Ajuntament
de Barcelona
Institut Municipal d'Informàtica
Direcció de serveis de Seguretat de la Informació

Plec de prescripcions tècniques per a la contractació dels Serveis d'Oficina de Govern, Risc i Compliment (GRC) i Oficina de Seguretat en Projectes de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible

ÍNDEX

1. INTRODUCCIÓ

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

Aquests serveis s'han d'oferir amb garanties i seguretat TIC per al ciutadà i per a la mateixa ciutat. Això implica protegir la informació personal del ciutadà, garantir la continuïtat dels serveis i salvaguardar la gestió de la ciutat i de l'Administració Municipal. La informació relativa a aquests serveis es troba distribuïda en un gran nombre de sistemes d'informació, la qual cosa requereix disposar de serveis d'identificació, protecció, prevenció i reacció davant les amenaces que poden afectar els sistemes d'informació i les infraestructures TIC. Aquestes mesures són essencials per reduir i minimitzar els riscos d'incidents de seguretat i ciberatacs.

En un escenari on el concepte de seguretat lògica o ciberseguretat avança ràpidament, els serveis de ciberseguretat que requereix l'Ajuntament han de ser confiables, àgils i configurats amb la flexibilitat suficient per afrontar riscos sovint impredictibles.

L'Ajuntament segueix com a marc de compliment el Real Decret 311/2022, de 3 de maig, que regula l'Esquema Nacional de Seguretat (ENS), per adaptar-se a l'evolució de la tecnologia, les ciberamenaces i el context regulador europeu i internacional. L'objectiu principal d'aquesta normativa és establir les condicions necessàries per a la seguretat en l'ús dels mitjans electrònics, definint mesures que garanteixin la seguretat dels sistemes, les dades, les comunicacions i els serveis electrònics, permetent així l'exercici de drets i el compliment de deures a través d'aquests mitjans.

Per aquest assolir aquest objectiu l'ENS estableix uns principis bàsics a considerar en les decisions de seguretat i uns requisits mínims que permetin la protecció adequada de la informació i ofereix uns mecanismes uns requisits mínims mitjançant l'adopció de mesures de seguretat que es proporcionen en base a la naturalesa de la informació i els serveis a protegir.

El mandat principal de l'ENS s'estableix en l'article 12 'Política de seguretat i requisits mínims de seguretat', segons el qual "cada administració pública comptarà amb una política de seguretat formalment aprovada per l'òrgan competent", la qual "és el conjunt de directrius que regeixen la forma en què una organització gestiona i protegeix la informació que tracta i els serveis que presta".

En el cas que la transposició de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.o 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (Texto pertinente a efectos del EEE) (NIS2) apliqui a les entitats locals s'haurà d'abordar l'adequació de la norma a l'Ajuntament.

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

L'ajuntament estableix el **Model de Gestió de la Seguretat** que és el marc on s'hi desenvolupen els programes de Seguretat Corporatius. El marc és en primera instància l'ENS així com els marcs internacionals de seguretat com poden ser el NIST *framework* de Ciberseguretat (Identificar, Protegir, Detectar, Respondre i Recuperar) i les normes ISO de la família 27000 (27001, 27002, 27017,...) i en especial la ISO 27001.

Aquest model es manté a través d'una Oficina de Govern de la Seguretat, que gestiona les tasques derivades definició del govern de la seguretat fins a la gestió de riscos i supervisió del compliment de les normatives i controls establerts en el model.

Actualment aquest **Model de Gestió de la Seguretat corporatiu** està en revisió per donar resposta a la necessitat d'integrar i coordinar tots els esforços relacionats amb la seguretat de la informació en un únic marc de treball coherent. per definir les línies d'actuació, projectes i serveis necessaris per donar resposta als reptes de protecció i seguretat que afronta l'Ajuntament, amb l'objectiu de: garantir una gestió segura, fiable i eficient de la informació i els serveis públics que ofereix a la ciutadania.

Aquesta revisió es concretarà a través d'un **Pla Director de Seguretat de la Informació de l'Ajuntament de Barcelona** en resposta a la necessitat d'integrar i coordinar tots els esforços relacionats amb la seguretat de la informació en un únic marc de treball coherent.

Mentrestant no es defineix i s'executa el Pla Director de Seguretat, s'han identificat les serveis que es requereixen executar per mantenir el model actual que permetin mantenir la seguretat d'ofici.

Aquestes serveis identificats són la gestió de riscos, auditories, control de Proveïdors, compliment del ENS dels sistemes d'informació corporatius i el servei de Seguretat en el Disseny i Projectes. D'igual manera, també es consideren tasques concretes com són el Registre d'incidents de Seguretat, el Registre d'Excepcions i la Categorització de Sistemes d'informació.

Es licita en aquest contracte per realitzar les tasques necessàries per mantenir el govern de la Seguretat en la seva vessant de supervisió del compliment del model actual tant de sistemes i serveis existents com en la construcció de nous serveis durant el període necessari per a l'elaboració i implementació del nou Pla Director de Seguretat Integral.

2. OBJECTE

L'objecte del contracte és proporcionar amb estricte compliment de l'ENS els àmbits introduïts següents:

- Govern de la seguretat: Servei de GRC

- Seguretat en el disseny: Servei de Seguretat en el Disseny i Projectes

2.1. **EN L'ÀMBIT DEL GOVERN DE LA SEGURETAT DE LA INFORMACIÓ**

La prestació del servei mitjançant una Oficina Tècnica de GRC (Oficina GRC) encarregada de garantir l'alt nivell de seguretat en el tractament i gestió de la informació i serveis TIC que l'IMI proporciona a l'Ajuntament de Barcelona, donant compliment als estàndards internacionals en matèria de seguretat, la legislació aplicable, el marc normatiu propi de l'IMI i la jurisprudència i resolucions dictades en aquest àmbit per tribunals i organismes independents.

Dins d'aquest àmbit es desenvolupen les tasques que es relacionen a continuació:

- Govern :
  - Gestió del risc corporatiu
- Control i seguiment de la normativa:
  - Compliment proveïdors
  - Control normatiu
  - Plans d'auditoria
- Suport en matèria de seguretat de la informació:
  - Classificació i categorització dels sistemes d'informació
  - Gestió del registre d'incidents de seguretat
  - Gestió d'excepcions.

2.2. **EN L'ÀMBIT DE LA SEGURETAT EN DISSENY I PROJECTES**

Securitzar la posada en producció de nous sistemes d'informació i minimitzar la probabilitat que s'implantin amb vulnerabilitats de seguretat, incompleixin les normatives de seguretat que li siguin d'aplicació (tant internes de l'IMI com externes) i/o no estiguin alineats amb l'estratègia de seguretat de l'IMI. Aquesta securització es concreta mitjançant els procediments, controls i tasques durant el cicle de vida dels projectes, tot augmentant el nivell de protecció dels sistemes de l'Ajuntament de Barcelona i garantint la gestió de la seguretat en totes les etapes del cicle de vida de cada projecte.

Dins d'aquest àmbit es desenvolupen les tasques que es relacionen a continuació:

- Servei de Seguretat en Projectes
- Seguretat en el disseny

- Servei de participació en projectes de seguretat
- Atenció a la demanda de la bústia de projectes

2.3. **PROCEDIMENT DE CONTRACTACIÓ**

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

3. ABAST

L'abast d'aquest contracte rau en el govern de la seguretat amb visió global a tot el grup municipal. Això suposa:

- Tenir la visió i gestió global del risc corporatiu
- Identificar responsables dels sistemes d'informació i responsables de Seguretat i promoure les revisions de compliment i auditories de seguretat dins del grup municipal
- Assessorament a l'Ajuntament, i a tot el Grup Municipal, en matèria de seguretat TIC.

Fora d'aquesta governança d'alt nivell, els serveis que conformen l'abast d'aquest plec van destinats als ens que l'IMI aprovisiona serveis TIC i exerceix de Responsable dels Sistemes d'informació (ENS). Inclou tots els Sistemes d'Informació de l'Ajuntament de Barcelona i de l'organització Municipal classificats i gestionats per l'IMI, així com tota la infraestructura que dóna suport als sistemes d'informació, tant si estan ubicats a l'IMI com si estan sota contractes de serveis TIC realitzats per l'IMI basats en Cloud, així com eines de suport al treball del personal corporatiu com són les estacions de treball, dispositius de mobilitat, correu corporatiu, eines de col·laboració, gestors documentals, etc.

- Definir i garantir el compliment de la seguretat de tots els Sistemes d'Informació de l'Ajuntament de Barcelona i de l'organització Municipal gestionats per l'IMI i tota la infraestructura que dóna suport als sistemes d'informació i sistemes digitals de suport al lloc de treball, tant si estan ubicats a l'IMI com si estan sota contractes de serveis TIC basats en Cloud.
- Garantir la seguretat en la construcció de nous serveis i incorporació de noves tecnologies (Seguretat en el disseny/Projectes)

En definitiva, el fet de tenir el cos normatiu de l'Ajuntament estructurat tot seguint les directrius d'un estàndard internacional com de la ISO 27002, ens facilita la seva revisió per adequar-lo als canvis normatius que es puguin produir.

Es pot trobar més informació sobre la volumetria dels sistemes d'informació gestionats per l'IMI a l'apartat *14.1 Annex 1: Abast a Organització Municipal i 14.2 Annex 2 Volumetria dels sistemes d'informació de l'Ajuntament* d'aquest plec.

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

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

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

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

3.1. **SERVEIS NO INCLOSOS**

Queden exclosos de l'objecte d'aquest contracte els aspectes més jurídics relacionats amb la protecció de dades personals (exercici de drets dels ciutadansrecollits en la normativa de protecció de dades, consentiments, procediments de declaració de tractaments, acords d'encarregat de tractament, etc.), que estan sota la responsabilitat de les gerències municipals sota les directrius, i, amb supervisió de l'Oficina de la Delegació de Protecció de Dades de l'Ajuntament i que són coordinats mitjançant la Taula de Protecció de Dades.

També queden exclosos els serveis d'adquisició de llicències de software que quedin en propietat de l'IMI.

4. **DESCRIPCIÓ DEL SERVEI**

4.1. **GOVERN DE LA SEGURETAT DE LA INFORMACIÓ**

El grau de complexitat i nombre d'aspectes a tenir en compte per tal de definir i garantir un nivell de seguretat acceptable per l'organització, fa necessari l'establiment d'una estructura i un model organitzatiu sòlid en l'àmbit de la seguretat, amb capacitat per a controlar i prendre decisions en totes aquelles accions que així ho requereixin.

D'altra banda, cal dotar al Govern de la Seguretat de la Informació d'un marc de referència normatiu consistent i coherent, que marqui les normes, criteris i polítiques per assegurar i controlar el nivell de seguretat de la informació.

Per tal d'assolir aquests objectius, l'adjudicatari prestarà els següents serveis:

4.1.1.**Gestió del Risc TIC corporatiu**

Aquest servei respon a l'objectiu últim de governar el risc corporatiu en TIC per donar una cobertura completa de gestió de riscos a totes les Gerències i organismes de l'Ajuntament de Barcelona del quals l'IMI gestiona els sistemes d'informació, així com recollir i gestionar els riscos d'alt nivell de la resta del grup Municipal que tenen gestió pròpia de sistemes d'informació i la gestió de riscos.

El servei de Risc Tecnològic ha d'identificar, avaluar i fer el seguiment dels riscos de seguretat tecnològics de l'Ajuntament de Barcelona. L'abast del servei, per tant, inclou el seguiment i gestió dels riscos identificats a l'Organització Municipal i als proveïdors TIC de l'Ajuntament de Barcelona.

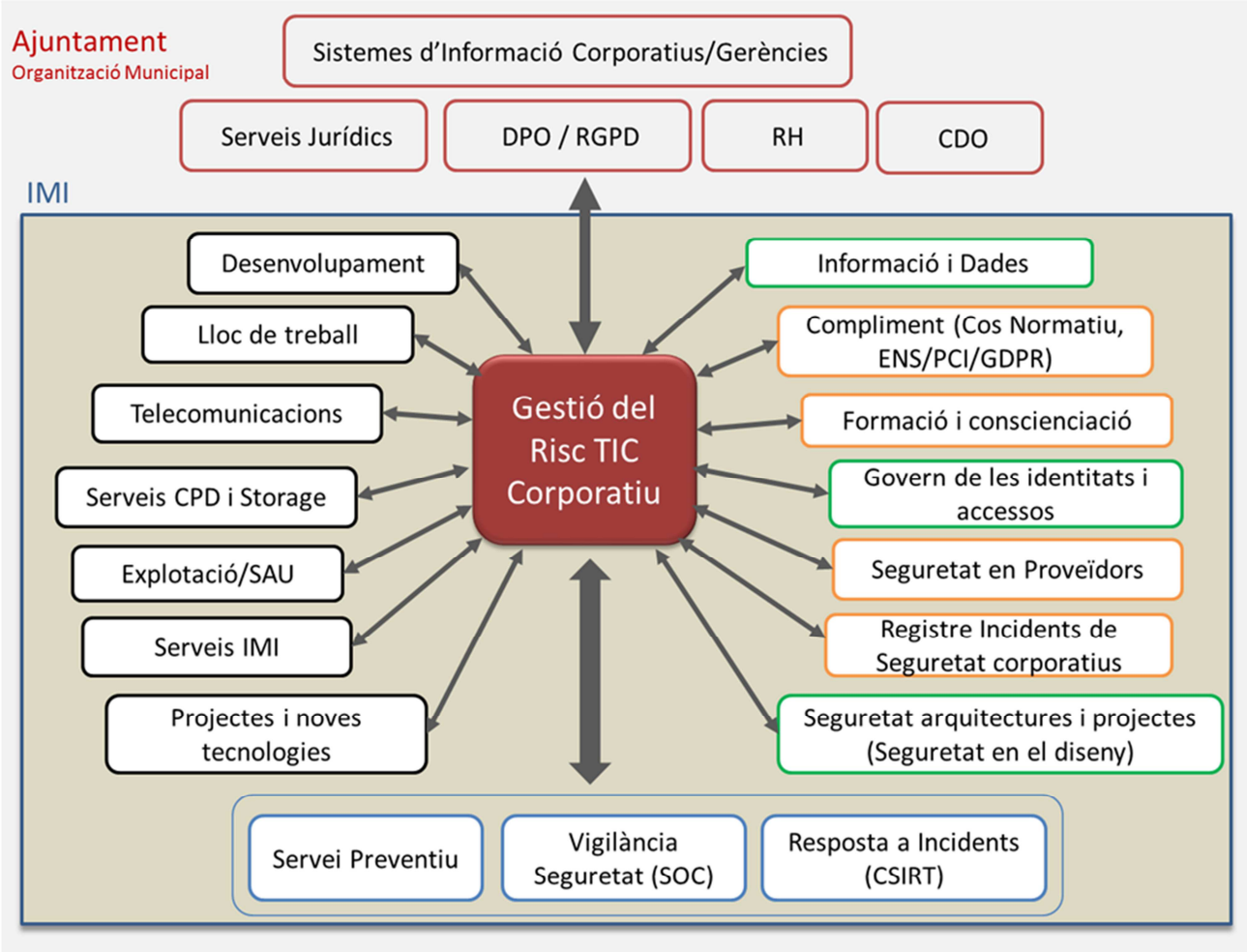
Aquest enfocament s'allunya de la visió on el risc és directament proporcional al número de controls que no es compleixen. Per això, la Gestió del Risc TIC del servei objecte d'aquest plec ha de tenir una relació estreta amb la resta d'àrees operatives i de projectes de l'IMI, per poder valorar millor i amb més amplitud aquests riscos.

La Direcció de Seguretat de l'IMI disposa d'una metodologia per a la valoració i determinació del risc dels actius de l'Ajuntament. L'Oficina GRC definirà els criteris per a l'informe periòdic dels nivells de risc així com el mecanisme de notificació en cas de superar-se el nivell de risc assumible.

L'objectiu d'aquesta gestió del risc és determinar el risc final de qualsevol actiu de l'Ajuntament.

La gestió de riscos sistemàtica i documentada es durà a terme mitjançant l'eina de GRC (Archer) desplegada pels àmbits funcionals de compliment i per gestió de riscos.

L'anàlisi de risc es realitzarà de forma contínua, amb l'objectiu de determinar els nivells de risc existents en cada moment, d'acord amb els criteris de valoració i la metodologia definits i donant compliment del control ([op.pl.1] d'Anàlisis de Riscos de nivell MIG de l'ENS.



Les activitats a realitzar s'emmarquen en diferents línies d'acció:

- Catàleg d'amenaces
- Desenvolupament i aplicació de la metodologia de gestió del risc
- Identificació de nous riscos
- Seguiment dels riscos
- Indicadors de la gestió del risc

4.1.1.1.*Catàleg d'amenaces*

El Servei de GRC mantindrà el procediment per a la gestió del catàleg d'amenaces que contempla tant el mecanisme d'identificació com el seu inventariat.

La identificació, classificació i valoració de les amenaces registrades en el catàleg sustentarà i donarà evolució i continuïtat al model existent.

4.1.1.2.***Desenvolupament i aplicació de la metodologia de gestió del risc***

L'adjudicatari, inicialment, haurà d'adoptar la metodologia de gestió del risc desenvolupada per l'IMI, sobre la qual podrà proposar millores per tal d'evolucionar i millorar els processos. Actualment, aquesta gestió es realitza a través de l'eina GRC Archer, on es poden donar d'alta riscos i associar-los al propietari.

La metodologia ha de permetre gestionar els riscos corporatius i dels sistemes d'informació corporatius categoritzats en el marc de l'ENS:

- Identificar i utilitzar criteris de valoració homogenis que faciliti als responsables la categorització de sistemes d'informació d'acord amb l'ENS.
- Donar suport a les Unitats de Negoci en l'especificació dels requisits de seguretat i la implantació dels mateixos durant les fases de disseny i posada en marxa de serveis i en la valoració i categorització de sistemes d'informació.
- Verificar la implantació real d'aquells requisits de seguretat que s'hagin identificat com a aplicables en la fase de disseny d'un servei.
- Determinar la maduresa dels requisits de seguretat implantats d'acord amb la metodologia evidenciant i documentant els resultats en informes i aplicacions corporatives.
- Conjuntament amb el propietari del risc, determinar el valor del dany que produiria la degradació o pèrdua de funcionalitat d'un actiu i la definició d'un pla de mitigació d'aquells riscos que el seu tractament ho requereixi.

4.1.1.3.***Identificació de nous riscos***

A través dels diferents canals d'entrada d'informació que pugui rebre el servei (tant interns com externs, tal com mostrem en la imatge anterior), s'ha de detectar i escalar riscos de seguretat de la informació, que s'han de notificar i comunicar pels canals definits segons la naturalesa del risc (Archer, Seguiment a proveïdors, etc.).

Els *inputs* interns a partir dels quals el servei podrà identificar riscos són:

- Auditories
- Projectes
- Seguiment de proveïdors
- Referents Sectorials de l'IMI
- Responsables dels Sistemes d'informació/Gerències i Ens Municipals
- Serveis Finalistes i serveis interns/Àrees Operatives de l'IMI
- Àrea de Qualitat

- Incidents de seguretat gestionats
- Indicadors del quadre de comandament
- Informes de seguretat (INES, específics de processos)
- Gestió d'excepcions
- Altres vies.

En aquesta identificació de nous riscos cal analitzar si se'n deriven requisits de seguretat i la seva aplicabilitat per incorporar-los en els actius d'informació a fi d'eliminar, o minimitzar la probabilitat d'explotació de les possibles vulnerabilitats.

4.1.1.4.*Seguiment de riscos*

Els riscos identificats s'han de gestionar per tal que el risc residual associat a aquests no superi mai el llindar de risc de l'Ajuntament. Per tal de dur a terme aquesta tasca, s'ha de portar el seguiment a través de l'eina Archer a fi de recollir les accions preses per mitigar, transferir, evitar o, en el seu defecte, acceptar els riscos.

Conjuntament amb el propietari del risc, serà necessària la definició d'un pla de mitigació d'aquells riscos que el seu tractament ho requereixi.

L'adjudicatari haurà de dona suport en la gestió del risc a les capes directives de l'IMI i l'Ajuntament mitjançant la preparació d'informes, o altres vies que es puguin establir.

4.1.1.5.*Indicadors de l'estat en la gestió del risc – reporting*

L'adjudicatari haurà de dissenyar i implantar indicadors relacionats amb la gestió del risc per tal de poder fer seguiment de l'estat i evolució dels mateixos.

Aquests indicadors han de fer l'extracció per reflectir el risc corporatiu al Quadre de Comandament de Seguretat Corporativa.

Aquest quadre d'indicadors és manté, s'actualitza de forma contínua i s'estructura d'acord amb les directrius que estableixi el servei de Govern de la Seguretat.

4.1.1.6.*Lliurables*

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Aplicació de la metodologia de gestió del risc	S'haurà de gestionar i revisar els riscos corporatius de manera recurrent, incloent els riscos propis dels sistemes d'informació (ENS)	1 revisió mensual	Informe de resultats de la revisió
Informes de seguiment de riscos	Preparar informes de seguiment dels riscos per escalar als comitès de Seguretat segons l'àmbit d'actuació	6 informes anuals	Informes de seguiment de riscos
Actuacions especials	Elaboració d'informes per a comunicar i informar riscos a la Gerència Municipal o a altres òrgans de l'Ajuntament	2 actuacions anuals	Informe de riscos
Indicadors de risc	Proposar quins haurien de ser els indicadors necessaris per a una correcta gestió del risc	1 proposta anual	Document de proposta dels indicadors de risc
Quadre de comandament del risc	Alimentar el Quadre de Comandament de Seguretat amb els riscos identificats	1 actualització trimestral	Informació per actualitzar el Quadre de Comandament

4.2. **CONTROL I SEGUIMENT DE LA NORMATIVA**

Disposar d'un marc normatiu actualitzat i alineat a l'estratègia de seguretat a seguir requereix el control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat i, en el cas de tractar-se de la part legal, per evitar sancions econòmiques.

4.2.1. **Seguretat en proveïdors**

L'IMI ha definit una ***metodologia de control de proveïdors*** dels contractes amb l'objectiu de poder sistematitzar el control del compliment de la normativa per obtenir i mantenir un nivell de seguretat adequat automatitzar i industrialitzar aquest control. Aquesta metodologia es basa, en la seva versió actual, principalment en la validació del compliment de les mesures de seguretat descrites a l'ENS.

L'adjudicatari haurà d'incorporar la metodologia de gestió de tercers desenvolupada per l'IMI, sobre la qual podrà proposar millores per tal d'evolucionar i millorar els processos. Entre d'ells establir el sistema en què els responsables dels contractes municipals puguin fer autoavaluació amb el proveïdor per garantir el compliment de la seguretat del seu contracte.

A alt nivell, aquesta metodologia es basa en la implementació en 4 fases diferenciades que garanteixen la seguretat dels proveïdors de serveis:

- FASE1 - Clàusules de seguretat: fase preliminar a la contractació on s'estableixen les obligacions del proveïdor.
- FASE2 - Lliurament de documentació: a l'inici del contracte, s'ha de fer el lliurament de documentació als nous proveïdors. Si bé aquesta activitat correspon al responsable del contracte, el servei ha de prestar suport a l'activitat, essent el responsable del manteniment dels documents així com formar i assistir els responsables dels contractes.
- FASE3 - Seguiment del proveïdor: El Seguiment de Proveïdors el realitzaran els responsables dels contractes municipals en base al sistema de control de la seguretat proposat com a millora de la metodologia.

  A un conjunt de contractes, escollits segons criticitat o per mostreig, addicionalment es realitzarà un seguiment específic pel personal d'aquest contracte segons el nivell assignat al proveïdor (en funció del sistema d'informació emprat en les seves tasques i/o l'activitat desenvolupada). S'estableixen 3 graus de seguiment amb periodicitat i activitats diferenciades.
- FASE4 - Auditories: com a fase addicional, es presenta la possibilitat de realitzar auditories de seguretat basades en els controls de l'ENS per aquells proveïdors de criticitat especial.

El detall de la metodologia es trobarà a disposició de l'adjudicatari un cop iniciat el servei.

Com a activitats incloses dins de la gestió de la metodologia trobem:

- **Revisió i adaptació de la documentació:** Com a part integral d'un procés de millora contínua, l'adjudicatari haurà de revisar periòdicament la documentació disponible i associada a la metodologia, on s'inclouen manuals de bones pràctiques, documentació del cos normatiu, clàusules de seguretat, etc.

  Addicionalment, es preveuen activitats associades a l'adaptació de la documentació existent en funció del perfil específic de l'adjudicatari sobre el qual realitzar el seguiment.

- **Formació als responsables dels contractes**: Amb la finalitat de traslladar el model de la metodologia als responsables dels contractes, és necessari establir sessions periòdiques amb aquests, on poder reforçar el seu paper i introduir possibles modificacions en la metodologia que els hi resultin d'aplicació. Se'ls explicarà la metodologia de control que han d'aplicar.

- **Seguiment dels proveïdors**: Per una selecció de proveïdors, durant la prestació del servei pels proveïdors, s'establiran una sèrie de punts de control per garantir que el proveïdor està donant compliment a allò que la normativa de seguretat que li és d'aplicació li requereix.

  Es classifiquen els proveïdors en 3 nivells que són:

  - Nivell 1: serveis que per desenvolupar les seves activitats fan servir sistemes d'informació de nivell baix. Es preveu el seguiment anual de proveïdors. Els proveïdors s'escolliran per risc, per rellevància (imatge, interès corporatiu, etc.) i/o per mostreig.
  - Nivell 2: serveis que per desenvolupar les seves activitats fan servir sistemes d'informació de nivell mig. Es preveu el seguiment semestral de proveïdors. Els proveïdors s'escolliran per risc, per rellevància (imatge, interès corporatiu, etc.) i/o per mostreig.
  - Nivell 3: serveis estratègics, els quals presenten requisits de seguretat més específics. S'inclouen els serveis transversals com el correu o lloc de treball, infraestructurals/ de grans serveis de CPD o sistemes d'informació rellevants que involucrin a moltes organitzacions municipals. Es preveu el seguiment trimestral individualitzat de proveïdors.

Durant la fase de Seguiment dels proveïdors es valorarà el nivell assignat a cada proveïdor i servei prestat, sent possible la requalificació de proveïdors, ja sigui augmentant o disminuint el nivell que tenien assignat.

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Responsabilitats i Formació als responsables de contractes	Incidir en la responsabilitat del lloc de treball a través de Recursos Humans. Establir sessions periòdiques amb els responsables de contractes	2 formacions específiques anuals online	Convocatòria Reunions Documentació curs

Descripció	Tasques	Volumetria	Lliurables
Control de proveïdors	Control de proveïdors de nivell 1	15 proveïdors 1 control/any	Informe de resultats del control (1 per proveïdor analitzat)
	Control de proveïdors de nivell 2	12 proveïdors 2 controls/any	Informe de resultats del control (1 per proveïdor analitzat)
	Control de proveïdors de nivell 3	7 Proveïdors 3 controls/any	Informe de resultats del control (1 per proveïdor analitzat)
Control de proveïdors de contractes AM de desenvolupament	Proposta de metodologia per delegar el compliment de seguretat dels contractes dels AM de desenvolupament al servei de l'IMI centralitzat en els diferents contractes de manteniment i evolutius de desenvolupament (18 contractes) de manera única i centralitzada. Realitzar revisions semestrals als que estan al servei de l'IMI	1 proposta 2 controls/any	Informe de resultats del control dels AM

4.2.2.**Control normatiu**

La Direcció de Seguretat, mitjançant el Departament de Compliment (GRC), gestiona i coordina la seguretat de la informació dins de diferents marc normatius aplicables (ENS, EIDAS, GDPR,...) i estableix les pautes i normes generals d'implementació tècnica de la reglamentació per al tractament de la informació fora d'aquest àmbit.

L'objectiu d'aquest servei és el de mantenir i, en el seu cas, adequar les mesures de seguretat aplicades per l'Ajuntament i per l'IMI d'acord amb els requeriments normatius que els són d'aplicació actualment o davant dels canvis normatius que es produeixin durant la prestació d'aquest servei, amb atenció especial als canvis que afectin al compliment de l'ENS o de la normativa de protecció de dades personals.

Queden exclosos de l'objecte d'aquest contracte els aspectes més jurídics (exercici de drets ARCO, consentiments, acords d'encarregat de tractament,...), que estan sota la responsabilitat de l'Oficina del Delegat de Protecció de Dades[1], i que són coordinats mitjançant la Taula de Protecció de Dades.

S'inclou a l'abast del contracte els informes de seguretat dels riscos tecnològics derivats de les PIAs (avaluacions d'impacte en la privacitat dades personals) tal com està establert en la Instrucció per la qual es fixen els criteris d'aplicació del Reglament General Europeu de Protecció de Dades i la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals a l'Ajuntament de Barcelona.

Pel desenvolupament d'aquest servei es duran a terme les següents tasques:

- Coordinar i donar suport a la resta d'àrees de l'IMI i/o als proveïdors TIC de l'IMI durant l'execució dels plans d'acció.
- Satisfer les necessitats d'informes en matèria de compliment normatiu als que està obligat o requerit complir l'Ajuntament (Informe Anual de Compliment de l'ENS,...).
- Servei d'adequació dels sistemes a la legislació (ENS, eIDAS, LOPDGDD,...) i al marc normatiu corporatiu.
- Identificació de nous requeriments que siguin d'aplicació a l'Ajuntament de Barcelona i la seva incorporació en el marc normatiu actual
- Col·laboració amb l'Oficina del Delegat de Protecció de Dades donant suport tècnic als requeriments imposats pel RGPD i la LOPDGDD.
- Elaboració d'informes de compliment per aprovació de Serveis/Aplicatius/Convenis de l'Ajuntament.
- Anàlisi d'impacte, gestió de riscos i proposta de mesures de sistemes d'informació crítics.
- Gestionar que els Sistemes d'Informació municipals apliquin les mesures de seguretat corresponents al marc de control de l'ENS tot identificant els riscos que presenten. Per dur a terme aquesta tasca, el contracte haurà de mantenir aquest marc de control i gestionar els riscos mitjançat l'eina RSA Archer disponible a l'IMI. Així mateix, també serà missió del contracte incorporar a l'eina RSA ARcher els nous sistemes d'informació que es creïn i els riscos emergents que puguin tenir impacte en els sistemes d'informació municipals.
- Reportar, de forma anual, a l'Estat el grau de compliment de l'ENS mitjançant l'eina INES propietat del Centro Criptológico Nacional.
- Revisar i, si s'escau, evolucionar el marc de controls a aplicar en entorns cloud.

[1] Excepte d'aquelles parts dels procediments explícitament assignades al departament de Seguretat

- Facilitar suport i assistència a la taula de Ciberseguretat de l'Ajuntament de Barcelona.

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Realització de tasques d'assessorament	Els temes més habituals seran: - Assessorament, impuls i suport al compliment de l'ENS. - Assessorament i suport al compliment de la normativa de protecció de dades - Assessorament, impuls i suport al compliment de normatives sectorials com PCI-DSS i LSSICE. - Assessorament legal general (en matèries com ara cloud, drets fonamentals recollits per la Constitució Espanyola, anàlisis forenses...)	4 assessories/ any	Informe d'assessoria
Elaboració d'informes sota demanda	Els més habituals són: - Informes de compliment legal, - Informes de seguretat per requeriments tals com l'aprovació de sistemes d'informació de l'Ajuntament, - Informes consultius específics.	6 informes / any	Informe

Descripció	Tasques	Volumetria	Lliurables
Compliment ENS	Anàlisis i revisió dels sistemes d'informació específics municipals per garantir el compliment de l'Esquema Nacional de Seguretat , amb l'objectiu de la certificació. Aquesta anàlisi s'incorporarà en Identificació, actualització i seguiment plans d'adequació	10 sistemes nous anuals Informe sistemes d'informació existents (màx. uns 150-200, p.ex. Padró).	Informe de compliment dels sistemes revisats
Documents del marc normatiu	Desenvolupament de les normes, guies, estàndards i procediments necessaris per a cobrir noves necessitats que no estiguin cobertes pel marc normatiu vigent.	Màxim 12 documents anuals	Norma, guia, estàndard (Aprovada i/o implantada)

4.2.3.**Plans d'auditoria**

Com s'indicava a la definició i gestió del marc normatiu, aquest servei és la base per **establir controls i poder mesurar el seu compliment** per tal de conèixer el nivell de seguretat dels sistemes d'informació i poder **prioritzar la resolució dels incompliments** que es detectin.

El seguiment dels compliments dels controls i les accions que s'estableixin de les deficiències detectades, permetrà **conèixer l'estat d'adequació de la seguretat definida a la normativa**.

Aquestes accions es poden portar a terme a través de la realització d'auditories i col·laborant en el desenvolupament dels projectes i transformacions de sistemes de manera que es puguin **controlar les accions** que es realitzen **i confirmar que van alineats amb el marc establert**.

Les activitats que s'han de desenvolupar dins de la prestació d'aquest servei són:

- Disseny del pla d'auditories anual corporatiu.
- Execució del pla d'auditories
- **Auditories puntuals** a sistemes d'informació corporatius o de serveis rellevants de l'IMI i de l'Ajuntament sota petició del Departament de Seguretat. Aquestes auditories estaran

relacionades amb les necessitats detectades en cada moment i poden ser de qualsevol tipus (compliment normatiu de l'IMI, compliment tècnic de la legalitat, vulnerabilitats...).

- **Auditories sectorials** a les diferents gerències de l'ajuntament amb l'objectiu de determinar el grau de compliment de l'ENS per part dels Sistemes d'Informació que es troben sota el seu control.
- Donar suport (és a dir, facilitar i acompanyar la feina i en cap cas elaborar l'auditoria) als requeriments propis de les **auditories externes de l'IMI** (entre 2 i 3 a l'any). Aquest suport consisteix, bàsicament, en proporcionar recepció i acompanyament i donar informació detallada de l'operativa habitual de seguretat demandada pels auditors externs i fer seguiment posterior dels incompliments detectats.
- Coordinació i seguiment de la implantació de les millores identificades en les revisions i auditories.
- Implantació de las millores identificades en què la responsabilitat recaigui en la Seguretat de l'IMI.
- Definir un sistema de consolidació dels resultats de les auditories realitzades.
- Definir un sistema d'informes a la Direcció dels resultats de les auditories realitzades.

Donada la normativa aplicable actualment, adquireix una major importància el control del compliment normatiu per part dels proveïdors respecte dels serveis que presten a l'Ajuntament.

Les auditories descrites en l'apartat *4.2.1 Seguretat en proveïdors* es realitzaran mitjançant l'aplicació de la ***metodologia de control de proveïdors*** definida per l'IMI.

Serà objecte d'aquest servei l'execució de les auditories als proveïdors per garantir el compliment de la normativa que els és d'aplicació respecte dels serveis prestats a l'Ajuntament.

El servei ha de tenir la dedicació necessària per a preparar i gestionar les sessions, recollir i analitzar les evidències, detectar les no conformitats respecte la normativa aplicable i fer proposta d'accions de millora sobre les que haurà de fer el corresponent seguiment.

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Definició i Aprovació del Pla Anual de Auditoria	Dissenyar el pla d'auditoria de seguretat i planificar la seva execució amb les àrees i proveïdors TIC de l'IMI (que ha d'incloure mínim 3 auditories de compliment globals)	1 pla anual	Pla anual d'auditories de seguretat

Descripció	Tasques	Volumetria	Lliurables
Execució auditories internes de compliment (puntuals o sectorials)	Realitzar auditories internes puntuals o específiques de compliment	3 auditories anuals	Informe d'auditoria i pla d'acció.
Auditoria general del compliment de l'ENS	Realitzar auditoria interna per a la conformitat de l'ENS, avaluant els controls generals aplicables a tota l'organització i conforme al cos normatiu i auditant els controls específics d'una mostra de sistemes d'informació corporatius significatius.	1 anual	Informe d'auditoria del compliment de l'ENS corporatiu
Donar suport en l'execució auditories externes de compliment (Servei de cortesia)	Actuar com a punt únic de contacte entre el personal de l'IMI i els auditors externs.	Màxim 3 auditories anuals	Obtenció de les evidències sol·licitades pels auditors externs.
Gestionar la implementació de les millores sorgides	El servei haurà de coordinar i donar suport a les àrees i proveïdores TIC de l'IMI responsables de les accions correctives sorgides de les auditories.	2 informes anuals de seguiment	Informe indicant l'execució de la millora o acció requerides.

4.3. **SUPORT EN MATÈRIA DE SEGURETAT DE LA INFORMACIÓ**

Per tal de garantir el compliment normatiu des de l'inici de qualsevol iniciativa, l'Oficina de GRC ofereix a la resta d'àrees un servei d'atenció i resolució de dubtes o de suport tècnic especialitzat en matèria de Seguretat.

D'aquesta manera, l'adjudicatari haurà de disposar d'un Servei d'Assessorament per a la implementació tecnològica, procedimental i organitzativa per al compliment normatiu en general amb el qual es resoldran dubtes que es puguin despendre de l'aplicació del marc normatiu tant conceptual, legal o tècnic.

a) Pel desenvolupament d'aquest servei es duran a terme les següents tasques regulars de suport:

- Atenció a la bústia de consultes i peticions de Seguretat de l'Oficina de GRC. Gestions internes d'assignació de tasques dins del Departament. Gestió de Govern de Seguretat d'escalats de tiquets de SAU.
- Suport orientatiu de funcionament de processos i procediments dels serveis.
- Servei de consultoria orientativa de temes puntuals.
- Incidències i canvis que derivin en tasques del servei.
- Serveis d'ajuda al diagnòstic d'incidents, problemes i canvis que derivin en tasques del Servei.
- Recepció incidents de seguretat.
- Resolució de dubtes o consultes sobre la interpretació o aplicació del marc normatiu de seguretat.
- Resolució d'aquelles peticions d'usuaris que requereixin de la validació i/o autorització per part del departament de seguretat.

b) Així mateix, existeixen una sèrie **de tasques especials de suport**, que en definitiva seran consultories i/o tasques que l'oficina ha d'executar de forma puntual, com són tasques de suport i adaptacions dins l' àmbit dels serveis que prestarà:

- Elaboració d'informes de compliment per la categoria del desplegament o utilització de nous serveis / aplicatius / tecnologies.
- Elaboració d'informes de noves normatives de seguretat que ens siguin d'aplicació.
- Elaboració de guies sobre matèries concretes i específiques
- Anàlisi de riscos de seguretat de sistemes o tecnologies específiques.
- Manteniment dels serveis derivats de canvis o adaptacions al nou model de serveis basats en Cloud.
- Impacte de Seguretat d'Evolutius específics, que no es trobin dins l'abast de l'Oficina de Projectes.
- Avaluació i anàlisi d'arquitectures específiques.

Donat que la bústia de servei de l'Oficina de GRC s'ha posicionat com a punt de connexió entre el departament de Seguretat i la resta d'àrees, tant de l'IMI com de l'Ajuntament, per a la comunicació de dubtes, incidències, etc. relacionades amb la seguretat dins de l'àmbit de l'Ajuntament, es requereix disposar de la capacitat necessària per poder gestionar-la.

Aquest posicionament comporta que es rebin correus electrònics destinats a les altres àrees del departament de Seguretat i que seran avaluats per aquest servei i redirigits a qui correspongui.

A més, l'adjudicatari haurà de ser flexible, en el sentit d'assumir altres tasques encomanades no contemplades al plec, però directament relacionades amb la gestió de l'Oficina de GRC i que poden entendre's dins l'objecte d'aquest contracte.

Si això fos necessari, es valorarà com afecta aquesta incorporació al compliment de la resta de tasques encomanades. L'adjudicatari explicarà la metodologia que emprarà i els serveis experts que posarà a disposició al contracte per poder donar sortida a aquest servei així com els SLA d'atenció a la bústia.

L'adjudicatari plantejarà els àmbits concrets (legals, arquitectura, tecnologies concretes, metodologies, ITIL, Ciberseguretat, Anàlisi de Riscos, Controls en entorns cloud, ...) en què donarà suport.

L'adjudicatari posarà a disposició de l'IMI, per suports puntuals del contracte, els serveis experts disponibles en modalitat de backoffice.

L'adjudicatari destinarà un mínim de 450 hores anuals en el servei regular de gestió de les entrades de peticions, tiquets de seguretat i en la gestió d'incidències operatives del servei abast d'aquest plec i destinarà a més a mes 10 actuacions de suport puntuals anuals estimats en una dedicació mitjana de 10 hores per suport.

L'adjudicatari realitzarà el control de les hores a través de les eines que se li requereixen a l'apartat *4.7.3 Eina de Gestió Interna del Servei* del present plec. La volumetria es basarà en el número de correus electrònics, tickets i hores que consumeixin en serveis especials.

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Gestions de la bústia de seguretat i actuacions de suport regular i incidències de servei	L'oficina ha d'executar de forma puntual tasques de suport i adaptació recurrent dins de l'àmbit dels serveis que prestarà	450 hores actuacions de suport anual	Informes de suport realitzats i dedicació
Tasques de suport especials, puntuals del Servei	L' oficina ha d'executar de forma puntual tasques de suport puntual	15 actuacions de suport anuals	Informes de suport realitzats i dedicació

4.3.1.**Acord de Nivells de servei (ANS)**

Els nivells de servei i terminis exigibles per a atendre la demanda de la bústia de seguretat principal corporativa que gestiona l'Oficina de GRC per franges de temps és el següent:

Temps de resposta	Temps de diagnòstic	Temps de resolució	Perfil mínim assignat
8 hores laborables	16 hores laborables	40 hores laborables	Tècnic sènior

Franges de temps:

- Temps de resposta. És el temps transcorregut des què el servei que presta l'adjudicatari rep la consulta fins que un tècnic qualificat es posa en contacte amb l'usuari.
- Temps de diagnòstic. És el temps transcorregut des què la consulta és comunicada a l'adjudicatari fins que l'adjudicatari fa un diagnòstic de la necessitat.
- Temps de resolució. És el temps transcorregut des què la consulta és comunicada a l'adjudicatari fins que es considera tancada o correctament derivada per l'afectat o el responsable.

Hores naturals: són consecutives, laborables o festives.

Hores laborables es consideren del calendari laboral de la ciutat de Barcelona de 09:00 a 18:00.

La millora dels ANS seran objecte de valoració a les ofertes dels licitadors.

4.4. **CLASSIFICACIÓ I CATEGORITZACIÓ DELS SISITEMES D'INFORMACIÓ**

Actualment l'IMI té desenvolupat un sistema de Classificació de la Informació corporativa adequat als requeriments de les diferents normatives que li són d'aplicació (ENS, LOPDGDD, ...)

En el procés de classificació hi han identificats al voltant de 200 sistemes d'informació ratificats i incorporats a l'eina Archer.

En el desenvolupament d'aquest servei s'hauran de dur a terme les tasques corresponents a:

- **Mantenir el Sistema de Gestió de la categorització de la Informació Corporativa en base a les 5 dimensions de l'ENS**. Això inclou:
  - Suport a la categorització dels sistemes d'informació nous i revisió i, si s'escau, actualització de la categorització dels sistemes d'informació amb les Gerències responsables de la Informació i els Serveis.
- Definició del cicle de vida de la informació segons el tipus de suport sobre el que es trobi, d'acord amb les directrius marcades des de l'Arxiu Municipal respecte de la conservació de documents ja sigui en paper o en format digital.

El següent quadre resumeix els volums i els lliurables exigits de cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Suport a la categorització dels sistemes d'informació	Suport a la categorització dels sistemes d'informació nous i revisió (i, si s'escau, actualització de la categorització) dels sistemes d'informació amb les Gerències responsables de la Informació i els Serveis.	Aprox. 10 sistemes d'informació nous anuals 1 revisió amb cada gerència responsable de la informació i/o del servei anual	Sistemes categoritzats nous. Revisions amb les gerències realitzades.

4.5. **GESTIÓ DE REGISTRE D'INCIDENTS**

Donada la seva importància, l'Ajuntament de Barcelona i la seva organització municipal es veuen sotmesos a diferents incidents de seguretat i de tots aquests incidents que es produeixen se n'ha de dur un registre.

La coordinació de la gestió dels incidents i l'assegurament de la qualitat d'aquest registre corresponen a l'Oficina de GRC qui, evidentment, requerirà el suport dels equips tècnics implicats en cada incident per què facilitin tota aquella informació que sigui necessària i pertinent respecte tant pel que fa a la resolució de l'incident com de les mesures adoptades per evitar, en la mesura del possible, que es torni a produir aquest incident.

Inicialment la gestió del Registre d'Incidents era totalment manual i no permetia, de manera senzilla, poder relacionar un incident amb un incident que ja hagués ocorregut en el passat i poder determinar si la solució que es va adoptar en el seu moment va ser la correcta. Per aquest motiu s'està implantant una eina de Gestió d'Incidents (descrita en l'apartat 4.7.2 d'aquest plec) que també actuarà com a Registre dels Incidents.

L'adjudicatari haurà de desenvolupar les tasques següents:

- Manteniment i evolució d'una eina per la gestió del registre d'incidents corporatius que proporcioni la confidencialitat, els informes i càrrega i gestió dels formularis de registre.
- La normativa aplicable, tant nacional com europea, obliga a notificar incidents de seguretat relatius a ciberseguretat (Directiva CNIS i ENS) i a privacitat (RGPD i LOPDGDD). El servei haurà establir i implementar els mecanismes i processos corporatius per fer les

notificacions d'incidents de seguretat a les que l'Ajuntament està obligat legalment en forma, en temps i en els diferents organismes establerts pels diferents tipus d'incident.

- Fer revisions periòdiques quadrimestrals per assegurar el correcte registre dels incidents.
- Fer revisions periòdiques quadrimestrals per assegurar que es segueixen els procediments de notificació i registre establerts.
- Realitzar un informe anual sobre els incidents registrats pel posterior anàlisi i millores.
- Desenvolupar un pla de divulgació de l'eina de Gestió del Registre d'incidents (descrita al punt 4.7.2) als grups resolutoris corresponents

En el següent quadre es resumeixen la volumetria i lliurables exigibles per a cada una de les tasques esmentades:

Descripció	Tasques	Volumetria	Lliurables
Gestió de les notificacions d'incidents de ciberseguretat i privacitat a organismes.	Gestionar les notificacions de seguretat que sorgeixin.	No hi ha previsió s'estima màxim de 4 mes.	Registre gestió incidents
Gestió i control del Registre d'incidències de Seguretat de l'Ajuntament de Barcelona	Fer revisions periòdiques quadrimestrals per assegurar el correcte registre i notificació dels incidents	1 informe cada 4 mesos	Informe
	Fer revisions periòdiques quadrimestrals per assegurar que es segueixen els procediments de notificació i registre establerts	1 informe cada 4 mesos	Informe
	Realitzar un informe anual sobre els incidents registrats pel posterior anàlisi i millores.	1 informe anual	Informe

4.6. **GESTIÓ D'EXCEPCIONS**

El Servei de gestió d'excepcions té per objectiu gestionar el cicle de vida de les excepcions de seguretat que, en el dia a dia, poden ocórrer en els diferents àmbits de gestió TIC (a nivell de proveïdor TIC, en el desenvolupament, en la gestió de la xarxa de comunicacions, en la gestió de volums de informació, proveïdors o serveis corporatius, etc.)

En base al cos normatiu, arquitectures establertes o riscos incipients, el Departament de Seguretat gestiona les peticions d'excepcions de seguretat. La generació d'excepcions se sotmeten a l'existència de causes degudament justificades (mitjans tècnics, organitzatives, legals o econòmiques) que no permetin una implantació proporcionada dels controls que demana la norma, arquitectura o gana de risc. Aquestes excepcions han de tenir un caràcter temporal fins que es trobi solució per poder donar degut compliment a la normativa de referència.

La gestió de les excepcions forma part de la gestió operativa diària del risc, donat que tota excepció de seguretat pot portar un risc de seguretat associat que cal que gestionar.

L'adjudicatari haurà d'implementar un sistema de gestió d'excepcions que, entre d'altres, haurà d'incloure les següents activitats:

- Recepció de les excepcions de seguretat (internes i de proveïdors TIC) amb un primer filtre per determinar si l'excepció incorpora prou informació per la seva correcta avaluació. Inclou un responsable de l'Ajuntament o Directiu de l'IMI (segons l'excepció) i un responsable tècnic de l'excepció (peticionari).
- Valoració del Risc d'acord a la informació rebuda.
- Seguiment de l'aprovació o denegació per part de la persona identificada com a responsable del risc.
- Seguiment de l'excepció fins la seva expiració i gestió de les renovacions en cas que siguin necessàries.
- Gestió dels lliurables.
- Com a resultat de tota aquesta gestió, el servei genera periòdicament informes de situació per determinar quins proveïdors són els més afectats pels riscos vinculats a les excepcions. Aquesta informació es comunicarà i coordinarà amb el servei de control de proveïdors i amb el servei de Gestió de Risc Corporatiu.
- Les excepcions es mantenen en el Quadre de Comandament de Seguretat Corporatiu i en els reportings existents de àrees operatives i serveis IMI, Gerències i ens de l'Ajuntament, Proveïdors.
- Tota la informació també és incorporada al repositori de Registre de Seguretat que gestiona el Departament de Seguretat.
- Construcció, de forma coordinada amb el servei de govern del risc, d'indicadors de referència que permetin qualificar les principals àrees de risc.

La volumetria associada a aquest servei es pot quantificar, de mitjana, en unes 15 excepcions per any.

Descripció	Tasques	Volumetria	Lliurables
Gestió d'excepcions	Mantenir inventari de gestió d'excepcions i gestionar les excepcions que vencen els terminis. Revisió i proposta de millora del model de gestió d'excepcions Manteniment del QDM Comunicació a altres dependències que han de registrar les excepcions de seguretat que es produeixin.	1 Revisió mensual 1 revisió anual	Informe inventari amb excepcions gestionades Proposta de millora i gestió de la implantació de la millora.
Incorporar excepcions al registre	Les noves excepcions s'incorporaran al registre	Es preveuen unes 15 excepcions anuals	Entrada al registre d'excepcions.

4.7. **EINES DE SUPORT AL SERVEI GRC**

Donat el creixement de la demanda dels serveis proporcionats per l'Oficina de GRC, així com de l'ampliació del catàleg de serveis que es proporcionen des d'aquesta oficina, és necessari dotar-la d'una sèrie d'eines que permetin simplificar, i/o automatitzar la gestió interna del servei.

La principal entrada de peticions es produeix via correu electrònic a la bústia de servei que té assignada l'Oficina de GRC i llavors aquestes peticions es gestionen segons els criteris següents:

- Si no és una petició per l'Oficina de GRC s'ha de reenviar, en cas que es conegui el destinatari, a qui correspongui o retornar al peticionari si es desconeix qui hauria de ser el destinatari de la petició.
- Si es tracta d'una petició per l'Oficina de GRC s'ha de classificar (segons criticitat i urgència), assignar a un dels membres de l'Oficina de GRC, gestionar-la i donar resposta el més àgilment possible.

Com a eines principals d'ús per part de l'Oficina de GRC haurien de constar les eines de:

- Eina de Govern, Risc i Compliment.

- Eina de Registre d'Incidents.
- Eina de Manteniment del Cos Normatiu.
- Eina de Gestió interna del Servei.

Aquestes eines es troben descrites a continuació.

4.7.1.**Eina de Govern, Risc i Compliment**

Actualment l'IMI té desplegat RSA Archer, que serà l'eina principal de l'Oficina de GRC per fer el seguiment i control de l'estat de la seguretat dels diferents Sistemes d'Informació que es troben sota control o supervisió del departament de Seguretat de l'IMI.

L'IMI disposa dels següents mòduls d 'RSA Archer:

- Issues Management.
- IT Controls.
- IT RIsk Management.

L'adjudicatari d'aquest contracte haurà de dur a terme el manteniment de l'esmentada eina, per això haurà de desenvolupar les tasques següents:

- Establir els mecanismes necessaris per automatitzar la interoperabilitat d'aquesta eina amb altres sistemes corporatius dels quals s'alimenta i amb aquells als quals servirà de font d'actualització de la informació.
- Avaluar l'estat actual de l'eina.
- Proposar evolucions i millores de l'eina.

L'adjudicatari documentarà, seguint la metodologia i les plantilles facilitades per l'IMI, els diferents procediments que es duguin a terme per a la configuració i/o interconnexió de l'eina Archer amb altres sistemes d'informació amb els que s'hagi de produir intercanvis d'informació.

L'adjudicatari s'encarregarà de:

- Gestionar l'actualització de l'eina amb els diferents pegats proporcionats pel fabricant.
- Donar el suport necessari respecte de l'eina instal·lada sense que comporti un cost addicional per l'IMI.

4.7.2.**Eina de Registre d'Incidents**

L'IMI es troba en fase de configuració i desplegament d'una eina per al Registre i la Gestió dels incidents de seguretat que pateix l'Ajuntament, i la seva organització municipal, de manera que aquestes tasques de registre i gestió puguin simplificar-se, en quant a complexitat i rapidesa, tot

establint els circuits pertinents per a la gestió dels incidents. L'eina que s'està desplegant per a la Gestió d'incidents de Seguretat és **LUCIA**.

L'adjudicatari del contracte haurà de definir i implementar, d'acord amb el departament de seguretat de l'IMI, i en aquells casos que sigui necessari d'acord amb l'Oficina del Delegat de Protecció de Dades, els circuits necessaris per automatitzar en la mesura que sigui possible tot aquest circuit de gestió d'incidents.

L'adjudicatari documentarà, seguint la metodologia i les plantilles facilitades per l'IMI els diferents procediments que es duguin a terme per a la configuració i/o interconnexió de l'eina amb altres sistemes d'informació amb els que s'hagi de produir intercanvis d'informació.

També serà missió de l'adjudicatari, conjuntament amb el Departament de Seguretat posar a disposició de personal extern al propi Departament de Seguretat, la possibilitat d'accedir a l'eina tant per poder procedir a notificar un incident com per informar de les passes dutes a terme per a la resolució del mateix.

4.7.3.**Eina de Gestió Interna del Servei**

Donat l'increment de peticions de servei que es reben a l'Oficina de GRC, tant en nombre com en diversitat de temàtiques, s'ha produït un augment proporcional en quant a la dificultat en la gestió interna del servei.

Per aquest motiu, l'adjudicatari haurà de proposar durant els 3 primers mesos del contracte una eina ja adoptada corporativament per l'IMI que permeti una millor gestió de les diferents peticions que arriben i que permeti tant als membres de l'Oficina com als responsables de l'IMI que es determini, poder en qualsevol moment obtenir una fotografia de l'estat de les diferents peticions gestionades.

Un cop proposada l'eina, aquesta proposta haurà de ser acceptada per l'IMI abans no es pugui procedir a la seva implantació. Els costos inicials d'implantació de l'eina, cas d'haver-n'hi, seran assumits per l'adjudicatari.

L'adjudicatari lliurarà a l'IMI l'eina implantada i preparada per començar a treballar.

4.8. **SERVEI DE SEGURETAT EN PROJECTES**

L'Oficina de Seguretat en Projectes (OSP d'ara en endavant) serà l'encarregada de garantir les diferents activitats necessàries per garantir el funcionament del servei de seguretat en projectes. Aquestes activitats seran diferents en funció de la fase del projecte.

Aquest servei de seguretat en disseny (*Security by Design*) es l'encarregat de dur a terme les tasques de securització de la construcció de nous serveis o esmenes dels existents, es a dir, dels Projectes i els aplicatius que construeixen o milloren un servei en tot el seu cicle de vida, i l'adequació al model de Ciberseguretat de l'Ajuntament establert a través de l'IMI. En tot aquest procés es manté sempre una visió del risc potencial que pot tenir la posada en marxa d'una determinada aplicació, tecnologia o solució per la incorporació o millora d'un servei corporatiu.

4.8.1.**Govern i seguiment de la *seguretat* en els projectes**

A l'inici del servei caldrà establir i documentar el **model de govern i seguiment** de la **Seguretat en el Disseny** (Seguretat en projectes), que en termes generals haurà de cobrir les tasques que garanteixin la securització dels projectes així com la vista global dels riscos de seguretat en que s'incorporen les noves solucions o funcionalitats.

Per assolir els objectius de govern dels projectes el servei haurà d'articular les següents tasques:

1. **Establiment i documentació d'un Model de Govern de la Seguretat en Projectes** alineada amb els objectius de estratègics de seguretat i amb la metodologia proposada pel licitador. Establir una política que haurà d'incloure com a mínim, **les figures clau i els comitès** participants **del procés**.
2. Establiment de nous processos o adaptació dels existents que siguin necessaris per tal d'**implantar el servei de Seguretat en Projectes**. Aquests processos treballaran les diferents fases del cicle de vida d'un projecte des de la conceptualització inicial fins a la certificació dels requeriments establerts i posada en producció. Aquests processos es materialitzaran en **procediments que hauran de ser redactats per l'OSP (Oficina de Seguretat en Projectes)** d'acord a les metodologies de l'IMI.

   El procés que actualment es realitza al participar des de seguretat en un projecte té les següents etapes:

   I. Coneixement del projecte

      a. Presentació formal del Projecte: els projectes es presenten en uns comitès anomenat taula de la demanda, on es defineix la dedicació dels diversos departaments que han de participar en el projecte.

      b. Presentació informal del Projecte: existeixen projectes en els quals no s'ha detectat en fases preliminars la necessitat de participació de l'equip de Seguretat però s'ha generat aquesta amb el seu desenvolupament, requerint el suport d'un enllaç de Seguretat.

   II. Petició Informació: es demana més dades al projecte per tal de disposar d'informació a la hora de realitzar l'estudi dels diferents requeriments aplicables per part de seguretat. Es compta amb plantilles que serveixen com a línia base dels projectes per tal de detectar els requeriments de seguretat.

   III. Revisió Informació i Definició de Requeriments: l'enllaç de seguretat analitza la informació disponible i genera documentació interna del projecte amb els requeriments que haurà de complir el projecte amb l'objectiu de garantir els estàndards de seguretat. Aquests requeriments son la base de treball de l'enllaç de seguretat sobre la qual basa el seu seguiment del projecte.

   IV. Participació en el projecte: depenent de la metodologia de treball emprada, la participació de l'enllaç de seguretat pot variar. En qualsevol casuística, s'empren les

diverses sessions del projecte per fer un seguiment actiu dels requeriments establerts i detectar desviacions dels paràmetres originals.

3. Definició d'un **quadre de comandament per identificar el nivell de seguretat dels nous serveis corporatius que es construeixen. Aquest quadre de comandament ha d'incloure els indicadors de risc i el nivell de compliment dels requeriments de seguretat dels projectes** de l'IMI.

4. **Informe de nivell de seguretat i riscos dels projectes corporatius** per a avaluar la seguretat i reporting de seguiment mensual, que es reportaran a la PMO i al Comitè de Direcció de Projectes.

5. Supervisar el Llibre blanc d'arquitectures de referència en l'àmbit de la seguretat tal com s'estableix a l'apartat *4.9.1 Llibre blanc d'arquitectures de referència*.

Descripció	Tasques	Volumetria	Lliurables
Establiment d'un Model de Govern en la Seguretat en Projectes de la Seguretat en Projectes	**Establiment i documentació d'un Model de Govern de la Seguretat en Projectes** alineat amb els objectius estratègics de seguretat i amb la metodologia proposada pel licitador. Aquest model haurà d'incloure com a mínim, **les figures clau i els comitès** participants **del procés**.	1 Model de Govern de la Seguretat en Projectes	Model de Govern de la Seguretat en Projectes
Revisar i millorar el processos del Servei de Seguretat en Projectes	Establiment de nous processos o adaptació dels existents que siguin necessaris per tal d'implantar el servei de Seguretat en Projectes. Aquests processos es materialitzaran en procediments que hauran de ser redactats per la OSP d'acord a les metodologies de l'IMI.	Una Revisió anual dels processos del Servei de Seguretat en Projectes Un Pla d'Implantació de millores per cada Revisió Anual	Document de millores proposades Pla d'implantació

Descripció	Tasques	Volumetria	Lliurables
Quadre de Comandament dels la Seguretat en el disseny	Definició i implantació d'un quadre de comandament que inclogui els indicadors de risc i de rendiment i compliment de la seguretat en relació als projectes de l'IMI Informe de nivell de seguretat i riscos dels projectes corporatius	1 Quadre de Comandament 1 informe quinzenal	Presentació dels riscs i nivells de compliment Quadre de Comandament Informe nivell seguretat i riscos projectes

4.8.2.**Metodologia de Seguretat en projectes**

El proveïdor haurà de fer una revisió de l'actual metodologia i realitzar una proposta de millora per a donar-li maduresa, més capacitats i més cobertura en tot el cicle de vida dels Projectes.

La metodologia tindrà un **mecanisme de classificació de seguretat del projecte** com a mínim en base a:

- Rellevància o estratègic
- Nivell confidencialitat
- Requeriments específics de seguretat

La metodologia ha d'habilitar que la major part de projectes puguin desenvolupar-se sense o amb poca participació explícita de l'Àrea de Seguretat gràcies a la classificació i mitjançant l'**autoavaluació i paràmetres, i** les **indicacions d'estàndards**.

Per als projectes que requereixin la participació explícita de l'Àrea de Seguretat, la metodologia haurà de d'incloure les següents tasques:

- Fase conceptualització (previ al Plec Tècnic)
- Identificació de clàusules específiques de seguretat prèvies a la redacció del plec tècnic.
- Requeriments específics de seguretat en base a riscos detectats.
- Classificació de la informació en base a criteris de seguretat.
- Revisió del document d'arquitectura (DA) de la solució o aplicació.
- Revisió del qüestionari d'autoavaluació del projecte.
- Oferir el suport necessari per ajudar a la interpretació dels requeriments i a la seva implementació final.

- Establir el conjunt de proves necessàries per poder realitzar les comprovacions de les mesures i requeriments de seguretat establertes prèviament.
- En els projectes que inclouen desenvolupament s'ha de incorporar controls per validar que surtin amb les condicions establertes per la *Pipeline* o els passos a producció que garanteixin codis segurs.

Anomenem ***Enllaç de Seguretat*** al perfil que participa en la seguretat en projectes. És la persona que respon per l'activitat del servei de consultoria de l'OSP en relació a un projecte concret, esdevé doncs la figura d'enllaç per aquell projecte. El paper d'enllaç de seguretat neix amb l'objectiu de coordinar les interaccions entre l'equip d'un Projecte i el Direcció de Seguretat i si cal fer de enllaç amb els diferents interlocutors i de l'àrea durant el cicle de vida d'un projecte.

L'Oficina de Seguretat en Projectes (d'ara endavant, OSP) actualment té establertes **4 tipologies o nivells de participació** per part de la Consultoria de Projectes a la seguretat de projectes en funció de:

- Suport d'alta participació: Si és necessària una dedicació constant per part de l'OSP.
- Suport inicial: Si es preveu que la dedicació per part de l'OSP serà rellevant sobretot durant la fase inicial del projecte, mentre que més endavant és probable que es redueixi només a una activitat de seguiment en les fases d'implementació i proves.
- Suport puntual: Si es preveu recórrer a OSP només de manera ocasional, o sigui per a consultes puntuals, serà suficient definir per endavant un model de comunicació entre el projecte i OSP per resoldre de la manera més eficient possible les consultes o peticions que siguin necessàries.
- Sense Suport: Només es farà el seguiment automatitzat d'autoavaluacions dels projectes.

El contracte actuarà d'enllaç en aquells projectes que s'estableixi la participació de seguretat.

Les tasques prèviament identificades tindran una dedicació i activitats diferents segons el tipus de projecte i es poden agrupar per cada fase del cicle de vida del projecte:

- **En fase de conceptualització i definició / Gestió de la Demanda**
- **En fase de desenvolupament del projecte**
- **En fase de posada en producció del projecte**

Descripció	Tasques	Volumetria	Lliurables
Revisió de l'actual metodologia de seguretat en el disseny	El proveïdor haurà de fer una revisió de l'actual metodologia i realitzar una proposta de millora per a donar-li maduresa, més capacitats i més cobertura en tot el cicle de vida dels Projectes.	Revisió anual de la metodologia del Servei de Seguretat en Projectes Un Pla d'Implantació de millores per cada Revisió Anual	Document de millores proposades Pla d'implantació
Implementació i gestió de l'execució de la metodologia definida	El proveïdor haurà de implementar i gestionar l'execució de la metodologia i assistir o gestionar l'assistència de referents de seguretat en les 4 tipologies o nivells de participació identificades en tot el cicle de vida dels projectes.	Seguiment de l'execució de la metodologia i estat dels projectes mensual	Document de seguiment

Per madurar i implementar la metodologia s'han de tenir en consideració i incloure els següents aspectes:

- Gestió de la demanda de la demanda de seguretat.
- Consultoria de projectes.
- Inventari de projectes i documentació.

Detallem aquests aspectes en els següents apartats:

4.8.2.1.*Gestió de la demanda de seguretat*

Els projectes s'aborden en funció de la demanda generada a través de la Taula de la Demanda i la Cartera de Projectes de l'IMI, que són els encarregats de detectar les necessitats dels diferents clients i, conjuntament amb el Responsable del Projecte i/o del Servei de l'IMI, prioritzar l'execució dels diferents projectes, tant per projectes de desenvolupament clàssics, amb

metodologies de DevSecOps com per projectes de implantació de noves tecnologies o tecnologies emergents, d'igual manera es consideren els projectes que es preveu que s'ofereixin en el núvol (Iaas, Paas, Saas).

De forma contínua es treballa amb l'Àrea que gestiona els projectes de l'IMI per tal de posar els procediments i eines per poder assegurar que els nous sistemes, aplicacions i/o canvis importants en les mateixes es construeixen de forma segura incorporant-se al cicle de vida segur d' aquests serveis.

Aquesta gestió de la demanda suposarà tenir en tot moment identificats els projectes i conèixer el tipus de dedicació esperada en base a una primera classificació i quin tipus de seguiment es requerirà.

Actualment els projectes tenen un model de participació requerida per part de seguretat de diferents tipus que pot passar de cap participació mitjançant el model d'autoavaluació a diferents grau de participació que s'explicita en el Model de Consultoria.

4.8.2.2.***Consultoria de projectes***

La consultoria de projectes compren aquelles consultes puntuals no incloses dins l'abast d'un projecte que ja s'està gestionant.

L'equip de consultoria de projectes ha de garantir la seguretat en el disseny realitzant, entre d'altres, les següents tasques:

- Suport tècnic.
- Especificació de requeriments.
- Seguiment i control de requeriments.
- Execució de proves de seguretat.

4.8.2.3.***Inventari de projectes i documentació***

Per tal de mantenir el coneixement a l'organització municipal, es mantindrà un inventari de projectes i la documentació relacionada.

Els lliurables dels projectes dependran de la tipologia del projecte:

- Document de Classificació de la Informació.
- Document de Seguretat del Projecte on s'informa dels requeriments detallats de seguretat a implementar al projecte.
- Document de flux de Dades del Projecte.
- Document d'Arquitectura del Projecte.

- *Pla de Traces* o de perfilats d'autoritzacions.
- Informes de vulnerabilitats que s'hagin considerat.
- Informe de seguiment de projecte.
- Informe de riscos de seguretat final.
- Presentació executiva del projecte.

Aquests lliurables es gestionaran en un repositori de la documentació de Seguretat del Projecte.

4.8.3.**Atenció a la demanda de la bústia de projectes**

Per tal de garantir una correcta comunicació amb tots els interlocutors de les diferents àrees de l'IMI, el Servei de Seguretat en Projectes oferirà a la resta d'àrees i departaments de l'Ajuntament aquest canal d'entrada especialitzat en matèria de Seguretat en Projectes i del SDLC.

Per al desenvolupament d'aquest servei es duran a terme les següents tasques regulars de gestió de la demanda:

- Atenció a la bústia de consultes i peticions dels diferents serveis que conforma l'Oficina de Seguretat: Seguretat en Projectes, de Servei de Seguretat en el Disseny i del Servei de Projectes de Seguretat.
- Aportació en seguretat en projectes en quant a procediments establerts (plantilles i pla de traces).
- Aportació en matèria del *pipeline* de seguretat (DevSecOps).
- Recepció de dubtes o consultes sobre la interpretació o aplicació del marc normatiu de seguretat a resoldre pel servei de governança.
- Lliurament mensual de l'informe de les accions de participació en projectes realitzades i dedicació, especificant com a mínim el nombre de tiquets, l'estat, i la dedicació.

L'adjudicatari destinarà un mínim de 150 hores/any en peticions de projectes, consultories d'arquitectures i del servei regular de gestió de les entrades de peticions i tiquets de seguretat escalats de SAU i en la gestió d'incidències i consultes del servei abast d'aquest plec.

Es valorarà l'increment de les hores dedicades a aquest servei a l'oferta del licitador.

4.8.4.**Acord de Nivells de servei (ANS)**

Els nivells de servei i terminis exigibles per a atendre la demanda de la bústia de projectes de l'Oficina de Seguretat en projectes per franges de temps és el següent:

Temps de resposta	Temps de diagnòstic	Temps de resolució	Perfil mínim assignat
8 hores laborables	16 hores Laborables	40 hores laborables	Tècnic sènior

Franges de temps:

- Temps de resposta. És el temps transcorregut des què el servei que presta l'adjudicatari rep la consulta fins que un tècnic qualificat es posa en contacte amb l'usuari.
- Temps de diagnòstic. És el temps transcorregut des què la consulta és comunicada a l'adjudicatari fins que l'adjudicatari fa un diagnòstic de la necessitat.
- Temps de resolució. És el temps transcorregut des què la consulta és comunicada a l'adjudicatari fins que es considera tancada o correctament derivada per l'afectat o el responsable.

Hores naturals: són consecutives, laborables o festives.

Hores laborables es consideren del calendari laboral de la ciutat de Barcelona de 09:00 a 18:00.

La millora dels ANS seran objecte de valoració a les ofertes dels licitadors.

4.9. **SERVEI DE SEGURETAT EN EL DISSENY (ARQUITECTURES)**

Dins l'Oficina de Seguretat en Projectes, el Servei de Seguretat en el Disseny haurà d'oferir **l'estandardització i normalització d'arquitectures** que formen part de la infraestructura que consumeixen els projectes. Amb aquest propòsit haurà de redactar d'un llibre blanc que reculli les arquitectures de referència en base als escenaris aplicables dins dels models d'arquitectura més coneguts .

Aquest servei de Seguretat en el Disseny és l'encarregat de dur a terme les tasques d'anàlisi i proposta d'arquitectures existents i noves a l'organització, de tal forma que tindrà un objectiu d'auditoria tant a les arquitectures productives de l'IMI com a les noves propostes d'arquitectures de components, tant software com hardware. Serà, per tant, el nexe entre els diferents interlocutors inter departamentals de l'IMI i l'Àrea de Seguretat, tot realitzant documentació classificada de totes les accions relatives a acceptació i inventariat d'excepcions d'arquitectures corporatives.

El servei donarà suport de consultoria en referència a la seguretat en noves arquitectures, així com idoneïtat a aquestes en funció del grau de maduresa de la organització i de millores que puguin requerir, o que siguin necessàries a mode de requeriment de seguretat. Establirà requisits d'arquitectura de ciberseguretat més adequada a les noves tecnologies, als riscs emergents i a les noves implementacions de modificacions de serveis.

Aquest servei tindrà 4 activitats principals:

4.9.1.**Llibre blanc d'arquitectures de referència**

El Servei de Seguretat en el Disseny s'encarregarà de l'estandardització i normalització d'arquitectures de seguretat mitjançant la creació i redacció del llibre blanc on es recullin les arquitectures de referència en base als escenaris aplicables dins dels models d'arquitectura amb els controls de seguretat requerits en cada cas.

L'OSP serà responsable del desenvolupament, manteniment i actualització d'aquest llibre blanc. S'entén com a llibre blanc una estructura documental amb autoritat que conté guies documentals i que té com a objectiu d'ajudar a l'IMI a resoldre o afrontar com han d'implementar la seguretat en les diferents escenaris i en els diferents aspectes a abordar en la seguretat en el disseny o Projectes.

Entre d'altres s'estandarditzaran:

- Model tradicional *on-premise*
- Arquitectura de microserveis
- Estàndards d'Identitats, autoritzacions i accessos
- Arquitectura de Xarxes i accessos remots
- Arquitectura cloud
- Framework de desenvolupament
- Tecnologies de IOT: Sensors i smartcities
- Projectes d'IA
- Etc.

4.9.2.**Disseny de solucions de Seguretat**

El servei farà propostes de disseny de les solucions de manera segura, tant a l'arquitectura de components com de comunicacions. Aquestes solucions arquitecturals seran principalment en entorns *cloud* (OCP), però també en àmbit *legacy* dins de l'organització així com models híbrids.

Establirà arquitectures de seguretat de noves tecnologies o tecnologies encara no existents o no estandarditzades a l'Ajuntament i l'IMI.

També participarà en definir l'arquitectura de projectes que incorporin nous reptes no desenvolupats en la organització.

4.9.3.**Donar solucions a necessitats de seguretat i/o riscos detectats**

Avaluarà i proposarà plans de millora a riscos que l'Oficina de GRC (Compliment) li escali. També donarà suport a l'àrea que gestiona auditories per presentar propostes de millores a debilitats o millores detectades per les auditories.

Participarà a la Taula Operativa de Seguretat quan calgui per aportar propostes.

Avaluarà solucions de Seguretat- Laboratoris, dintre de seguretat o participant d'altres àrees tecnològiques/Operatives de l'IMI.

Implementant o col·laborant en la implementació de plans de millora derivats de:

- Marc Normatiu.
- Auditories.

Descripció	Tasques	Volumetria	Lliurables
Llibre blanc d'arquitectures de referència	Gestió del llibre blanc d'arquitectures de referència on es recullin tots els escenaris d'infraestructura amb els controls de seguretat requerits en cada cas. L'OSP serà responsable del desenvolupament, manteniment i actualització d'aquest llibre blanc.	Elaboració del Llibre blanc arquitectures Revisió anual del Llibre blanc	Document del Llibre blanc
Disseny de solucions de seguretat	Establir arquitectures de seguretat de noves tecnologies o tecnologies encara no existents o no estandarditzades i participar en nous reptes dels projectes no desenvolupats en el l'Ajuntament i l'IMI	Estimat en uns 6 anuals	Document de disseny de la solució
Donar solucions a necessitats de govern, normatives i/o riscos detectats a Govern de la seguretat	Donar suport a les àrees de Govern i gestió del risc així com a les troballes de les auditories	Estimat en uns 6 anuals	Document de seguiment

4.9.4. **Pipeline DEVSECOPS**

Referent a les tasques de Seguretat relacionades amb el manteniment i gestió d'eines del *pipeline* de l'IMI, aquestes s'hauran de revisar amb l'objectiu de detectar oportunitats de millora en els processos que gestionen. En concret, l'adjudicatari durà a terme a les següents activitats:

- Elaborar un **informe amb la revisió de les polítiques de detecció de vulnerabilitats de codi** i llenguatges emprats a l'IMI així com els components de seguretat implementats en la *pipeline.* Aquest informe ha d'incloure un pla de millora que permeti assolir un procés de millora contínua de l'eina d'anàlisi de codi estàtic.
- Revisar periòdicament les imatges oficials que empren els projectes a l'hora de desplegar imatges en la plataforma de contenidors. **Serà necessari recollir un catàleg d'imatges que doni comptes de les revisions dutes a terme i les versions vigents de les mateixes**.
- Revisar periòdicament les polítiques de desplegament d'imatges de contenidors.
- Realitzar revisions periòdiques del repositori central d'imatges de contenidors de l'IMI a fi de detectar oportunitats de millora en els processos establerts.
- Definir l'estratègia associada a la monitorització de contenidors per tal de poder detectar comportaments anòmals. Aquesta activitat ha de desenvolupar-se conjuntament amb el servei que gestioni l'eina SIEM corporativa, donant suport en la seva posterior implementació i operació.
- Resoldre dubtes associats al *pipeline* en la part de seguretat, de funcionament i d'arquitectura
- Proposar millores infraestructurals al *pipeline*, per tal d'afegir nous components que millorin el control i govern
- Revisar els components existents, i les seves configuracions, en cerca de millores evolutives dels productes del *pipeline* (actualització de versions o canvi de productes)

Descripció	Tasques	Volumetria	Lliurables
Revisió i supervisió de les parametritzacions i la seguretat de la Pipeline	Revisar periòdicament les imatges estandarditzades	Revisió mensual de les imatges estandarditzades	Informe de la revisió i proposta de millora
	Revisar periòdicament les polítiques de desplegament d'imatges de contenidors	Revisió trimestral de les polítiques de desplegament	Informe de les polítiques de desplegament i proposta de millora

Descripció	Tasques	Volumetria	Lliurables
	Realitzar revisions periòdiques del repositori central d'imatges corporatiu	Revisió trimestral de les imatges dins del repositori corporatiu	Informe de les imatges dins del repositori corporatiu
	Revisió de l'estratègia associada a la monitorització de contenidors	Revisió trimestral de l'estratègia associada a la monitorització dels contenidors. Pla d'Implantació de millores de la monitorització (trimestral) Obtenció mensual d'indicadors de la monitorització	Document de Millores Millores implantades Informe de monitorització
	Resoldre dubtes associats al *pipeline* en la part de seguretat, de funcionament i d'arquitectura	5 dubtes/any	Informe de resposta
	Proposar millores infraestructurals al *pipeline*, per tal d'afegir nous components que millorin el control i govern	Revisió anual de l'estat actual de la infraestructura del pipeline Pla Implantació de millores a la pipeline	Informe d'estat pipeline Pla d'implantació de millores
	Revisar els components i configuracions en cerca de millores evolutives dels productes del *pipeline* (actualització de versions, canvi de productes o actualització de la configuració)	Revisió trimestral dels components actuals	Document de l'estat actual i de possibles millores Pla d'implantació

5. MODEL DE PRESTACIÓ DEL SERVEI

5.1. MODEL DE RELACIÓ IMI/ADJUDICATARI

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

L'adjudicatari pot ampliar, millorar i detallar, partint de les directrius aquí marcades, l'organització proposada i l'esquema específic de la relació amb l'IMI, així com els mecanismes de control propis de cada servei i funció transversal.

L'equip de treball dels proveïdors, haurà de disposar del dimensionament, la formació i els mitjans adequats per a desenvolupar les tasques assignades.

L'adjudicatari haurà de plantejar de forma explícita, i el més exhaustiva possible, un model de relació amb l'IMI, dissenyat de manera que s'asseguri el correcte acompliment de les seves funcions.

L'esmentat model de relació haurà de fer explícits els rols i responsabilitats del contracte, els nivells de relació i l'estructura i funcionament dels Comitès de relació i coordinació que siguin precisos per mantenir una interlocució permanent amb els actors involucrats en el procés.

Aquest model de relació establirà les figures i els responsables de blocs de serveis o agrupacions de serveis en base a la seva dimensió i/o funcionalitat que cobreixin, així com la responsabilitat de transformació del servei cap al model proposat.

Aquest contracte està basat amb la premissa que l'adjudicatari tindrà les capacitats necessàries i suficients per abordar el contracte, disposant de capacitats expertes en matèries específiques que posarà disposició al personal adscrit al contracte de manera que permeti avançar en les necessitats de manera efectiva i àgil.

L'adjudicatari ha de plantejar el model de relació amb aquests equips especialitzats, indicat les especialitats que es podran disposar en el contracte i com es podran disposar d'aquests serveis experts de manera que es garanteixi que qualsevol necessitat dins de l'abast del contracte es podrà disposar de aquest coneixement i acompanyament en la implementació a les necessitats de l'IMI i Ajuntament.

5.2. ORGANITZACIÓ

Hi haurà d'haver, com a mínim, els següents òrgans de govern:

- Comitè Estratègic.
- Comitè de Direcció.
- Comitè de Seguiment Operatiu.

L'organització del servei s'haurà d'ajustar-se als requisits mínims que s'especifiquen als següents apartats.

5.2.1.**Comitè Estratègic**

Ha de vetllar perquè els objectius del contracte es duguin a terme d'acord als requisits i abast descrites en aquest plec per als dos àmbits del contracte, GRC i Seguretat en Projectes.

Els membres del comitè han d'informar en tot moment dels aspectes més rellevants del seu àmbit compartint en tot moment aquells aspectes transversals i que tenen incidència en diferents aspectes dins l'àmbit de seguretat de l'IMI i l'organització municipal.

D'entre les funcions del Comitè Estratègic es troba la necessitat d'identificar les oportunitats, impediments o desviacions dels objectius que es derivin dels àmbits estratègics corresponents i traslladar les mateixes en les diferents sessions del Comitè que es celebrin, revisar compromisos del contracte i visió global dels mateixos, marcar les directius estratègiques, gestionar i identificar canvis o modificacions d'objectius o canvis d'abast, o modificacions puntuals dels serveis del contracte, sempre dins l'àmbit de l'objecte del contracte. Si s'arribés a donar el cas, des d'aquest Comitè s'elevaran a l'òrgan de contractació aquells aspectes que puguin originar la modificació de contracte o propostes del règim sancionador.

Correspondrà als membres del Comitè Estratègic implantar els objectius i executar dins de l'àmbit de les seves competències aquells aspectes decisoris que així hagin estat adoptats pel Comitè.

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

Es reuneix normalment amb una periodicitat trimestral, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

En formen part:

- Direcció de serveis de Seguretat de la Informació de l'IMI.
- Cap del Departament de Seguretat de l'IMI.
- Responsable de l'Oficina de GRC per part de l'IMI.
- Responsable de l'Oficina de Seguretat en Projectes per part de l'IMI.
- Responsable del Servei per part de l'adjudicatari.

El responsable del servei per part de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Puntualment poden assistir-hi aquelles persones, integrants o no del servei de GRC o de Seguretat en Projectes, que es considerin necessàries en funció dels temes a tractar.

5.2.2.**Comitè de Direcció de GRC**

Les funcions del Comitè de Direcció són les de supervisar la marxa del servei i la presa de decisions que afecten a l'objectiu i abast del mateix, especialment per definir i encarregar tasques sota demanda de nous projectes o iniciatives no identificades inicialment. Aquest comitè farà un seguiment exhaustiu de l'execució dels serveis tecnològics i de negoci dels dos àmbits del contracte, realitzar el seguiment tàctic de les activitats definides al catàleg de serveis i l'assoliment d'objectius.

El Cap de l'Oficina GRC de l'adjudicatari assistirà a les reunions d'aquest Comitè sempre que sigui requerit per qualsevol dels seus membres. Quan ho facin seran responsables de l'elaboració de la documentació de seguiment del servei necessària per a tal fi i també d'aixecar l'acta de les reunions d'aquest Comitè a les que hi assisteixi.

Es reuneix normalment amb una periodicitat mensual, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

En formen part:

- Cap del Departament de Seguretat de l'IMI.
- Responsable de l'Oficina GRC per part de l'IMI.
- Responsable del servei per part de l'adjudicatari.
- Cap de l'Oficina GRC per part de l'adjudicatari.

El responsable del servei de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Puntualment poden assistir-hi aquelles persones, integrants o no del contracte, que es consideri necessari en funció dels temes a tractar

5.2.3.**Comitè de Direcció de Seguretat en Projectes**

Les funcions del Comitè de Direcció són les de supervisar la marxa del servei i la presa de decisions que afecten a l'objectiu i abast del mateix, especialment per definir i encarregar tasques sota demanda de nous projectes o iniciatives no identificades inicialment. Aquest comitè farà un seguiment exhaustiu de l'execució dels serveis tecnològics i de negoci dels dos àmbits del contracte, realitzar el seguiment tàctic de les activitats definides al catàleg de serveis i l'assoliment d'objectius.

El Responsable de Seguretat en Projectes de l'adjudicatari assistirà a les reunions d'aquest Comitè sempre que sigui requerit per qualsevol dels seus membres. Quan ho facin seran responsables de l'elaboració de la documentació de seguiment del servei necessària per a tal fi i també d'aixecar l'acta de les reunions d'aquest Comitè a les que hi assisteixi.

Es reuneix normalment amb una periodicitat mensual, encara que es podrà convocar amb caràcter extraordinari sempre que es consideri necessari.

En formen part:

- Cap del Departament de Seguretat de l'IMI.
- Responsable de l'Oficina de Seguretat en Projectes per part de l'IMI.
- Responsable del servei per part de l'adjudicatari.
- Responsable de Seguretat en Projectes de l'adjudicatari.

El responsable del servei de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Puntualment poden assistir-hi aquelles persones, integrants o no del contracte, que es consideri necessari en funció dels temes a tractar

5.2.4.**Comitè de Seguiment Operatiu GRC**

S'encarrega del dia a dia de l'Oficina. Resol les incidències i conflictes menors que apareguin al llarg de la prestació del servei.

Es reuneix normalment un cop per setmana.

En formen part:

- Responsable de l'Oficia GRC per part de l'IMI
- Integrants de l'Oficina GRC

A petició de l'IMI, o per petició pròpia, també hi poden assistir el Cap de l'Oficina per part de l'adjudicatari i/o el Responsable del servei per part de l'adjudicatari.

El Cap de l'Oficina GRC de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

5.2.5.**Comitè de Seguiment Operatiu Seguretat en Projectes**

L'IMI anomenarà un Comitè de seguiment que s'encarregarà de la gestió del dia a dia de l'execució del contracte. També resoldrà les incidències i conflictes menors que apareguin al llarg de la vida d'aquest contracte. El Responsable del servei de Seguretat en Projectes de l'adjudicatari és l'encarregat de fer les convocatòries i d'aixecar acta de les reunions d'aquest Comitè.

Es podrà reunir quinzenalment.

El Comitè de Seguiment està format com a mínim pel Responsable del servei de Seguretat en Projectes de l'empresa adjudicatària i el responsable del contracte per part de l'IMI. Quan calgui,

es podrà convidar a les reunions del Comitè de Seguiment als membres de l'equip necessaris per a tractar en profunditat determinats temes.

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

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

5.3. **SEGUIMENT DEL CONTRACTE**

L'adjudicatari haurà de presentar un model de seguiment d'aquest contracte.

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

També s'inclourà un quadre de comandament amb un model d'indicadors de compliment dels compromisos associats i un esquema de reporting dels mateixos pel seguiment, control i gestió del servei. Es valorarà el contingut del quadre de comandament, el detall del seu model d'indicadors i la facilitat d'interpretació de l'esquema de reporting.

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

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

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

Informe de seguiment de l'avenç: (mensual)

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

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

Serà objecte de valoració el model de seguiment de contracte que millori el contingut dels informes previstos en aquest apartat i el quadre de comandament proposat que proporcioni un accés més àgil, clar i ajustat a la realitat del servei.

6. METODOLOGIA DEL PLA DE CONTRACTE

L'adjudicatari definirà un Pla de contracte on establirà com portarà a terme els serveis de seguretat previstos sobre les tasques, propostes, projectes i iniciatives que cobrirà el conjunt total de les funcions i tasques objecte del contracte establerts en l'apartat 4 d'aquest plec.

El servei es desplegarà seguint les següents fases:

6.1. LLANÇAMENT DE CONTRACTE

Es presentarà el Pla de Contracte servei amb el model de govern del servei i es definiran les tasques necessàries per crear i activar els serveis les tasques i activitats objecte del contracte. Es definiran les tasques necessàries per crear i activar l'Oficina de govern de la seguretat.

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

Es realitzaran les tasques de comunicació necessàries per informar de la posada en marxa del contracte.

6.2. PLA DE RECEPCIÓ DEL SERVEI

Durant els primers 15 dies naturals a partir de l'inici del contracte es farà la transferència de coneixement dels serveis de govern, de les iniciatives en curs o previstes en aquest contracte detallades en l'apartat 4 d'aquest plec, mitjançant sessions planificades entre l'IMI i l'adjudicatari actual i el nou adjudicatari.

Durant aquest període la responsabilitat del contracte serà del nou adjudicatari. Serà en aquest moment que de forma consensuada s'estableixin els indicadors de nivell de servei (ANS) d'acord amb la proposta de la seva oferta i que hauran de regir per aquest contracte entre l'IMI i l'adjudicatari.

6.3. EXECUCIÓ DEL SERVEI

Es realitzaran les tasques necessàries per la gestió del contracte.

Es planificaran els comitès del contracte.

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

6.4. **RESOLUCIÓ DEL SERVEI**

Es definiran les tasques necessàries per realitzar el traspàs del contracte a l'IMI.

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

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

6.5. **PLA DE DEVOLUCIÓ DEL SERVEI**

Li correspon a l'adjudicatari elaborar el Pla de devolució del contracte sobre el coneixement del conjunt d'iniciatives i projectes que s'han executat dins el contracte

En el Pla de devolució del contracte s'haurà d'incloure totes les activitats de transferència del servei i de coneixement a l'IMI o a un tercer proveïdor, en els casos en el quals així es decideixi per part de la Direcció de l'IMI.

En cas de cessament o finalització del contracte, el proveïdor estarà obligat a tornar el control del serveis objecte del contracte, havent de realitzar en paral·lel els treballs de devolució amb la prestació del servei, sense cost addicional per l'IMI.

Tanmateix el Pla de devolució del contracte haurà de complir com a mínim els següents principis i continguts:

- El termini d'execució serà d'un mes abans de la finalització del contracte.
- Inclourà la metodologia de transferència de coneixement dels aspectes fonamentals d'operació i, com a mínim, descriurà:
  - Suport al nou adjudicatari,
  - Formació i documentació sobre els procediments de negoci i del servei.
- L'accés al maquinari, el programari, la informació, la documentació i altre material utilitzat per l'adjudicatari o l'IMI en la provisió del servei.
- La formació pràctica tutelada, en la qual el personal designat pel l'IMI realitzi els treballs propis de cada procés o funcionalitat tutelats pel personal de l'adjudicatari.
- L'adjudicatari haurà d'oferir tota l'ajuda en la transferència l'IMI, o a terceres parts anomenades per aquest.
- L'adjudicatari assegurarà un correcte traspàs de tots els entregables, assegurant-ne la completesa i que estigui tot actualitzat.

- L'adjudicatari haurà d'oferir un pla per definir les responsabilitats i gestionar la resolució de problemes entre el nou adjudicatari, l'IMI i/o altres adjudicataris.
- Presentarà el pla de devolució que millor aprofiti la feina implementada a les eines en ús i menys disruptiu sigui per l'IMI.
- Durant el període de devolució del contracte, l'adjudicatari ha de complir els acords de nivell de servei. El pla de devolució no ha de causar cap discontinuïtat en el contracte.
- L'IMI no assumirà una dedicació significativa de recursos propis o de la corporació en les activitats de devolució.
- S'establirà el pla per devolució de la migració de la informació de les eines emprades pel servei per tal de ser incorporades en el nou servei.

El pla s'executarà dins el termini del contracte.

Els licitadors detallaran prèviament en la seva oferta un pla de devolució del contracte, indicant les tasques que assegurin el tancament de totes les tasques correctament, la qualitat dels lliurables finals, i de traspassar completament tota la informació a l'IMI. Aquest Pla es presentarà amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa i previsible de la seva realització material.

7. RECURSOS HUMANS

L'adjudicatari proposarà un equip de treball adequat per a l'execució dels serveis.

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

El proveïdor proposarà un equip de treball adequat per a l'execució dels serveis i n'assegurarà la seva estabilitat mentre estigui vigent el contracte. L'adjudicatari indicarà de forma detallada els recursos amb els perfils i les certificacions de cadascú. No obstant, l'IMI considera que **es necessiten com a mínim els següents perfils que es detallen a continuació**, i exigirà que aquests hi participin amb les dedicacions que s'expliciten:

7.1. **FUNCIONS PER PERFIL**

D'acord a les volumetries anteriorment descrites, s'estima necessària la implicació d'un equip mínim equivalent a uns 4,94 FTEs, considerant que el servei inclourà com a mínim 2,36 FTEs dels perfils indicats de GRC i 2,58 FTEs dels perfils indicats de Seguretat en Projectes

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

Perfil	Responsabilitat
Responsable del Servei	Màxim responsable de l'equip de l'adjudicatari, i en conseqüència de la provisió en temps i qualitat dels serveis inclosos en aquest contracte. Actuarà com a Coordinador del Contracte i donarà Suport a la Direcció de Serveis de Seguretat de la Informació de l'IMI en la definició del full de ruta d'evolució del Servei.
Cap d'Oficina GRC	Màxim interlocutor de l'equip, revisa amb la direcció del contracte per part de l'IMI el correcte avenç de les activitats previstes, l'adequació dels recursos humans, i gestiona riscos, desviacions, peticions fora de l'abast inicial, etc. Tasques: • Participació als comitès de seguiment del servei • Reporting de l'evolució del servei als responsables del servei de l'IMI • Definició del catàleg de serveis • Aplicació de les bones pràctiques en la gestió dels serveis TIC • Coordinació del personal que forma part del servei • Nexe d'unió i comunicació entre l'equip de l'Oficina i l'IMI És important que tingui experiència dilatada en projectes de l'àmbit de seguretat de la informació. • Participació Comitès de Seguiment del Servei fent reporting de l'evolució del servei • Definició del catàleg de serveis • Aplicació de les bones pràctiques en la gestió de serveis TIC • Elaboració de quadres de comandament • Reporting de l'estat general del servei, amb indicadors de seguretat en projectes
Responsable del servei de Seguretat en Projectes	Gestiona l'adequació dels recursos humans, i gestiona riscos, desviacions, peticions fora de l'abast inicial, etc. Tasques:

	• Participació Comitès de Seguiment del Servei fent reporting de l'evolució del servei als responsables de l'IMI • Definició del catàleg de serveis • Aplicació de les bones pràctiques en la gestió de serveis TIC • Elaboració de quadres de comandament Reporting de l'estat general del servei, amb indicadors de seguretat en projectes
Consultor GRC	Responsable de l'operativa diària, defineix, gestiona i executa les accions a realitzar en cadascun dels àmbits del contracte. Garanteixen la qualitat dels lliurables. Especialista en estàndards i normatives de seguretat, elaboració de cossos normatius de seguretat, gestió de riscos de seguretat de la informació i eines GRC, així com compliment tècnic de la legalitat. Tasques: • Suport, desenvolupament, elaboració, control, manteniment, modificació i seguiment del marc normatiu corporatiu. • Suport, desenvolupament, elaboració, control, manteniment, evolució, modificació i seguiment de la classificació de la Informació corporativa. • Suport, anàlisi, elaboració d'informes i assessorament del compliment tècnic de les lleis (LOPD, ENS, ENI,...) • Suport, elaboració, control, seguiment d'auditories i Gestió de Riscos. • Control i seguiment dels nivells de compliment de proveïdors de l'IMI. • Participació de Seguretat en el desenvolupament de nous Projectes propis del Departament de Seguretat. • Revisió periòdica del Registre d'incidents de Seguretat TIC corporatiu. • Definició d'estàndards de signatura i Procediment. • Tasques de suport puntuals del Servei. • Gestió i evolució de les eines pròpies de l'Oficina de GRC (Archer, Lucia,...)

Auditor GRC	Especialista en realitzar auditories de protecció de dades, d'Esquema Nacional de Seguretat (ENS) i Sistemes de Gestió de Seguretat de la Informació (SGSI). Tasques: • Definició i aprovació del Pla Anual d'Auditoria • Execució auditories internes de compliment • Donar suport en la execució auditories externes de compliment • Gestionar la implementació de les millores sorgides • Implementació de les millores sorgides • Elaboració d'auditories de Protecció de Dades, en l'àmbit TIC • Elaboració d'auditories de compliment de l'ENS • Auditories i control a Proveïdors • Acompanyament d'auditories de tercers efectuades en els sistemes de l'IMI.
Tècnic sènior especialista en consultoria de seguretat	**Responsable tècnic** de la realització del **servei de Seguretat en Projectes**. Tècnic expert en seguretat, especialitat en seguretat en projectes i SDLC. **Consultor tècnic** amb coneixements en establiment de requisits de seguretat en projectes. Tasques: • Determinació de risc per projecte • Gestió i reporting de la cartera projectes de Seguretat • Definició de controls basats en requeriments establerts • Establiment de plans de remediació • Formació a rols no tècnics involucrats • Suport a implantació de metodologia SDLC segura • Evolucionar la metodologia de SDLC • Elaboració d'informes de riscos

	• Interlocució amb diferents perfils professionals • Gestió de recursos i projectes • Suport d'eines usades al SDLC • Suport a arquitectures basades en microserveis • Gestió de la demanda pròpia de Seguretat
Tècnic sènior especialista en arquitectures de seguretat	**Responsable tècnic** del **servei de Seguretat en el Disseny.** Tècnic expert en seguretat, especialitat en arquitectures de seguretat. Seguretat al lloc de treball, entorns col·laboratius, ofimàtica o serveis al *cloud*. **Arquitecte** amb coneixements d'arquitectures de seguretat, amb intensificació al *cloud*. Tasques: • Disseny de solucions de seguretat • Definició de requisits de seguretat aplicables a noves tecnologies • Elaboració de plans de millora per riscos • Definició d'evidències necessàries per a compliment de requisits • Avaluació del compliment dels requisits • Incorporar i mantenir el llibre blanc d'arquitectures estandarditzades de l'IMI • Estandardització i normalització d'arquitectures • Suport en elements de xarxa de baix nivell • Suport en definició de xarxes segures • Suport i definició en disseny d'arquitectures *cloud* segures • Parametrització d'eines específiques de seguretat • Millora de la seguretat de les arquitectures tècniques

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

7.2. **CARACTERÍSTIQUES PROFESSIONALS**

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

Perfil	Coneixements i experiència
Responsable del servei	Cal que acrediti, durant els últims 5 anys, 3 anys d'experiència en la gestió de contractes relacionats amb projectes dins de l'àmbit de les TIC,
Cap d'oficina GRC	Cal que acrediti, durant els últims 5 anys, 3 anys d'experiència en projectes de l'àmbit de seguretat TIC Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement, en Informàtica o Telecomunicacions
Consultor GRC	Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència en projectes de l'àmbit de seguretat TIC Cal que acrediti participació en 1 o més projectes de l'àmbit d'elaboració de normatives. Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement, en Informàtica o Telecomunicacions
Auditor GRC	Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència en projectes de l'àmbit de seguretat TIC. Cal que acrediti participació en 1 o més projectes de l'àmbit d'elaboració d'auditories de compliment. Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement, en Informàtica o Telecomunicacions
Responsable de Seguretat en Projectes	Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència mínima en projectes de l'àmbit de seguretat TIC Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement, en Informàtica o Telecomunicacions.

Perfil	Coneixements i experiència
Tècnic sènior especialista en consultoria de seguretat	Cal que acrediti durant els darrers 5 anys, 2 anys d'experiència mínima en gestió de projectes des de la vessant de la seguretat i SDLC. Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement, en Informàtica o Telecomunicacions.
Tècnic sènior especialista en arquitectures de seguretat	Cal que acrediti durant els darrers 5 anys, 2 anys d'experiència mínima en projectes de seguretat al cloud. Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement en Informàtica o Telecomunicacions.

Esdevindran objecte de valoració d'acord amb allò previst a la clàusula 10a del PCAP que el perfil a adscriure, si escau, disposi de les següents certificacions:

Perfil	Coneixements i experiència
Cap d'oficina GRC	• Gestió de Serveis TIC (ITIL) • Seguretat de la informació (ISACA o similars)
Consultor GRC	• Gestió de Serveis TIC (ITIL) • Seguretat de la informació (ISACA o similars) • Gestió de riscos (CRISK o similar) • RSA Archer Certified Associate o RSA Archer Certified Professional
Auditor GRC	• Auditories de compliment (ISO27001 Lead Auditor o similar) • Seguretat de la informació (ISACA o similar)
Responsable de Seguretat en Projectes	• Certificació ITIL (a partir versió 3) • PMP • Seguretat de la informació (ISACA o similars)

Perfil	Coneixements i experiència
Tècnic sènior especialista en consultoria de seguretat	• PMP • CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) • AWS Solutions Architect Associate, Azure Solutions Architect Expert o similars. • CSX (Cybersecurity Fundamentals Certificate) • OSCP (Offensive Security Certified Professional)
Tècnic sènior especialista en arquitectures de seguretat	• CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) o • AWS Solutions Architect Associate, Azure Solutions Architect Expert o similars.

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

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

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

- Un període de formació, a càrrec de l'adjudicatari, pel nou membre que s'incorpori a l'execució del contracte.
- Un període de coexistència, d'un mínim de 15 dies, entre la persona que causa baixa i la persona que s'incorpora.

8. CONDICIONS D'EXECUCIÓ

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

8.1. **CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT**

Les Administracions públiques per donar garanties i protecció als ciutadans s'han dotat de RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (d'ara endavant, ENS), que és un marc comú de mesures a implementar per garantir l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informació i serveis que gestionen en l'exercici de les seves competències

Per tal de garantir que les empreses que treballen i col·laboren amb les administracions públiques compleixen amb els requeriments de Seguretat exigits a les Administracions Públiques.

Així doncs, l'adjudicatari haurà d'acreditar la conformitat amb l'ENS de nivell MIG mitjançant alguna de les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.
- Informe d'auditoria de compliment. L'adjudicatari serà responsable de disposar d'un informe d'auditoria (en el que l'ENS formi part del seu abast) de compliment on es detalli que els productes de seguretat, equips, sistemes i aplicacions compleixen amb totes les mesures aplicables de l'Esquema Nacional de Seguretat.

8.2. **LLOC DE PRESTACIÓ DEL SERVEI**

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

És responsabilitat de l'IMI posar a disposició de l'adjudicatari aquelles eines corporatives municipals que li siguin necessàries per al correcte desenvolupament del servei.

En les ocasions que ho requereixin, ja sigui per causes sobrevingudes, per requeriments del servei o per sol·licitud explícita del cap de contracte de l'IMI, es podrà demanar el desplaçament a les oficines de l'IMI per a la prestació d'aquell servei que sigui necessari, essent obligació de l'adjudicatari l'aportació de les eines que siguin necessàries per a la prestació del servei requerit.

La connexió amb l'IMI es podrà fer amb les següents alternatives:

- Mitjançant un enllaç dedicat amb algun dels operadors existents en el mercat. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol actuació necessària per a la posada en marxa de la connexió: esteses de fibra i electrònica addicional, manipulacions de connexions de fibra a la via pública, etc.
- A través d'una connexió al servei Macrolan o VPN de l'adjudicatari actual o del contracte del GIX municipal i amb una connexió d'ample de banda suficient per a garantir un adequat rendiment. L'enllaç a establir serà una connexió Ethernet amb separació i translació d'adreces en el costat de l'adjudicatari. Correran a càrrec de l'adjudicatari els costos derivats de qualsevol adquisició o actuació necessària per a la posada en marxa de la connexió. També serà al seu càrrec la quota mensual de la línia a contractar.

- Alternativament, mitjançat solució VPN (lan-to-lan, si son servidors) o VPN-Client si es per a usuaris remots, sobre l'accés a Internet existent a les dependències de l'IMI d'acord amb la normativa establerta per l'IMI per a l'accés remot als seus sistemes d'informació. És responsabilitat de l'adjudicatari la contractació i manteniment del seu accés a Internet així com disposar d'un equip que suporti aquest tipus de connexions i d'un ample de banda suficient en aquesta línia.

És responsabilitat de l'adjudicatari la contractació i manteniment del seu accés a Internet així com disposar d'un equip que suporti aquest tipus de connexions i d'un ample de banda suficient en aquesta línia.

En cas de dificultats per a l'establiment d'aquest circuit, l'IMI es reserva el dret de comprovar, amb equips de la seva propietat, la causa del problema amb l'objectiu de determinar responsabilitats en la resolució de qualsevol incidència.

Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'adjudicatari. Queden excloses les llicències corresponents a les aplicacions corporatives que l'IMI faciliti a l'adjudicatari tant per a la connexió als sistemes corporatius o per al desenvolupament d'aquelles tasques que requereixin d'una eina propietat de l'IMI.

8.3. **HORARI DE PRESTACIÓ DEL SERVEI**

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

- L'horari de prestació del servei serà el de l'IMI, aplicable als dies que siguin laborables a la ciutat de Barcelona, de dilluns a divendres, de 9:00h a 18:00h.

En casos excepcionals (s'estima com a màxim 6 a l'any), i si és possible de forma prèviament planificada, es podrà requerir l'execució de determinats serveis fora de l'horari normal, incloent disponibilitat en horari nocturn (fins a un màxim de 72 hores). En els darrers 3 anys no s'han hagut de prestar serveis fora de l'horari normal.

Aquests casos es poden donar, per exemple, per:

- Emergències i/o esdeveniments crítics i/o importants per l'Ajuntament de Barcelona amb requeriments directes als serveis d'aquest contracte.
- En desplegaments crítics que es realitzen fora de l'horari de servei, per tal de minimitzar l'impacte al ciutadà amb necessitats directes dels serveis d'aquest contracte.

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

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

Les hores dedicades als serveis previstos en aquest contracte es prestaran en horari laboral de l'IMI tot tenint en compte el calendari de festes de Catalunya i el municipi.

8.4. **DURADA DEL CONTRACTE**

La durada del contracte és la definida al Plec de clàusules administratives particulars, apartat "Durada del contracte".

8.5. **IDIOMA**

Les llengües de treball del contracte seran, per la mateixa naturalesa de la feina, el català i el castellà.

Tot document que es generi amb destinació fora de l'àmbit del contracte haurà de ser redactat en català.

També hauran de ser redactats en català tots aquells documents que tinguin la consideració de lliurables del servei.

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

8.6. **PLA DE QUALITAT**

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

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

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

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

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

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

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

8.7. **QUALITAT DEL SERVEI I TREBALLS REALITZATS**

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

En aquest sentit, l'IMI exigirà l'acompliment dels nivells de servei descrits als apartats *4.3.1. Acord de Nivells de servei (ANS)* i *4.8.4.Acord de Nivells de servei (ANS)* del plec de prescripcions tècniques.

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

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

8.7.1.**Auditories**

8.7.1.1.***Introducció***

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

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

- Periodicitat: semestral.
- Abast: totalitat del servei.
- Serveis a auditar: compliment del contracte amb la qualitat desitjada.

- Equip: Empresa externa i independent.
- Resultat: informe d'auditoria.

8.7.1.2.***Objectiu de les Auditories***

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

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

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

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

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

8.7.1.3.***Procediment d'Auditoria***

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

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

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

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

8.7.1.4.***Resultats de l'Auditoria***

L'auditoria es realitzarà mitjançant revisions dels diferents aspectes que es contemplen en aquest plec, en el pla de qualitat del servei, formació, model de prestació del servei , així com qualsevol

altre pla detallat en aquest plec. L'equip auditor buscarà la conformitat amb els aspectes establerts en aquests documents. Per a cada aspecte revisat existiran quatre possibles valoracions:

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

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

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

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

8.7.1.5.*Resultats de la Revisió*

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

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

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

8.8. **CLÀUSULA DE GARANTIA**

Donat l'objecte del contracte, no aplica demanar clàusula de garantia sobre els treballs desenvolupats.

8.9. **FACTURACIÓ**

Els serveis es facturaran per trimestres vençuts i a partir de l'inici del servei efectiu. L'import a facturar per un trimestre sencer serà el resultat de dividir el preu ofert per aquest servei per l'adjudicatari entre els 12 mesos de servei efectiu del contracte, amb excepció de la primera i darrera factura si el contracte no ha estat formalitzat el primer dia del mes. En aquest cas, el primer i últim termini de facturació contindrà l'import corresponent des del primer dia de servei del contracte fins al darrer dia de servei del trimestre que correspongui.

Addicionalment es sol·licita que en el detall de la factura es faci constar la relació de serveis realitzats.

9. **PROPOSTA TÈCNICA I ECONÒMICA**

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

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

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

Es presentaran dos sobres electrònics, el **sobre B** on s'inclourà la documentació tècnica i aquella que haurà de ser valorada segons els criteris de judici de valor assenyalats en les clàusules del plec de clàusules administratives particulars, i el **sobre C** que haurà de contenir la oferta econòmica i la resta de 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 cada sobre s'ha d'incorporar una relació, en arxiu independent, dels documents que hi conté ordenats numèricament, especialment en el **sobre B** ja que aquest ha de respondre a les explicacions i compromisos sobre tots i cadascun dels criteris de valoració subjectius definits.

En el sobre B s'inclourà la documentació següent **indexada de manera que faciliti la seva localització**. Per a cada apartat i entre parèntesi s'ha indicat el nombre màxim de pàgines de què pot constar i amb tipus de lletra **Arial o Times New Roman, grandària 12 i interlineat simple amb una extensió màxima de 72 pàgines (sense comptar portada ni índex)**.

1.- Resum executiu (màxim 3 pàgines)

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

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

2.- Plantejament general i tècnic del contracte (màxim 10 pàgines)

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

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

3.- Model de relació (màxim 4 pàgines)

En aquesta secció el licitant ha d'exposar el seu enteniment i la seva proposta de models de relació entre l'IMI, l'equip del licitador adscrit al contracte i els equips especialitzats que el licitador proposi posar a disposició del contracte, segons està descrit a l'apartat 5.*1 Model de Relació IMI/Adjudicatari* del plec de prescripcions tècniques, fent especial incís amb el model de relació amb els serveis experts que es demana disposar en el marc dels serveis d'aquest contracte.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

4.- Gestió del risc TIC corporatiu (màxim 6 pàgines)

Presentar la proposta del model de gestió del risc descrit a l'apartat *4.1.1 Gestió del risc TIC corporatiu* del plec de prescripcions tècniques que doni resposta a l'objectiu últim de governar el risc corporatiu en TIC de l'Ajuntament de Barcelona i el seu grup municipal. Es valorarà especialment les millores que l'oferta del licitador aporti a la metodologia descrita en el plec de prescripcions tècniques, així com es planteja gestionar la gestió de riscos (especialment els més crítics) a nivell del grup municipal.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

6.- Auditoria Seguretat Informació (màxim 6 pàgines)

Presentar la proposta d'enfoc i com es realitzaran les auditories millorant i detallant el que es descriu a l'apartat *4.2.3 Plans d'auditoria* del plec de prescripcions tècniques, descrivint com gestionarà aspectes de continguts, metodologia, sessions, evidències i no conformitats i proposta de millores. També es descriuran les eines que es posen a disposició per aquest servei amb les funcionalitats que incorporen, així com totes aquelles condicions que es considerin distintives i que millorin el pla d'auditoria exigit al plec de prescripcions tècniques.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

7.- Control de Proveïdors (màxim 4 pàgines)

Presentar la proposta de metodologia per planificar, executar i fer el seguiment dels diferents tipus de proveïdor de l'Ajuntament, millorant i detallant el que s'explicita en l'apartat *4.2.1 Seguretat en proveïdors* del plec de prescripcions tècniques, tot identificant explícitament les propostes de millora respecte del que s'ha descrit en aquest apartat.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

8.- Quadre de comandament - Seguretat en Projectes (màxim 4 pàgines)

Presentar la proposta de plantejament del quadre de comandament de la Seguretat en el disseny millorant i detallant el descrit en el apartat *4.8.1 Govern i seguiment de la Seguretat en el Disseny (Seguretat en projectes)* del plec de prescripcions tècniques. Es plantejarà l'enfoc i plantejament així com el pla d'implantació del quadre de comandament de la Seguretat en el disseny.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

9.- Metodologia de Seguretat en el Disseny (màxim 8 pàgines)

Presentar la proposta de plantejament del servei de la metodologia de Seguretat en Projectes millorant i detallant el descrit en l'apartat *4.8.2. Metodologia de Seguretat en el Disseny* del plec de prescripcions tècniques, plantjeant l'enfoc general porposada així com detallant les tasques i activitats proposades en les diferents fases (disseny, desenvolupment, pas a producció,..) d'un projecte de desenvolupament.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

10.- Llibre blanc d'arquitectures de seguretat (màxim 4 pàgines)

Presentar la proposta de plantejament per a la construcció del llibre blanc d'arquitectures de seguretat millorant i detallant el descrit en l'apartat *4.9.1. Llibre blanc d'arquitectures de referència*, plantejant l'enfoc general de la construcció del llibre blanc, i detallant l'estructura, l'índex i els aspectes a incloure així com la proposta de tecnologies i arquitectures a abordar i amb una planificació estimativa.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

11.- *Pipeline* DEVSECOPS (màxim 4 pàgines)

Presentar la proposta de revisió i informe resultant que permeti abordar la revisó d'una pipeline les polítiques de detecció de vulnerabilitats de codi i llenguatges emprats a l'IMI així com els components de seguretat implementats en la pipeline que permeti coneixer l'estat de la implemetació de la seguretat en d'una pipeline (DEVSECOPS) segons s'indica a l'apartat *4.9.4. Pipeline DEVSECOPS* del plec de prescripcions tècniques.

No es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà d'aquest número màxim de pàgines especificat per a cada un dels apartats i, aquelles que excedeixin per al global de la proposta.

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

10.CLÀUSULES GENERALS DE SEGURETAT

10.1.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 311/2022 de 3 de maig pel que es regula l'Esquema Nacional de Seguretat (ENS).

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

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

10.2.**CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT**

Pel què fa als aspectes propis de seguretat quan per l'objecte del contracte sigui d'aplicació, es tindrà especial cura de preveure que els productes finals compleixin amb el que estableix el RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS).

Donada la naturalesa del contracte, l'adjudicatari haurà de donar compliment als requeriments establerts a l'ENS pel **nivell MIG**

D'igual manera per qualsevol obligació legal que recaigui en l'Ajuntament, el proveïdor haurà de donar compliment per la part que li correspongui segons l'abast del contracte.

L'adjudicatari haurà d'acreditar la conformitat amb l'ENS mitjançant alguna de les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.
- Informe d'auditoria de compliment. L'adjudicatari serà responsable de disposar d'un informe d'auditoria (en el que l'ENS formi part del seu abast) de compliment on es detalli que els productes de seguretat, equips, sistemes i aplicacions compleixen amb totes les mesures aplicables de l'Esquema Nacional de Seguretat.

L'adjudicatari garantirà l'accés per part de l'IMI a auditar tota la informació necessària per donar compliment a aquestes regulacions (procediments, anàlisi de riscos, registre d'incidents, pla d'adequació, etc.).

D'igual manera, en el cas que es subcontracti, totalment o parcial, els serveis objecte del present contracte, les empreses subcontractades quedaran a totes les mesures de seguretat d'aplicació a l'adjudicatari dins de l'abast dels servis subcontractats. És responsabilitat de l'adjudicatari assegurar-se que l'empresa subcontractada compleix amb el nivell de l'ENS corresponent, així com amb el conjunt de mesures de seguretat determinades en aquest clausulat de seguretat.

10.3.**CLÀUSULA DE PROPIETAT INTEL·LECTUAL**

Tot i reconeixent l'autoria de les persones que els hagin elaborat, 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 ni es permet el seu ús sense autorització expressa d'aquest ajuntament.

L'empresa adjudicatària 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.

10.4.**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.

10.5.**CONFIDENCIALITAT**

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

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

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

L'adjudicatari serà responsable de les violacions del deure de secret que es puguin produir per part del personal al seu càrrec. Així mateix, s'obliga a aplicar les mesures necessàries per a garantir l'eficàcia dels principis de mínim privilegi i necessitat de conèixer, per part del personal participant en el desenvolupament del contracte.

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

11.**CLÀUSULES D'ACCÉS ALS SISTEMES D'INFORMACIÓ**

11.1.**AUDITORIA**

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

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

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

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

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

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

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

11.2.**GESTIÓ D'INCIDENTS**

L'adjudicatari informarà la Direcció de Serveis de Seguretat de la Informació de l'IMI de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per l'IMI.

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

11.3.**DIMENSIONAMENT/GESTIÓ DE CAPACITATS**

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

11.4.**ACCÉS A LA INFORMACIÓ**

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

11.5.**ANÀLISIS FORENSES**

L'execució d'anàlisis forenses és responsabilitat exclusiva del Departament de Seguretat de l'IMI. L'adjudicatari haurà de col·laborar proporcionant la informació requerida i el coneixements de les

plataformes i tecnològics que facin falta. Les peticions de col·laboració es realitzaran a través dels procediments que s'acordin entre el Departament de Seguretat de l'IMI i el Proveïdor.

11.6.**CONTROL D'ACCÉS**

11.6.1.**Accés local**

L'adjudicatari haurà de protegir les estacions de treball i es compromet a complir les següents condicions:

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

11.6.2.**Accés remot**

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

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

11.7.**GESTIÓ DEL PERSONAL**

11.7.1.**Deures i obligacions del personal**

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

L'empresa adjudicatària està obligada a implantar i donar a conèixer al seu personal els mecanismes i controls necessaris per a garantir l'accessibilitat, la confidencialitat, integritat i la disponibilitat de la informació de l'Ajuntament, i de donar-los a conèixer al seu personal.

El Cap de l'Oficina de l'empresa adjudicatària, abans de l'inici de la prestació del servei objecte del contracte, haurà de notificar al seu personal qualsevol obligació a la que l'empresa estigui sotmesa per contracte i formar al seu personal en la política i instruccions de l'Ajuntament que els sigui d'aplicació.

El Cap de l'Oficina haurà d'informar a tothom que presti serveis dins del marc del contracte, dels deures i responsabilitats del seu lloc de treball en matèria de seguretat de la informació i protecció de dades de caràcter personal, especificant les mesures disciplinàries al fet que pertoqui i fer signar al seu personal un document d'acceptació de les obligacions relatives a la seguretat de la informació i protecció de dades de caràcter personal de l'Ajuntament.

El Cap de l'Oficina de l'empresa adjudicatària haurà de mantenir actualitzada, i en tot moment disponible, una llista de les persones adscrites a l'execució del contracte on s'indicarà la data en què van rebre la formació en política i instruccions de l'Ajuntament, així com el document d'acceptació de les obligacions relatives a la seguretat de la informació.

El document d'acceptació de les obligacions signat per les persones adscrites a l'execució d'aquest contracte serà entregat al Responsable de l'Oficina GRC, abans de ser donats els permisos per accedir als Sistemes d'Informació de l'Ajuntament o bé abans de ser facilitada la informació per al correcte compliment del servei contractat, i restarà en poder de l'empresa adjudicatària que haurà de presentar-los quan siguin requerits per l'Ajuntament.

Es contemplarà el deure de confidencialitat respecte de les dades a les que tingui accés, tant durant el període de duració del contracte, com posteriorment a la seva terminació.

L'empresa adjudicatària haurà de mantenir disponible en tot moment la informació o treballs resultants de l'objecte del contracte, amb la finalitat de comprovar el compliment de les mesures i controls previstos en aquest apartat.

11.7.2.**Formació i conscienciació**

L'adjudicatari realitzarà les accions necessàries per conscienciar regularment al personal sobre el seu paper i responsabilitat respecte a la seguretat dels sistemes. Es recordarà regularment:

- Normatives sobre l'ús dels sistemes i tecnologies de la informació i comunicació per part del personal al servei de l'Ajuntament de Barcelona.
- Normativa de seguretat relativa al bon ús dels sistemes.
- Normativa d'identificació i comunicació d'incidents, activitats o comportaments sospitosos que hagin de ser reportats per al seu tractament per personal especialitzat.

L'adjudicatari haurà de formar regularment al personal en aquelles matèries que requereixin per a l'acompliment de les seves funcions, en particular en relació a configuració de sistemes, detecció i reacció a incidents, i gestió de la informació i dades personals en qualsevol tipus de suport.

L'Ajuntament podrà demanar evidències de les diferents accions de formació i conscienciació que l'adjudicatari ha realitzat sobre el personal assignat a l'execució del contracte.

11.8.**CLÀUSULA DE COMUNICACIONS EXTERNES**

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

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

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

11.9.**PROTECCIÓ DEL LLOC DE TREBALL**

11.9.1.**Lloc de treball buit**

L'adjudicatari haurà d'establir una política de "taules netes" respecte a la documentació de l'Ajuntament. Únicament es podrà disposar del material requerit per a l'activitat que s'està realitzant a cada moment.

El material haurà de quedar guardat en un espai tancat quan no s'estigui utilitzant.

11.9.2.**Bloqueig del lloc de treball**

L'adjudicatari garantirà que els seus equips es bloquejaran al cap d'un temps prudencial d'inactivitat, requerint una nova autenticació de l'usuari per reprendre l'activitat.

11.9.3.**Protecció d'equips**

L'adjudicatari es compromet a que els equips que surtin, o puguin sortir de l'empresa adjudicatària, estaran protegits adequadament contra accessos no autoritzats en cas de pèrdua o robatori.

Sense perjudici de les mesures generals que els afectin, es requereix a l'adjudicatari que porti un inventari d'equips juntament amb una identificació de la persona responsable del mateix i un control regular que està positivament sota el seu control. Els usuaris hauran de disposar d'un canal de de comunicació per informar al servei de gestió d'incidents de pèrdues o robatoris, que hauran de ser comunicades a l'IMI.

S'evitarà, en la mesura del possible, que l'equip contingui claus d'accés remot a l'organització. Es consideraran claus d'accés remot aquelles que habilitin un accés a altres equips de l'organització, o unes altres de naturalesa anàloga.

Addicionalment, els equips hauran de disposar:

- Solució antivirus actualitzada a la última versió i configurada per a que realitzi anàlisis regulars de l'equip.
- Política d'actualització que instal·li els últims pegats de seguretat en un temps raonable, prioritzant aquelles actualitzacions crítiques.
- *Firewall* habilitat restringint el tràfic entrant a l'equip al mínim necessari.

11.9.4.**Medis alternatius**

L'adjudicatari garantirà l'existència i disponibilitat de mitjans alternatius de tractament de la informació per al cas que fallin els mitjans habituals. Aquests mitjans alternatius hauran d'estar subjectes a les mateixes garanties de protecció. Igualment, s'haurà d'establir un temps màxim perquè els equips alternatius entrin en funcionament.

11.10.**GESTIÓ D'EXCEPCIONS**

Qualsevol excepció als anteriors apartats no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials al Departament de Seguretat de l'IMI per al seu corresponent tractament i valoració.

S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

12.**CLÀUSULES DE SEGURETAT PER A L'IMPLANTACIÓ DE PRODUCTES**

12.1.**GESTIÓ D'IDENTITATS, AUTENTICACIÓ D'USUARIS**

La gestió d'identitats dels usuaris del sistema haurà de complir les polítiques d'usuaris, administradors i contrasenyes definides per l'IMI les quals es troben a disposició dels sol·licitants.

L'empresa proveïdora haurà de validar i revisar accessos dels usuaris i perfils administradors de forma semestral, i haurà d'establir i implementar els plans d'acció per corregir les mancances identificades. Els comptes d'usuari estaran integrats amb l'eina que l'IMI posa a disposició.

Autenticació interna

Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant, IDP) per a l'autenticació dels usuaris.

La integració amb la solució IDP es podrà fer mitjançant les següents opcions:

- Integració mitjançant l'estàndard OpenID Connect (OAuth 2.0), utilitzant el flux d'autenticació de codi d'autorització amb PKCE (intercanvi de clau codificada)
- En cas de que l'aplicació no suporti l'ús del protocol OpenID Connect, la integració es farà mitjançant l'estàndard SAML 2.0.

Autenticació externa

Els usuaris externs (fora de l'àmbit municipal, empreses i altres persones físiques - clients de l'aplicació) hauran d'autenticar-se mitjançant la solució corporativa (Mòdul Comú d'Autenticació).

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació (2FA), requerint així una verificació de la identitat de l'usuari que sol·licita accés. L'adjudicatari aplicarà el mateix 2FA que sigui d'aplicació a l'Ajuntament i, en cas de no ser possible haurà de justificar aquesta impossibilitat tècnica, tot aplicant un 2FA diferent que haurà de ser validat per l'IMI.

12.2.**AUTORITZACIÓ DELS USUARIS ALS SISTEMES**

L'IMI disposa d'un repositori centralitzat d' autoritzacions dels usuaris corporatius, basat en un directori actiu, que és d'on recull les autoritzacions el IDP corporatiu. L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en aquest repositori central d'autoritzacions.

En cas que l'adjudicatari no pugui delegar l'autorització per impediments greus del sistema, com a mínim, hauran d'integrar-se amb l'eina de gestió i govern de les identitats corporativa per tal de poder relacionar els rols del producte (tècnica de sistemes) amb els rols funcionals definits a GID (capa de negoci).

Aquesta integració podrà ser de dos tipus:

- Integració directa amb la GID, si l'aplicació pot publicar els usuaris i perfils a través d'un servei web que es pugui consumir mitjançant un connector des de l'eina de gestió d'identitats.
- En cas de no ser possible la connexió directa amb la GID, l'aplicació haurà d'enviar un fitxer diari a la GID i configurar un connector de processament de fitxers per tal de representar les autoritzacions a l'eina.

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats.

Perfilat d'usuaris

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i la Direcció de serveis de Seguretat de la Informació de l'IMI.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.
- Mínim privilegi, els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir les seves obligacions.
- Necessitat de Conèixer, els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.
- Capacitat d'autorització, només i exclusivament el personal amb competència d'autorització, podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.

La gestió de permisos haurà de ser en base a perfils i rols, podent un usuari tenir múltiples perfils. Els usuaris només podran accedir a aquelles funcions que tinguin expressament autoritzades. La implementació ha de permetre la implementació de matrius de segregació de funcions i l'agilitat en l'administració d'aquests permisos.

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant rols de seguretat, entenent com a rol una entitat que dona accés a una sèrie d'operacions.

Sota la premissa d'aquests criteris generals, l'adjudicatari haurà de dissenyar el joc de permisos i autoritzacions requerits pels sistemes d'informació implementats, en base al document 'Pla d'Autoritzacions'. Aquest document serà revisat i actualitzat per l'adjudicatari per incloure nous punts a tractar o adaptacions dels punts existents.

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

Aquest plec de prescripcions tècniques ha estat emès per la Sra. Neus Bellavista Arimany, tècnica responsable del contracte, adscrita a la Direcció de serveis de Seguretat de la Informació de l'Institut Municipal d'Informàtica, amb el vistiplau de:

David Esteban de Haro

Direcció de Serveis de Seguretat de la Informació de l'IMI

14.ANNEXOS

14.1. ANNEX 1: ABAST A ORGANITZACIÓ MUNICIPAL

L'abast del Plec són els sistemes d'informació en què l'IMI proveeix les TIC i que per tant, exerceix com a responsable dels Sistemes d'aquestes gerències o entitats municipals. Aquesta llista pot variar, pot incorporar-se alguna entitat sota el paraigües de l'IMI, tot i que no està previst en aquests moments.

Per a establir el govern de la seguretat de la informació a nivell estratègic de tot l'Ajuntament, l'abast s'amplia a la columna "grup Municipal", en especial a les entitats públiques empresarials i Societats Municipals Mercantils. Essent cada entitat la que implementi el govern de la seguretat però de manera pautada i coordinada per tal d'obtenir un nivell de seguretat i de risc municipal.

Aprovisió de serveis / IMI - Responsable dels Sistemes d'informació	Grup Municipal
Alcaldia	Entitats Públiques empresarials
Gerència Municipal	Institut de Cultura de Barcelona (ICUB)
Gerències d'Àrea	Institut Municipal de Parcs i Jardins (IMPiJ)
Gerència d'Àrea de Recursos i Transformació Digital	Institut Municipal de l'Habitatge i Rehabilitació de Barcelona (IMHAB)
Gerència d'Àrea d'Urbanisme i Habitatge	Institut Municipal d'Urbanisme (IMU)
Gerència d'Àrea de Mobilitat, Infraestructures i Serveis Urbans	Societats Mercantils Municipals
Gerència d'Àrea de Drets Socials, Salut, Cooperació i Comunitat	Grup Barcelona d'infrastructures (BIMSA)
Gerència d'Àrea de Cultura, Educació, Esports i Cicles de Vida	Informació i Comunicació de Barcelona, SA (ICB)
Gerència d'Àrea de Seguretat, Prevenció i Convivència	Barcelona Activa SAU SPM (BASA)
Gerència d'Àrea d'Economia i Promoció Econòmica	Barcelona Cicle de l'Aigua (BACSA)
Gerències sectorials	Foment de Ciutat SA
Gerència de Serveis Generals	Grup Barcelona de Serveis Municipals (BSM)
Gerència de l'Arquitecta en Cap	Fundacions i Consorcis
Gerència de Persones, Organització i Administració Electrònica	Consorci del Besos
Gerència de Serveis Urbans i Manteniment de l'Espai Públic	Consorci del Mercat de les Flors
Gerència de Pressupostos i Hisenda	Consorci MNAC
Gerència d'Urbanisme	Consorci Museu de Ciències Naturals
Gerència de Promoció Econòmica	Consorci de Biblioques de Barcelona
Gerències territorials	Consorci Local Local/ret
Gerència de Coordinació Territorial i Proximitat. Districtes	Consorci de Turisme
Gerència del Districte de Ciutat Vella	Fundació Barcelona Capital Nautica
Gerència del Districte de l'Eixample	Fundació Barcelona Cutura
Gerència del Districte de Sants- Montjuïc	Fund. Barcelona Mobile World Capital
Gerència del Districte de les Corts	Fundació Carles Pi i Sunyer
Gerència del Districte de Sarrià - Sant Gervasi	Mercabarna
Gerència del Districte de Gràcia	Red Internacional de Ciutats Educadores
Gerència del Districte d'Horta- Guinardó	Fundació Mies van der Rohe
Gerència del Districte de Nou Barris	Agencia d'Ecologia Urbana de Barcelona
Gerència del Districte de Sant Andreu	Institut Infantil i Adolescencia
Gerència del Districte de Sant Martí	Consorci d'Educació de Barcelona
Organismes autònoms locals	
Institut Municipal d'Informàtica (IMI)	
Institut Municipal de Serveis Socials (IMSS)	
Institut Municipal d'Hisenda (IMH)	
Institut Municipal de Persones amb Discapacitat	
Institut Municipal de Mercats de Barcelona (MERCATS)	
Institut Municipal del Paisatge Urbà i Qualitat de Vida	
Institut Barcelona Esports (IBE)	
Institut Municipal d'Educació de Barcelona (IMEB)	

14.2. **ANNEX 2: VOLUMETRIA DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT**

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

Volumetria aproximada dels SISTEMES D'INFORMACIÓ	
Núm. de SI	242
Protecció de Dades	A la URL: https://seuelectronica.ajuntament.barcelona.cat/sites/default/files/relacio_tractaments.pdf podeu trobar la relació de tractaments declarats de l'Ajuntament de Barcelona. Del total, aproximadament el 90% són gestionats per l'IMI.

En els últims 3 exercicis s'ha participat en diferents intensitats en actuacions repartides de la següent manera:

	2021	**2022**	**2023**
Incidents de seguretat	71	97	48

14.3.**ANNEX 2B: VOLUMETRIA DE SEGURETAT EN PROJECTES**

Es detalla a continuació la volumetria de la participació en projectes i projectes de seguretat en que ha participat el Departament de Seguretat de l'IMI.

En els últims 3 anys s'ha participat en diferents intensitats en 84 projectes i 42 suports a les licitacions de projectes TIC repartits amb diferents intensitats. De la participació en 84 projectes. La dedicació prevista d'1 FTE cobreix la participació en 25 projectes per any (exercici).

14.4.**ANNEX 3: INFORMACIÓ ADDICIONAL / ACLARIMENTS**

L'IMI posarà a disposició la següent adreça de correu on els licitadors podran fer les seves consultes: voliveras@bcn.cat

En l'assumpte del correu indicar:

R0031 **-** *Contracte Oficina GRC i Oficina Gestió de Projectes*

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

Per tal que les empreses licitadores interessades a presentar oferta puguin aclarir els dubtes que els hi sorgeixin, l'IMI posa a la seva disposició les bústies de correu abans indicades per qüestions tècniques i la d' imi_gestio_contractacio@bcn.cat per consultes de caràcter administratiu.

Així mateix, s'indica que, inicialment, no es convocarà sessió informativa per a aquesta licitació. Malgrat això, si alguna de les empreses licitadores estigués interessada a realitzar-la, pot fer-ne la petició a través del correu imi_gestio_contractacio@bcn.cat.

Les consultes rebudes dins dels 3 dies hàbils anteriors a la data de finalització del termini de presentació de proposicions es respondran i es publicaran" al perfil del contractant de l'IMI:

https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903