Ajuntament
de Barcelona
Institut Municipal d'Informàtica
Direcció de Qualitat i Seguretat

Plec de prescripcions tècniques per a la contractació dels Serveis d'Oficina de Govern, Risc i Compliment (GRC) i Oficina de Seguretat en Projectes l'Ajuntament de Barcelona i implantació de les eines necessàries per a la prestació dels serveis, 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, etc. sempre amb la vocació de servir a la ciutadania i a realitzar la gestió de la ciutat que té encomanada de forma òptima, àgil i eficient.

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

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

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

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

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

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

- Incrementar els Serveis de seguretat TIC
- Dotar a l'Ajuntament d'una estructura que asseguri el compliment de la seguretat i la minimització dels riscos de Seguretat TIC corporatius.
- Assegurar un Marc Normatiu de referència per l'Ajuntament
- Garantir el compliment de la legalitat (ENS, RGPD, eIDAS, LPACAP...)
- Implantar Projectes de Seguretat per donar resposta a les necessitats TIC en matèria de seguretat i protecció

- Protegir els projectes del pla de digitalització: Establir a partir dels riscos els requeriments de seguretat dels projectes del Pla de transformació digital. Establir, implementar i governar el model i les condicions de seguretat per a tots projectes i iniciatives que se'n deriven del Pla de transformació Digital de l'Ajuntament de Barcelona.
- Tenir Govern dels accessos TIC a partir dels principis de mínim privilegi i necessitat de saber per tal de poder conèixer qui fa què i quan dins dels sistemes d'informació i infraestructures TIC de l'Ajuntament.
- Disposar de vigilància activa, reactiva i preventiva de la seguretat

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

Marc de Seguretat : línies d'actuació

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

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

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

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

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

Estableix els serveis següents:

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

En l'àmbit **de Seguretat en el Disseny**:

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

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

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

- **<u>Serveis d'Identitats i Accessos</u>**: Arquitectura d'identitats, autenticació, autoritzacions i controls d'accés (CAAA). Aquest servei ha definir els processos i tecnologies pel govern de les identitats, credencials, autoritzacions i accessos de tot l'Ajuntament, amb l'objectiu de garantir la protecció requerida i proporcional de la informació i serveis TIC corporatius.

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

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

Estableix els serveis següents serveis que conformaran el Centre d'Operacions de Seguretat (**SOC – Security Operations Center)**:

- **<u>Serveis de Preventiu.</u>** El servei de seguretat preventiva ha de disposar i ingerir múltiples fonts de ciberintel·ligència i realitzar proves d'intrusió d'infraestructures i serveis amb

la finalitat de garantir que les infraestructures o serveis siguin segurs i de realitzar la gestió completa del cicle de vida de les vulnerabilitats i posterior revisió. També ha d'assessorar en la definició de les arquitectures dels sistemes i tecnologies que té actualment l'IMI, que dintre de la seva funció de donar servei informàtic a l'Ajuntament de Barcelona, necessita per donar el correcte i segur servei, analitzant les millores que es poden implantar relacionat amb les novetats tecnològiques del mercat i els nous paradigmes d'atacs informàtics que es poden patir.

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

I per tal de fer un pas endavant, s'estableix en aquest contracte la licitació dels Serveis de GRC dins de l'àmbit de Govern de la Seguretat i la participació de Seguretat en Projectes en l'àmbit de la Seguretat en el Disseny i Projectes

2. OBJECTE

Aquest contracte té per objecte dos grans àmbits dels introduïts a l'apartat anterior, govern de la seguretat i seguretat en projectes.

2.1. EN L'ÀMBIT DEL GOVERN DE LA SEGURETAT

La prestació de serveis de govern de la seguretat mitjançant una oficina tècnica encarregada de garantir un 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, i la legislació aplicable, inclòs el marc normatiu propi de l'IMI i la jurisprudència i resolucions dictades en aquest àmbit per tribunals i organismes independents.

- Govern de la seguretat de la informació
  - Govern de la seguretat corporativa
  - Gestió del risc corporatiu
  - Gestió del cos normatiu de seguretat
- Control i seguiment de la normativa

- Seguretat en proveïdors
- Control normatiu
- Plans d'auditoria

- Divulgació normativa
  - Divulgació
  - Formació
- Suport en matèria de seguretat de la informació
- Classificació de la informació
- Gestió del registre d'incidents de seguretat
- Gestió d'excepcions

2.2. **EN L'AMBIT DE LA SEGURETAT EN 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, mitjançant els procediments, controls i tasques durant el cicle de vida dels projectes, augmentant el nivell de protecció dels sistemes de l'Ajuntament de Barcelona i garantir-ne la gestió de la seguretat en totes les etapes del cicle de vida de cada projecte.

- Servei de Seguretat en Projectes
- Seguretat en el disseny
- Projectes específics 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**

En l'àmbit de la governança i la seva oficina l'abast dels serveis inclou tots els Sistemes d'Informació de l'Ajuntament de Barcelona i organització Municipal classificats i gestionats per l'IMI i 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.

En definitiva, els diferents dominis que determina l'estàndard internacional ISO 27002 i que es troben incorporats en el cos normatiu de l'Ajuntament que està en permanent revisió l'IMI per la seva completa adequació als canvis normatius que es produeixin.

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

Es pot trobar més informació sobre la volumetria dels sistemes d'informació gestionats per l'IMI a l'apartat *14.1 Annex 1A Volumetria dels sistemes d'informació de l'Ajuntament* d'aquest plec.

També forma part de l'abast d'aquest contracte l'assessorament a l'Ajuntament en matèria de seguretat TIC de sistemes no gestionats per l'IMI i en la definició dels compliments i controls generals Corporatius (cos normatiu i plans de ciberseguretat) que han de desenvolupar i complir aquests Ens/Organismes .

En l'àmbit de la participació de Seguretat en Projectes l'abast inclou tots els projectes que actuen en els sistemes d'informació i components TIC de l'Ajuntament de Barcelona gestionats per l'IMI i/o connectats a la xarxa corporativa a través dels seus serveis. Això inclou serveis *on-premise*, en el *cloud* públic i en *clouds* privats.

L'abast del servei no és únicament projectes de desenvolupament programari sinó que qualsevol classe de projecte TIC o desplegament de serveis en entorns TIC de canvi que es produeixin en els sistemes de l'Ajuntament i/o la posada en marxa de nous serveis i sistemes.

Es pot trobar més informació sobre la volumetria dels sistemes d'informació gestionats per l'IMI a l'apartat *14.2 Annex 1B Volumetries de Seguretat en Projectes* 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 dos anys es realitzaran canvis progressius orientats a implantar un model de serveis evolucionat i, el contracte derivat d'aquest plec no n'estarà al marge.

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

- L'IMI és en tot moment responsable del disseny dels processos relatius als serveis TIC que proporciona.
- L'IMI facilitarà les eines bàsiques de suport a l'operativa i la gestió dels serveis.
- L'adjudicatari del present contracte serà responsable de la implantació de les diferents versions del model de l'IMI que es vagin consensuant, en el conjunt dels seus equips i en el seu àmbit de servei.

- L'adjudicatari acceptarà tenir una actitud oberta vers aquesta evolució i participarà en la mateixa, proporcionant la realimentació oportuna, alhora que aportant solucions a problemes i riscos identificats.

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

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 ARCO, consentiments, procediments de declaració de tractaments, acords d'encarregat de tractament,...), que estan sota la responsabilitat de la Oficina del Delegat de Protecció de Dades i que són coordinats mitjançant la Taula de Protecció de Dades.

També queden exclosos serveis d' adquisició de llicències de software per la 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 de 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 a aquest 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 d'informació.

Per tal d'assolir aquest objectiu, serà necessari treballar en les següents línies d'actuació:

4.1.1.**Govern de la Seguretat Corporativa**

Dins d'aquest servei es contemplen les estructures de govern de la Seguretat a partir de la definició dels rols i responsabilitats que tindran cadascun dels actors implicats dels comitès de Seguretat de la Informació i de la Taula de Protecció de Dades.

La celebració dels comitès definits permetrà obtenir el control i la presa de decisions sobre temes rellevants i que podrien tenir un impacte elevat tant organitzatives com econòmiques en l'àmbit de la Seguretat de la Informació dins del marc de l'Organització Municipal.

Actualment hi ha definit un model de seguretat i estructures de comitès dins de l'àmbit de l'IMI. El servei haurà de mantenir aquestes eines de govern i haurà de consolidar i madurar el model de Govern de Seguretat de la informació revisant el model i establint la organització en la seva

visibilitat, govern i control en l'Ajuntament. L'eix central per aquesta evolució del model serà l'aprovació per part de l'Ajuntament de la política de seguretat corporativa.

Per aquesta evolució es procedirà a la millora de les eines de mesura i control d'indicadors de la seguretat, gestió de riscos i la capacitat acurada de presa de decisions.

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

- Planificar el Servei general amb revisions anuals, establint enfoc per abordar el servei, àrees d'actuació, fites a assolir i recursos i serveis implicats.
- Definició dels plans de Ciberseguretat dins dels programes de seguretat
- Seguiment del Pla de Ciberseguretat de la Informació.
- Seguiment i evolució del model d'estructures i comitès de Seguretat de la informació, rols i responsabilitats corporatives en matèria de seguretat.
- Manteniment i evolució de la política de seguretat corporativa.
- Celebració de comitès de Seguretat de la Informació.
- Evolució del Quadre de comandament. Seguiment i evolució de les mètriques de seguretat. Interpretació dels indicadors. Suport en informes i comitès de direcció:
    - Nivell d'implantació del cos normatiu
    - Grau de compliment ENS
    - Indicadors de Protecció, vulnerabilitats i incidències
    - Indicadors de Ciberseguretat
- Reporting a l'estat i a les gerències del grau de compliment i adequació a l'ENS.
- Elaboració de la Memòria anual de l'estat de la seguretat corporativa.
- Establir, conjuntament amb el responsable de cada actiu amb informació corporativa, el nivell de criticitat de la informació continguda. Aquest nivell s'establirà d'acord amb el que es determini en el procediment corresponent.

Aquestes activitats es treballaran principalment pel coneixement i control de la seguretat de la informació, de manera que la Direcció i les Gerències Ajuntament tinguin visibilitat i control sobre aquest aspecte.

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

Descripció	Tasques	Volumetria	Lliurables
Establir pla del Servei anual	Establir el pla del servei alineat amb l'Estratègia i Programa de Seguretat corporatiu amb revisions de millora de la proposta objecte del plec per ajustar a les necessitats de seguretat corporatives.	1 revisió anual per ajustar el Servei a les necessitats corporatives.	Informe de resultats de la revisió anual.
Tendències de ciberseguretat	Informar de les tendències en ciberseguretat. Reportant les tendències emergents en el moment en què es detectin	1 informe anual 4 comunicacions de tendències emergents	Informe de tendències ciberseguretat
Estructures, comitès, rols i responsabilitats	Configuració d'estructures i comitès de Seguretat de la informació. Definició de rols i responsabilitats corporatives.	1 definició de Rols i responsabilitats corporatives. 1 constitució del comitè de seguretat en àmbit Ajuntament de Barcelona	Primera acta del comitè. Document d'Aprovació de la norma de rols i responsabilitats.
Celebració de comitès de Seguretat de la Informació.	Preparació de les sessions dels comitès i elaboració d'actes i seguiment dels compromisos.	1 bimensual Comitè IMI 1 semestral a Ajuntament de Barcelona	Actes dels Comitès
Política de seguretat corporativa.	Establir la política de seguretat corporativa.	Política aprovada per decret d'alcaldia o mecanisme equivalent per delegació	Document d'aprovació de la política.

Descripció	Tasques	Volumetria	Lliurables
Proposta d'implantació gradual d'un Quadre de Comandament	Definir, revisar o millorar un sistema de controls que permeti mesurar el nivell d'implantació del cos normatiu mitjançant auditories periòdiques a les instal·lacions gestionades per l'IMI, així com als diferents proveïdors que li donen servei. La Proposta ha d'incloure el pla d'implantació gradual i els elements de report periòdics.	1 Proposta Mínim 4 informes anuals. 4 Informes executius per Comitès Seguretat	Proposta del Sistema de mesura i indicadors. Informes resultants.
Definició del pla de ciberseguretat	Establir conjuntament amb el Responsable de Seguretat per definir el pla de ciberseguretat (PAM del mandat) Ha de contenir: definició, pressupostos i executors	1 Pla de ciberseguretat per mandat 1 pla concret per resoldre alguns risc específics (anual)	Pla de Ciberseguretat 1 Pla específics
Revisió del pla de ciberseguretat	Revisar i actualitzar el pla de ciberseguretat	1 revisió anual	Document de revisió del pla de ciberseguretat
Riscos i modelat amenaces	Formalitzar la gestió i escalat de riscos de Seguretat de la informació a nivell de Gerències i comitès.	1 Procediment de gestió 1 matriu d'escalat de riscos	Document d'aprovació procediment al Comitè de l'IMI
Establir la criticitat de la informació corporativa	Establir la criticitat de la informació corporativa a alt nivell	Document de Criticitat	Document d'aprovació criticitat al Comitè de l'IMI

Descripció	Tasques	Volumetria	Lliurables
Informe Periòdic de compliment	Elaborar els informes periòdics en relació amb el resum de compliment en matèria de Seguretat del cos normatiu i les legislacions aplicables.	6 informes anuals	Informes de nivell de compliment en matèria de seguretat
Informar a Gerències sobre Protecció de la informació i sobre els seus Sistemes d'Informació.	Informar mensualment a les gerències dels incidents de seguretat, autoritzacions de sortida d'informació i revisions d' accessos segons el procediment establert.	Enviament informe Mensual	Correus electrònics d'enviament mensual als Referents IMI de cada gerència o equivalent
Reportar als ens municipals i a l'estat de la seguretat de l'ENS	Reportar a les gerències i organismes autònoms l'estat de l'adequació a l'ENS dels Sistemes d'informació sota la seva responsabilitat executiva. Reportar al Govern espanyol l'estat de la seguretat segons indicacions de les guies a la eina que posen a disposició per tal efecte (INES)	15 reports anuals a entitats corporatives 1 report anual estat	15 reports entitats 1 reporting estat

4.1.2.**Gestió del risc TIC corporatiu**

Aquest servei respon a l'objectiu últim de governar el risc i donar una cobertura total a totes les Gerències i organismes de l'Ajuntament de Barcelona,

El servei de Risc Tecnològic té per objectiu la identificació, avaluació i seguiment dels riscos de seguretat tecnològics de l'Ajuntament de Barcelona. D'acord a aquest abast, el servei focalitza majoritàriament els seus esforços en el seguiment i gestió dels riscos identificats en els proveïdors TIC de l'Ajuntament de Barcelona i la Organització Municipal.

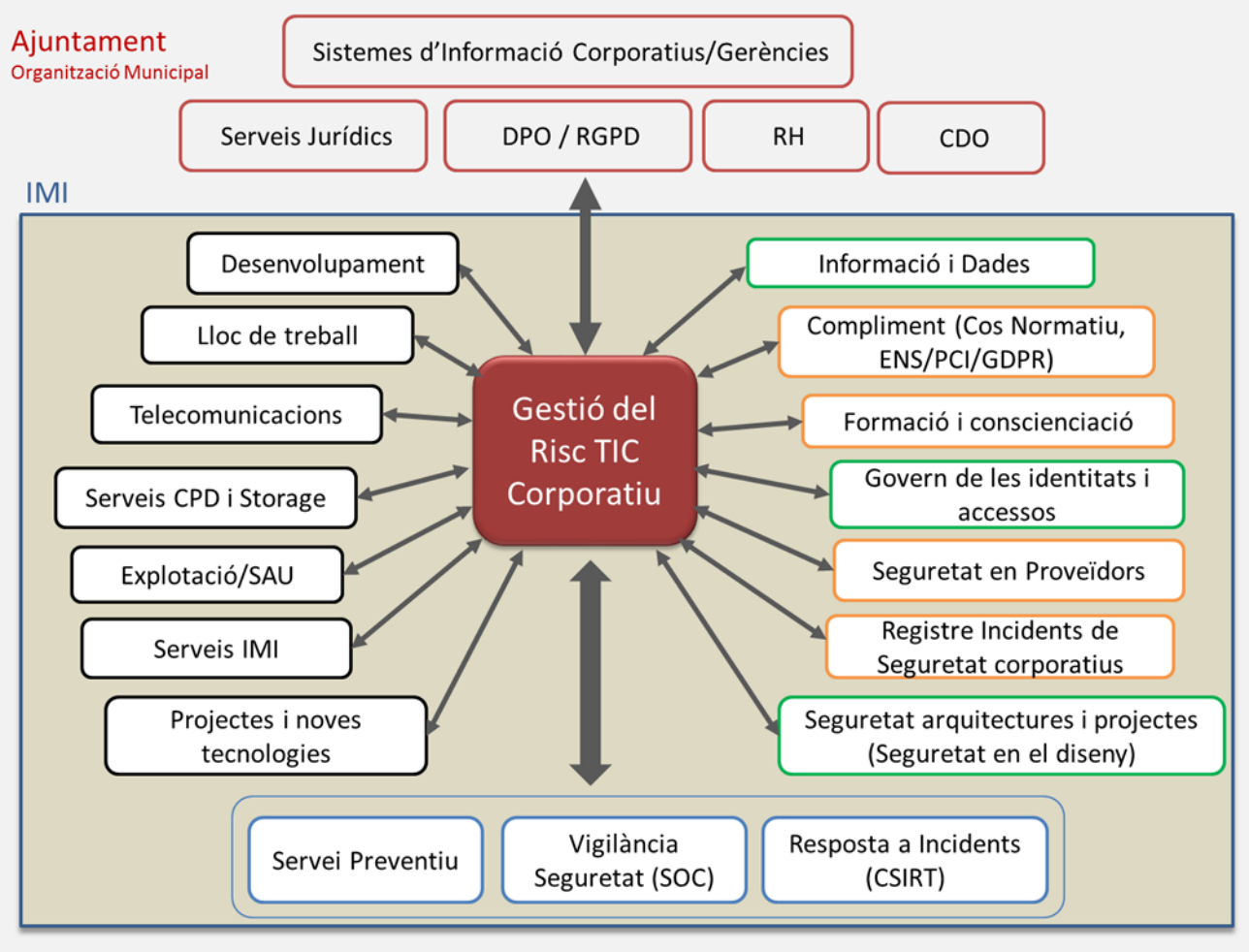
Aquesta visió s'allunya d'una visió on el risc és directament proporcional a un número de controls que no es compleixen. Per això, l'àmbit de la Gestió del Risc tecnològic té una relació estreta amb la resta d'àrees operatives i de projectes de l'IMI, per poder valorar millor aquesta valoració del Risc Tecnològic d'una manera més àmplia.

L'Oficina de GRC establirà una metodologia que satisfaci els requisits legals i de normativa interna per a la valoració i determinació de el risc dels actius de l'Ajuntament. Es definiran els criteris per al report periòdic dels nivells de risc així com el mecanisme de notificació en cas de superar-se la gana de risc.

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.



Per tractar els riscos de seguretat més rellevants identificats pel servei i establir plans s'establiran els següents grups de treball:

- Comitè de Seguretat de l'IMI (Bimensual): seguiment a nivell de Direcció dels riscos de seguretat més rellevants i acordar el seu tractament si aquest repercuteix dins de 'IMI o establir com s'escala i gestiona si aquest repercuteix escalar fora de l'IMI i a l'Ajuntament.
- Taula Operativa de Seguretat (reunió bimensual): seguiment a nivell de responsables de serveis operatius de l'IMI dels riscos de seguretat de CPD, lloc

de treball, comunicacions, aplicacions, referents sectorials. En aquest comitè es revisen els riscos del comitè de Seguretat IM i es concreta un pla d'acció.

- Comitè de Projectes: per reportar el nivell de risc en que surten els projectes i escalar riscos rellevants.
- Comitè de Seguretat a nivell d'Ajuntament (Semestral a partir de quan es constitueixi o en si és requerit explícitament des de l'Ajuntament encara que no estigui formalitzat el Comitè)

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

- Catàleg d'amenaces
- Desenvolupament i aplicació de la metodologia de gestió del risc
- Formalització de la participació de la direcció de l'IMI i l'Ajuntament en la gestió del risc
- Identificació de nous riscos
- Identificació de propietaris del risc
- Seguiment dels riscos
- Indicadors de la gestió del risc

4.1.2.1.*Catàleg d'amenaces*

El Servei de GRC mantindrà i millorarà una metodologia per a la gestió del catàleg d'amenaces que contempli tant el mecanisme d'identificació com el seu inventariat. Ha d'establir a més un criteri per a la valoració de les amenaces i la seva actualització, de manera que serveixin com a base permanent del corresponent anàlisi de riscos.

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

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

L'adjudicatari s'haurà d'adscriure a 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, sobre la qual es poden donar d'alta riscos i associar-los al propietari.

La metodologia ha de permetre:

- Identificar i utilitzar criteris de valoració homogenis que faciliti als responsables la categorització de sistemes d'informació d'acord amb l'Esquema Nacional de Seguretat.
- 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.

4.1.2.3.*Formalització de la participació de la direcció de l'IMI i l'Ajuntament en la gestió del risc*

Als comitès de Seguretat bimensuals, es du a terme el seguiment del mapa de riscos corporatius, el qual recull els riscos de seguretat de la informació més rellevant que cal tractar de forma prioritària.

L'adjudicatari haurà de dona suport en l'elevació de la gestió del risc (per exemple definició de l'apetit al risc, presa de decisions sobre els riscos identificats, etc.) a les capes directives de l'IMI i l'Ajuntament mitjançant la preparació d'informes. sessions divulgatives, etc.

4.1.2.4.*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 poder detectar i escalar riscos de seguretat de la informació, els quals han de poder-se transmetre pels canals disposats segons la naturalesa del mateix (Archer, Comitè de Seguretat, seguiment a proveïdors,...).

Els *inputs* interns a partir dels quals el servei haurà d'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.

4.1.2.5.***Identificació de propietaris del risc***

Com a part central en la gestió del risc, és necessari la identificació del propietari del risc per tal de poder-ho escalar i fer el posterior seguiment del mateix.

4.1.2.6.***Seguiment de riscos***

Els riscos identificats s'han de gestionar per tal de que el risc residual associats 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 necessari la definició d'un pla de mitigació d'aquells riscos que el seu tractament ho requereixi.

4.1.2.7.***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.

Per tractar els riscos rellevants identificats pel servei GRC i establir plans d'acció coordinats per a la seva mitigació, s'hauran de tractar amb reunions periòdiques en els fòrums que pertoqui dins de la organització Municipal/Ajuntament. S'ha de fer l'incís que aquests fòrums a mida que la seguretat maduri en la organització, anirà variant o afegint actors.

Del resultat del servei es passarà i coordinarà amb el servei de govern de la Seguretat i el Risc perquè incorpori en el quadre de comandament. Aquest quadre és mantingut i actualitzat de forma continua i s'estructura que el servei de Govern de la Seguretat indiqui.

4.1.2.8.***Lliurables***

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

Descripció	**Tasques**	**Volumetria**	**Lliurables**

Metodologia d'Anàlisis de Riscos	Anàlisis de la metodologia actual i detecció de punts de millora amb indicació de com millorar la metodologia	1 proposta anual	Proposta anual de millora de la metodologia
Informes de seguiment de riscos	Preparar informes de seguiment dels riscos per escalar al comitè de Direcció	6 informes anuals	Informe 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 propostes anuals	Document de proposta dels indicadors de risc
	Revisió dels indicadors proposats.	1 revisió cada 3 mesos	Informes de revisió dels indicadors
Quadre de comandament del risc	Alimentar el Quadre de Comandament de Seguretat amb els riscos identificats	1 actualització trimestral	Informació per actualitzar Quadre de Comandament

Per avaluar el nivell de maduresa actual de la Gestió de Riscos corporatiu s'incorpora a l'apartat *14.4 Annex 3: Gestió de Riscos*, informació relativa al Catàleg d'amenaces i a les plantilles usades per definir els riscos i per resumir el risc identificat.

4.1.3.**Gestió del Cos Normatiu**

El govern de la Seguretat de la Informació necessita un marc normatiu que serveixi de **referència tant sobre l'estratègia de seguretat** a seguir en els àmbits d'actuació, **com d'ajuda en la presa de decisions**. Amb aquesta motivació, es defineix el conjunt d'estàndards a seguir i es gestionen per mantenir-los actualitzats i alineats.

Les activitats relacionades amb el cos normatiu:

- Identificació de nous requeriments: de normes, lleis, polítiques a aplicar i riscos a mitigar, entre d'altres.

- Revisió i evolució del marc normatiu, per mantenir-lo actualitzat a les normes aplicables en cada moment.

El marc normatiu serveix de base per **definir els controls a seguir i el seguiment del seu compliment o incompliment**, i permet establir accions per tal de reduir les mancances de seguretat i poder garantir-la dins de la normativa establerta.

El cos normatiu es troba estructurat en 4 nivells:

- Política - Declaració d'alt nivell dels objectius, directrius i compromisos de l'Ajuntament de Barcelona per dur a terme la Gestió de la Seguretat de a Informació.
- Normes - Les normes descriuen l'objectiu de control i desenvolupen les pautes a seguir per assolir els objectius de control que corresponguin.
- Procediments - La materialització dels controls es documenta als procediments. Incloent els controls de l'ENS que no contempli la ISO.
- Documents operatius - Tots els documents que complementen al procediments, ja poden ser guies, instruccions operatives, formularis, etc.

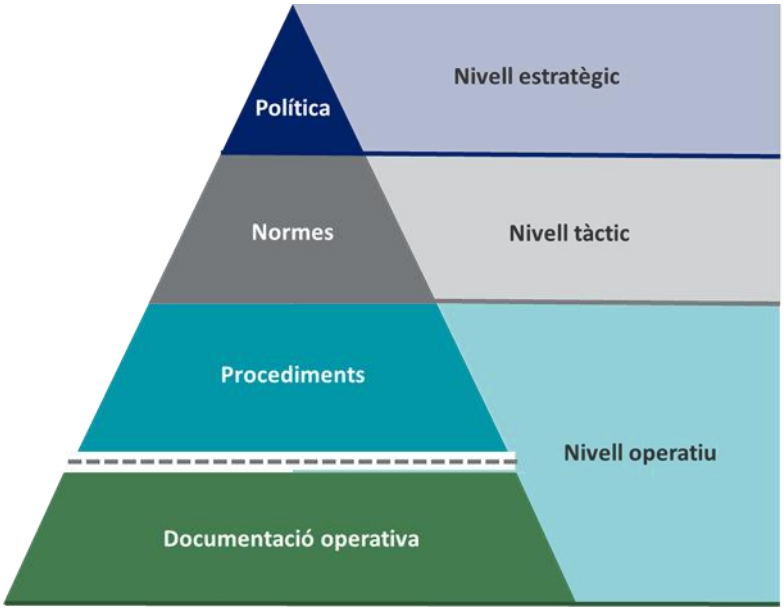


Figura 1 – Estructura del cos normatiu

Actualment, el cos normatiu de seguretat de l'IMI està format per uns 110 documents, entre normes, procediments i documents operatius.

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

- **Manteniment del cos normatiu** (normes, procediments, guies...). L'adjudicatari serà responsable de mantenir i evolucionar el marc:

  - Per cobrir les noves necessitats que es vagin detectant i no estiguin cobertes pel marc normatiu actual, com per acabar de desenvolupar aquells documents que es troben en fase d'esborrany o de treball..
  - Per període de revisió establerts en els documents
  - Per canvis en els entorns tècnics que regulen
  - Incorporació i normalització en el Cos Normatiu de Normes, guies o estàndards elaborades per altres
  - Definició d'arquitectures de referència sobre les que aplicar mesures de compliment normatiu i elaboració de les corresponents guies de bastionat.

- **Identificació de nous requeriments** de normatives que siguin d'aplicació a l'Ajuntament de Barcelona i la seva incorporació en el marc normatiu actual. Per aquest motiu s'haurà de:
  - dissenyar i implementar canals que permetin a l'IMI identificar la necessitat d'incorporar nous elements al Cos Normatiu de Seguretat o actualitzar les existents
  - dissenyar un pla d'evolució anual del cos normatiu de Seguretat de l'IMI, que contempli tant la incorporació de nous elements com l'actualització dels ja existents.
- Posteriorment, s'hauran de fer les gestions necessàries per portar-los a **aprovació seguint el procediment establert en l'IMI i/o als Òrgans de l'Ajuntament** que correspongui, si s'escau.
- Dotar el Cos Normatiu duna eina que permeti el seu emmagatzemament, el versionat dels documents que el composen i la seva consulta per part de la organització.

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

Tasques	**Volumetria**	**Lliurables**
Desenvolupament de les normes, guies, estàndards i procediments necessaris per a cobrir noves necessitats que no estiguin cobertes pel marc normatiu vigent.	15 documents anuals	Norma, guia, estàndard (Aprovada i/o implantada)
Desenvolupament de procediments necessaris per a cobrir els requeriments que exigeixi marc normatiu.	10 procediments anuals	10 procediments redactats i implantats

Tasques	Volumetria	Lliurables
Actualització, revisió periòdica o incorporació de normes, guies o estàndards existents i operatius. També incorporació de normes, guies i estàndards elaborats per tercers.	30 documents anuals	Documents actualitzats o incorporats

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 els 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*** amb l'objectiu de poder sistematitzar, 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.

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 - Entrega de documentació: a l'inici del contracte, s'ha de fer l'entrega 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: 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 nivells 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 siguin d'aplicació.

- **Seguiment dels 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. El 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. El proveïdors s'escolliran per risc, per rellevància (imatge, interès corporatiu,...) 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 de proveïdors es valorarà el nivell assignat a cada proveïdor i servei prestat, sent possible la requalificació de proveïdors ja sigui augmentant el nivell que tenien assignat o bé disminuint el nivell que teníem assignat.

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

Descripció	Tasques	Volumetria	Lliurables
Revisió i adaptació de la documentació	Revisar metodologia de seguiment de Proveïdors	1 proposta anual	Proposta anual de millora de la metodologia
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 4 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 de AM de desenvolupament al servei de l'IMI centralitzat dels 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 Qualitat i Seguretat 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.

Per tal d'assolir els nivells de seguretat s'haurà de evolucionar i madurar el model de classificació la informació (implementat a la CMDB) i el sistema de controls unificats en dos sentits:

- Millorar el sistemes existents
- Adequar-lo per tal que pugui absorbir els requeriments del nou reglament europeu de protecció de dades i les adequacions a l'ENS.

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

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

- Fer l'**anàlisi dels canvis significatius** que suposarà qualsevol canvi reglamentari que tingui lloc durant la vigència del contracte així com les repercussions que puguin tenir en la organització la seguretat de la informació de l'Ajuntament.
- Elaboració del pla de compliment normatiu: realitzar un anàlisis de situació actual de l'IMI respecte als requeriments actuals i a canvis normatius i dissenyar un pla d'acció per alinear les mesures de seguretat aplicades per l'IMI i per l'Ajuntament a aquests nous requeriments.
- 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 del ENS,...).
- Servei d'adequació dels sistemes a la legislació (ENS, eIDAS, LOPDGDD,...) i al marc normatiu corporatiu.
- 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 Ajuntament.
- Anàlisi d'impacte, gestió de riscos i proposta de mesures de sistemes d'informació crítics.
- Gestionar que eles 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 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.
- Establir un marc de controls a aplicar en entorns cloud
- Facilitar suport i assistència a la taula de Ciberseguretat de l'Ajuntament de Barcelona
- **Mesura del nivell d'implantació del cos normatiu.** Per tal de poder mesurar el nivell d'implantació del cos normatiu, l'adjudicatari haurà de desenvolupar i implementar mecanismes de avaluació del grau de implantació i compliment del cos normatiu de Seguretat. A tal efecte haurà de mantenir, completar i evolucionar el sistema unificat del Marc de control global que permeti avaluar el nivell de compliment dels sistemes d'informació i actius corporatius.

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

Descripció	Tasques	Volumetria	Lliurables
Actualització i seguiment plans d'adequació	Identificar nous canvis normatius que es vagin produint i actualització dels plans d'acció existents en l'IMI. Seguiment del grau d'avanç dels projectes d'adequació recollits en els diferents plans d'adequació	2 / any	Informes semestrals de seguiment
Implementació dels projectes d' adequació	El servei haurà de implementar projectes les tasques d'adequació als diferents marcs reguladors en que recaigui la responsabilitat a Seguretat de l'IMI.	6 accions/ tasques / millores any	Informe mensual indicant l'execució de la millora o acció requerides (seguiment dels projectes d'execució de millores)
Servei d'adequació dels sistemes a la legislació	Servei d'adequació dels sistemes a la legislació aplicable	3 / any	Informes d'adequació anuals

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.	3 informes / any	Informe
Compliment ENS	Anàlisis i revisió dels sistemes d'informació municipals per garantir el compliment de l'Esquema Nacional de Seguretat	10 sistemes nous anuals 50 sistemes analitzats en anys anteriors	

4.2.3.**Plans d'auditoria**

Com s'indicava amb la definició i gestió del marc normatiu, aquest serveix de 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...).
- Donar suport (es 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 que 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	1 pla anual	Pla anual d'auditories de seguretat

Descripció	Tasques	Volumetria	Lliurables
	d'incloure mínim 3 auditories de compliment globals)		
Execució auditories internes de compliment	Realitzar auditories internes per valorar el nivell de compliment del cos normatiu de seguretat.	3 auditories anuals	Informe d'auditoria i pla d'acció.
Donar suport en la execució auditories externes de compliment (Servei de cortesia)	Actuar com a punt únic de contacte entre el personal del IMI i els auditors externs.	3 auditories anuals	Obtenció de les evidencies sol·licitades pels auditors externs.
Gestionar la implementació de les millores sorgides	El servei haurà de coordinar i donar suport a las àrees i proveïdores TIC de l'IMI responsables de les accions correctives sorgides de les auditories.	4 informes anuals de seguiment (informe trimestral)	Informe indicant l'execució de la millora o acció requerides.
Implementació de les millores sorgides	El servei haurà d'implementar les accions correctives sorgides de les auditories en què la responsabilitat recaigui en l'Àrea de Seguretat de l'IMI.	4 informes anuals de seguiment (trimestral)	Informe indicant l'execució de la millora o acció requerides.

4.3. **DIVULGACIÓ NORMATIVA**

Per tal d'assegurar el correcte coneixement i enteniment del marc definit és necessària la divulgació d'aquest en els àmbits d'actuació adients i mantenir el personal format i coneixedor de la normativa que s'aplica. Aquesta tasca es realitza amb l'**assegurament tant legal TIC, com tècnic de seguretat** i es porta a terme des de dues vessants:

- Divulgativa – actuacions puntuals sobre temes relacionats amb la seguretat de la informació
- Formativa – actuacions de caire estructurat sobre temes relacionats amb la seguretat de la informació.

D'aquesta manera es resolen dubtes que es puguin despendre de l'aplicació del marc normatiu tant conceptual, legal o tècnica, i **es fa divulgació** d'aquelles parts que es considerin d'interès per grups concrets.

El continguts per a la impartició de la formació, que aporti l'usuari, hauran de ser adaptats en funció del públic destinatari (personal tècnic IMI, personal adscrit al Departament de seguretat, usuaris finals de l'Ajuntament, personal directiu IMI, personal directiu Ajuntament,...) i a la realitat de l'Ajuntament de Barcelona.

L'adjudicatari haurà de definir un Quadre de Comandament que permeti fer un seguiment dels resultats obtinguts en les diferents accions de divulgació executades.

4.3.1.**Divulgació**

Donada la importància que el personal municipal (Ajuntament i organismes municipals) tinguin les nocions de seguretat necessàries per al desenvolupament segur de les seves tasques, es complementa l'oferta formativa amb una sèrie de píndoles, o accions d'altre caire, orientades a fer de recordatori periòdic respecte de temes de seguretat que es considera, per part del departament de Seguretat important remarcar, ja sigui per què s'hagi detectat manca de compliment o per què es tracti de temes nous sobre els que no es pugui plantejar una activitat formativa.

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

- Dissenyar programes de conscienciació en matèria de Seguretat pel personal de l'IMI i de l'Ajuntament. Aquest pla haurà d'incloure necessàriament per a cada una de les accions previstes informació relativa a l'abast, objectius, canals, eines disponibles (si cal), processos i material necessari.
- Desplegament i execució de les accions incloses en aquests programes.
- Obtenció de les mètriques que siguin necessàries per avaluar els objectius previstos en els plans de conscienciació.
- Avaluar els resultats obtinguts i proposar millores respecte de les previsions del pla pla de conscienciació

Aquestes accions es treballen per mitigar, entre altres riscos, el desconeixement en la normativa per tal d'**evitar l'incompliment normatiu**.

D'acord amb el departament de l'IMI que es determini, s'establiran una sèrie de nivells que permetran determinar el nivell de conscienciació obtingut, determinant en aquells casos en que el nivell obtingut no sigui l'esperat, les accions a prendre per tal de millorar els resultats obtinguts o per focalitzar noves iniciatives envers aquells grups de risc que no l'hagin.

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

Descripció	Tasques	Volumetria	Lliurables

Descripció	Tasques	Volumetria	Lliurables
Proposta del pla de Divulgació	Es farà una proposta del pla anual i el general del servei	1 proposta	Proposta amb continguts, metodologia, tipus d'accions i planificació
Conscienciació continua	Realitzar accions de conscienciació per als empleats sobre bones pràctiques de seguretat (publicació de butlletins, píndoles i notes informatives, manuals, etc.)	12 accions anuals	Material formatiu desenvolupat Pla de comunicació online.

4.3.2.**Formació**

Addicionalment es poden realitzar accions formatives en relació a normes o a lleis recollides en el marc normatiu amb l'objectiu de divulgar-lo segons sigui necessari.

Amb aquests propòsits, es requereix per una banda l'adequació normativa en matèria de seguretat de la informació (assegurament legal TIC i tècnic de seguretat) i per l'altre, la divulgació d'aquesta normativa.

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

- Dissenyar programes de formació en matèria de Seguretat pel personal de l'IMI i de l'Ajuntament. Aquest pla haurà d'incloure necessàriament per a cada una de les accions previstes informació relativa a l'abast, objectius, canals, eines disponibles (si cal), processos i material necessari.
- Desplegament i execució de les accions incloses en aquests programes.
- Realitzar tallers de formació de determinats aspectes del cos normatiu als col·lectius de l'IMI o del Ajuntament que ho requereixin.
- Obtenció de les mètriques que siguin necessàries per avaluar els objectius previstos en els plans de formació.
- Avaluar els resultats obtinguts i proposar millores respecte de les previsions del pla de formació

Aquestes accions treballen per mitigar, entre altres riscos, el desconeixement en la normativa per tal d'**evitar l'incompliment normatiu**.

D'acord amb el departament de l'IMI que es determini, s'establiran una sèrie de nivells que permetran determinar el nivell d'assoliment obtingut, determinant en aquells casos en que el

nivell obtingut no sigui l'esperat, les accions a prendre per tal de millorar els resultats obtinguts o per focalitzar noves iniciatives envers aquells grups de risc que no l'hagin assolit .

Es valorarà que l'adjudicatari aporti sense cost eines pròpies d'impartició de formació en línia tant pel personal de l'Ajuntament com pel personal de l'IMI. Aquestes eines hauran de respondre a les necessitats de conscienciació de la seguretat amb solucions del tipus:

- Presentacions
- Elements interactius
- Qüestionaris
- Elements de comunicació

També es valorarà que l'adjudicatari ofereixi eines de simulació amb les quals testar les capacitats en matèria de ciberseguretat tan pel personal de l'Ajuntament com pel personal de l'IMI. Les eines han de validar les capacitats de l'Ajuntament en la detecció i resposta davant determinats comportaments, les solucions vàlides seran del tipus:

- Campanyes d'enginyeria social
- Recreació d'atacs específics
- Simulacres d'escenaris de crisi
- Atacs dirigits

Aquestes eines han d'estar a disposició del servei almenys durant la durada del contracte sense cost addicional per l'IMI.

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

Descripció	Tasques	Volumetria	Lliurables
Proposta del pla de Formació	Es farà una proposta del pla anual i el general del servei	1 proposta	Proposta amb continguts, metodologia, tipus de sessió i planificació
Tallers de formació en seguretat	Realitzar tallers de formació i conscienciació de determinats aspectes del cos normatiu als col·lectius de l'IMI, o del Ajuntament, que ho requereixin.	3 formacions anuals	Material formatiu desenvolupat. Fulls d'assistència presencial signades o pla de comunicació online.
Desenvolupament de materials	Realització de continguts formatius específics per l'Ajuntament o tècnics de l'IMI	5 continguts formatius anuals	Material formatiu desenvolupat

4.4. **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 és puguin despendre de l'aplicació del marc normatiu tant conceptual, legal o tècnic.

a) Pel desenvolupament d'aquest servei és duren 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.
- 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 anàlisis 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,... 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 5 actuacions de suport puntuals anuals a cobrir en tasques de suport puntuals del servei 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 4.8.4 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	5 actuacions de suport anuals	Informes de suport realitzats i dedicació

4.4.1.**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 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 de que 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 de que 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 de que 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.

4.5. **CLASSIFICACIÓ DE LA INFORMACIÓ**

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

En el procés de classificació es van identificar al voltant de 200 sistemes d'informació carregats a l' Eina d' Inventari d'Actius de l'IMI (CMDB).

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

- **Evolucionar i mantenir el Sistema de Gestió de la Classificació de la Informació Corporativa**. Això inclou:
  - Millora del sistema de classificació desenvolupat amb les metodologies ja existents de gestió de nous desenvolupaments i evolutius implantada a l'IMI (ADINET i Agile), Gestió del Canvi (CMDB) i SIA.

  - Revisar la informació relativa als sistemes d'informació ja classificats a la CMDB, en relació a la qualitat de la informació i la seva relació amb els serveis i infraestructura relacionada.
  - Gestionar l'acceptació (i possibles canvis) amb cadascuna de les gerències de l'Ajuntament.
  - Demanar als responsables dels sistemes d'informació l'actualització de la CMDB amb els possibles canvis detectats en els passos anteriors.
  - Establir les Mesures de seguretat per cada nivell de seguretat de la normativa de classificació corporativa. Establir procediment i sistema de comunicació del la seguretat a implementar per nivell.
- 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.

4.6. **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 lo 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 4.6.2 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 la 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 4.6.2) 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 de 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.	Anual	Informe
	Desenvolupament d'un Pla de divulgació de l'eina als grups resolutoris corresponents	Anual	Pla de divulgació

4.7. **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 sigui gestionat.

Aquesta gestió inclou 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 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. Aquest output 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.

4.8. **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 s'han de gestionar 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

Totes elles es descriuen a continuació.

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

Actualment l'IMI ha implementat RSA Archer, que serà l'eina principal de l'Oficina de GRC, mitjançant la qual es pugui fer un 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.

Actualment l'IMI ha implementat els següents mòduls de l'eina 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.

4.8.2.**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. Actualment l'eina desplegada per a la Gestió d'incidents de Seguretat és l'eina **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.

4.8.3.**Eina de Manteniment del Cos Normatiu**

Tal i com s'ha descrit en l'apartat *4.1.3 Gestió del Cos Normatiu* una de les tasques que haurà de dur a terme l'adjudicatari serà la Gestió del Cos Normatiu.

El cos normatiu requereix la implementació de la gestió dels documents que el componen, és a dir: manteniment de versions, aprovacions i cicle de vida documental tot utilitzant el Gestor documental corporatiu.

L'adjudicatari serà l'encarregat de mantenir les diferents versions dels documents del Cos Normatiu dins del Gestor documental corporatiu o eina equivalent que es determini. En qualsevol cas s'haurà de prioritzar l'ús d'eines corporatives ja disponibles que permetin dur a terme aquesta tasca.

Donat que els documents del Cos Normatiu duen associat un procés de validació i aprovació dels diferents documents, aquesta eina hauria de ser capaç, en la mesura de lo possible, no només de guardar les diferents versions dels documents sinó també poder gestionar i emmagatzemar aquestes cadenes d'aprovació associades al document.

En el cas que l'adjudicatari decideixi aportar una eina diferent del gestor documental corporatiu, aquesta eina ha de poder garantir la seva integració amb el gestor documental i el gestor d'identitats corporatiu.

4.8.4.**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.

4.9. **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 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.

Es preveu per aquest apartat del servei una dedicació que representa com a total un màxim de 1.800 hores anuals per recurs aportat a l'equip que presta els serveis objecte del present contracte.

4.9.1.**Govern i seguiment de la *Seguretat en el Disseny* (Seguretat en projectes)**

Ja 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'una política de Seguretat en Projectes** alineada amb els objectius de estratègics de seguretat i amb la metodologia proposada pel licitador. Aquesta política 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 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 la OSP** 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 demanada, 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 que inclogui els indicadors de risc i de rendiment** en relació als projectes de l'IMI i l'execució del servei.
4. Redacció del llibre blanc d'arquitectures de referència on es recullin tots els escenaris d'infraestructura amb els controls de seguretat requerits en cada cas. La OSP serà responsable del desenvolupament, manteniment i actualització d'aquest llibre blanc.

4.9.2.**Metodologia de Seguretat en el Disseny**

El proveïdor haurà de fer una proposta que millori la metodologia actual per a donar-li maduresa, més capacitats i més cobertura en tot el cicle de vida dels Projectes.

La metodologia és proposada pel propi servei, adequant en cada moment aquesta metodologia a les eines i processos existents.

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 mitjançant l'**autoavaluació i paràmetres, i** les **indicacions estàndards**.

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

- 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'autoevaluació 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.

Les tasques prèviament identificades i més, tindran una dedicació diferent segons el tipus de projecte i es poden agrupar per fase del cicle de vida del projecte:

En fase de definició / Gestió de la Demanda

- Assistir o recollir els *outputs* del Comitè de Gestió de la Demanda, taules necessàries o altres mecanismes pertinents
- Elaboració d'estimacions de dedicació de la OSP en funció dels casos de negoci de presentats.
- Participació en l'elaboració de requisits per als plecs tècnics.

En fase de Desenvolupament del projecte

- Revisió del disseny de la solució i assignació a l'escenari dins els escenaris plasmats al Llibre Blanc d'Arquitectures de Seguretat.
- Especificació de requisits de seguretat del projecte.
- Anàlisis d'amenaces sobre les arquitectures proposades pel projectes.
- Suport a les eines de seguretat del pipeline DevSecOps: parametrització de les eines, resolució de consultes sobre els resultats, revisió de resultats, etc.
- Revisió i vistiplau del compliment dels anàlisis requerits.
- Suport en la resolució de *findings* associats als anàlisis realitzats.
- Suport a preguntes i incidències sobre l'execució i els informes de les eines.
- Revisió i vistiplau de la implementació dels requeriments definits.
- Suport en la definició dels plans d'actuació.
- Suport en la definició de l'abast dels tests d'intrusió.
- Establiment i documentació de polítiques de protecció en el desplegament:
    - Integració del projecte amb solucions de seguretat tals com WAF, SIEM i IAM.
    - Bastionat de servidors i/o contenidors.
    - Gestió de vulnerabilitats (Clair, Vulnerability Advisor, BugBlast).
    - Gestió d'artefactes de codi propi i de tercers (Nexus).
    - Comprovació de la integritat del codi.
    - Procediments de marxa enrere en cas d'un desplegament fallit.
    - Seguretat en entorns de contenidors (Kubernetes, Segmentació de xarxa).
    - Gestió segura de Secrets.
- Gestionar els recursos materials per garantir l'efectivitat en l'execució de les tasques del nivell tàctic (accés als recursos de xarxa, gestió de credencials, etc.).
- Gestionar els escenaris de risc amb els interlocutors tècnics involucrats.
- Alimentació del quadre de comandament i dels informes periòdics amb els KPIs i KRIs definits.

En fase de posada en producció del projecte

- Seguiment dels plans de resolució d'inconformitats proposats pels responsables de projecte.

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

4.9.3.**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, amb excepció d'alguns projectes que s'aborden excepcionalment, directament des de l'Ajuntament. Ells 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, tenint en compte que no és el mateix un projecte típic de desenvolupament de SDLC que es desenvolupa en DEVSECOPS que una implantació d'una solució paquetitzada o la implantació d'una nova tecnologia, o integrar la organització en un servei ofertat al núvol.

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.

4.9.4.**Consultoria de projectes**

L'equip que ha de garantir la consultoria als projectes per garantir la seguretat en el disseny realitzarà:

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

Durant tota l'etapa de desenvolupament i provisió, els consultors hauran d'implementar la **Metodologia de Seguretat en el Disseny**.

Projectes experts

Els consultors assignats a aquesta àrea hauran de dur a terme també una altra tipologia de projectes internament anomenats "projectes experts" (o simplement "projectes").

Són projectes de consultoria de seguretat sobre sistemes, conjunts de sistemes, solucions i/o consultes puntuals que estiguin referides a analitzar-ne els riscos de seguretat però que no encaixen dins el cicle de vida de securització d'un projecte concret, doncs abasta tot l'univers de projectes.

Millora continua de la metodologia per estandardització

Els consultors hauran de promoure les arquitectures de seguretat i estàndards establerts i vetllar per la documentació i industrialització de la metodologia reportant possibles millores detectades o sol·licitant a l'àrea d'arquitectures que defineixi arquitectures model. Per als casos de projectes que afectin o modifiquin a arquitectures globals establertes, aquest equip haurà de coordinar-se igualment amb el *Servei d'Arquitectures de Seguretat*.

Model de Consultoria

Anomenem ***Enllaç de Seguretat*** aquest perfil que participa en la seguretat en projectes, a la persona que respon per l'activitat del servei de consultoria de *Seguretat en el Disseny* (Seguretat en Projectes) 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 l'Àrea de Seguretat i si cal, fer de enllaç amb els diferents interlocutors i de l'àrea durant el cicle de vida d'un projecte .

La Direcció de Seguretat 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'Àrea de Seguretat.
- Suport inicial: Si es preveu que la dedicació per part de l'Àrea de Seguretat 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 l'Àrea de Seguretat només de manera ocasional, o sigui per a consultes puntuals, serà suficient definir per endavant un model de comunicació entre el projecte i l'Àrea de Seguretat per resoldre de la manera més eficient possible les consultes o peticions que siguin necessàries.
- Sense Suport: Només es farà el seguiment industrialitzat d'autoavaluacions dels projectes.

4.9.5.**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. S'haurà de determinar els lliurables a entregar dins del marc del projecte (depenent de la tipologia del projecte).

Els lliurables dels projectes poden ser (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.

Cal contemplar el model d'enllaços pel nivell de participació de l'equip de consultoria de seguretat en els projectes (4 tipologies vistes a *4.1.4 Consultoria de Projectes*)

Cartera de projectes de Seguretat securitzats

Cal disposar d'un seguiment inventari de projectes amb demanda de seguretat durant tot el cicle de vida.

L'adjudicatari ha de poder reportar en qualsevol moment el detall i els informes executius sobre el nivell de seguretat dels projectes corporatius.

Informe de nivell de seguretat i riscos dels projectes corporatius

Es disposarà d'un quadre de comandament que inclogui els indicadors de risc i de rendiment en relació als projectes de l'IMI i l'execució del servei per a avaluar la seguretat i reporting de seguiment mensual, que es reportaran a diferents públics objectius: Comitè de Direcció de Projectes de l'IMI, Comitè de Direcció del Servei en qüestió o Gerències.

4.9.6.El *Pipeline* en el cicle de vida de desenvolupament de programari (SDLC)

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 anual amb la revisió de les polítiques de detecció de vulnerabilitats de codi** i llenguatges emprats a l'IMI. Aquest informe ha d'incloure un pla de millora que

permetin assolir un procés de millora contínua de l'eina d'anàlisi de codi estàtic (actualment SonarQube).

- 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 en l'eina Anchore.
- Realitzar revisions periòdiques del repositori central d'imatges Docker de l'IMI amb Nexus 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 de l'Administració, 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 en cerca de millores evolutives dels productes del *pipeline* (actualització de versions o canvi de productes)
- Revisar configuracions de polítiques dels components, per tal d'assegurar que la seguretat dels projectes vagi alineada amb les directrius de l'organització

4.9.7.**Proactivitat i caràcter multidisciplinari de l'equip de Seguretat en Projectes**

El servei demandat busca disposar d'un equip proactiu i multidisciplinari de consultors de seguretat de la informació, amb coneixements de tecnologies de seguretat d'avantguarda, així com coneixements globals i generals d'aspectes TIC (desenvolupament, xarxes/comunicació, operació, plataformes TIC habituals de grans organitzacions – ERPs, BBDD., J2EE, Pipeline DEVSECOPS, mobilitat ...-), habituats a treballar en equip interdisciplinaris, amb un clar enfoc a riscos de seguretat, entesos de manera amplia i amb enfoc en impacte en el negoci, més enllà d'aspectes merament tècnics.

Aquest equip, sota les directrius de l'Àrea de Seguretat de l'IMI, donarà resposta a la demanda que arribi, segons la planificació i priorització que el seu responsable determini.

4.10. **SERVEI DE SEGURETAT EN EL DISSENY**

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 interdepartamentals 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 3 activitats principals:

1. Estandarditzación i normalització d'arquitectures de seguretat

El Servei de Seguretat en el Disseny s'encarregarà de l'estandarditzación i normalització d'arquitectures. Redacció d'un llibre blanc que reculli les arquitectures de referència en base als escenaris aplicables dins dels models d'arquitectura més coneguts.

Model tradicional *on-premise*

Model *legacy*, d'arquitectures tradicionals (màquines físiques, appliances i màquines virtuals monolítiques). Les funcions engloben:

- Diferenciació en termes de segregació de xarxes i zones de seguretat
- Identificació d'elements de seguretat en xarxa i endpoints
- Requisits de seguretat aplicables a alt nivell

Arquitectura de microserveis

En el nou model de virtualització a nivell d'instàncies, i dins de l'entorn corporatiu (actualment amb Kubernetes a IBM Cloud Private corporatiu on-premise, i en un futur amb Openshift), es requereix coneixement per a dur a terme tasques de validació d'arquitectures de:

- Diferenciació de les diferents capes emprades (REST/SOAP)
- Identificació dels components relatius al model (Config Server, API Gateway, Service Registry, Fallback, Load Balancing…)
- Requisits de seguretat aplicables a alt nivell

Arquitectura cloud

La seguretat al *cloud* ha d'assegurar la protecció de la informació (dades, aplicacions i infraestructures) a aquest. Al ser un entorn dinàmic, aquest està subjecte al canvi, a l'igual que les amenaces.

- Definició dels escenaris en funció del tipus de servei (SaaS, PaaS, IaaS) i el context de la solució (exposició, sensibilitat de la informació)
- Requisits de seguretat aplicables a alt nivell
- Diferenciació entre cloud privat, públic i híbrid
- Seguretat del perímetre

Framework de desenvolupament

- Definició d'estàndards de llibreries aplicables als projectes

2. Disseny de solucions de Seguretat

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

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

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

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

Avaluarà i proposarà plans de millora a riscos que la Oficina de GRC (Compliment) li escali.

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

4.11.**PARTICIPACIÓ EN PROJECTES DE SEGURETAT**

Al marge d'atendre la cartera de projectes que s'impulsen dins l'IMI, la pròpia funció de seguretat podrà recaure sobre l'execució de projectes propis de millora del model de seguretat de la informació de l'IMI. L'objectiu principal d'aquest servei serà col·laborar amb el rol de Gestor de

Projecte en una dedicació pre-establerta que no superarà el 12 % d'un recurs Full time Equvalent (FTE) que representa un màxim de 216 hores. En funció de la dimensió en seguretat de cada projecte es requeriran diferents dedicacions d'esforç:

- Projecte amb una dedicació alta: 10% d'un FTE
- Projecte amb una dedicació mitjana: 6% d'un FTE
- Projecte amb una dedicació baixa: 3 % d'un FTE

Es valorarà l'ampliació d'aquesta dedicació i aquest servei serà ampliable quan hi hagin mes demanda de Gestió de projectes en el departament de Seguretat.

4.12.**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 conforme la 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 quan 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 el 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.

4.12.1.**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 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 de que 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 de que 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 de que 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.

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.

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 Cap de Contracte 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 Qualitat i Seguretat de l'IMI.
- Cap del Departament de Seguretat de l'IMI.
- Responsable de GRC per part de l'IMI.
- Responsable de Seguretat en Projectes per part de l'IMI.
- Responsable del contracte per part de l'adjudicatari.

El responsable del contracte 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 de GRC o Seguretat en Projectes, que es consideri necessari 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 contracte per part de l'adjudicatari.
- Cap de l'Oficina GRC per part de l'adjudicatari.

El responsable de contracte 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 Seguretat en Projectes per part de l'IMI.
- Responsable del contracte per part de l'adjudicatari.
- Responsable de Seguretat en Projectes de l'adjudicatari.

El responsable de contracte 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 contracte 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 Cap de Contracte 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 contracte 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:

<u>Informe de feina en curs i prioritats establertes</u>: (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.

<u>Informe de seguiment de l'avenç</u>: (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.

Amb l'objectiu de millorar la qualitat de la participació en projectes i generar coneixement sobre les diferents activitats i l'esforç i el seu pes relatiu que suposen en el global del servei, caldrà que el personal adscrit al servei registri diàriament la dedicació en temps a les diferents tasques o activitats. Aquestes tasques o activitats necessàriament hauran d'estar correctament identificades en la taxonomia o classificació de totes les tasques o activitats del contracte. Per tal que aquest registre sigui útil al seu objectiu la granuralitat de les tasques o activitats sobre les que es reportin han der suficientment detallades o petites sense que això suposi un esforç significatiu per al membre de l'equip en reportar la dedicació. Aquest reporting es farà sobre l'eina corporativa que l'IMI determini (actualment JIRA). És desitjable que l'eina de registre de la dedicació estigui integrada amb la resta d'eines de reporting i/o que l'adjudicatari utilitzi per al contracte.

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.

La dedicació per part del nou adjudicatari corresponent a la fase de recepció del servei seran sense cost per l'IMI.

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 4,92 FTEs, considerant que:

-Les tasques de perfil Consultor GRC han de ser cobertes com a mínim per un perfil amb la dedicació corresponent al 100% d'un FTE, o d'un 90% d'un FTE de dedicació de consultor de GRC si aquest fos el mateix perfil que assumeixi també les tasques de Cap d'Oficina GRC. Si els licitadors oferissin dedicacions superiors a aquest mínim, sempre i en tot cas hauran d'adscriure un d'aquests perfils al 100% FTE o 90% si aquest fos el mateix perfil que assumeixi també les tasques de Cap d'Oficina GRC, no podent adscriure, per exemple, dos perfils al 50% per cobrir aquest mínim.

-Les tasques de Tècnic sènior especialista en consultoria de seguretat han de ser cobertes com a mínim per un perfil amb la dedicació corresponent al 100% d'un FTE, o d'un 90% d'un FTE de dedicació de Tècnic sènior especialista en consultoria de si aquest fos el mateix perfil que assumeixi també les tasques de Responsable del servei de Seguretat en Projectes. Si els licitadors oferissin dedicacions superiors a aquest mínim, sempre i en tot cas hauran d'adscriure un d'aquests perfils al 100% FTE o 90% si aquest fos el mateix perfil que assumeixi també les tasques de Cap d'Oficina GRC, no podent adscriure, per exemple, dos perfils al 50% per cobrir aquest mínim.

- Es considera que el servei inclourà com a mínim 3 FTEs dels perfils indicats de GRC i 1 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 de contracte	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 l'Àrea 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. Perfil: Gestor 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, anàlisis, 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 el 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.
Divulgació i comunicació GRC	Responsable de les tasques relacionades amb la formació i conscienciació del personal de l'Ajuntament i òrgans de la corporació municipal. Tasques: • Elaboració de materials de divulgació de conceptes de seguretat • D'acord amb el Cap d'Oficina i el responsable IMI definirà el pla de formació en matèria de seguretat dirigit al personal municipal. • D'acord amb el Cap de l'Oficina i el responsable IMI definirà el pla de conscienciació del personal municipal. • Execució dels plans de formació i conscienciació definits. • Seguiment dels resultats obtinguts en les diferents activitats formatives • Seguiment dels resultats obtinguts en les diferents activitats de divulgació • Obtenció d'indicadors • Proposta de millora sobre les activitats executades.
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. SDLC. Perfil: Tècnic. Coneixements en establiment de requisits de seguretat en projectes. Perfil: **Consultor** 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 remeiació • 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*. Perfil: **Arquitecte**. 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	Responsabilitat
Responsable del contracte	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: Enginyer de Telecomunicació o Informàtica • Certificacions recomanades: o Gestió de Serveis TIC (ITIL) o Seguretat de la informació (ISACA o similars)

Perfil	Responsabilitat

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
	• Certificacions recomanades
	  ○ En gestió de serveis (ITIL)
	  ○ En gestió de seguretat de la informació (ISACA o similars)
	  ○ En gestió de riscos
	  ○ RSA Archer Certified Associate o RSA Archer Certified Professional

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
	• Certificacions recomanades
	  ○ En auditories de compliment (ISO27001 Lead Auditor o similar)
	  ○ En gestió de la seguretat de la informació (ISACA o similar)

Perfil	Responsabilitat
Divulgació i comunicació GRC	Cal que acrediti, durant els darrers 5 anys, 3 anys d'experiència mínima en formació de l'àmbit de seguretat TIC. Cal que acrediti experiència en l'elaboració de continguts formatius i/o de divulgació en matèria de seguretat de la informació. Haurà de disposar: • Titulació: Enginyeria Superior, preferiblement en Informàtica o Telecomunicacions • Recomanable: o Formació complementària específica relacionada amb les tasques a desenvolupar. o En gestió de la seguretat de la informació (ISACA o similar)
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 Certificacions recomanades: o Certificació ITIL (a partir versió 3) o PMP o Seguretat de la informació (ISACA o similars)
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. Certificacions recomanades: • PMP • CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) o AWS Solutions Architect Associate. • CSX (Cybersecurity Fundamentals Certificate) • OSCP (Offensive Security Certified Professional)

Perfil	Responsabilitat
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. Certificacions recomanades: • CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) o AWS Solutions Architect Associate.

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. 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.

8.2. **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.

8.3. **DURADA DEL CONTRACTE**

Aquest contracte tindrà vigència a partir del dia 1 de desembre de 2021 o del dia següent al de la seva formalització si aquest fos posterior, i tindrà una durada de 26 mesos i 15 dies comptats a partir d'aquesta data.

Els primers quinze dies corresponen a la fase de recepció del servei. A tal efecte s'estableix aquest període inicial per a procedir al traspàs del servei del proveïdor actual al nou adjudicatari, si fos el cas. Aquesta fase de l'execució del contracte serà sense cost per l'IMI, per tant l'adjudicatari no podrà emetre cap factura per les tasques efectuades durant l'esmentada fase. Aquesta fase de transició no tindrà lloc pel cas que el proveïdor actual esdevingui també adjudicatari d'aquest contracte, i conseqüentment en aquest supòsit l'inici del contracte serà el 15 de desembre de 2021.

8.4. **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.

8.5. **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.

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

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

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

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

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

8.6.1.**Auditories**

8.6.1.1.***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.

8.6.1.2.***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.

8.6.1.3.***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.

8.6.1.4.***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.

8.6.1.5.***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".

8.7. **CLÀUSULA DE GARANTÍA**

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

8.8. **FACTURACIÓ**

Els serveis es facturaran per trimestres vençuts i a partir de l'inici del servei efectiu, és a dir, un cop finalitzat el període inicial de recepció del servei. L'import a facturar per un trimestre sencer serà el resultat de dividir el preu ofert per aquest servei per l'adjudicatari entre els 26 mesos de servei efectiu del contracte multiplicat per tres, 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.

En tot cas s'hauran de respectar les anualitats del contracte a l'hora de facturar, no podent facturar-se serveis de diferents anualitats en una mateixa factura.

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

9. **PROPOSTA TÈCNICA**

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

El licitador haurà de presentar la seva oferta 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**.

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 per document.

1.- Resum executiu (màxim 3 pàgines)

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

2.- Plantejament 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. 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.

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 gestió del risc descrit a l'apartat 5.*1 Model de Relació IMI/Adjudicatari* del plec de prescripcions tècniques a generar per al servei als diferents destinataris.

4.- Govern de la Seguretat de la Informació (màxim 15 pàgines)

Es descriurà amb detall el sistema de Govern de la Seguretat de la informació, d'acord amb el preveu l'apartat *4.1.1 Govern de la seguretat corporativa* del plec de prescripcions tècniques, amb indicació del grau d'automatització que s'assolirà en relació a l'amplitud i claredat dels models de reporting, enfoc i indicadors que es compromet a obtenir en quadres de comandament executius,...

Es detallarà tot el que es consideri necessari respecte d'aspectes com la gestió del risc, els sistemes de reporting, l'evolució i automatització del quadre de comandament, la preparació dels diferents comitès.

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

Es valorarà l'amplitud i claredat de la proposta del model de gestió del risc descrit a l'apartat *4.1.2 Gestió del risc TIC corporatiu* del plec de prescripcions tècniques a generar per al servei als diferents destinataris

6.- Adequació normativa a la seguretat informació (màxim 10 pàgines)

Es descriurà en detall la proposta que, d'acord amb el que està descrit a l'apartat *4.2.2 Control normatiu* del plec de prescripcions tècniques, permeti donar resposta als requeriments de les diferents tasques descrites dins d'aquest apartat.

En aquesta proposta es detallarà tot el que es consideri necessari respecte a les metodologies a emprar per al control de proveïdors,.

7.- Auditoria Seguretat Informació (màxim 10 pàgines)

Es descriurà en detall la proposta que, d'acord amb el que es descriu a l'apartat *4.2.3 Plans d'auditoria* del plec de prescripcions tècniques, definiràs els continguts, metodologia, tipus de sessions, així com públic objectiu a què es destinarà. També es descriuran les eines que es posen a disposició per aquest servei amb les funcionalitats que incorpora, així com totes aquelles condicions que es considerin distintives i que millorin el pla de divulgació exigit al plec de prescripcions tècniques. S'inclouran també la proposta de pla de formació i de pla de divulgació amb detall dels temaris, número de sessions previstes, durada de les sessions i d'altres característiques que es considerin poden aportar valor a la seva proposta.

8.- Control de Proveïdors (màxim 4 pàgines)

Es valorarà la metodologia exposada pel licitador per planificar, executar i fer el seguiment dels diferents tipus de proveïdor tal com s'explicita en l'apartat *4.2.1 Seguretat en proveïdors*.

9.- Divulgació Seguretat de la Informació (màxim 4 pàgines)

Es valorarà l'exposició i la drescripció de les tasques destinades a la divulgació de la seguretat de la informació descrites a l'apartat *4.3 Divulgació normativa* en relació als continguts, metodologia, tipus de sessions, així com públic objectiu a què es destinarà, i totes aquelles condicions que es considerin distintives i que millorin el pla de divulgació requerit al plec de prescripcions tècniques.

10.- Suport en matèria de seguretat de la informació (màxim 8 pàgines)

S'hauran de desenvolupar i especificar les activitats així com l'organització del servei de suport d'acord amb el que s'estableix a l'apartat *4.4 Suport en matèria de seguretat de la informació* del plec de prescripcions tècniques; i, també haurà d'indicar els serveis de suport específics de backoffice que posi a disposició d'aquest servei de suport dins del contracte de manera que ampliïn els coneixements del servei.

11.- Gestió del registre d'incidents Corporatiu (màxim 15 pàgines)

Descriure el procés complert d'extrem a extrem dins l'eina de registre des de l'arribada d'una notificació fins a la generació dels informes i com serà el registre tant per la informació que contindrà com per la seva explotació segons el servei i les tasques de l'apartat *4.6 Gestió del registre dd'incidents* d'aquest plec de prescripcions tècniques. Es valorarà el detall i la claredat de la descripció del procés així com de les eines a utilitzar.

12.- Millora del seguiment del contracte (màxim 10 pàgines)

S'exposaran els aspectes detallats a continuació, d'acord amb el que preveuen els apartats 4 Descripció dels serveis i *5.3 Seguiment del contracte* del plec de prescripcions tècniques:

- Millora del contingut i estructura dels informes de comunicació
- Quadres de comandament del servei que facilitin el seguiment i presa de decisions del servei, amb un model d'indicadors exhaustiu i detallat.

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

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

14.-Model de govern i metodologia de la Seguretat en el disseny (màxim 24 pàgines)

Es valorarà el plantejament dels següents punts de l'àrea de Seguretat en el Disseny i Projectes (referents als apartats *4.9 de Servei de Seguretat en Projectes, 4.10 de Servei de Seguretat en el Disseny i 4.11 de Participació en projectes de seguretat*):

- Proposta metodològica per l'establiment polítiques de Seguretat en Projectes d'acord als mínims requerits a l'apartat *4.9.1. Govern i seguiment de la Seguretat en el Disseny*. (**màxim 3 pàgines)**
- Proposta metodològica per l'establiment de nous processos o adaptació dels existents per la implantació de Seguretat en Projectes d'acord als mínims requerits a l'apartat 4.9.1. Govern i seguiment de la Seguretat en el Disseny. (**màxim 3 pàgines)**
- Proposta d'estructura per al Llibre Blanc d'arquitectures d'acord als mínims requerits a l'apartat *4.9 Servei de Seguretat en el Disseny*. (**màxim 3 pàgines)**
- Proposta metodològica per garantir les tasques establertes per la fase de Definició/Gestió de la Demanda. Ha d'incloure els mínims requerits a l'apartat *4.9.2 Metodologia de la Seguretat en el Disseny* del plec de prescripcions tècniques. (**màxim 3 pàgines)**

- Proposta metodològica per garantir les tasques establertes per la fase de Desenvolupament. Ha d'incloure els mínims requerits a l'apartat *4.9.2 Metodologia de la Seguretat en el Disseny* del plec de prescripcions tècniques. (**màxim 3 pàgines)**
- Proposta metodològica per garantir les tasques establertes per la fase de Posada en producció. Ha d'incloure els mínims requerits a l'apartat *4.9.2 Metodologia de la Seguretat en el Disseny* del plec de prescripcions tècniques. (**màxim 3 pàgines)**
- Proposta metodològica per garantir que la major part de projectes puguin desenvolupar-se sense o amb poca participació explícita de l'Àrea de Seguretat gràcies a la classificació mitjançant l'autoavaluació i paràmetres, i les indicacions estàndard segons s'indica a *l'apartat 4.9.2 Metodologia de la Seguretat en el Disseny* del plec de prescripcions tècniques. (**màxim 3 pàgines)**
- Proposta metodològica relacionada amb el manteniment i gestió d'eines del pipeline de l'IMI segons s'indica a l'apartat *4.9.6 El Pipeline en el cicle de vida de desenvolupament* del plec de prescripcions tècniques, que garanteixi l'execució de les activitats descrites amb eficàcia i amb la menor despesa de recursos possible. (**màxim 3 pàgines)**

15.-Pla de devolució del servei (màxim 5 pàgines)

Es detallarà el 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 al nou adjudicatari o a l'IMI.

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

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

10.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 3/2010 de 8 de gener pel que es regula l'Esquema Nacional de Seguretat en l'Àmbit de l'Administració Electrònica.

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

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.**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.

10.3.**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.

10.4.**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 a l'IMI-Seguretat de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per l'IMI.

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

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

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 a IMI-Seguretat per al seu corresponent tractament i valoració.

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

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 repositori central per a l'autenticació dels usuaris. La

solució d'autenticació corporativa utilitzada per l'IMI és l'Oracle Access Manager (OAM) que proveeix el Single Sign On corporatiu.

La integració amb l'OAM es podrà fer mitjançant les següents opcions:

- Integració mitjançant capçaleres.
- Integració mitjançant l'estàndard SAML 2.0.
- Integració mitjançant l'estàndard OAuth 2.0.

Autenticació externa

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

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació, requerint així una verificació de la identitat de l'usuari que sol·licita accés. Actualment, la solució implantada al IMI fa ús de Google Authenticator.

12.2.**AUTORITZACIÓ DELS USUARIS ALS SISTEMES**

L'IMI disposa d'un mecanisme d'autorització d'usuaris corporatiu basat en el producte Oracle Unified Directory (OUD). L'adjudicatari haurà d'assegurar que les autoritzacions es troben delegades en el repositori central d'autorització (OUD).

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

La integració d'aquest connector anirà a càrrec de l'empresa adjudicatària i comptarà amb el suport i la supervisió de l'equip de gestió d'identitats. El temps dedicat normalment a integrar un connector estàndard amb una BBDD Oracle és aproximadament 80 hores d'un tècnic.

Perfilat d'usuaris

Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i per IMI-Seguretat.

El model proposat haurà de complir amb els següents principis:

- Segregació de funcions, de manera que s'exigeixi la concurrència de dues o més persones per realitzar tasques crítiques, anul·lant la possibilitat que un sol individu autoritzat pugui abusar dels seus drets per cometre alguna acció il·lícita.

- Mínim privilegi, els privilegis de cada usuari es reduiran al mínim estrictament necessari per complir les seves obligacions.

- Necessitat de Conèixer, els privilegis es limitaran de manera que els usuaris només accediran al coneixement d'aquella informació requerida per complir les seves obligacions.
- Capacitat d'autorització, només i exclusivament el personal amb competència d'autorització, podrà concedir, alterar o anul·lar l'autorització d'accés als recursos, conforme als criteris establerts pel seu responsable.

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

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant perfils (rols) de seguretat. Entenent com a perfil o rol una entitat que dona accés a una sèrie d'operacions.

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

13. PROTECCIÓ DE DADES DE CARACTER PERSONAL

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Sra. Ana Bastida Vila

Directora de Qualitat i Seguretat

14.**ANNEXOS**

14.1.**ANNEX 1A: VOLUMETRIA DELS SISTEMES D'INFORMACIÓ DE L'AJUNTAMENT**

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

SISTEMES D'INFORMACIÓ	
Núm. de SI	317
Núm. de SI basats en productes específics	no inventariats, aproximadament 40.
Núm. SI Classificats	314
Núm. SI afectats per l'ENS	317
Núm. SI revistats	60
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.

Es detalla a continuació la volumetria de la participació en que ha participat directament el Departament de Seguretat de l'IMI en el mateix objecte d'aquest contracte.

En els últims 3 exercicis s'ha participat en diferents intensitats en 60 projectes repartits:

2018	**2019**	**2020**
7	14	39

Els aspectes dels projectes que s'han revisat ad-hoc:

Clausulat seguretat	Marc normatiu	Incidents	Control normatiu
58	2	25 x any	8 x any

14.2.**ANNEX 1B: 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 exercicis s'ha participat en diferents intensitats en 82 projectes i 17 licitacions repartits amb diferents intensitats. De la participació en 82 projectes, 9 van ser projectes de seguretat distribuïts per exercicis. La dedicació prevista d'1 FTE cobreix la participació en 25 projectes per exercici.

Els aspectes del projectes que s'han revisat ad-hoc:

Arquitectura	Ubicació (cloud)	Integracions/ connectivitat	Clausulat	Criptografia	Traçabilitat
21	1	23	58	2	48

14.3.**ANNEX 2: CRITERIS DE LA CLASSIFICACIÓ DE LA INFORMACIÓ**

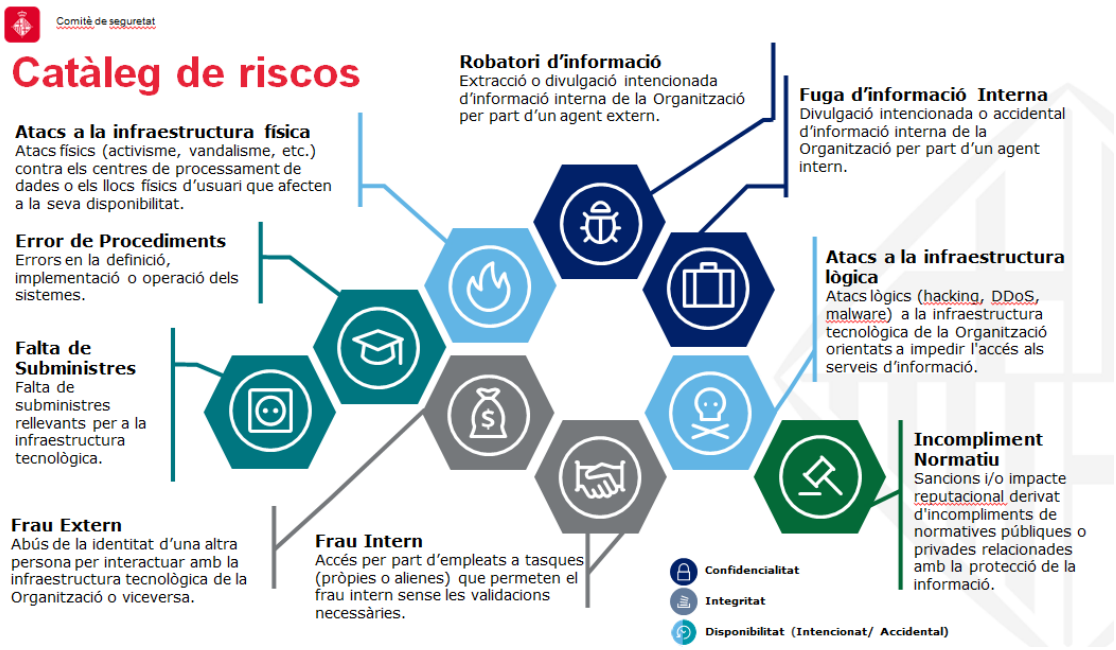
Els criteris comuns aplicables a totes les dimensions de tipus d'informació i serveis serien els que es detallen a continuació:

	No Adscrit (N/A)	BAIX	MIG	ALT
Disposició legal o administrativa	No existeix cap disposició legal que condicioni el seu nivell.	Per disposició legal o administrativa: llei, decret, ordre, reglament...	Per disposició legal o administrativa: llei, decret, ordre, reglament...	Per disposició legal o administrativa: llei, decret, ordre, reglament...
Perjudici Directe al ciutadà	No suposa cap prejudici directe al ciutadà	Algun perjudici al ciutadà	Danys importants, encara que reparables al ciutadà	Danys greus de difícil o impossible reparació al ciutadà

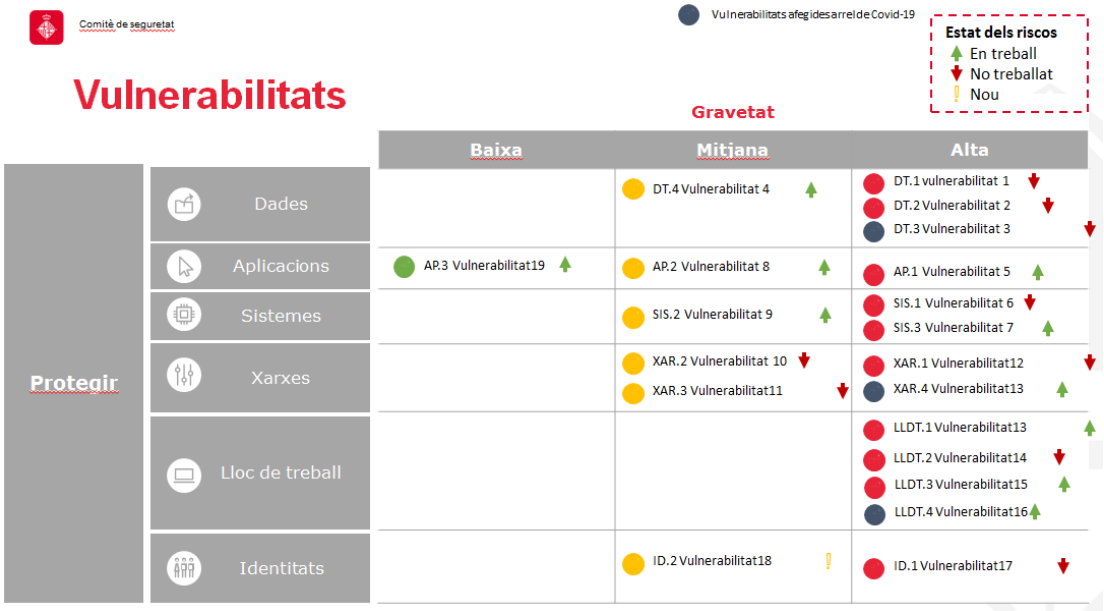
		No Adscrit (N/A)	BAIX	MIG	ALT
Incompliment d'una Norma	**Legal**	No implica incompliment d'una norma jurídica	Implica un incompliment de forma lleu d'una norma jurídica, de caràcter reparable	Incompliment material d'una norma jurídica, o incompliment formal no reparable	Incompliment greu d'una norma jurídica
	Regulatòria	No implica incompliment d'una normativa de regulador	Implica incompliment d'una normativa de regulador	Implica sanció significativa d'un regulador	Implica sanció greu d'un regulador i/o pèrdua de la llicencia d'operar
	Contractual	No implica incompliment d'una obligació contractual	Incompliment lleu d'una obligació contractual	Incompliment material o formal d'una obligació contractual	Incompliment greu d'una obligació contractual
	Interna	No implica incompliment d'una normativa interna	Incompliment lleu d'una norma interna	Incompliment material o formal d'una norma interna	Incompliment greu d'una norma interna
Pèrdues econòmiques		No implica pèrdues econòmiques	Pèrdues econòmiques apreciables (inferior a 100.000 €)	Pèrdues econòmiques importants (entre 100.000 i 1.000.000 €)	Pèrdues econòmiques o alteracions financeres significatives (superiors a 1.000.000 €)
Reputació		No implica dany reputacional	Dany reputacional apreciable amb els ciutadans o amb altres organitzacions	Dany reputacional important amb els ciutadans o amb altres organitzacions	Dany reputacional greu amb els ciutadans o amb altres organitzacions
Protestes		No es preveu que pugui desembocar en protestes	Múltiples protestes individuals	Protestes publiques (alteració de l'ordre públic)	Protestes massives (alteració seriosa de l'ordre públic)
Delictes		No facilitaria la comissió de delictes ni dificultaria la seva investigació	Afavoriria la comissió de delictes	Afavoriria significativament la comissió de delictes o dificultaria la seva investigació	Incitaria a la comissió de delictes, constituiria en sí un delicte, o dificultaria enormement la seva investigació.

14.4.**ANNEX 3: GESTIÓ DE RISCOS**

Catàleg de Riscs actual:



Fixes resum de Vulnerabilitats que apliquen a la Organització:



Fitxa descriptiva de la vulnerabilitat:

Comitè de seguretat

Mapa de riscos

Identitats

ID.2– Vulnerabilitat2

Vulnerabilitat	Riscos associats	Gravetat
Accions de mitigació	**Cost estimat**	

14.5.**ANNEX 4: 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:

*Contracte Oficina GRC: [**Número d'expedient del contracte**]*

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

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

La sessió informativa presencial, on es dona resposta a totes les consultes rebudes per correu electrònic, podrà resultar anul·lada, amb motiu de les mesures organitzatives que se n'adoptin a causa de la COVID-19, determinades pel Comitè de Seguiment de l'Ajuntament de Barcelona en coordinació amb l'Agència de Salut Pública de Barcelona.

En cas que es pugui convocar aquesta sessió informativa, aquesta sessió es celebrarà a partir dels 5 dies hàbils posteriors al dia següent de la data de publicació de l'anunci de licitació a la plataforma de contractació pública del perfil del contractant. El lloc, el dia i l'hora d'aquesta sessió es publicarà a l'anunci de licitació en el perfil del contractant.https://contractaciopublica.gencat.cat/ecofin_pscp/AppJava/cap.pscp?reqCode=viewDetail&idCap=15990903