopilació inicial de les eines de seguretat operativa implementades actualment, l'adjudicatari elaborarà un portfoli que s'anirà actualitzant i millorant de forma progressiva al llarg del contracte, amb el seu suport.

En base a l'anàlisi d'aquest portfoli, l'adjudicatari proposarà millores a les eines de seguretat operativa de forma proactiva i també proposarà incorporar-ne de noves, identificant les capacitats necessàries per dur a terme la seva implementació, i acordant amb el SOC i amb la resta d'equips operatius, abans de ser presentades a l'autoritat competent per a la seva aprovació.

L'objectiu serà proporcionar un benefici, tant per a la organització com per a la millora dels actuals serveis a la ciutadania, així com aixecar riscos en aquest àmbit.

L'objectiu d'aquesta activitat també és l'avaluació de les necessitats de negoci a les quals la nova eina de seguretat operativa ha de donar cobertura, per tal d'identificar l'aplicabilitat i idoneïtat de la utilització de la nova eina.

En aquesta fase, l'adjudicatari haurà de realitzar una avaluació per tal d'identificar possibles riscos en relació al projecte d'implantació de la nova eina. Entre d'altres, es podran identificar riscos relacionats amb:

- Riscos de seguretat.
- Riscos de privacitat.
- Ús i gestió de la infraestructura
- Ús i gestió del cicle de vida les dades
- Manteniment i cicle de vida del servei

3.1.3.2. Identificació i definició de requeriments tecnològics i metodològics

En aquesta activitat, l'adjudicatari haurà d'acompanyar i donar suport al projecte d'implementació de la nova eina, identificant i definint els requeriments tecnològics i metodològics a seguir, tenint en compte tant la normativa aplicables com les bones pràctiques nacionals i internacionals.

Durant la fase de conceptualització del projecte d'implantació de la nova eina de seguretat operativa, l'adjudicatari haurà d'identificar els processos necessaris per tal d'abordar la seva implantació amb garanties de seguretat, confidencialitat, integritat i ètica.

Serà responsabilitat de l'adjudicatari la identificació del processos que requeriran de l'estandardització i de la definició de metodologies, així com de l'acompanyament i la transferència de coneixement a les diferents parts implicades en el projecte.

3.1.3.3. Identificació i definició de noves eines que facilitin el govern i la gestió de la seguretat operativa

En aquesta activitat, l'adjudicatari haurà d'acompanyar i donar suport a l'equip de seguretat operativa en la identificació de les eines i la definició de la solució tecnològica que permeti donar cobertura als requeriments de seguretat de l'organització.

De forma proporcionada a la categoria del sistema i al nivell de seguretat requerit, s'utilitzarà el Catàleg de Productes i Serveis de Seguretat de les Tecnologies de la Informació i Comunicació (CPSTIC) del CCN, per a seleccionar els productes o serveis subministrats per un tercer que formin part de l'arquitectura de seguretat del sistema i aquells que es referenciïn expressament a les mesures del reial decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat (ENS).

En cas que no existeixin productes o serveis al CPSTIC que implementin les funcionalitats requerides, s'empraran productes o serveis certificats d'acord a allò descrit a l'article 19 de l'ENS.

En la definició de les noves eines que facilitin el govern i la gestió de la seguretat operativa, l'empresa adjudicatària haurà de tenir en compte els principis i l'estratègia TIC de l'Ajuntament especificats a les condicions generals d'execució.

A més, la proposta de la solució tecnològica, haurà de vetllar per l'ús eficient dels recursos de l'Ajuntament de Barcelona, així com per l'estandardització i re-usabilitat de les arquitectures proposades.

3.1.3.4. Elaboració d'un pla de governança de la seguretat operativa

En aquesta activitat, l'adjudicatari haurà d'elaborar un pla que permeti la governança de la seguretat operativa, mitjançant l'obtenció d'indicadors a partir de les eines de seguretat operativa existents, i la proposta de noves eines i metodologies per millorar la governança.

El pla de governança de la seguretat operativa haurà de respectar la política de seguretat de l'organització, els principis bàsics i els requisits mínims recollits a l'Esquema Nacional de Seguretat, i haurà de contribuir a millorar l'adequació a l'ENS dels sistemes d'informació corporatius.

3.1.3.5. Suport a la implementació i desplegament de noves eines de seguretat operativa

En aquesta activitat, l'adjudicatari haurà d'elaborar les guies bàsiques de manteniment, administració, operació i monitorització de les noves eines de seguretat operativa (p.e. MFA, EDR, XDR, SWG, etc) per tal de facilitar la transferència de coneixement i el traspàs de cadascuna de les tasques al SOC o bé a l'equip operatiu encarregat de dur-les a terme.

Durant el desplegament previ de l'eina, mentre aquestes tasques no hagin estat traspassades a un altre equip operatiu, l'adjudicatari col·laborarà amb les tasques de manteniment i administració de les noves eines de seguretat operativa, i oferirà suport a l'equip operatiu encarregat de dur a terme l'operació i la monitorització.

3.1.3.6. Suport a la realització d'avaluacions d'impacte relatives a la protecció de dades de les noves eines de seguretat operativa

L'objectiu d'aquesta activitat és oferir suport en la realització d'avaluacions d'impacte relatives a la protecció de dades de les noves eines de seguretat operativa.

L'adjudicatari elaborarà informes en aquest àmbit en cas que siguin requerits.

3.1.4. Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat

L'objectiu d'aquest servei és desenvolupar i implementar un pla de formació en resposta a incidents de ciberseguretat específic pels membres de l'equip de seguretat operativa, un segon pla pels integrants de l'equip de resposta a incidents de ciberseguretat, i un tercer pla per oferir formació a altres col·lectius de l'organització vinculats a la ciberseguretat.

Dins d'aquest servei es contemplen els següents subserveis o activitats:

3.1.4.1. Elaboració d'un pla de formació específic pels membres de l'equip de seguretat operativa

En aquesta activitat, l'adjudicatari elaborarà un pla de formació específic per capacitar els membres de l'equip de seguretat operativa en el manteniment, administració, operació i

monitorització de les eines de seguretat operativa que hagin de fer servir, i també en els protocols i procediments que hagin d'aplicar o supervisar.

L'adjudicatari haurà d'oferir mensualment com a mínim 2h de formació a l'equip de seguretat operativa, en grups de com a màxim 12 persones.

3.1.4.2. Elaboració d'un pla de formació específic pels membres de l'equip de resposta a incidents de ciberseguretat

En aquesta activitat, l'adjudicatari elaborarà un pla de formació específic per capacitar els membres de l'equip de resposta a incidents de ciberseguretat en la resposta als diferents tipus d'incidents de seguretat, d'acord al protocol general de gestió d'incidents de seguretat, i a cadascun dels procediments específics de gestió d'incidents de seguretat (p.e. phishing, ransomware, etc).

L'adjudicatari haurà d'oferir mensualment com a mínim 2h de formació a l'equip de resposta a incidents de ciberseguretat, en grups de com a màxim 12 persones.

3.1.4.3. Elaboració d'un pla de formació específic per altres col·lectius vinculats a la ciberseguretat

En aquesta activitat, l'adjudicatari elaborarà un pla de formació específic per capacitar altres col·lectius vinculats a la resposta a incidents de ciberseguretat, relacionats amb la gestió de sistemes d'informació o de serveis corporatius que puguin eventualment veure's afectats per un ciberincident, per tal de conèixer a alt nivell els protocols que s'aplicaran i si la seva participació serà requerida.

L'adjudicatari haurà d'oferir mensualment com a mínim 2h de formació a altres col·lectius vinculats a la ciberseguretat.

3.1.4.4. Elaboració de material de suport

Aquest subservei contempla l'elaboració de material que permeti millorar la capacitació del personal de l'IMI per tal de donar resposta de forma més eficaç i eficient a un incident de seguretat.

Els diferents tipus de materials contemplats en aquest serveis seran:

- ***Suport per la definició de metodologies i estàndards de treball en l'àmbit de la seguretat operativa***. Aquesta activitat fa referència a la definició de guies de bones pràctiques per tal d'abordar la implementació de metodologies i estàndards de treball en l'àmbit de la seguretat operativa. Alguns dels processos que poden requerir d'estandardització seran:
    - *Definició de clàusules tècniques i administratives a incloure a futurs contractes de servei per incorporar el suport requerit per a la seguretat operativa.*
    - *Definició del la gestió del cicle de vida de les eines de seguretat operativa.*

  Aquest llistat només suposa un exemple de guies que es podrien abordar durant el projecte, durant l'execució del projecte i amb l'ajuda del adjudicatari, es definiran i s'aprovaran el processos a estandarditzar.

- ***Formació en eines, processos i procediments:*** Aquest tipus de materials estan orientats a la capacitació dels diferents actors que intervenen en la detecció, anàlisi, contenció, eradicació, i recuperació d'un incident de seguretat, així com la revisió post-incident.

Addicionalment el licitador haurà d'identificar les necessitats de formació i d'estandardització de processos, i proposar-ne la seva execució per tal de millorar les capacitats dels equips interns de l'IMI en la resposta a incidents de ciberseguretat. Aquestes tasques s'acordaran a l'inici de cada Sprint i podran ésser executades per l'adjudicatari o per altres especialistes de l'IMI.

3.1.5. Suport a l'equip de seguretat operativa en la resposta a ciberincidents

3.1.5.1. Anàlisi del model actual de l'equip de seguretat operativa en la resposta a ciberincidents i proposta de millores, si escau

Aquesta activitat té com a objectiu analitzar com s'està organitzat actualment l'equip de seguretat operativa i com participa en la resposta a ciberincidents. L'adjudicatari també haurà d'analitzar com es gestionen actualment els incidents de seguretat i les vulnerabilitats, mitjançant les eines de gestió d'incidències i de peticions corporatives, i proposar millores, si escau.

3.1.5.2. Col·laboració en l'elaboració de la matriu d'escalat d'incidents i de gestió de vulnerabilitats

Aquesta activitat té com a objectiu l'elaboració de la matriu d'escalat d'incidents i de gestió de vulnerabilitats, que ha de permetre al SOC i a l'equip de resposta a incidents de ciberseguretat donar resposta de forma més eficaç i eficient als incidents de seguretat.

3.1.5.3. Col·laboració en la identificació dels rols operatius que han de formar part de l'equip de resposta a ciberincidents

Aquesta activitat consistirà en la identificació dels rols operatius que han de forma part de l'equip de resposta a ciberincidents, així com identificar la formació mínima en resposta a incidents de ciberseguretat que haurien d'assolir per poder dur a terme la seva funció de forma eficaç i eficient.

3.1.5.4. Oferir suport i formar part de l'equip de resposta a incidents de ciberseguretat, dins i fora d'horari laboral

L'adjudicari haurà d'oferir suport i formar part de l'equip de resposta a incident de ciberseguretat, dins i fora d'horari laboral, en cas que sigui requerit el seu suport.

S'estima una dedicació de 8h mensuals de suport a l'equip de seguretat operativa en la resposta a ciberincidents dins d'horari laboral ordinari, i de 4h mensuals fora d'horari laboral ordinari.

Es considera horari laboral ordinari de 8h a 18h de dilluns a divendres, excloent els dies festius a la ciutat de Barcelona.

Es considera que una hora de suport fora d'horari laboral ordinari equival a dues hores dins d'horari laboral ordinari.

Les hores de suport no consumides s'acumularan a les hores disponibles el mes següent.

3.1.5.5. Col·laboració en la realització de ciberexercicis

Aquest subservei consistirà en col·laborar amb l'organització en la realització de ciberxercicis, en modalitat 'tabletop' i 'dry run', per poder validar l'adequació dels procediments de resposta als diferents tipus de ciberincidents, i la preparació dels diferents equips encarregats d'executar i gestionar aquests procediments de resposta.

En la modalitat 'tabletop' els diferents equips que participarien en la resposta a un determinat tipus de ciberincident es reuneixen, revisen de forma teòrica el procediment a seguir, i discuteixen els seus rols, les seves funcions i les tasques a executar, per tal d'alinear-se i millorar el procediment.

En la modalitat 'dry run' es simula un determinat tipus de ciberincident i cadascun dels equips ha d'assumir el seu rol i aplicar el procediment establert, com si fos un incident real, per tal de validar l'eficàcia i l'eficiència del procediment de gestió del ciberincident al llarg de tot el seu cicle de vida.

L'adjudicatari haurà de col·laborar amb l'organització com a mínim en la realització d'un ciberexercici de tipus 'tabletop' mensual, i d'un de tipus 'dry run' trimestral.

3.2. Lliurables

De cada una de les activitats descrites anteriorment s'indiquen, en la següent taula, els productes a lliurar per part de l'adjudicatari al finalitzar la corresponent fita. S'especifica també el contingut mínim de la documentació generada i el format en el que caldrà que s'entregui:

3.2.1. Servei de Coordinació

Quan	Lliurable	Descripció	Format
Llançament del contracte	3.2.1.1 - Documentació llançament del contracte	Exposició dels aspectes rellevants del projecte amb: • Objectius i abast del projecte • Identificació de riscos inicials • Definició inicial del planning	Presentació
	3.2.1.2 - Creació de l'entorn de seguiment de contracte	Creació de l'entorn col·laboratiu per a la gestió del contracte. Actualment la plataforma de seguiment de projectes es Jira/Confluence. Es podran valorar altres eines a proposta del proveïdor i aprovació del responsable del contracte.	Jira/Altre
Cada 2 setmanes	3.2.1.3 - Seguiment del contracte	Manteniment de les tasques del product backlog i sprint backlog. • Creació i actualització de les tasques • Registre de projectes en curs • Identificació i gestió de riscos	Jira/Altre

		Identificació i gestió dels implicats	
	3.2.1.4 - Acta Seguiment del contracte	Acta dels temes tractats així com relació de participants, decisions preses, etc..	Document
Trimestral	3.2.1.5 – Presentació executiva de seguiment del contracte	Presentació executiva amb l'estat del projecte amb: • Relació de tasques • Resultats de productes/lliurables • Planificació, desviacions de tasques i riscos identificats • Properes passes	Presentació
Tancament de contracte	3.2.1.6 - Presentació de tancament de contracte	Presentació amb la relació de tasques realitzades, documentació generada, lliçons apreses i proposta de continuïtat	Presentació
Mensual	3.2.2.6 – Informe que detalli les hores dedicades a la coordinació del projecte.	Document que detalli les hores dedicades a la coordinació del projecte.	Document

3.2.2. Col·laboració en la confecció de protocols i procediments operatius de seguretat

Quan	Lliurable	Descripció	Format
Trimestral	3.2.3.1 – Portfoli actualitzat de protocols i procediments operatius de seguretat	Informe que detalli el portfoli actualitzat de protocols i procediments operatius de seguretat de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.2.1**	Document
Trimestral	3.2.2.2 – Inventari actualitzat d'actius i serveis crítics de l'organització	Informe que detalli l'inventari actualitzat d'actius i serveis crítics de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.2.2**.	Document
Trimestral	3.2.2.3 – Informe de necessitats i oportunitats dins l'àmbit de la seguretat operativa als serveis TIC de l'Ajuntament de Barcelona	Informe que detalli les necessitats i oportunitats dins l'àmbit de la seguretat operativa als serveis TIC de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.2.3**.	Document
A demanda	3.2.2.4 – Informe sobre aplicació de normativa, i de bones pràctiques.	Informe que ofereixi suport a l'equip de seguretat operativa en l'adopció i l'aplicació de la normativa, i de les bones pràctiques nacionals i internacionals. Inclou el punts descrits a l'apartat **3.1.2.4**.	Document
Trimestral	3.2.2.5 – Portfoli actualitzat de procediments operatius de bastionat de sistemes i serveis	Informe que detalli el portfoli actualitzat de procediments operatius de bastionat de sistemes i serveis de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.2.5**	Document
Mensual	3.2.2.6 – Informe que detalli les hores dedicades a la col·laboració en la confecció de protocols i procediments operatius de seguretat.	Document que detalli les hores dedicades a la col·laboració en la confecció de protocols i procediments operatius de seguretat.	Document

3.2.3. Recomanació i suport en l'adopció de noves eines de seguretat operativa

Quan	Lliurable	Descripció	Format
Trimestral	3.2.3.1 – Portfoli actualitzat d'eines de seguretat operativa	Informe que detalli el portfoli actualitzat d'eines de seguretat operativa de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.3.1**	Document
A demanda	3.2.3.2 – Informe sobre necessitats de negoci i possibles riscos d'una nova eina de seguretat operativa.	Informe que identifiqui les necessitats de negoci, els possibles riscos (de seguretat i de privacitat), el seu cicle de vida, i les capacitats necessàries per implementar una nova eina de seguretat operativa. Inclou el punts descrits a l'apartat **3.1.3.1**.	Document
A demanda	3.2.3.3 – Informe sobre requeriments tecnològics i metodològics d'una nova eina de seguretat operativa.	Informe que identifiqui els requeriments tecnològics i metodològics a seguir per implementar una nova eina de seguretat operativa, tenint en compte les bones pràctiques nacionals i internacionals. Inclou el punts descrits a l'apartat **3.1.3.2**.	Document
Trimestral	3.2.3.4 – Informe sobre noves eines que facilitin el govern i la gestió de la seguretat operativa dels serveis TIC de l'Ajuntament de Barcelona	Informe que identifiqui noves eines de seguretat operativa que permetin donar cobertura als requeriments de seguretat dels serveis TIC de l'Ajuntament de Barcelona. Inclou el punts descrits a l'apartat **3.1.3.3**.	Document
Trimestral	3.2.3.5 – Pla de governança de la seguretat operativa.	Presentació del pla de governança actualitzat de la seguretat operativa. Inclou el punts descrits a l'apartat **3.1.2.4**.	Presentació
A demanda	3.2.3.6 – Guies bàsiques de manteniment, administració, operació i monitorització d'una nova eina de seguretat operativa.	Guies bàsiques de manteniment, administració, operació i monitorització d'una nova eina de seguretat operativa. Inclou el punts descrits a l'apartat **3.1.3.5**.	Document
A demanda	3.2.3.7 – Informe de suport a la realització d'una avaluació d'impacte relativa a la protecció de dades d'una nova eina de seguretat operativa.	Informe de suport a la realització de l'avaluació d'impacte relativa a la protecció de dades d'una nova eina de seguretat operativa. Inclou el punts descrits a l'apartat **3.1.3.6.**	Document
Mensual	3.2.3.8 – Informe que detalli les hores dedicades a la recomanació i suport en l'adopció de noves eines de seguretat operativa.	Document que detalli les hores dedicades a la recomanació i suport en l'adopció de noves eines de seguretat operativa.	Document

3.2.4. Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat

Quan	Lliurable	Descripció	Format
Trimestral	3.2.4.1 – Pla de formació per capacitar l'equip de	Document que detalli el pla de formació actualitzat per capacitar l'equip de	Document

	seguretat operativa	seguretat operativa en el manteniment, administració, operació i monitorització de les eines de seguretat operativa, i en els protocols i procediments. Inclou el punts descrits a l'apartat **3.1.4.1.**	
Trimestral	3.2.4.2 – Pla de formació per capacitar l'equip de resposta a incidents de ciberseguretat	Document que detalli el pla de formació actualitzat per capacitar l'equip de resposta a incidents de ciberseguretat en la resposta als diferents tipus d'incidents de seguretat. Inclou el punts descrits a l'apartat **3.1.4.2**.	Document
Trimestral	3.2.4.3 – Pla de formació per capacitar altres col·lectius vinculats a la resposta a incidents de ciberseguretat	Document que detalli el pla de formació actualitzat per capacitar altres col·lectius vinculats a la resposta a incidents de ciberseguretat. Inclou el punts descrits a l'apartat **3.1.4.3**.	Document
A demanda	3.2.4.4 – Guies de bones pràctiques en l'àmbit de la seguretat operativa, i altres materials de suport.	Guies de bones pràctiques per tal d'abordar la implementació de metodologies i estàndards de treball en l'àmbit de la seguretat operativa, i altres materials de suport. Inclou el punts descrits a l'apartat **3.1.4.4**.	Document
Mensual	3.2.4.5 – Informe que detalli les hores dedicades al desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat.	Document que detalli les hores dedicades al desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat.	Document

3.2.5. Suport a l'equip de seguretat operativa en la resposta a ciberincidents

Quan	Lliurable	Descripció	Format
Trimestral	3.2.5.1 - Informe d'anàlisi del model actual de l'equip de seguretat operativa en la resposta a ciberincidents	Documentació que detalli com està organitzat actualment l'equip de seguretat operativa i com participa en la resposta a ciberincidents. Inclou els punts descrits a l'apartat **3.1.5.1**.	Document
Trimestral	3.2.5.2 – Matriu d'escalat d'incidents de seguretat i de gestió de vulnerabilitats	Documentació que detalli la matriu d'escalat d'incidents de seguretat i de gestió de vulnerabilitats. Inclou els punts descrits a l'apartat **3.1.5.2**.	Document
Trimestral	3.2.5.3 – Identificació rols operatius que han de formar part de l'equip de resposta a ciberincidents	Documentació que detalli els rols operatius que han de formar part de l'equip de resposta a ciberincidents. Inclou els punts descrits a l'apartat **3.1.5.3**.	Document
A demanda	3.2.5.5 – Informe del resultat d'un ciberexercici de tipus 'tabletop'.	Document que detali els resultats d'un ciberexercici de tipus 'tabletop'. Inclou el punts descrits a l'apartat **3.1.5.5**.	Document
A demanda	3.2.5.6 – Informe del	Document que detali els resultats d'un	Document

	resultat d'un ciberexercici de tipus 'dry run.	ciberexercici de tipus 'dry run'. Inclou el punts descrits a l'apartat **3.1.5.5**.	
Mensual	3.2.5.4 – Informe que detalli les hores de suport en la resposta a la ciberincidents.	Document que detalli les hores de suport dedicades a la resposta a ciberincidents, dins i fora de l'horari laboral ordinari. Inclou el punts descrits a l'apartat **3.1.5.4**.	Document

4. CONDICIONS GENERALS DE LA PRESTACIÓ DEL SERVEI

4.1. Localització de la prestació dels serveis

Els serveis objecte del contracte es prestaran des de les instal·lacions del proveïdor, essent obligació de l'adjudicatari l'aportació de les eines necessàries per a la prestació d'aquest servei en forma remota i assumint els costos de tots els mitjans necessaris per aquesta modalitat de prestació. Durant l'horari de prestació del servei l'adjudicatari haurà d'estar accessible per via telefònica i disposar de les eines necessàries per assistir a reunions de forma remota.

La instal·lació i configuració de l'estàndard corporatiu municipal serà a càrrec de l'adjudicatari sota la supervisió dels equips especialitzats de l'IMI.

4.2. Horaris de la prestació dels serveis

L'horari de prestació dels serveis ordinari és el següent:

- Horari laboral de l'IMI 10 x 5 (de dilluns a divendres de 8 h a 18 h).

Tanmateix, en cas que sigui necessari, es podrà requerir la prestació de serveis fora de l'horari ordinari per tal d'oferir suport i col·laborar en la resposta a ciberincidents greus.

4.3. Idioma

Obligatòriament, l'adjudicatari elaborarà tota la documentació durant l'execució del contracte en català i en anglès quan sigui necessari.

4.4. Període de garantia

Les tasques del contracte tindran una garantia de 3 mesos a partir de la seva finalització i validació per part de l'IMI i l'usuari referent.

Durant aquest període l'adjudicatari es compromet a resoldre satisfactòriament totes aquelles incidències o defectes detectats als serveis lliurats que li siguin imputables a ell per acció o per omissió, sense cost algun per IMI.

4.5. Infraestructura necessària per a la prestació del servei

Per al cas dels ordinadors de sobretaula i equips portàtils, el prestatari estarà obligat a configurar la maquinària d'acord amb els requeriments que els equips tècnics de l'IMI indiquin en cada ocasió. El programari de base i d'usuari haurà de complir l'estàndard corporatiu propi de l'Ajuntament de Barcelona, de manera que el proveïdor adjudicatari estarà obligat a proveir-se d'aquest de forma prèvia.

El programari estàndard no es podrà modificar per causes pròpies del material aportat pel proveïdor adjudicatari, i en cas que existeixi incompatibilitat entre programari i maquinari, el prestatari estarà obligat a proveir un equip homologat per l'IMI per tal de poder treballar amb l'estàndard corporatiu. Els equips homologats seran comunicats per l'IMI a petició del prestatari, que haurà d'informar de les característiques dels equipaments abans de connectar-los a la xarxa corporativa municipal.

En cas que la prestació del servei s'ubiqui a les instal·lacions del proveïdor adjudicatari, la connexió amb l'IMI es portarà a terme mitjançant una connexió LAN-to-LAN i la instal·lació d'un software a les estacions del client.

4.5.1. Connexió LAN-to-LAN

La connexió LAN-to-LAN entre l'empresa adjudicatària i l'IMI es podrà realitzar a través d'Internet (VPN) o mitjans de comunicació privats (ex: fibra òptica propietària).

En cas que es realitzi a través de mitjans de comunicació privats, s'haurà de garantir que la informació viatgi correctament xifrada.

En cas que es realitzi a través d'Internet (VPN), serà responsabilitat de l'adjudicatari:

- La contractació i manteniment del seu accés a Internet
- La disposició d'un ample de banda suficient per garantir la prestació del servei
- La disposició d'un equip que suporti aquest tipus de connexions

A més a més, el proveïdor adjudicatari haurà de disposar del personal tècnic necessari per a la correcta configuració dels equips que acaben el circuit VPN del seu costat i dels seus sistemes de seguretat i translació d'adreces IP. L'IMI col·laborarà en la seva implantació facilitant els paràmetres de configuració i el certificat per a l'equip que acaba el circuit.

De forma opcional, l'IMI podrà oferir un model de configuració tipus si aquest equip final es tracta d'un Router Cisco de la sèrie 800. En cas de dificultats per establir 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.

4.6. Facturació

El servei de *Coordinació* (apartat 3.1) la facturació del servei serà **trimestral, a trimestre vençut**.

El Comitè de Seguiment serà l'encarregat de validar i acceptar els treballs realitzats i d'autoritzar la facturació dels mateixos. En cas que el Comitè de Seguiment no autoritzés l'emissió de la factura trimestral corresponent, els treballs no podran ser facturats fins a la seva aprovació.

En el detall de la factura haurà de constar la relació de serveis realitzats, així com l'aplicació de les penalitzacions corresponents, si fos el cas, a aplicar per incompliment dels ANS del servei, establerts a l'apartat 8 d'aquest document.

Pels serveis que a continuació es detallen, la facturació serà **variable per fites d'obligat compliment per part de l'adjudicatari**, i es realitzarà **a trimestre vençut segons les validacions realitzades per l'IMI** als comitès de seguiment.

A continuació es detallen el lliurables que suposen fita de facturació per a cadascun dels serveis. Per a cadascuna de les fites, s'especifica el percentatge a facturar sobre el preu total del servei, que suposarà la validació dels corresponents lliurables.

- Servei de coordinació

Fites	Facturació %
Lliurable 3.2.1.3 – Seguiment del contracte Lliurable 3.2.1.4 – Acta seguiment del contracte	50 %
Lliurable 3.2.1.5 – Presentació executiva de seguiment del contracte	50 %

- Col·laboració en la confecció de protocols i procediments operatius de seguretat

Fites	Facturació %
Lliurable 3.2.3.1 – Portfoli actualitzat de protocols i procediments operatius de seguretat	25 %
Lliurable 3.2.2.2 – Inventari actualitzat d'actius i serveis crítics de l'organització	25 %
Lliurable 3.2.2.3 – Informe de necessitats i oportunitats dins l'àmbit de la seguretat operativa als serveis TIC de l'Ajuntament de Barcelona	25 %
Lliurable 3.2.2.5 – Portfoli actualitzat de procediments operatius de bastionat de sistemes i serveis	25 %

- Recomanació i suport en l'adopció de noves eines de seguretat operativa

Fites	Facturació %
Lliurable 3.2.3.1 – Portfoli actualitzat d'eines de seguretat operativa	30 %
Lliurable 3.2.3.2 – Informe sobre noves eines que facilitin el govern i la gestió de la seguretat operativa	30 %
Lliurable 3.2.3.3 – Pla de governança de la seguretat operativa	40 %

- Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat

Fites	Facturació %
Lliurable 3.2.4.1 – Pla de formació per capacitar l'equip de seguretat operativa	30 %
Lliurable 3.2.4.2 – Pla de formació per capacitar l'equip de resposta a incidents de ciberseguretat	40 %
Lliurable 3.2.4.3 – Pla de formació per capacitar altres col·lectius vinculats a la resposta a incidents de ciberseguretat	30 %

- Suport a l'equip de seguretat operativa en la resposta a ciberincidents

Fites	Facturació %
Lliurable 3.2.5.1 - Informe d'anàlisi del model actual de l'equip de seguretat operativa en la resposta a ciberincidents	30 %
Lliurable 3.2.5.2 - Matriu d'escalat d'incidents de seguretat i de gestió de vulnerabilitats	40 %
Lliurable 3.2.5.3 - Identificació de rols operatius que han de formar part de l'equip de resposta a ciberincidents	30 %

Un cop realitzats els treballs, el Comitè de Seguiment serà l'encarregat de validar i acceptar els treballs realitzats i d'autoritzar la facturació dels mateixos. En cas que el Comitè de Seguiment no autoritzés l'emissió de la factura trimestral corresponent, els treballs no podran ser facturats fins a la seva aprovació.

En el detall de la factura haurà de constar la relació de serveis realitzats per a cada servei d'aplicació, així com l'aplicació de les penalitzacions corresponents, si fos el cas, a aplicar per incompliment dels ANS del servei, establerts a l'apartat 8 d'aquest document.

5. MODEL DE PRESTACIÓ DEL SERVEI

5.1. Model de govern

Per la correcta prestació dels serveis i la consecució de l'èxit en qualitat, terminis i homogeneïtat del treball a realitzar, s'estableix que el contracte estarà governat per 3 comitès:

- Comitè de seguiment
- Comitè de direcció
- Comitè de crisi

L'acta de cada comitè/reunió haurà de ser enviades a l'IMI abans de **2 dies laborables** després de la seva realització.

5.1.1. Comitè de seguiment

S'encarrega del dia a dia del projecte. Resol les incidències i conflictes menors que apareguin al llarg de la vida del projecte.

Es reunirà mensualment. Està format pel Responsable del contracte de l'adjudicatari i el responsable del contracte de l'IMI. Quan calgui, es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip de projecte necessaris per tractar en profunditat determinats temes.

Amb caràcter obligatori, es convocarà una **reunió de Kick-off** o llançament de projecte amb els principals membres del projecte (Directors de l'IMI, Responsables de sector i transversals, Equip de l'adjudicatari i Equip IMI).

Li corresponen al Comitè de Seguiment les funcions de control de l'execució del contracte:

- Establir el llistat de tasques a dur a terme
- Validació de la feina
- Verificació de l'acompliment del contracte
- Proposta del règim sancionador
- Validació i aprovació de l'emissió de la factura corresponent als treballs realitzats
- Verificació de l'acompliment dels ANS i del contracte
- Resolució dels conflictes que puguin sorgir en l'execució del contracte

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

El Responsable del contracte de l'adjudicatari és l'encarregat de fer les convocatòries i enviar la documentació necessària als participants com a mínim amb 3 dies laborables d'antelació, i d'aixecar acta de les reunions d'aquest Comitè.

5.1.2. Comitè de direcció

Les seves funcions són les de supervisar la marxa del contracte i la presa de decisions que afecten a l'objectiu i abast del mateix.

Es reunirà amb caràcter trimestral encara que l'IMI el podrà convocar amb caràcter extraordinari sempre que es consideri necessari. En formen part:

- Directora d'Operacions de l'IMI
- Cap de Departament de Seguretat de l'IMI
- Responsable del SOC de l'IMI
- Responsable de contracte de l'IMI
- Coordinador del contracte de l'adjudicatari
- Altres assistents requerits

Li corresponen al Comitè de Direcció les funcions de:

- Aprovar ampliacions/reduccions de contracte
- Aprovar l'execució de les penalitzacions
- Gestió de riscos i oportunitats

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

El Responsable del Servei de l'adjudicatari és l'encarregat de fer les convocatòries i enviar la documentació necessària als participants com a mínim amb 3 dies laborables d'antelació, i d'aixecar acta de les reunions d'aquest Comitè.

5.1.3. Comitè de crisi

En cas que l'IMI ho consideri necessari, es podrà convocar un Comitè de Crisi. L'objectiu d'aquest comitè serà la posada en comú i solució d'una problemàtica o situació crítica.

La sol·licitud del Comitè de Crisi la realitzarà únicament l'IMI, qui establirà els assistents, l'hora i localització de la reunió, així com l'agenda i punts a tractar.

Aquest comitè de Crisi es podrà convocar amb una antelació mínima de 4 hores a l'adjudicatari. El comitè de Crisi s'anirà reunint amb la periodicitat que estableixi l'IMI mentre duri la contingència.

Li corresponen al Comitè de Crisi les funcions de:

- Analitzar el problema o situació i establir-ne la gravetat
- Definir un pla de contingència per a la resolució immediata de la situació, i fer-ne seguiment
- Definir un pla d'acció, si escau, per implantar mesures que impedeixen que el problema o situació torni a succeir, i fer-ne seguiment
- Designar els responsables de l'execució de les accions definides
- Designar els responsables encarregats de fer una investigació del succés, i fer-ne seguiment
- Definir les penalitzacions, si fossin necessàries, a aplicar sobre els responsables del succés
- Establir les responsabilitats

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

6. EINES DEL SERVEI

A continuació es detallen algunes de les eines que s'utilitzen en l'actualitat a l'IMI per a la gestió de la demanda i seguiment del portfoli de projectes. L'ús de les mateixes està descrit en ADINET/Metodologia AGILE així com en els diversos procediments vigents a l'IMI. L'IMI es reserva el dret de modificar aquestes eines amb el previ avís suficient perquè els proveïdors puguin adaptar-se a les mateixes.

Les eines esmentades anteriorment tenen les següents característiques:

- **Eina de seguiment de projectes**: Aplicació de gestió dels projectes, de seguiments de fites i checkpoints, riscos i pressupost, en l'actualitat Sciforma.

- **Eina de seguiment de desenvolupament per equips Scrum**: eina que d'una banda els permet una efectiva col·laboració i un flux de treball integrat i interoperable, a més que els facilita la gestió àgil i el seguiment de projectes desenvolupats amb la metodologia Scrum@IMI, en l'actualitat Jira Software i Confluence.

- **Eina de gestió de codi**: Eina per a la gestió distribuïda de codi i la gestió de versions. Actualment el repositori corporatiu es tracta d'un desplegament de GitLab.

L'IMI comunicarà a l'adjudicatari a l'inici del contracte la relació concreta d'eines del servei i podrà canviar-les durant l'execució del contracte, informant al corresponent adjudicatari amb un període mínim de 30 dies.

7. QUALITAT DELS SERVEIS

7.1. Pla de qualitat

L'adjudicatari haurà de definir i presentar, un Pla de Qualitat del Servei específic que asseguri la qualitat dels serveis oferts.

El Pla de Qualitat del Servei és un document de gestió interna dels serveis objecte del contracte i conté informació detallada dels procediments per a la prestació dels serveis. Com a mínim el Pla de Qualitat haurà de contenir els següents punts:

- Detall dels serveis, incloent els rols responsables de cada tasca o activitat.
- Gestió de riscos i problemes relatius a la gestió del servei.
- Gestió de la documentació i dels requeriments del servei, incloent la gestió del control de la traçabilitat de la documentació que assegura que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Procediments que garanteixin la millora contínua del servei.
- Revisions internes que asseguren que els serveis s'han proporcionat d'acord amb els procediments definits.
- 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 del Servei.
- Gestió de riscos que possibiliti una reducció o eliminació dels possibles impactes en el servei.

Es valorarà la proposta tècnica que proposi un Model de mesura de qualitat dels serveis oferts.

7.2. Auditories

L'IMI podrà realitzar auditories per verificar el compliment dels compromisos contractuals i la fiabilitat de la informació facilitada a l'IMI.

L'adjudicatari proporcionarà la seva total cooperació a la realització d'aquestes auditories. Això inclourà el lliurament de documentació i l'accés físic a les instal·lacions on s'estiguin realitzant els serveis objecte del contracte, al personal que el client determini, que podrà ser tant personal propi del client com subcontractat.

No caldrà donar avís previ per realitzar tasques d'auditoria on no es requereixi col·laboració activa del personal de l'adjudicatari. En els casos en què el client demani una col·laboració activa del personal de l'adjudicatari, es donarà avís amb dues setmanes d'antelació

8. ACORDS DE NIVELL DE SERVEI (ANS)

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

Els licitadors hauran de presentar a la seva oferta la proposta de ANS, detallant els llindars objectius proposats, la periodicitat del càlcul i la font d'informació per obtenir-los. Aquests indicadors han de ser els necessaris per controlar l'execució dels seus treballs.

Els indicadors tindran la següent estructura en comú:

- **Descripció:** definició de l'indicador i objecte de mesura.
- **Càlcul:** fórmula per al càlcul de l'indicador.
- **Periodicitat:** interval de temps de mesura i presentació del resultat de l'indicador.
- **Valor límit:** valor mínim/màxim a partir del qual l'indicador compleix amb el nivell de servei acordat. El valor indicat a les taules serà el valor requerit per al contracte.

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

Es definiran com a mínim els següents indicadors, el càlcul dels ANS s'haurà de fer per indicador **amb periodicitat mensual** i considerant dies laborables.

Indicador	Descripció	Càlcul	Periodicitat	ANS
Entrega d'actes i documentació **(Tdocu)**	Retard en l'entrega d'actes i documentació (*)	Tdocu = data d'entrega real de cada document –data prevista d'entrega	Mensual	Tdocu <=1 dia
Qualitat dels documents entregats **(Qinf)**	Rati de documents (actes, informes i documentació) acceptats sense iteracions o amb una única iteració en la seva elaboració	Qinf = nº documents entregats sense o amb una iteració / nº documents entregats	Mensual	Qinf >= 85%

9. EQUIP DE TREBALL

En el present apartat es descriuen les principals funcions i experiència de cada un dels perfils professionals que hauran de participar en l'execució del contracte.

A continuació es resumeixen els perfils tècnics mínims obligatoris que caldrà posar a disposició per cada servei i que seran detallats en els propers apartats:

- Servei de Coordinació
  - Cap de projecte
- Col·laboració en la confecció de protocols i procediments operatius de seguretat
  - Expert en ciberseguretat
- Recomanació i suport en l'adopció de noves eines de seguretat operativa
  - Expert en ciberseguretat
- Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat
  - Expert en ciberseguretat
- Suport a l'equip de seguretat operativa en la resposta a ciberincidents
  - Expert en ciberseguretat

D'acord amb la demanda prevista dels serveis definits per a la durada del present contracte, s'ha calculat el nombre de recursos mínims necessaris per cadascun dels perfils

Perfil	Nº de recursos
Cap de projecte	1
Expert en ciberseguretat	1

Serà responsabilitat de l'adjudicatari el fet disposar dels recursos i dimensionament necessaris per tal de garantir la correcta execució dels serveis amb la qualitat i els acords de servei establerts en el present acord.

9.1. Funcions i característiques dels perfils

- **Cap de projecte**

Funcions
Màxim responsable de gestió i seguiment de l'execució del projecte, cercant la màxima eficiència, vetllant per la qualitat dels lliurables, i el compliment de la planificació operativa. Concretament:

Interlocució amb els responsables IMI i òrgans de govern del projecte agile.

- Gestió dels recursos (personals i materials) assignats al projecte agile.
- Gestió i control de projectes i de sistemes d'informació en metodologia ITIL i metodologies Àgils, seguint els principis i metodologies pròpies de l'IMI
    - Suport a planificació product backlog.
    - Gestió i seguiment diari.
    - Gestió del canvi: Garantir l'adequada implicació dels agents clau.
    - Gestió de riscos: anticipació i anàlisi de possibles desviacions del projecte (d'abast, qualitat temporals, econòmiques) i proposició de mesures correctores.
    - Planificació d'històries d'usuari i seguiment de les fites del projecte.
    - Anàlisi de desviacions del projecte (abast, cost).
- Report als òrgans de govern del projecte i de l'IMI.

Requeriments

- Cal que tingui com a mínim 3 anys d'experiència en el rol de cap de projectes de ciberseguretat.
- Cal que tingui com a mínim 3 anys d'experiència en el rol de cap de projectes de sistemes TIC.
- Cal que hagi participat en un mínim de 5 projectes com a cap de projecte de ciberseguretat.

- **Expert en ciberseguretat**

Funcions

El Responsable de Seguretat, haurà de vetllar perquè el projecte es realitzi d'acord al model i requeriments de seguretat establerts per l'IMI i la normativa de seguretat vigent i les millors pràctiques i estàndards del mercat:

- Garantir que el projecte es desenvolupa garantint un nivell adequat de confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat de les dades.
- Assegurar la informació regular a l'IMI de tot allò relacionat amb la seguretat.
- Participar en la definició de l'arquitectura del projecte.
- Assegurar una correcta gestió dels riscos de seguretat del projecte, identificant-los i escalant-los a les persones adequades.
- Informar al equip de qualsevol obligació a la que estigui sotmès i formar-lo en la política i instruccions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Administració Municipal.

Requeriments

Experiència:

- Cal que tingui com a mínim 3 anys d'experiència en implantació de projectes de

ciberseguretat.

- Cal que tingui com a mínim 3 anys d'experiència en implantació de projectes de sistemes TIC.
- Cal que hagi participat en un mínim de 5 projectes d'implantació de solucions de ciberseguretat.
- Cal que hagi participat en un mínim de 5 projectes d'implantació de sistemes TIC.
- Cal que tingui com a mínim 3 anys d'experiència com a formador en ciberseguretat.
- Cal que tingui com a mínim 3 anys d'experiència com a formador en sistemes TIC.

10. PROPOSTA TÈCNICA

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

Els licitadors hauran de presentar la seva oferta en format electrònic, a través de la plataforma electrònica de licitació de l'Ajuntament de Barcelona. A l'oferta 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.

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

Es presentaran dos sobres:

- **Sobre AB:** En el sobre B s'inclourà la documentació següent indexada de manera que faciliti la seva localització. A tipus de lletra Nimbus Roman o Liberation Sans, grandària 12 i interlineat simple.

- **Sobre C:** haurà d'incloure l'oferta econòmica i 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. A continuació, es descriuen els continguts de cadascun dels sobres.

10.1. Contingut sobre AB

- En el **sobre B** s'inclourà la següent documentació indexada de manera que faciliti la seva localització. L'extensió màxima de l'oferta tècnica és de 12 pàgines. Les pàgines que superin aquest límit no seran valorades.

    - **Plantejament general**

S'exposa l'enteniment del servei que s'ha de prestar i les línies principals de l'estratègia per dur-lo a terme i l'esquema de l'equip del treball disponible durant l'execució del contracte. Es detallarà tot el que es consideri interessant respecte a les metodologies de treball emprades i l'execució del contracte.

La proposta ha d'incloure un calendari d'alt nivell de les fites a abordar durant el desenvolupament del servei.

- **Metodologia de coordinació del servei**

En aquest apartat s'haurà de detallar la metodologia proposada per a la gestió dels serveis. La proposta ha de respectar i millorar el contingut mínim especificat a l'apartat 3.1.1 Servei de Coordinació i haurà d'incloure:

- Proposta de la metodologia i model de relació.
- Proposta per a la gestió de riscos, tasques detallades, lliurables i rols.
- Proposta per a la gestió de qualitat, detallant les fases, tasques, lliurables i rols de forma coherent, així com la descripció detallada dels mecanismes que permetin assegurar la qualitat dels lliurables.
- Proposta de nous ANS per al seguiment de l'execució dels serveis.
- Proposta de metodologia de gestió de l'abast dels serveis.
- Proposta de tancament i transició del servei.

- **Proposta de col·laboració en la confecció de protocols i procediments operatius de seguretat**

Ha d'incloure la proposta per a l'elaboració del portfoli de protocols i procediments operatius de seguretat i la definició del pla estratègic que inclogui de manera clara el mínims descrits a l'apartat *3.1.2 Col·laboració en la confecció de protocols i procediments operatius de seguretat.*

- **Proposta de recomanació i suport en l'adopció de noves eines de seguretat operativa**

Ha d'incloure la proposta de recomanació i suport en l'adopció de noves eines de seguretat operativa, d'acord als requeriments i les directrius de seguretat de l'organització, analitzant el seu impacte a nivell de seguretat i de privacitat, donant suport al SOC i a l'equip de seguretat operativa en les tasques prèvies a la implantació de la nova eina, incloent de manera clara i senzilla els mínims descrits a l'apartat *3.1.3 Recomanació i suport en l'adopció de noves eines de seguretat operativa*.

- **Proposta de desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat**

Ha d'incloure la proposta per desenvolupar i implementar un pla de formació en resposta a incidents de ciberseguretat específic pels membres de l'equip de seguretat operativa, un segon pla pels integrants de l'equip de resposta a incidents de ciberseguretat, i un tercer pla per oferir formació a altres col·lectius de l'organització vinculats a la ciberseguretat, incloent de manera

clara i senzilla els mínims descrits a l'apartat *3.1.4 Desenvolupament i implementació d'un pla de formació en resposta a incidents de ciberseguretat*.

- **Proposta de suport a l'equip de seguretat operativa en la resposta a ciberincidents**

Ha d'incloure la proposta de suport a l'equip de seguretat operativa i a l'equip de resposta a incidents de ciberseguretat, dins i fora d'horari laboral, en cas que sigui requerit, incloent d'una manera clara i senzilla els mínims descrits a l'apartat *3.1.5 Suport a l'equip de seguretat operativa en la resposta a ciberincidents*.

10.2. Contingut sobre C

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

11. CONDICIONS GENERALS D'EXECUCIÓ

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

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

Pel que 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

A les diferents clàusules d'aquesta secció es fa referència a l'Ajuntament de Barcelona, Administració Municipal i IMI indistintament. De conformitat amb els seus estatuts s'ha d'entendre que l'IMI actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les que no sigui directament titular.

11.1. 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.

11.2. Confidencialitat

L'empresa contractada 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'Administració Municipal.

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

L'empresa contractada 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 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'empresa contractada es compromet a destruir amb les garanties de seguretat suficients o retornar tota la informació facilitada per l'Administració Municipal, així com qualsevol altre producte obtingut com a resultat del present contracte.

11.3. 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.
- 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 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 l'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.

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.
- 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.

11.4. Clàusula programari i metodologia de desenvolupament

L'empresa contractada disposarà del programari necessari i farà servir la metodologia implantada per l'Institut Municipal d'Informàtica (IMI) pel 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 li corresponen sobre el programari i bases de dades instal·lats 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 amb respecte al programari, sistemes operatius i bases de dades cedides per l'Administració Municipal, i la seva obligació de:

- 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-ne ús únicament i exclusivament per a les tasques encomanades, incloses en els serveis contractats.

11.5. Clàusula d'ús de software lliure

En la prestació del Servei l'empresa adjudicatària haurà de tenir en compte que l'IMI advoca per reduir el nombre de components de software llicenciables, i recomana per tant l'ús de components Open Source.

Les solucions, sistemes, processos, metodologies que es defineixin hauran d'estar alineats, ser coherents amb les estratègies TIC de l'Ajuntament, que es poden concretar entre altres en:

- Transparència i participació
- Obertura al ciutadà.
- Agilitat i disseny centrat en l'experiència d'usuari
- Ús prioritari de Programari Lliure.
- Compartició i creació de solucions de forma col·laborativa amb comunitats i altres administracions.
- Interoperabilitat
- Dades obertes

• Aplicació d'estàndards oficials oberts i lliures, especialment en formats de dades i protocols

En tot el que es refereixi a la definició de programari lliure i estàndards oberts lliures s'aplicarà les definicions de l'Open Source Iniciative (https://opensource.org/).

En concret, respecte a l'ús de programari lliure, s'haurà de prioritzar solucions de codi obert, o la construcció de noves solucions que es lliuraran mitjançant llicències obertes.

En els casos que no es pugui construir la solució totalment amb mòduls de programari lliure o solucions noves a mida, s'intentarà dissenyar la solució de forma que contempli el màxim de peces o mòduls lliures.

11.6. Clàusula de comunicacions externes

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

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'empresa contractada serà la responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús del certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

11.7. Clàusules generals de seguretat

11.7.1. Seguretat dels sistemes d'informació, protecció de dades i compliment normatiu

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

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

Pel que fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD

3/2010 de 8 de gener pel qual es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

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

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i IMI indistintament. De conformitat als seus estatuts s'ha d'entendre que l'IMI actua als efectes d'aquest contracte en nom i representació de l'Ajuntament de Barcelona i de l'Administració Municipal, pel que fa referència als fitxers, sistemes d'informació i/o infraestructures de les quals no sigui directament titular.

11.7.2. Responsable de seguretat

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

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

- Mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Administració Municipal, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

11.7.3. Confidencialitat

L'empresa contractada 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'Administració Municipal.

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, que no podran copiar o utilitzar com a finalitat diferent a les que la informació te designada.

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

L'empresa contractada 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'empresa contractada es compromet a destruir amb les garanties de seguretat suficients o retornar a l'Ajuntament de Barcelona, d'acord amb allò que s'estableixi legalment o les indicacions que en aquell moment li transmeti aquest Ajuntament, tota la informació facilitada per aquesta administració, així com qualsevol altra producte obtingut com a resultat del present contracte.

11.7.4. Clàusula per accessos potencials

En aquesta contractació no es preveu tractament de dades personals per part de l'empresa contractista.

Per a l'execució de les prestacions derivades del compliment de l'objecte d'aquest contracte, el personal de l'empresa contractista no pot accedir a les dades de caràcter personal que figuren als arxius, documents i sistemes informàtics de l'òrgan de contractació.

No obstant el que estableix el paràgraf anterior, quan el personal de l'empresa contractista accedeixi a les dades personals incidentalment, estarà obligat a guardar secret fins i tot després de la finalització de la relació contractual, sense que en cap cas pugui utilitzar les dades ni revelar-les a tercers.

L'empresa contractista ha de posar en coneixement dels seus treballadors els deures i obligacions establerts anteriorment.

L'empresa contractista ha de posar en coneixement de l'òrgan de contractació, de forma immediata, qualsevol incidència que es produeixi durant l'execució del contracte que pugui afectar la integritat o la confidencialitat de les dades de caràcter personal. Aquesta incidència s'haurà d'anotar al Registre d'incidències.

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

11.7.5. 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.

11.7.6. Clàusula de comunicacions externes

Si escau, l'empresa contractada disposarà dels mitjans materials i el maquinari necessari per a la connexió amb els Sistemes d'Informació de l'Administració Municipal, sent els costos de connexió a càrrec de l'empresa contractada.

La connexió és realitzarà seguint els protocols de seguretat per a les comunicacions externes establerts per l'Administració Municipal.

L'empresa contractada serà la responsable de custodiar correctament els certificats digitals lliurats per la interconnexió segura de xarxes i de demanar la seva revocació una vegada finalitzada la prestació del servei. Així mateix, serà responsable subsidiària de l'ús del certificats personals individuals lliurats als seus empleats pel desenvolupament del producte o servei.

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

11.7.7. Clàusula de seguretat dels equips, programes i informació

L'empresa contractada 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.

L'adjudicatari serà responsable de la instal·lació i actualització de programes de protecció antimalware de les màquines que suporten serveis de l'IMI segons es recull al marc normatiu del l'IMI.

11.7.8. Clàusula de personal extern

El Cap responsable de contracte de l'empresa contractada durà a terme de forma correcta la gestió del personal i els aspectes relacionats amb la seguretat de la informació.

L'empresa contractada està obligada a implantar els mecanismes i controls necessaris per a garantir la confidencialitat, privacitat, integritat i continuïtat de la informació de l'Administració Municipal, i de donar-los a conèixer al seu personal.

El Cap responsable de contracte de l'empresa contractada, 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'empresa contractada 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 de contracte de l'empresa contractada 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 que 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 de 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'empresa contractada que haurà de presentar-los quan siguin requerits per l'Administració Municipal.

11.7.9. Gestió d'incidents

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

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

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

11.7.10. Anàlisis forenses

L'execució d'anàlisis forenses és responsabilitat exclusiva de l'IMI-Seguretat. 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 IMI-Seguretat i el Proveïdor.

Aquest plec de prescripcions tècniques ha estat emès pel Sr. Jorge Vicente López Portero, tècnic responsable del contracte, adscrit a la Direcció d'Operacions i Sistemes i amb el vistiplau de

La Directora d'Operacions i Sistemes

Amparo Rodríguez Rodríguez

12. ANNEX 1 : DUBTES I ACLARIMENTS

Si és de l'interès dels licitadors sol·licitar informació per la presentació de l'oferta, l'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: **jlopezpo@bcn.cat**.

A l'assumpte del correu indicar: ***SERVEIS ESPECIALITZATS DE SUPORT A LA SEGURETAT OPERATIVA***

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

A causa de les mesures de seguretat i prevenció ocasionades per la crisi sanitària de la COVID-19, no es convocarà una sessió informativa per aquesta licitació. Per tal que els licitadors interessats en presentar oferta, puguin aclarir tots els dubtes que els hi sorgeixin, l'IMI posa a disposició dels licitadors la bústia de correu abans indicada per qüestions tècniques i la de imi_gestio_contractacio@bcn.cat, per consultes de caire administratiu.

Les consultes rebudes dins dels 3 dies hàbils anteriors a la data de finalització d'entrega de les proposicions seran solucionades i publicades al perfil del contractant de l'IMI:

(https://contractaciopublica.gencat.cat/perfil/BCN_IMI/customProf).

13. ANNEX 2: METODOLOGIA AGILE SCRUM@IMI

Metodologia àgil per a projectes IMI

L'adjudicatari seguirà la metodologia de desenvolupament àgil d'aplicacions de l'IMI, anomenada Scrum@IMI, detallada en el present annex. Està basada en el marc de treball Scrum i pràctiques d'enginyeria provinents d'altres models com Extreme Programming o DevOps.

Aquesta metodologia, disponible per a l'empresa adjudicatària, se suporta sota l'ús d'una plataforma ALM (Application Lifecycle Managmenet) amb eines de:

- Planificació del desenvolupament (releases, sprints, paquets de treball, defectes, etc.)
- Repositoris de documentació, codi i binaris
- Gestió de requisits i proves
- Automatització de les proves unitàries i funcionals
- Integració continua i Desplegament continu
- Control de la qualitat del codi, entre d'altres

El seu ús és obligatori per part de l'adjudicatari sense que suposi un cost addicional en llicències per al mateix.

Tota la documentació que es generi internament al desenvolupament haurà de gestionar-se amb les eines que es determinin a l'inici del projecte, preferentment en format wiki.

Les principals característiques d'aquesta metodologia es comenten segons el seu cicle de vida al següent enllaç:

https://ajuntament.barcelona.cat/imi/sites/default/files/marc_de_treball_scrumimi_per_proveidors.pdf

(veure document adjunt "marc_de_treball_scrumimi_per_proveidors.pdf")