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

Plec de prescripcions tècniques per a la contractació dels Serveis d'elaboració del Pla Director de Seguretat Integral 2025-2028 de l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible

ÍNDEX

1. INTRODUCCIÓ

L'Ajuntament de Barcelona gestiona una ciutat d'1,6 milions de ciutadans, unes 200.000 empreses i un teixit associatiu format per més de 10.000 entitats. Disposa d'una oferta de serveis molt àmplia, emmarcada en diferents àmbits: serveis socials, mobilitat, educació, salut, cultura i oci, promoció econòmica, 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 per al ciutadà i per a la mateixa ciutat. Això implica protegir la informació personal del ciutadà, garantir la continuïtat dels serveis i salvaguardar la gestió de la ciutat i de l'Administració Municipal. La informació relativa a aquests serveis es troba distribuïda en un gran nombre de sistemes d'informació i fitxers legals, la qual cosa requereix disposar de serveis d'identificació, protecció, prevenció i reacció davant les amenaces que poden afectar els sistemes d'informació i les infraestructures TIC. Aquestes mesures són essencials per reduir i minimitzar els riscos d'incidents de seguretat i ciberatacs.

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

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

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

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

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

L'Institut Municipal d'Informàtica (d'ara endavant, IMI) té delegades les funcions de Seguretat en les Tecnologies de la Informació i Comunicació de l'Ajuntament de Barcelona, i exerceix de

Responsable de Seguretat TIC, en funció de la seva organització interna, d'acord amb els preceptes, estàndards internacionals en matèria de seguretat TIC i en especial, amb els requeriments que l'ENS i la normativa de Protecció de Dades Personals estableix respecte dels entorns automatitzats.

L'Ajuntament vol revisar el seu **Model de Gestió de la Seguretat**, que constitueix el marc en què es desenvolupen els programes de Seguretat Corporatius. Aquest marc, basat principalment en l'ENS i en estàndards internacionals com el NIST framework i les normes ISO de la família 27000, especialment la ISO 27001, defineix les línies d'actuació, projectes i serveis necessaris per donar resposta als reptes de protecció i seguretat que afronta l'Ajuntament, amb l'objectiu de: garantir una gestió segura, fiable i eficient de la informació i els serveis públics que ofereix a la ciutadania.

El **Pla Director de Seguretat de la Informació** de l'Ajuntament es desenvolupa en resposta a la necessitat d'integrar i coordinar tots els esforços relacionats amb la seguretat de la informació en un únic marc de treball coherent. Aquest pla es concep com un document viu, que ha de ser revisat i actualitzat periòdicament per adaptar-se a les noves amenaces, tecnologies emergents i canvis normatius que puguin afectar la seguretat de la informació.

Els objectius del Pla Director de Seguretat de la Informació de l'Ajuntament són els següents:

- **Protegir la informació sensible**: Garantir la confidencialitat, integritat i disponibilitat de la informació gestionada per l'Ajuntament, assegurant que només les persones autoritzades puguin accedir a dades sensibles i que aquestes es mantinguin íntegres i disponibles quan es necessiten.
- **Assegurar la continuïtat dels serveis:** Establir mesures de seguretat per a prevenir interrupcions en els serveis municipals, així com per a garantir la seva recuperació ràpida i eficient en cas d'incidents de seguretat o ciberatacs.
- **Complir amb la normativa vigent**: Assegurar que totes les activitats relacionades amb la gestió de la informació es realitzin en compliment amb les normatives locals, nacionals i internacionals, especialment l'Esquema Nacional de Seguretat (ENS) i altres regulacions aplicables.
- **Minimitzar els riscos de ciberseguretat**: Identificar, avaluar i mitigar els riscos associats a la seguretat de la informació mitjançant la implementació de controls de seguretat adequats, que redueixin la probabilitat i l'impacte dels incidents de seguretat.
- **Sensibilitzar i formar al personal**: Promoure una cultura de seguretat de la informació entre tots els empleats de l'Ajuntament, proporcionant formació contínua i sensibilització sobre les millors pràctiques en seguretat, així com sobre les seves responsabilitats per protegir la informació.
- **Millora contínua**: Establir un procés continu d'avaluació i millora dels mecanismes de seguretat, basat en auditories periòdiques, revisions de riscos i actualització de les polítiques de seguretat per adaptar-se a les noves amenaces i tecnologies.

- **Model de govern de seguretat**: Definir un model de Governança de la Seguretat de la Informació per a l'Ajuntament basat en un enfocament integrador i coherent, que asseguri una gestió unificada i alineada amb els objectius estratègics establerts. Aquest model s'ha d'aplicar a tots els ens municipals considerant la seva maduresa, garantint una estructura de governança robusta i eficient en matèria de seguretat de la informació.

Es licita en aquest contracte la elaboració del Pla Director de Seguretat Integral.

2. OBJECTE

L'objecte d'aquest contracte són els serveis per d'elaboració d'un Pla Director de Seguretat Integral per a l'Ajuntament de Barcelona, amb mesures de contractació pública sostenible.

Aquest Pla Director ha d'incloure tant la ciberseguretat com la seguretat física, i on estiguin presents actius de informació i comunicacions, amb la finalitat de poder anticipar esdeveniments d'alt impacte, d'acord amb diversos frameworks de referència.

A més a més haurà de contemplar els següents aspectes clau que es relacionen a continuació:

- Alineació estratègica amb el negoci.
- Integració entre seguretat lògica i física allà on es consideri necessari.
- Escalabilitat entre ens municipals.
- Anàlisi de riscos, amenaces i tendències en matèria de seguretat
- Estimació de costos (CAPEX i OPEX) per la execució del Pla
- Anàlisi de les capacitats de l'Organització per la execució del Pla

3. ABAST

L'abast del Pla Director de Seguretat Integral inclourà tots els àmbits i components crítics de l'organització, amb l'objectiu de garantir una protecció completa i coordinada davant de possibles riscos i amenaces. Aquest document definirà els límits i les àrees específiques en què s'implementaran les mesures de seguretat tant a nivell lògic com físic, assegurant que cap aspecte rellevant quedi fora de la seva cobertura.

- **Àmbit Organitzacional:** El Pla Director abastarà totes les Gerències, Organismes Autònoms Locals, Entitats públiques Empresarials i Societats Mercantils Municipals, tenint en compte les particularitats de cadascuna i assegurant que les mesures de seguretat siguin efectives i adequades a cada context i garantint una aplicació homogènia i adaptada a les necessitats i

normatives aplicables. De igual forma, en la definició del model de govern s'haurà de tenir en compte la existència de Societats Mercantils amb participació minoritària, Consorcis, Fundacions i Associacions.

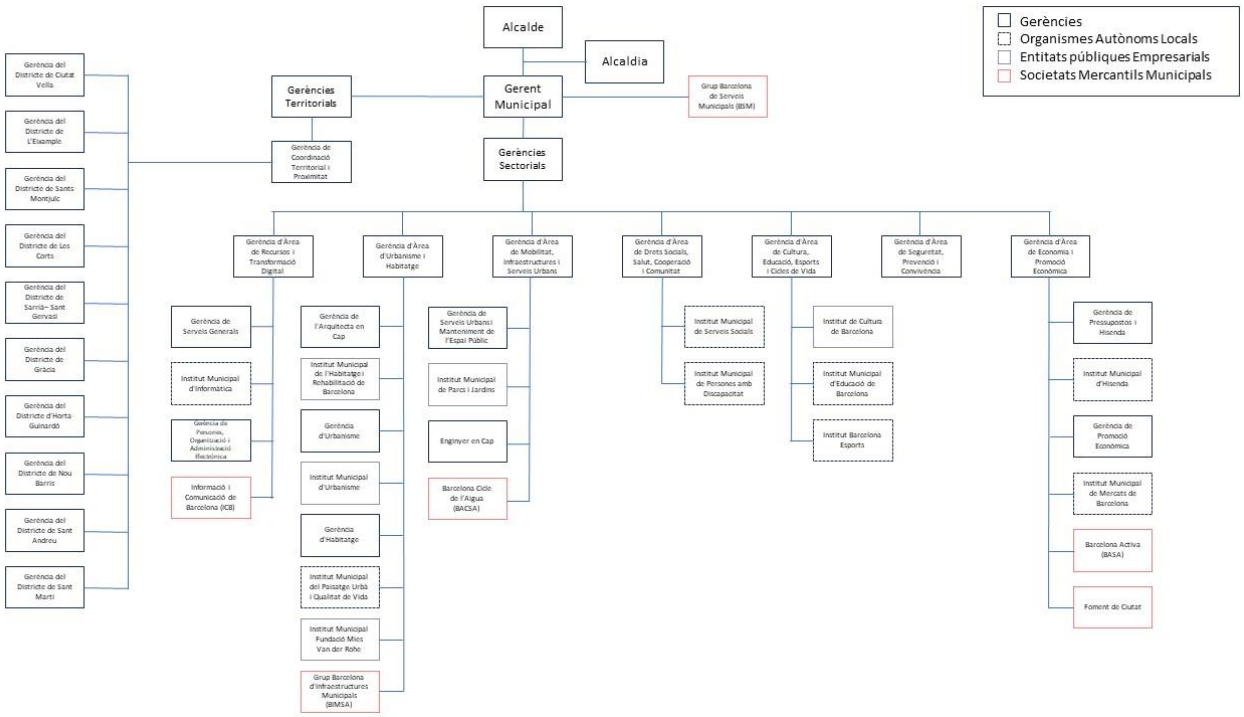

Figura 1 – Estructura organitzativa

- **Àmbit de Seguretat Lògica i Ciberseguretat**: El Pla inclourà totes les infraestructures tecnològiques i sistemes d'informació de l'organització, com ara xarxes, bases de dades, aplicacions, dispositius de maquinari (IT i OT), i qualsevol altre recurs digital. S'abordarà la protecció contra ciberamenaces, garantint la confidencialitat, integritat i disponibilitat de la informació, així com la resiliència dels sistemes davant de ciberatacs.

- **Àmbit de Seguretat Física**: El Pla Director cobrirà la protecció física de les infraestructures, incloent edificis, instal·lacions crítiques, centres de dades, i altres béns tangibles de l'organització amb possible impacte en la informació municipal. Es contemplaran mesures com el control d'accés, vigilància, protecció contra incendis, i altres estratègies per assegurar la integritat física de les dades.

- **Àmbit de Gestió de Riscos**: L'abast del Pla inclou un enfocament global en la gestió de riscos, considerant tant els riscos operatius com els tàctics i estratègics. Es desenvoluparà un mapa

de riscos que identifiqui i classifiqui els riscos a tots els nivells de l'organització, amb propostes específiques per a la seva mitigació, transferència, acceptació o eliminació.

- **Àmbit de Compliment Normatiu**: El Pla assegurarà el compliment de totes les normatives aplicables a la seguretat de la informació i seguretat física, tant a nivell nacional com internacional, incloent de forma explícita l'ENS (Esquema Nacional de Seguretat).

- **Àmbit Temporal**: El Pla Director de Seguretat Integral tindrà un abast temporal que cobrirà un període plurianual, amb revisions i actualitzacions periòdiques per adaptar-se als canvis en l'entorn de seguretat, les noves amenaces i les innovacions tecnològiques.

Aquest abast garantirà que el Pla Director de Seguretat Integral cobreixi de manera exhaustiva totes les dimensions de la seguretat necessàries per a la protecció eficient i efectiva de l'organització Municipal, assegurant la continuïtat del negoci i la confiança dels seus ciutadans i proveïdors.

Es pot trobar més informació sobre la volumetria dels sistemes d'informació gestionats per l'IMI a l'apartat 15.1 *Annex 1: Abast a Organització Municipal i 15.2 Annex 2 Volumetria dels tractaments i sistemes d'informació de l'Ajuntament* d'aquest plec.

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

3.1. SERVEIS NO INCLOSOS

Queden exclosos de l'objecte d'aquest contracte els serveis d'adquisició de llicències de software que quedin en propietat de l'IMI.

També 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

4. DESCRIPCIÓ DEL SERVEI

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

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

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

4.1. DEFINICIÓ DEL GOVERN DE SEGURETAT INTEGRAL

L'adjudicatari haurà de definir una estructura clara i funcional per al Govern de Seguretat Integral de l'Ajuntament, garantint una gestió eficaç i coordinada que englobi totes les dimensions de la seguretat: seguretat lògica (tant IT com OT), seguretat física, i la integració amb altres àmbits clau com la seguretat en la cadena de subministrament i en la gestió de projectes. L'estructura proposada haurà de permetre una resposta ràpida i eficient davant de qualsevol amenaça o incident, promovent una cultura de seguretat robusta i un alt nivell de resiliència organitzativa.

Es proposarà un model que combini una estructura centralitzada per a la presa de decisions estratègiques amb la flexibilitat necessària per a la gestió operativa descentralitzada en les diferents àrees de l'Ajuntament. Aquest model ha de permetre una coordinació efectiva entre els equips i departaments responsables de la seguretat.

L'adjudicatari haurà de definir clarament els rols i responsabilitats de cada participant en el govern de la seguretat integral. Això inclou la designació de responsables de seguretat tant a nivell corporatiu com en les diferents àrees funcionals, amb una atenció especial a la seguretat de la informació (IT i OT per separat), la seguretat física, i la gestió dels incidents.

El model de govern de Seguretat Integral haurà de cobrir els següents aspectes:

4.1.1.Estructura del Govern de la Seguretat

L'adjudicatari haurà de proposar una estructura organitzativa per al govern de la seguretat, que com a mínim inclogui els següents elements:

- **Comitè Executiu de Seguretat**: Aquest serà l'òrgan superior de governança, responsable de definir la política de seguretat integral i de prendre decisions estratègiques . L'adjudicatari definirà la composició, funcions i responsabilitats del Comitè.
- **Oficina de Seguretat de la Informació**: Aquesta serà l'encarregada de la implementació operativa de les polítiques i estratègies definides pel Comitè Executiu, coordinant les activitats de seguretat diàries a través de tots els departaments i sectors. L'adjudicatari proposarà la configuració d'aquesta Oficina, incloent les seves funcions específiques, el nombre de membres necessaris i les seves responsabilitats.
- **Coordinadors de Seguretat per Ens Municipal**: Serà la responsable de responsable de supervisar la implementació de les polítiques de seguretat i de gestionar els riscos específics

del seu àmbit . L'adjudicatari haurà de determinar els rols i funcions dels coordinadors de seguretat en els diferents ens municipals, així com la seva relació amb l'Oficina de Seguretat de la Informació.

4.1.2.Quadre de Comandament per al Govern de la Seguretat Integral

L'adjudicatari haurà de desenvolupar un Quadre de Comandament per al Govern de la Seguretat Integral que permeti monitoritzar de manera efectiva l'estat de la seguretat a l'Ajuntament. Aquest quadre de comandament serà una eina clau per a la presa de decisions, ja que proporcionarà una visió integral de l'acompliment en matèria de seguretat tant a nivell lògic com físic. Es valorarà la metodologia proposada així com el pla d'implantació viable amb referències a l'obtenció d'objectius i resultats.

Els aspectes que s'hauran de considerar per a la seva elaboració inclouen:

- **Definició d'Indicadors Clau de Rendiment (KPIs):** Es definiran indicadors específics que mesurin aspectes crítics de ciberseguretat en base a frameworks de referència, que permetin monitoritzar l'eficàcia dels controls implementats. S'inclouran indicadors que mesurin l'eficàcia de la coordinació tant interna com externa amb altres agents de seguretat, com el CCN, l'Agència de Ciberseguretat de Catalunya, i altres entitats col·laboradores.
- **Metodologia de Recollida de Dades:** Es detallarà quines seran les fonts de dades per a cada indicador, especificant si provindran de sistemes interns, auditories, o col·laboradors externs. S'establirà també la freqüència amb la qual es recolliran les dades per a cada indicador, garantint que aquesta sigui suficient per a proporcionar informació actualitzada i rellevant.
- **Estructura del Quadre de Comandament:** Es definiran els formats visuals i de presentació del quadre de comandament, assegurant que sigui intuïtiu i fàcil d'interpretar per als responsables de la seguretat i altres parts interessades. El quadre de comandament haurà de permetre visualitzar la informació a diferents nivells de detall, des d'una visió general estratègica amb un llenguatge entenedor per les diferents Gerències fins a una anàlisi específica per a cada àmbit de seguretat.
- **Procediment de Revisió i Actualització:** S'establiran procediments regulars per a la revisió i actualització del quadre de comandament, assegurant que es mantingui alineat amb els objectius estratègics de l'Ajuntament i amb les tendències i riscos emergents en matèria de seguretat. Es definirà un procés per a introduir de forma autònoma ajustaments i millores en els indicadors i metodologies utilitzades, basant-se en l'experiència adquirida i en els canvis en l'entorn de seguretat.
- **Integració amb el Sistema de Gestió de Seguretat** El quadre de comandament haurà de ser compatible i estar integrat amb el sistema global de gestió de seguretat de l'Ajuntament,

permetent una gestió centralitzada i coherent de tota la informació relacionada amb la seguretat.

Aquest Quadre de Comandament serà un element crític per a l'avaluació contínua i la millora del govern de la seguretat integral, oferint als responsables de l'Ajuntament una eina efectiva per a la presa de decisions informades.

4.1.3. Alineació Estratègica i Compliment Normatiu

L'adjudicatari haurà d'assegurar que el model de govern proposat estigui alineat amb els objectius estratègics de l'Ajuntament i compleixi amb totes les normatives legals i reguladores aplicables. Això inclou:

- **Alineació amb els Objectius Estratègics**: Demostrar com el model de govern de la seguretat contribuirà a l'assoliment dels objectius estratègics de l'organització.
- **Compliment Normatiu**: Garantir que el model complirà amb l'Esquema Nacional de Seguretat (ENS) i qualsevol altra normativa local, nacional o internacional pertinent.

4.1.4. Proposta de Mecanismes de Coordinació i Comunicació

L'adjudicatari haurà de definir els mecanismes de coordinació entre els diferents rols i nivells implicats en Seguretat Integral, així com els canals de comunicació interna i externa:

- **Mecanismes de Coordinació Interna**: Descripció de com es coordinaran les activitats de seguretat entre el Comitè Executiu de Seguretat, l'Oficina de Seguretat de la Informació , els coordinadors de seguretat locals i la resta de rols identificats.
- **Canals de Comunicació Interna**: Proposta de canals de comunicació que assegurin una transmissió fluïda i efectiva de la informació relacionada amb la seguretat a tots els nivells de l'organització.
- **Model de Relació amb Altres Agents Externs de Seguretat**: L'adjudicatari haurà de proposar un model de relació amb entitats externes clau, com el Centre Criptològic Nacional (CCN) i el CCN-CERT, l'Agència de Ciberseguretat de Catalunya i el Catalonia-SOC, els Mossos d'Esquadra, la Federació Espanyola de Municipis i Províncies (FEMP), les Agències de Certificació (CAOC Certificats) i/o el Grup de 50 Ciutats Grans. Aquest model ha de permetre una coordinació efectiva i fluida amb aquests actors externs, facilitant la col·laboració i l'intercanvi d'informació per a una millor gestió de la seguretat.

4.1.5. Planificació i recursos

L'adjudicatari haurà de proporcionar una estimació detallada dels recursos personals i econòmics necessaris per a la implementació i manteniment del govern de la seguretat integral. Això inclou la identificació de les competències clau, la formació necessària per als equips, i la planificació dels recursos materials i financers.

L'adjudicatari haurà de proposar quines funcions del govern de la seguretat podrien externalitzar-se per millorar l'eficiència operativa o reduir costos, mantenint sempre els estàndards de seguretat requerits. Aquesta proposta haurà de tenir en compte les capacitats internes de l'Ajuntament i les condicions del mercat.

4.1.6.Documentació i Justificació del Model Proposat

L'adjudicatari haurà de proporcionar tota la documentació necessària que justifiqui la seva proposta de model de govern de Seguretat Integral, incloent anàlisis comparatives amb models similars en altres administracions públiques similars, identificant avantatges i possibles àrees de millora.

Aquest apartat ha de ser desenvolupat amb la finalitat de garantir que el govern de Seguretat Integral sigui robust, coherent i capaç d'afrontar els desafiaments de seguretat actuals i futurs de l'Ajuntament.

Aquestes activitats es duen a terme també pel coneixement, visibilitat i control de la seguretat de la informació davant la Direcció i les Gerències de l'Ajuntament, i per tant inclouen també aquest objectiu.

4.1.7.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Organigrama del Govern de la Seguretat:	Definir les eines de govern del grup Municipal incloent un organigrama detallat que reflecteixi la distribució dels rols i responsabilitats que exigeix ENS, dins de l'estructura de govern de la seguretat, incloent el Comitè de Seguretat, el Responsable de Seguretat Corporativa, l'Oficina de Seguretat de la Informació, i els Coordinadors de Seguretat per Entitat Municipal.	1 Model de Govern al grup Municipal	Documentació on s'estableix el model de Govern Document d'assignació de membres al comitè
Descripció de Rols i Responsabilitats	Definir les funcions i responsabilitats de cada un dels rols identificats en l'organigrama, així com la seva interrelació.	1 definició de Rols i responsabilitats corporatives.	Document d'Aprovació de la norma de rols i responsabilitats.

Descripció	Tasques	Volumetria	Lliurables
Document de Disseny del Quadre de Comandament	Detallar les funcionalitats que ha de tenir el quadre de comandament, incloent els indicadors clau de rendiment (KPIs), la metodologia de recollida de dades, les fonts de dades, i els criteris de visualització.	1 Document d'Especificacions Funcional i Tècnica 1 Maqueta del Quadre de Comandament mostrant com es presentaran els indicadors i la informació de seguretat, així com els diferents nivells de detall disponibles	Document d'Especificacions Funcional i Tècnica Maqueta del Quadre de Comandament
Quadre de Comandament Operatiu	Elaborar una versió preliminar del quadre de comandament amb funcionalitats bàsiques, que permeti la visualització inicial dels indicadors clau.	1 Prototip Funcional	Prototip funcional

Descripció	Tasques	Volumetria	Lliurables
Manual d'Ús i Formació del Quadre de Comandament	Detallar el funcionament del quadre de comandament, incloent instruccions per a la navegació, la interpretació dels indicadors, la configuració de paràmetres, i la generació de informes. Elaborar material de formació del Quadre incloent presentacions, vídeos tutorials i guies ràpides, així com un calendari de sessions de formació presencial o virtual.	1 Guia d'Ús del Quadre de Comandament 1 Material didàctic per a la formació del personal de l'Ajuntament en l'ús del quadre de comandament	Guia d'Ús del Quadre de Comandament Material de Formació
Proposta de Funcions per a Outsourcing	Elaborar informe amb la identificació de les funcions de seguretat que es podrien externalitzar, incloent-hi una anàlisi dels avantatges i riscos associats a aquesta externalització.	1 Informe	Proposta de Funcions per a Outsourcing

Descripció	Tasques	Volumetria	Lliurables
Pla de supervisió i control	Detallar els mecanismes de supervisió i control que s'implementaran per garantir el compliment continu de les polítiques de seguretat, incloent la freqüència d'auditories i la gestió de no conformitats.	1 pla	1 pla de supervisió i control
Pla de Formació	Detallar la metodologia, el calendari, continguts i canals per a les activitats de formació per poder implementar el model de Govern proposat	1 pla	1 pla de Formació
Informe d'Alineació Estratègica	Descriure com el model de govern de la seguretat proposat s'alinea amb els objectius estratègics de l'Ajuntament, incloent una anàlisi detallada dels beneficis esperats.	1 Informe	1 Informe d'Alineació Estratègica

Descripció	Tasques	Volumetria	Lliurables
Pla de Coordinació Interna	Detallar com es coordinaran les activitats de seguretat entre els diferents rols dins de l'organització, incloent la dinàmica del Comitè de Seguretat i l'Oficina de Seguretat de la Informació.	1 pla	1 pla de Coordinació interna
Pla de Comunicació Interna	Detallar els canals i mètodes de comunicació interna per assegurar que tota la informació crítica en matèria de seguretat sigui compartida de manera eficient dins l'organització.	1 pla	1 pla de Comunicació interna
Model de Relació amb Agents Externs	Detallar el model de relació amb agents externs de seguretat, El model ha d'incloure els mecanismes de col·laboració, intercanvi d'informació i coordinació en cas de necessitats conjuntes.	1 Model de relació	1 Model de Relació amb Agents Externs

Descripció	Tasques	Volumetria	Lliurables
Anàlisi Comparativa	Comparar el model de govern de la seguretat proposat amb models existents en altres organitzacions del mateix sector, destacant avantatges, limitacions i possibles àrees de millora.	1 informe	1 informe comparatiu
Document justificatiu	Descriure en detall les raons per les quals el model de govern de la seguretat proposat és l'adequat per a l'Ajuntament, basat en l'anàlisi de riscos, necessitats operatives i normatives.	1 Document justificatiu	1 Document justificatiu

4.2. ELABORACIÓ DE L'ANÀLISI D'IMPACTE DE NEGOCI (BIA)

Aquest servei respon a l'objectiu últim de mesurar la gravetat de les amenaces potencials i com aquestes podrien afectar les operacions i les finances de l'Ajuntament. Aquest anàlisi ha d'identificar els processos de negoci més crítics per a l'Ajuntament, analitzant quin impacte es produiria en cas que ocorregués un incident que causés la interrupció d'aquests processos.

L'elaboració de l'anàlisi d'impacte de negoci (BIA) haurà de cobrir els següents aspectes:

4.2.1.Realització d'entrevistes amb departaments involucrats

La realització d'entrevistes amb els departaments involucrats és una part important de l'elaboració de l'Anàlisi d'Impacte de Negoci (BIA) de l'Ajuntament. Aquest procés té com a objectiu principal recollir informació detallada sobre els processos crítics de cada departament, les seves dependències, i els requisits específics de recuperació en cas d'incidència.

L'adjudicatari serà responsable de coordinar i programar entrevistes amb els responsables de cada departament, així com amb coordinadors i personal tècnic que juguen un paper clau en la gestió i operativa dels serveis crítics. Durant aquestes entrevistes, es recolliran dades essencials sobre com

cada procés interactua dins de l'organització, quines són les seves dependències externes i internes, i quin impacte tindria la seva interrupció sobre l'entitat.

Es farà especial èmfasi en identificar els punts de vulnerabilitat i en entendre les expectatives i necessitats de recuperació del personal entrevistat. L'adjudicatari haurà d'assegurar-se que el format de les entrevistes permeti una recollida de dades eficaç i ordenada, facilitant la posterior anàlisi i integració de la informació recollida en el document final del BIA.

Aquestes entrevistes no només ajudaran a identificar els processos més crítics, sinó que també fomentaran una major comprensió i col·laboració interdepartamental en matèria de seguretat i continuïtat de negoci.

4.2.2.Identificació de Processos de Negoci Crítics

Aquesta etapa té per objectiu determinar quins processos són essencials per al funcionament i la resiliència de l'organització, i quins requeririen una atenció prioritària en situacions d'emergència o de crisi.

L'adjudicatari haurà d'analitzar exhaustivament totes les funcions i serveis oferts per l'Ajuntament recollits en les entrevistes prèvies per identificar aquells que, en cas de fallida o interrupció, podrien provocar conseqüències severes per a l'operativitat, la seguretat, la reputació, o el compliment normatiu de l'entitat. Aquesta identificació es basarà en criteris com la importància estratègica del procés, l'impacte de la seva interrupció en els serveis ciutadans, i les conseqüències legals o econòmiques de la seva fallida.

Durant aquesta fase, l'adjudicatari també haurà de classificar els processos segons la seva criticitat i establir clarament els vincles entre aquests processos crítics i altres activitats o infraestructures de l'Ajuntament. Això inclou la identificació de les dependències crítiques internes i externes que poden afectar la continuïtat d'aquests processos.

Finalment, es desenvoluparà una documentació detallada que inclogui descripcions dels processos, els motius de la seva criticitat, i les implicacions d'una possible interrupció. Aquesta informació serà clau per prioritzar les accions de mitigació de riscos i planificar les estratègies de recuperació adequades.

4.2.3.Avaluació dels Tipus d'Impacte

Aquesta fase té com a objectiu quantificar i qualificar les repercussions que la interrupció dels processos de negoci crítics identificats pot tenir sobre l'Ajuntament.

L'adjudicatari haurà de realitzar un estudi detallat per determinar l'impacte operacional, econòmic, de reputació i legal de la interrupció de cada procés. Aquest anàlisi inclourà:

- **Impacte Operacional**: Mesurament de com la interrupció afecta la capacitat de l'Ajuntament per oferir serveis essencials, incloent la interrupció del servei a ciutadans i altres operacions internes.

- **Impacte Econòmic**: Avaluació de les pèrdues econòmiques directes i indirectes, incloent pèrdues d'ingressos, costos addicionals que s'han d'assumir per restablir el servei i possibles penalitzacions per incompliment de contractes.
- **Impacte de Reputació**: Anàlisi de com una interrupció podria afectar la percepció pública de l'eficàcia i la fiabilitat de l'Ajuntament.
- **Impacte Legal i Contractual**: Examinació de les possibles violacions de normatives o acords contractuals que podrien derivar en sancions o litigis.

Cada tipus d'impacte s'haurà de documentar detalladament, especificant els possibles escenaris d'interessos i les seves implicacions. Aquesta informació ajudarà a l'Ajuntament a entendre millor els riscos associats a cada procés i a desenvolupar plans de recuperació més efectius per mitigar els impactes identificats..

4.2.4.Definició d'Objectius Temporals de Recuperació

Aquesta tasca consisteix en l'establiment de paràmetres claus que orientaran la resposta de l'Ajuntament davant d'una interrupció de serveis. L'adjudicatari serà responsable de determinar els següents objectius per a cada procés de negoci crític identificat:

- **RTO (Recovery Time Objective):** L'adjudicatari haurà de definir el temps màxim acceptable que un procés pot romandre interromput abans que la restauració sigui imprescindible per evitar conseqüències inacceptables. Aquest objectiu ajudarà a prioritzar els esforços de recuperació basats en la criticitat dels processos.
- **MTD (Maximum Tolerable Downtime):** Especificació del temps màxim que l'Ajuntament pot tolerar sense aquest procés sense que es produeixin efectes catastròfics per a l'organització. Aquesta mètrica està estretament relacionada amb l'RTO i serveix per a fixar límits temporals en les estratègies de recuperació.
- **RPO (Recovery Point Objective):** Determinació de la quantitat màxima de pèrdua de dades que es pot acceptar resultant d'una interrupció del servei. L'RPO defineix fins a quin punt en el temps pot retrocedir el sistema en la restauració de dades, i es basa en la freqüència amb la qual es realitzen les còpies de seguretat de les dades crítiques.

L'adjudicatari haurà de treballar estretament amb els diferents departaments per assegurar que els objectius de recuperació estiguin alineats amb les necessitats operacionals i les expectatives de cada àrea. Aquesta informació serà essencial per desenvolupar plans de recuperació efectius que minimitzin el temps d'inactivitat i la pèrdua de dades, garantint així la continuïtat de l'operativitat municipal en cas d'incidència.

4.2.5.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Informe de BIA Complet	Identificar els processos de negoci crítics, avaluar els tipus d'impacte (operacional, econòmic, de reputació, legal i contractual), i definir els objectius temporals de recuperació (RTO, MTD, RPO) per a cada procés crític. Detallar les metodologies utilitzades per a l'avaluació i els resultats obtinguts.	1 informe per Gerència Sectorial de l'Ajuntament (7 en total) 1 informe per totes les Gerències Territorials 1 informe global agregat	Informe de BIA
Base de Dades de Processos de Negoci Crítics	Agrupar tota la informació recollida durant l'elaboració del BIA, incloent detalls sobre els processos crítics, les seves dependències, impactes potencials i els objectius de recuperació establerts.	1 Base de dades	Base de Dades de Procesos Crítics de Negoci
Pla de Priorització de Recuperació	Establir l'ordre de prioritat per la recuperació de serveis basat en els RTO i MTD identificats, assegurant que els recursos estiguin alineats amb les necessitats més crítiques en cas d'incident	1 Pla	Pla de Priorització de Recuperació
Directrius per a l'Actualització del BIA	Detallar el procés per a les revisions periòdiques i actualitzacions del BIA, incloent criteris per a la reavaluació dels processos de negoci i la seva criticitat en resposta a canvis en l'entorn operacional o estratègic de l'Ajuntament	1 Document	Directrius per a l'Actualització del BIA

Descripció	Tasques	Volumetria	Lliurables
Materials de formació	Elaborar materials de formació destinats a educar al personal de l'Ajuntament sobre la importància del BIA, el reconeixement de processos crítics i les pràctiques recomanades per a la gestió de la continuïtat del negoci. Aquests materials podrien incloure guies, tutorials, i seminaris web.	Materials de formació	Materials de formació
Informe dels Beneficis Clau del BIA	Detallar els beneficis clau obtinguts de l'anàlisi BIA, incloent la millora en la gestió de riscos, la reducció de costos per interrupcions, i la millora de la cooperació entre departaments.	1 Informe	Informe dels Beneficis Clau del BIA

4.3. ELABORACIÓ DEL MAPA DE RISCOS DE SEGURETAT INTEGRAL

Aquest servei respon a l'objectiu últim d'identificar i avaluar el risc de seguretat integral a totes les Gerències i organismes de l'Ajuntament de Barcelona incloses en l'abast del contracte. L'objectiu és elaborar un Mapa de Riscos de Seguretat Integral per a l'Ajuntament, que identifiqui, classifiqui i avaluï els riscos associats tant a la seguretat lògica (ciberseguretat en xarxes IT i OT) com a la seguretat física. Aquest mapa de riscos serà una eina fonamental per a la gestió proactiva dels riscos i la presa de decisions en matèria de seguretat integral i dona compliment del control ([op.pl.1] d'Anàlisis de Riscos de nivell MIG de l'ENS.

L'Ajuntament posarà a disposició de l'adjudicatari l'eina de GRC (RSA Archer) desplegada pels àmbits funcionals de compliment i per gestió de riscos. Actualment es disposa dels següents mòduls de RSA Archer: Issues Management, IT Controls i IT RIsk Management. En cas que per a l'execució del projecte es requereixin llicències addicionals a les que actualment posseeix l'Ajuntament, l'adjudicatari serà responsable d'obtenir-les i de transferir els drets d'aquestes llicències a l'Ajuntament un cop obtingudes.

L'elaboració del mapa de riscos de seguretat integral haurà de cobrir els següents aspectes:

4.3.1. Elaboració del Catàleg d'Amenaces

L'adjudicatari haurà d'elaborar un Catàleg de Amenaces que identifiqui les amenaces potencials a les quals pot estar exposat l'Ajuntament, considerant les últimes tendències en ciberseguretat i seguretat física, així com els canvis en el marc legal i regulador. Aquest catàleg haurà de basar-se en frameworks reconeguts a nivell internacional, com ara el definit a PILAR, l'ISO 27005, o el NIST Risk Management Framework, assegurant així una cobertura completa de les possibles amenaces.

El catàleg d'amenaces haurà de ser adaptat per reflectir les especificitats de l'Ajuntament, tenint en compte factors com la ubicació geogràfica, la infraestructura tecnològica, la naturalesa dels serveis prestats, i les interdependències entre sistemes.

Les amenaces identificades s'hauran de classificar segons diferents criteris, com ara la seva naturalesa (interna o externa), el tipus de risc (físic o lògic), i el seu possible impacte. Aquesta classificació facilitarà la posterior anàlisi de riscos i l'elaboració d'estratègies de mitigació.

4.3.2.Metodologia d'Anàlisi de Riscos

L'adjudicatari haurà **d'analitzar la metodologia de gestió de riscos de Seguretat** actualment en ús a l'Ajuntament, assegurant-se que aquesta metodologia s'alinea amb les necessitats actuals de l'organització i amb els estàndards internacionals de gestió de riscos.

En cas que la metodologia existent no sigui adequada, l'adjudicatari haurà de proposar una nova metodologia d'anàlisi de riscos, basada en frameworks reconeguts, com MAGERIT (Metodologia d'Anàlisi i Gestió de Riscos d'Informació), NIST SP 800-30 o altres metodologies compatibles amb les necessitats de l'Ajuntament.

L'adjudicatari haurà de revisar, millorar i incorporar la metodologia de gestió de **riscos associats a la cadena de subministrament**, sobre la qual podrà proposar millores per tal de garantir que els responsables dels contractes municipals puguin fer autoavaluació amb el proveïdor per garantir el compliment de la seguretat del seu contracte. Aquesta metodologia ha d'incloure la identificació de riscos vinculats amb els proveïdors, l'avaluació de la seva seguretat i la gestió de les interdependències amb els processos crítics de l'Ajuntament. Es valoraran aspectes com la ciberseguretat dels proveïdors, la seva solvència i la continuïtat del servei.

Es desenvoluparà una metodologia per a la **gestió de riscos específics en projectes**, incloent-hi projectes tecnològics, d'infraestructura i de desenvolupament. Aquesta metodologia haurà d'incloure l'avaluació de riscos des de la fase de planificació fins a la d'execució, assegurant que els projectes s'alineïn amb els objectius de seguretat i minimitzin els riscos identificats.

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

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

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

Un cop aprovada la metodologia, l'adjudicatari l'haurà d'aplicar per a, conjuntament amb el propietari del risc, identificar, analitzar i prioritzar els riscos associats a les amenaces catalogades. Això inclourà la determinació de la probabilitat de cada risc i el seu impacte potencial sobre les operacions de l'Ajuntament.

Per dur a terme aquesta tasca, l'adjudicatari haurà de documentar seguint la metodologia i les plantilles facilitades per l'IMI els riscos identificats mitjançat l'eina RSA Archer disponible a l'IMI. Així mateix, també serà missió del contracte incorporar a l'eina GRC els nous sistemes d'informació que es creïn.

4.3.3.Elaboració del Mapa de Riscos

El mapa de riscos haurà de reflectir els riscos operatius, tàctics i estratègics, amb especial èmfasi en aquells que poden tenir un impacte crític sobre la seguretat de les infraestructures, les dades, i els serveis municipals.

Es classificaran els riscos segons la seva probabilitat i impacte, identificant els riscos més crítics que requereixen una atenció immediata. Aquesta classificació haurà de ser fàcilment comprensible i utilitzable per a la presa de decisions estratègiques.

L'adjudicatari haurà de proposar estratègies de tractament per als riscos identificats, seguint el model d'acceptar, transferir, reduir o evitar el risc. Aquestes estratègies s'hauran de presentar en un Pla Plurianual de Tractament del Risc, detallant les accions a seguir, els recursos necessaris, i els terminis previstos.

4.3.4.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Catàleg d'Amenaces	Identificar i classificar de forma exhaustiva les amenaces, així com la seva actualització respecte al catàleg anterior.	1 catàleg per Gerència Sectorial de l'Ajuntament (7 en total) 1 catàleg per totes les Gerències Territorials 1 catàleg global agregat	Catàleg d'amenaces
Metodologia d'Anàlisis de Riscos de Seguretat	Elaborar un informe detallat sobre la metodologia d'anàlisi de riscos proposada o millorada, amb una justificació de la seva adequació a l'Ajuntament. Ha de donar compliment al què estableix l'ENS sobre la gestió de riscos	1 proposta de metodologia d'Anàlisis de Riscos de Seguretat Integral 1 proposta de metodologia d'Anàlisis de Riscos de Seguretat associats a la cadena de subministrament 1 proposta de metodologia d'Anàlisis de Riscos de Seguretat específics en projectes	Proposta de metodologia

Descripció	Tasques	Volumetria	Lliurables
Mapa de Riscos de Seguretat Integral	Elaborar un document visual i analític que mostri la identificació, classificació i priorització dels riscos de seguretat IT, OT i físics, incloent una proposta de tractament per a cada risc identificat.	1 mapa per Gerència Sectorial de l'Ajuntament (7 en total) 1 mapa per totes les Gerències Territorials 1 mapa global agregat	Mapa de riscos de seguretat integral

4.4. DETERMINACIÓ DEL NIVELL DE MADURESA OBJECTIU

L'objectiu d'aquesta tasca és definir el Nivell de Maduresa Objectiu en seguretat integral per a l'Ajuntament, basant-se en l'anàlisi del nivell de maduresa actual i la comparativa amb altres administracions públiques similars. Aquest procés serà clau per identificar les àrees de millora i establir un full de ruta per assolir els estàndards desitjats en seguretat lògica (tant IT com OT) i seguretat física.

Per determinar el nivell de maduresa s'hauran de cobrir els següents aspectes:

4.4.1. Anàlisi del Nivell de Maduresa Actual

L'adjudicatari haurà de realitzar una avaluació del nivell de maduresa actual dels controls de seguretat de l'Ajuntament utilitzant el model CMMI (Capability Maturity Model Integration).

L'anàlisi haurà de revisar els processos, procediments i controls implementats en l'àmbit de la seguretat de la informació, amb un enfocament particular en la governança, la gestió de riscos, el compliment normatiu, i la resposta a incidents de ciberseguretat.

De manera similar, s'haurà d'avaluar el nivell de maduresa dels sistemes OT (Operational Technology), que inclouen les infraestructures crítiques i els sistemes de control industrial. Aquest anàlisi haurà de considerar els controls específics per a la protecció d'aquests sistemes davant de ciberamenaces i altres riscos.

L'anàlisi de maduresa també haurà d'incloure els controls de seguretat física, avaluant la protecció de les instal·lacions, l'accés físic, i els protocols de seguretat davant de situacions d'emergència.

Finalment s'haurà de realitzar una associació dels controls existents a l'Ajuntament amb els controls definits en l'Esquema Nacional de Seguretat (ENS) i amb els definits en el NIST Cybersecurity Framework (NIST CSF 2.0). Aquesta associació permetrà identificar oportunitats de millora en relació amb les pràctiques i estàndards internacionals.

4.4.2. Benchmark amb Altres Administracions Públiques

L'adjudicatari haurà de realitzar una comparativa o benchmark del nivell de maduresa de seguretat de l'Ajuntament amb altres administracions públiques o Organitzacions que tinguin una complexitat i característiques similars. Aquesta comparativa haurà de cobrir tant la seguretat lògica (IT i OT) com la seguretat física. Aquest anàlisi haurà d'incloure una projecció del nivell de maduresa esperat per a aquestes entitats de referència al llarg del període temporal del pla plurianual de tractament del risc, permetent així a l'Ajuntament establir uns objectius de millora ambiciós i realistes.

Es comparará el nivell de maduresa dels controls de seguretat lògica (IT i OT) de l'Ajuntament amb els d'altres peers segons els frameworks de referència utilitzats per fer l'anàlisi (ENS i NIST CSF 2.0).

De manera paral·lela, es farà una comparativa del nivell de maduresa en seguretat física, centrant-se en la protecció de les infraestructures de comunicacions, la gestió de l'accés físic, i la preparació per a emergències.

4.4.3. Definició del Nivell de Maduresa Objectiu

Basant-se en l'anàlisi del nivell de maduresa actual i la comparativa amb altres administracions, l'adjudicatari haurà de proposar un Nivell de Maduresa Objectiu per a l'Ajuntament en cadascun dels àmbits analitzats (seguretat lògica IT, seguretat lògica OT i seguretat física) en els anys inclosos en el pla plurianual de tractament del risc. Aquest nivell haurà d'estar alineat amb les necessitats estratègiques de l'Ajuntament, els requisits legals i reguladors, i les millors pràctiques del sector.

4.4.4.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Informe d'Avaluació de Maduresa	Analitzar el nivell de maduresa actual, incloent-hi l'avaluació segons el model CMMI i l'associació amb ENS i NIST CSF 2.0.	1 informe per Gerència Sectorial de l'Ajuntament (7 en total) 1 informe per totes les Gerències Territorials 1 informe global agregat	Informe d'Avaluació de Maduresa
Informe de Benchmarking	Elaborar un informe amb els resultats de la comparativa de maduresa, i la projecció als 3 anys posteriors, amb altres administracions públiques o Organitzacions similars, detallant les diferències, similituds, i les millors pràctiques identificades.	1 informe per seguretat IT 1 informe per seguretat OT 1 informe per seguretat física	Informe de Benchmarking
Nivell de Maduresa Objectiu	Elaborar un informe que defineixi el nivell de maduresa objectiu per a l'Ajuntament en seguretat lògica IT, seguretat lògica OT, i seguretat física, juntament amb la justificació d'aquest nivell.	1 informe per seguretat IT 1 informe per seguretat OT 1 informe per seguretat física	Informe de Nivell de Maduresa Objectiu

4.5. ELABORACIÓ D'AUDITORIES TÈCNIQUES

L'objectiu d'aquesta tasca és garantir que l'avaluació de la seguretat en els sistemes i infraestructures de l'Ajuntament es basi en una metodologia tècnica avançada, centrada en proves d'intrusió (**pentesting**) i validació efectiva de les mesures de protecció implantades. Aquestes auditories complementaran les anàlisis de riscos i les entrevistes realitzades, aportant una visió realista de l'exposició i vulnerabilitats existents.

Les auditories tècniques hauran de permetre contrastar la informació recollida en les entrevistes i en els processos d'anàlisi de riscos, identificant desviacions entre la percepció dels riscos i la realitat tècnica dels sistemes i serveis. Per garantir un nivell d'exigència adequat, el servei haurà d'oferir un mínim de **10 jornades d'auditoria sobre xarxes IT** i **10 jornades d'auditoria sobre xarxes OT (tecnologies de ciutat)**.

4.5.1.Definició i abast de les auditories tècniques

Es duran a terme auditories tècniques avançades amb un enfocament proactiu basat en metodologies de pentesting, identificació de vulnerabilitats i verificació del compliment de controls de seguretat. S'inclouen les següents tipologies d'auditories:

- **Tests d'intrusió externs i interns**: Simulació d'atacs reals per identificar possibles vies d'explotació d'actius digitals, tant des d'Internet com des de la xarxa interna de l'Ajuntament.
- **Anàlisi de configuració i seguretat d'infraestructures**: Revisió en profunditat de sistemes on-premise i entorns cloud per detectar configuracions insegures i possibles bretxes.
- **Avaluació de seguretat en aplicacions web i mòbils**: Revisió tècnica basada en OWASP per detectar errors de desenvolupament, vulnerabilitats explotables i deficiències en mecanismes d'autenticació i protecció de dades.
- **Test de seguretat en xarxes i segmentació**: Anàlisi de la resistència de la segmentació de xarxes internes, polítiques de tallafocs i gestió d'accés a recursos crítics.

4.5.2.Metodologia d'execució

El procés d'auditoria seguirà un model estructurat basat en estàndards reconeguts com OWASP, OSSTMM, NIST 800-115 i PTES. Aquest inclourà les següents fases:

1. **Planificació i definició de l'abast:** Identificació d'actius a avaluar, aprovació de l'escenari d'auditoria i establiment de criteris d'èxit.
2. **Recerca i identificació de vectors d'atac:** Recopilació d'informació sobre els objectius a través de tècniques de reconeixement i anàlisi de serveis exposats.
3. **Explotació i validació de vulnerabilitats:** Execució de proves controlades per confirmar la seva explotabilitat i l'impacte real sobre els serveis.
4. **Post-explotació i anàlisi d'impacte:** Avaluació de les conseqüències potencials d'un atac i identificació de possibles escenaris de compromís.
5. **Propostes de mitigació i lliurament d'informes:** Presentació d'un informe tècnic detallat amb evidències, recomanacions i pla de millora prioritzat.

4.5.3.Criteris de selecció de les àrees auditades

Les àrees i sistemes que seran objecte d'auditoria es seleccionaran segons criteris de criticitat i exposició al risc, prioritzant:

- **Serveis essencials** per al funcionament de l'Ajuntament.
- **Sistemes d'informació** que gestionen dades sensibles o crítiques.
- **Infraestructures clau** per a la prestació de serveis públics.
- **Entorns cloud i híbrids** on s'allotgin serveis estratègics.
- **Aplicacions i plataformes digitals** que tinguin interacció amb ciutadans o tercers.

4.5.4.Integració amb l'Anàlisi de Riscos

Les auditories tècniques proporcionaran dades objectives que permetran alimentar i millorar el mapa de riscos de l'Ajuntament. Els resultats de les proves d'intrusió i validació tècnica seran incorporats en el model de governança de riscos, facilitant la presa de decisions informada i l'optimització dels controls de seguretat.

4.5.5.Lliurables

Descripció	Tasques	Volumetria	Lliurables
Informe d'auditoria tècnica	Elaborar un informe detallat sobre les proves realitzades, vulnerabilitats detectades i riscos associats.	1 informe xarxa IT 1 informe xarxa OT	Informe tècnic amb detalls de cada test realitzat, evidències i recomanacions.
Propostes de correcció i mitigació	Identificar mesures correctives per cada vulnerabilitat crítica detectada, incloent recomanacions tècniques i de millora.	1 informe xarxa IT 1 informe xarxa OT	Document amb mesures correctives i pla de mitigació per cada risc identificat.
Presentació executiva	Elaboració d'un resum amb conclusions principals i línies d'acció.	1 presentació	Document de presentació amb resultats clau per a la presa de decisions.

4.6. ELABORACIÓ D'UN PLA PLURIANUAL DE TRACTAMENT DEL RISC 2025-2028

L'objectiu d'aquesta tasca és desenvolupar un Pla Plurianual de Tractament del Risc per al període 2025-2028, que permeti a l'Ajuntament mitigar els riscos identificats en el mapa de riscos, augmentar el nivell de maduresa de la seguretat integral al nivell proposat i garantir la continuïtat operativa i la protecció dels actius municipals. Aquest pla haurà de ser clar, executable i alineat amb les necessitats estratègiques de l'Ajuntament, incorporant un sistema de mesura per avaluar l'impacte de les accions en la reducció del risc o l'augment del nivell de maduresa.

A més, el pla haurà de permetre que l'Ajuntament **aconsegueixi la certificació en l'Esquema Nacional de Seguretat (ENS) nivell MIG** en un termini de 12 mesos des de la finalització de l'elaboració del Pla Director per tots els sistemes d'informació identificats com a crítics. Tanmateix, en funció de la naturalesa i sensibilitat d'alguns serveis**, determinats sistemes d'informació podran requerir l'assoliment del nivell ALT de certificació ENS**, per garantir una protecció reforçada d'aquells actius més sensibles o estratègics. Per aquest motiu, el pla haurà d'incloure un anàlisi específic per determinar els serveis que han d'assolir aquest nivell ALT, establint els requisits tècnics i operatius necessaris per complir amb aquesta exigència.

Per determinar el nivell de maduresa s'hauran de cobrir els següents aspectes:

4.6.1. Identificació i Priorització de Projectes de Tractament del Risc

Partint del mapa de riscos elaborat prèviament, es determinaran els riscos que s'hagin acordat mitigar. Es prioritzaran els riscos en funció de la seva criticitat, tenint en compte tant la probabilitat d'ocurrència com l'impacte potencial sobre els processos municipals. A més, s'integraran en aquesta priorització tant els resultats de les auditories tècniques realitzades en el marc d'aquest contracte, com qualsevol altre que l'IMI determini. Aquesta anàlisi permetrà disposar d'una visió realista i actualitzada dels riscos, assegurant que les mesures de mitigació es focalitzin en les vulnerabilitats identificades de manera més efectiva.

Per a cada risc que es decideixi mitigar, l'adjudicatari haurà de proposar projectes específics de tractament del risc. Aquests projectes hauran de ser descriptius i detallats, incloent-hi:

- **Descripció i Objectius de l'Acció Proposada**: Explicació detallada de l'acció o conjunt d'accions a implementar, i els objectius específics que es volen assolir.
- **Riscos Operatius Mitigats**: Identificació dels riscos que es pretenen reduir amb l'execució del projecte, especificant com l'acció afecta la probabilitat d'ocurrència o l'impacte del risc.
- **Nivell de Mitigació**: Estimació quantitativa i qualitativa de la reducció del risc, especificant com es modificarà el mapa de riscos.
- **Nivell de Augment de Maduresa**: Estimació quantitativa i qualitativa de l'augment del nivell de maduresa en cadascun dels àmbits analitzats prèviament, especificant com es modificarà el nivell de maduresa actual i projectat per els anys inclosos en el cicle del Pla Director.

- **Estratègies d'Implementació**: Descripció de les estratègies que es seguiran per dur a terme el projecte, tenint en compte els recursos disponibles i els requisits d'implementació.
- **Costos d'Implantació**: Estimació detallada dels costos associats a l'execució del projecte, incloent-hi costos de capital (CAPEX), costos operatius (OPEX), i la necessitat de recursos humans (FTEs).
- **Durada del Projecte i Dificultat d'Implantació**: Estimació del temps necessari per implementar el projecte, així com els reptes associats al canvi organitzatiu o tecnològic que podrien afectar l'execució.
- **Associació amb el controls de ENS**: Avaluació de com cada projecte, individualment, contribueix a complir els requisits necessaris per obtenir la certificació ENS nivell mig o alt en el termini establert.

4.6.2. Agrupació de Projectes en Línies Estratègiques o Contractes

Els projectes es classificaran i agruparan en línies estratègiques coherents amb els objectius de l'Ajuntament, facilitant una visió integral i coordinada del tractament dels riscos. Aquesta agrupació ha de permetre una gestió eficient dels recursos i una implementació ordenada dels projectes.

L'adjudicatari haurà d'avaluar els contractes actualment vigents a l'Ajuntament que tinguin relació amb la seguretat integral. Això inclou la seva data de finalització, la seva efectivitat actual en la mitigació de riscos i la possibilitat de renovació o substitució.

S'haurà de proposar un calendari per a la finalització dels contractes existents i l'inici de nous contractes que millor s'ajustin a les necessitats del pla de tractament del risc. Aquest calendari ha de garantir una transició suau i efectiva, evitant qualsevol discontinuïtat en la seguretat integral i assegurant que els nous contractes permetin complir amb els requisits de l'ENS.

4.6.3.Elaboració d'Especificacions Tècniques i Casos d'Ús per als Nous Contractes

L'adjudicatari haurà de redactar les especificacions tècniques per als nous contractes necessaris per a la implementació dels projectes proposats (màxim 5), seguint el format i les normatives establertes per l'Ajuntament. Aquestes especificacions hauran de detallar els requisits tècnics i funcionals, així com els criteris de rendiment i seguretat que han de complir les solucions proposades.

A més, es definiran casos d'ús específics que facilitin la comprensió dels requeriments i garanteixin que es cobreixin les necessitats identificades en el Pla Director.

4.6.4.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Informe executiu del Pla Plurianual De Tractament Del Risc 2025-2028	Elaborar powerpoint i presentar el Pla Plurianual De Tractament Del Risc 2025-2028	1 informe executiu 1 presentació a Organismes de Direcció Municipal	Informe Executiu
Fitxes de Projecte	Elaborar documentació detallada de cada projecte, incloent-hi la descripció, objectius, riscos mitigats, nivell de mitigació, estratègies d'implementació, costos, durada i dificultat d'implantació , així com el control d'ENS associat.	1 fitxa per cada projecte proposat	Fitxes de Projecte
Declaració de conformitat	Actualització de la Declaració de conformitat d'acord amb l'annex II de l'ENS	1 Declaració	Declaració de conformitat
Pla Plurianual de Tractament del Risc	Elaborar un document integrat que descrigui la planificació estratègica per al període 2025-2028, agrupant els projectes en línies estratègiques o contractes, amb una visió detallada de la seva execució temporal.	1 pla plurianual	Pla plurianual de tractament del risc
Calendari de Contractes	Elaborar una programació detallada de la finalització dels contractes vigents i la proposta d'inici de nous contractes.	1 calendari	Calendari de Contractes

Descripció	Tasques	Volumetria	Lliurables
Especificacions Tècniques i Casos d'Ús per a Nous Contractes	Redactar les especificacions tècniques i casos d'ús identificats, seguint les directrius i requeriments de l'Ajuntament. Aquestes especificacions definiran els requisits tècnics i funcionals, així com els criteris de rendiment i seguretat, per garantir que les solucions contractades compleixin els estàndards establerts, inclosos els requerits per a la certificació ENS..	Màxim de 5 especificacions tècniques amb casos d'ús	Documentació tècnica amb les especificacions i casos d'ús per als nous contractes

4.7. ACTUALITZACIÓ DEL COS NORMATIU DE SEGURETAT INTEGRAL

El govern de la Seguretat de la Informació requereix 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, l'Ajuntament ha definit un conjunt d'estàndards a seguir que es gestionen per mantenir-los actualitzats i alineats.

El cos normatiu actual s'estructura 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 als procediments, ja poden ser guies, instruccions operatives, formularis, etc.

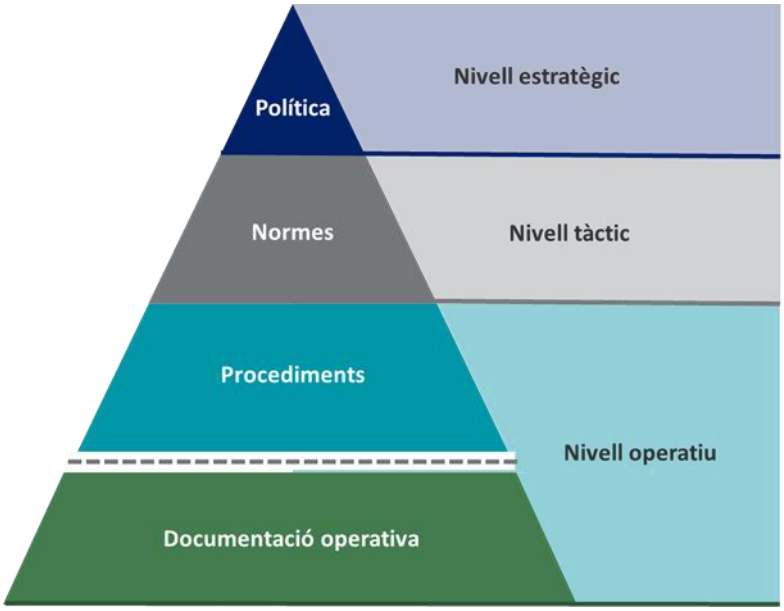

Figura 2 – Estructura del cos normatiu

L'objectiu d'aquesta tasca és garantir que el cos normatiu de seguretat de l'Ajuntament (política, normes i procediments) estigui completament alineat amb els resultats del Pla Director De Seguretat Integral. Aquesta actualització és fonamental per assegurar que les polítiques, procediments i directrius de seguretat siguin coherents amb les noves necessitats identificades i amb els estàndards de seguretat més recents. La modernització del cos normatiu haurà de reflectir tant la seguretat lògica (IT i OT) com la seguretat física, integrant aquestes àrees de manera holística i eficient.

Per realitzar la actualització del cos normatiu de seguretat integral s'hauran de cobrir els següents aspectes:

4.7.1. Revisió i Adaptació del Cos Normatiu Actual

L'adjudicatari haurà de dur a terme una revisió exhaustiva de les polítiques, normes i procediments de seguretat vigents a l'Ajuntament, identificant aquelles àrees que requereixen adaptació per complir amb els resultats del Pla Director De Seguretat Integral i per aconseguir la **certificació en l'Esquema Nacional de Seguretat (ENS) nivell MIG o ALT**, si s'escau**.**

S'haurà de redactar i actualitzar el cos normatiu existent per garantir que incorpori les millores i ajustos derivats del Pla Director, incloent-hi noves amenaces, canvis tecnològics i les millors pràctiques en seguretat, d'acord amb els requeriments normatius que els són d'aplicació actualment (ENS, eIDAS, LOPDGDD,...) amb atenció especial als canvis que afectin al compliment de l'ENS o de la normativa de protecció de dades personals.

4.7.2. Elaboració de Llibres Blancs

Per reforçar el cos normatiu de seguretat integral, l'adjudicatari haurà de desenvolupar tres llibres blancs clau que serveixin com a guies de referència per a l'arquitectura i el desenvolupament dins de l'Ajuntament i on es recullin les arquitectures de referència en base als escenaris aplicables dins dels models d'arquitectura amb els controls de seguretat requerits en cada cas.

S'entén com a llibre blanc una estructura amb guies documentals i que té com a objectiu d'ajudar a l'Ajuntament a resoldre o afrontar com han d'implementar la seguretat en les diferents escenaris i en els diferents aspectes a abordar en la seguretat en el disseny o Projectes.

Entre d'altres s'estandarditzaran:

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

De forma específica l'adjudicatari haurà d'elaborar:

- **Llibre Blanc d'Arquitectura IT**: Aquest document ha d'establir els principis fonamentals i les millors pràctiques per a la infraestructura IT de l'Ajuntament. Inclourà directrius per al disseny de l'arquitectura, la gestió de la xarxa, la seguretat dels sistemes, la protecció de dades, la integració de tecnologies emergents i la interoperabilitat amb altres sistemes.

- **Llibre Blanc d'Arquitectura OT**: Aquest llibre blanc abordarà l'arquitectura dels sistemes operacionals (OT) de l'Ajuntament. Haurà de proporcionar directrius específiques per a la protecció d'infraestructures que donen servei al ciutadà, la seguretat dels sistemes de control industrial, la gestió de l'internet de les coses (IoT) i la integració de les tecnologies OT amb les IT, assegurant que les dues es tractin de manera coherent i segura.

- **Llibre Blanc de Desenvolupament de Software**: Aquest document establirà els estàndards i les millors pràctiques per al desenvolupament de software dins de l'Ajuntament. Inclourà recomanacions per al codi segur, la gestió del cicle de vida del desenvolupament (SDLC), la protecció de dades, les proves de seguretat, i la integració contínua i entrega contínua (CI/CD), així com pautes per a la gestió d'amenaces en l'àmbit del software.

4.7.3.Implementació de Normatives i Procediments

Un cop elaborades i actualitzades les normatives, s'haurà de planificar un desplegament efectiu dins de l'Ajuntament. Això inclou la difusió de les noves polítiques, la formació dels empleats i la integració de les normatives dins dels processos operacionals diaris.

Es definirà un procés per a l'avaluació contínua de l'efectivitat de les normatives de seguretat, amb mecanismes per a la seva millora constant basats en els resultats obtinguts i l'evolució del context de seguretat.

4.7.4.Lliurables

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

Descripció	Tasques	Volumetria	Lliurables
Revisió de l'estructura documental del cos normatiu per ajustar-la als resultats del Pla Director De Seguretat Integral.	Revisió general del cos normatiu	Cos normatiu revisat	

Descripció	Tasques	Volumetria	Lliurables
Política de Seguretat Integral	Definir un esborrany de la política de seguretat integral que haurà de ser revisada i aprovada pel Comitè de Seguretat. Aquesta política ha de cobrir tots els aspectes crítics de la seguretat de la informació i la seguretat física.	1 Política aprovada o revisada per decret d'alcaldia o mecanisme equivalent per delegació	Document amb la Política de seguretat integral
Desenvolupament de les normes, guies, estàndards i procediments necessaris per a cobrir noves necessitats que no estiguin cobertes pel marc normatiu vigent.	Elaborar documentació completa de totes les polítiques, normes i procediments actualitzats, adaptats als resultats del Pla Director De Seguretat Integral.	Màxim 20 documents. En cas de requerir un nombre superior, l'Ajuntament decidirà quins 20 s'hauran d'elaborar o modificar.	Norma, guia, estàndard.
Llibre Blanc d'Arquitectura IT	Elaborar document de referència per a la gestió i seguretat de l'arquitectura IT de l'Ajuntament.	1 document	Llibre Blanc d'Arquitectura IT
Llibre Blanc d'Arquitectura OT	Elaborar document de referència per a la gestió i seguretat de l'arquitectura OT de l'Ajuntament.	1 document	Llibre Blanc d'Arquitectura OT
Llibre Blanc de Desenvolupament de Software.	Elaborar guia de referència per al desenvolupament segur de software dins de l'Ajuntament.	1 document	Llibre Blanc de Desenvolupament de Software

Descripció	Tasques	Volumetria	Lliurables
Pla de Desplegament i Difusió	Preparar l'estratègia per a la implementació efectiva de les noves normatives dins de l'organització, incloent-hi programes de formació i comunicació interna.	1 pla	Pla de Desplegament i Difusió

5. MODEL DE PRESTACIÓ DEL SERVEI

5.1. MODEL DE RELACIÓ IMI/ADJUDICATARI

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

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

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

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

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

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

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

L'adjudicatari ha de plantejar el model de relació amb aquests equips especialitzats, indicat les especialitats que es podran disposar en el contracte i com es podran disposar d'aquests serveis experts de manera que es garanteixi que qualsevol necessitat dins de l'abast del contracte es podrà

disposar de aquest coneixement i acompanyament en la implementació a les necessitats de l'IMI i Ajuntament.

5.2. ORGANITZACIÓ

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

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

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

5.2.1.Comitè Estratègic

Ha de vetllar perquè els objectius del contracte es duguin a terme d'acord als requisits i abast descrites en aquest plec.

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

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

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

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

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

En formen part:

- Gerent de l'Institut Municipal de Informàtica

- Director de Serveis de Seguretat de la Informació de l'IMI.
- Responsable del Servei per part de l'adjudicatari.

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

Puntualment poden assistir-hi aquelles persones que es considerin necessàries en funció dels temes a tractar.

5.2.2.Comitè de Direcció

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 del contracte, realitzar el seguiment tàctic de les activitats definides al catàleg de serveis i l'assoliment d'objectius.

El Cap de Projecte 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:

- Director de Serveis de Seguretat de la Informació de l'IMI.
- Cap del Departament de Govern de Seguretat de l'IMI.
- Responsable del servei per part de l'adjudicatari.
- Cap de Projecte per part de l'adjudicatari.

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

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

5.2.3.Comitè de Seguiment Operatiu

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

Es reuneix normalment un cop per setmana.

El Comitè de Seguiment està format com a mínim pel Responsable del servei 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

5.2.4.Seguiment del contracte

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

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

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

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

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

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

Informe de seguiment de l'avenç: (mensual)

- Estat general de les tasques o serveis que s'estan realitzant:
  - Estat actual.
  - Passos que s'han realitzat fins la data actual.
  - Passos pendents per tal de finalitzar-ho.
  - Detecció i proposta de resolució de problemes.

    - Revisió segons planificació i dates previstes d'execució.
- Tasques futures previstes.
- Quadre de comandament / Dashboard de gestió del contracte.

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

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

6. METODOLOGIA DEL PLA DE CONTRACTE

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

El servei es desplegarà seguint les següents fases:

6.1. LLANÇAMENT DE CONTRACTE

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

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

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

6.2. 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.

6.3. 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 lliurables, tasques i accions del contracte.

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

7. RECURSOS HUMANS

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

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

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

7.1. FUNCIONS PER PERFIL

D'acord a les volumetries anteriorment descrites, s'estima necessària la implicació d'un equip mínim equivalent a uns 3,5 FTEs en el període de 9 mesos (correspondria a 2,6 FTEs d'un any).

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

Perfil	Responsabilitat
Responsable del Servei	Màxim responsable de l'equip de l'adjudicatari, i en conseqüència de la provisió en temps i qualitat dels serveis inclosos en aquest contracte. Tasques: • Alineació amb els objectius estratègics de l'Ajuntament.
Cap de Projecte	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. Actuarà com a Coordinador del Contracte i donarà Suport a la Direcció de Serveis de Seguretat de la Informació de l'IMI en la definició del full de ruta d'evolució del Servei Tasques: • Participació als comitès de seguiment del servei

	• Reporting de l'evolució del servei als responsables del servei de l'IMI • Coordinació del personal que forma part del servei • Nexe d'unió i comunicació entre l'equip de Projecte i l'IMI És important que tingui experiència dilatada en gestió de projectes de seguretat integral a gran escala. • Participació Comitès de Seguiment del Servei fent reporting de l'evolució del servei • Elaboració de quadres de comandament • Reporting de l'estat general del servei, amb indicadors de seguretat en projectes
Consultor GRC sènior	Responsable de l'operativa diària, defineix, gestiona i executa les accions del contracte a realitzar. Garanteix 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: • Anàlisis, elaboració, i modificació del marc normatiu corporatiu. • Suport, anàlisi, elaboració d'informes i assessorament del compliment tècnic de les lleis (RGPD, ENS, NIS2...) • Elaboració del quadre de comandament. • Tasques de suport puntuals del Servei. Gestió de les eines pròpies del servei (Archer,...)
Consultor GRC junior	Dona suport a l'operativa diària, defineix, gestiona i executa les accions del contracte a realitzar. Consultor amb experiència 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 en la anàlisis, elaboració, i modificació del marc normatiu corporatiu.

	• Suport en l'elaboració del quadre de comandament. • Gestió de les eines pròpies del servei (Archer,...)
Tècnic sènior especialista en consultoria de seguretat IT	Tècnic expert en seguretat, especialitat en seguretat IT i SDLC. **Consultor tècnic** amb coneixements en establiment de requisits de seguretat IT. Especialista en estàndards i normatives de seguretat IT, elaboració de cossos normatius de seguretat IT, gestió de riscos de seguretat de la informació i eines GRC, així com compliment tècnic de la legalitat. Tasques: • Anàlisi de la seguretat en infraestructures tecnològiques IT. • Definició de controls basats en requeriments establerts • Elaboració de pla de projectes IT • Anàlisis, elaboració, i modificació del marc normatiu corporatiu per IT. • Suport, anàlisi, elaboració d'informes i assessorament del compliment tècnic de les lleis (LOPD, ENS, ENI,...) • Tasques de suport puntuals del Servei. • Suport a implantació de metodologia SDLC segura • Suport a elaboració del llibre blanc d'arquitectures estandarditzades de l'IMI.
Tècnic sènior especialista en consultoria de seguretat OT i IoT	Tècnic expert en seguretat, especialitat en seguretat OT i IoT. **Consultor tècnic** amb coneixements en establiment de requisits de seguretat OT i IoT. Especialista en estàndards i normatives de seguretat OT i IoT, elaboració de cossos normatius de seguretat OT i IoT, gestió de riscos de seguretat de la informació i eines GRC, així com compliment tècnic de la legalitat. Tasques: • Anàlisi de la seguretat en infraestructures tecnològiques OT i IoT. • Definició de controls basats en requeriments establerts • Elaboració de pla de projectes OT i IoT.

	• Anàlisis, elaboració, i modificació del marc normatiu corporatiu per OT i IoT. • Suport, anàlisi, elaboració d'informes i assessorament del compliment tècnic de les lleis (LOPD, ENS, ENI,...) • Tasques de suport puntuals del Servei.
Tècnic sènior especialista en consultoria de seguretat física	Especialista en estàndards i normatives de seguretat física, elaboració de cossos normatius de seguretat física, gestió de riscos de seguretat física, així com compliment tècnic de la legalitat. Tasques: • Anàlisi de la seguretat física en infraestructures tecnològiques. • Integració de les estratègies de seguretat física amb les polítiques generals de seguretat. • Anàlisis, elaboració, i modificació del marc normatiu de seguretat física. • Suport, anàlisi, elaboració d'informes i assessorament del compliment tècnic de les lleis • Tasques de suport puntuals del Servei.
Tècnic sènior especialista en arquitectures de seguretat	Tècnic expert en seguretat, especialitat en arquitectures de seguretat. Seguretat al lloc de treball, entorns col·laboratius, ofimàtica o serveis al *cloud*. **Arquitecte** amb coneixements d'arquitectures de seguretat, amb intensificació al *cloud*. Tasques: • Disseny de solucions de seguretat IT, OT i IoT • Elaboració del llibre blanc d'arquitectures estandarditzades de l'IMI • Estandardització i normalització d'arquitectures IT, OT i IoT.

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 servei	Cal que acrediti, durant els últims 5 anys, 3 anys d'experiència en la gestió de contractes relacionats amb projectes d'elaboració de Plans Director de Seguretat Integrals.

Cap de Projecte	Cal que acrediti, durant els últims 5 anys, 3 anys d'experiència en projectes d'elaboració de Plans Director de Seguretat Integrals.
	Haurà de disposar:
	• Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya)
	• Certificacions recomanades:
	  ○ Gestió de Serveis TIC (ITIL)
	  ○ Seguretat de la informació (ISC2, 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.
	
	Cal que acrediti participació en 1 o més projectes de l'àmbit d'elaboració de Plans Directors de Seguretat Integrals.
	
	Haurà de disposar:
	
	• Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya)
	• Certificacions recomanades
	  ○ En gestió de serveis (ITIL)
	  ○ En gestió de seguretat de la informació (ISC2, ISACA o similars)
	  ○ En gestió de riscos
	  ○ Esquema Nacional de Seguridad (CCN) o Auditories en el ENS (CCN)
	  ○ RSA Archer Certified Associate o RSA Archer Certified Professional

Perfil	Responsabilitat
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 com a mínim 1 projecte de l'àmbit d'execució d'auditories de compliment de l'ENS. Haurà de disposar: • Titulació: Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya) • Certificacions recomanades o En auditories de compliment (CISA, ISO27001 Lead Auditor o similar) o En gestió de la seguretat de la informació (ISC2, ISACA o similar) o Esquema Nacional de Seguridad (CCN) o Auditories en el ENS (CCN)

Perfil	Responsabilitat
Tècnic sènior especialista en consultoria de seguretat IT	Cal que acrediti durant els darrers 5 anys, 2 anys d'experiència mínima en gestió de projectes des de la vessant de la seguretat IT i SDLC. Ha d'acreditar suport en un mínim de 3 projectes d'elaboració de Plans Director de Seguretat Integrals en els darrers 3 anys. Haurà de disposar: • Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya) Certificacions recomanades: • PMP • CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) • AWS Solutions Architect Associate, Azure Solutions Architect Expert o similars. • CSX (Cybersecurity Fundamentals Certificate) • OSCP (Offensive Security Certified Professional)

Perfil	Responsabilitat
Tècnic sènior especialista en consultoria de seguretat OT	Cal que acrediti durant els darrers 5 anys, 2 anys d'experiència mínima en gestió de projectes des de la vessant de la seguretat OT i IoT. Ha d'acreditar suport en un mínim de 3 projectes d'elaboració de Plans Director de Seguretat Integrals en els darrers 3 anys. Haurà de disposar: • Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya) Certificacions recomanades: • PMP • CISSP (Certified Information Systems Security Professional) • Certificacions de Seguretat en entorn OT. • Certificacions de Seguretat en entorn IoT.
Tècnic sènior especialista en consultoria de seguretat física	Cal que acrediti durant els darrers 5 anys, 2 anys d'experiència mínima en gestió de projectes des de la vessant de la seguretat física. Ha d'acreditar experiència en suport en un mínim de 3 projectes en l'elaboració de Plans Director de Seguretat Integrals en els darrers 3 anys. Haurà de complir un dels següents requisits: • Estar en possessió d'un títol universitari oficial de grau (o l'equivalent en les titulacions anteriors al Pla Bolonya) en l'àmbit de la seguretat que acrediti l'adquisició de les competències que es determinin, o bé del títol del curs de direcció de seguretat, reconegut pel Ministeri de l'Interior. • Acreditar experiència, durant cinc anys, com a mínim, en llocs de direcció o gestió de seguretat pública o privada, i haver superat les corresponents proves sobre les matèries a què es refereix l'article 12 de l'Orde INT/318/2011, d'1 de febrer, sobre personal de seguretat privada.

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. Haurà de disposar: • Titulació: Grau Universitari en Enginyeria i Màster, preferiblement en Informàtica o Telecomunicacions (o Enginyeria Superior per les titulacions anteriors al Pla Bolonya) Certificacions recomanades: • CISSP (Certified Information Systems Security Professional) • CCSP (Certified Cloud Security Professional) • AWS Solutions Architect Associate, Azure Solutions Architect Expert o similars.

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.

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.

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

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

8. CONDICIONS D'EXECUCIÓ

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

8.1. CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT

Les Administracions públiques per donar garanties i protecció als ciutadans s'han dotat de RD 311/2022 de 3 de maig pel qual es regula l'Esquema Nacional de Seguretat (en endavant ENS), que

és un marc comú de mesures a implementar per garantir l'accés, integritat, disponibilitat, autenticitat, confidencialitat, traçabilitat i conservació de les dades, informació i serveis que gestionen en l'exercici de les seves competències

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

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

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

8.2. LLOC DE PRESTACIÓ DEL SERVEI

L'adjudicatari haurà d'aportar els 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. A més, les entrevistes per a l'avaluació de riscos hauran de realitzar-se de forma presencial, llevat que l'IMI indiqui el contrari.

La connexió amb l'IMI es podrà fer a través d'una connexió VPN amb una connexió d'ample de banda suficient per a garantir un adequat rendiment, 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.

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

8.3. HORARI DE PRESTACIÓ DEL SERVEI

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

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

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.

8.4. DURADA DEL CONTRACTE

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

8.5. IDIOMA

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

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

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

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

8.6. PLA DE QUALITAT

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

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

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

- Cicle de Vida d'un servei:
  - Checkpoints.
  - Rols responsables de cada tasca o activitat.
- Gestió de la Configuració: Assegura que els canvis no afecten els nivells de qualitat del servei.
- Resolució dels problemes relatius a la gestió del servei.
- Control de la documentació:
  - Procediments que assegurin que la documentació s'ha actualitzat d'acord amb els canvis o peticions realitzades al llarg del cicle de vida del servei.
- Gestió de la documentació i dels requeriments del servei.
- Regles i procediments que garanteixin la millora contínua del servei.

- Planificació de les auditories internes que asseguren l'adequada documentació dels resultats i accions dutes a terme.
- Mètriques i indicadors.
- Pla de validació de la qualitat.
- Gestió de les responsabilitats relatives a l'actualització del Pla de Qualitat.
- Gestió de riscos que possibiliti una reducció o eliminació dels possibles impactes en el servei.
- Plans de continuïtat del servei que garanteixin que el servei podrà ser restaurat en cas de produir incidències en el mateix.
- Pla de formació que cobreixi les necessitats dels rols implicats en el servei. Aquest Pla es presentarà amb el detall suficient garantint la seva viabilitat, coherència, realisme, estructura organitzativa i previsible de la seva realització material.

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

Igualment, els licitadors han de presentar prèviament el Pla de Qualitat proposat. Aquest Pla de Qualitat el presentarà amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa.

8.7. QUALITAT DEL SERVEI I TREBALLS REALITZATS

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

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

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

8.7.1.Auditories

8.7.1.1.*Introducció*

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

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

- Periodicitat: semestral.
- Abast: totalitat del servei.

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

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

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

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

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

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

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

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

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

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

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

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

8.7.1.4.*Resultats de l'Auditoria*

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

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

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

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

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

8.7.1.5.*Resultats de la Revisió*

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

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

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

8.8. CLÀUSULA DE GARANTIA

Ateses les característiques de l'objecte i abast del present contracte, no s'exigeix cap període de garantia sobre els treballs realitzats.

8.9. TERMINIS D'EXECUCIÓ I FITES DE FACTURACIÓ

Els serveis objecte del contracte es facturaran segons el següent desglossament de fites i segons el percentatge de l'esforç que cadascuna d'elles comporta respecte del total. El període màxim d'acabament de les fites associades serà segons la planificació de detall acceptada i aprovada en el darrer Comitè de Direcció de Projecte.

1. **Definició del Govern de Seguretat Integral**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.1.7.
    - Percentatge d'import facturable: **15,00 %**
    - Període màxim d'entrega: **Mes 2**
    - Data de facturació: **Mes 2 de contracte**
2. **Elaboració de l'Anàlisi d'Impacte de Negoci (BIA)**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.2.5
    - Percentatge d'import facturable: **15,00 %**
    - Període màxim d'entrega: **Mes 6**
    - Data de facturació: **Mes 6 de contracte**
3. **Elaboració del Mapa de Riscos de Seguretat Integral**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.3.4
    - Percentatge d'import facturable: **15,00 %**
    - Període màxim d'entrega: **Mes 6**
    - Data de facturació: **Mes 6 de contracte**
4. **Determinació del Nivell de Maduresa Objectiu**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.4.4
    - Percentatge d'import facturable: **15,00 %**
    - Període màxim d'entrega: **Mes 6**
    - Data de facturació: **Mes 6 de contracte**

5. **Elaboració d'Auditories Tècniques**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.5.5
    - Percentatge d'import facturable: **5,00 %**
    - Període màxim d'entrega: **Mes 9**
    - Data de facturació: **Mes 9 de contracte**
6. **Elaboració d'un Pla Plurianual de Tractament del Risc 2025-2028**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.6.4
    - Percentatge d'import facturable: **10,00 %**
    - Període màxim d'entrega: **Mes 9**
    - Data de facturació: **Mes 9 de contracte**
7. **Actualització del Cos Normatiu de Seguretat Integral**
    - Els lliurables associats a aquesta fita són tots els detallats en l'apartat 4.7.4
    - Percentatge d'import facturable: **25,00 %**
    - Període màxim d'entrega: **Mes 9**
    - Data de facturació: **Mes 9 de contracte**

En el detall de la factura s'haurà de fer constar la relació de serveis realitzats.

Per tant, durant el sisè més de contracte, un cop entregats els lliurables corresponents, es facturarà el 60 % de l'import del contracte, i a la finalització del contracte, això és durant el novè mes de contracte es facturarà, un cop entregats els lliurables corresponents, es facturarà el restant 40 % de l'import del contracte.

9. PRESSUPOST DEL CONTRACTE

L'import del contracte és el determinat al Plec de clàusules administratives particulars, clàusula 2a "Pressupost base de licitació i valor estimat del contracte".

10. PROPOSTA TÈCNICA

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

El licitador haurà de presentar la seva oferta en format paper i en format electrònic, on tots els arxius han d'estar en format OpenDocument (.odt, .ods, .odp), Word, Excel, Power Point, MSProject o PDF, 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:

- **Sobre electrònic 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,
- **Sobre electrònic 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.

10.1.CONTINGUT DEL SOBRE ELECTRÒNIC B

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

Exceptuant el contingut corresponent a les plantilles dels lliurables quan sigui preceptiu en determinats criteris (marcats amb un *), no es tindrà en compte als efectes de la valoració de propostes tota la informació que quedi mes enllà del número màxim de pàgines especificat per a cada un dels apartats.

La valoració del criteris de valoració de judici de valor tindrà en compte únicament la informació presentada en la proposta tècnica del sobre electrònic B dintre de l'epígraf corresponent del criteri a valorar en qüestió, i que es relacionen a continuació:

1.- Resum Executiu (màxim 3 pàgines)

En aquesta secció el licitador ha de presentar un resum dels continguts més significatius de la proposta del projecte, destacant l'abast i els objectius principals, així com els punts forts que distingeixen la seva oferta.

2.- Plantejament General i Tècnic del Contracte (màxim 6 pàgines)

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

3.- Definició del Govern de la Seguretat Corporativa (màxim 8 pàgines)

En aquesta secció el licitador ha de detallar la proposta per definir una estructura clara i funcional per al Govern de Seguretat Integral de l'Ajuntament, garantint una gestió eficaç i coordinada que englobi totes les dimensions de la seguretat: seguretat lògica (tant IT com OT), seguretat física, i la integració amb altres àmbits clau com la seguretat en la cadena de subministrament i en la gestió de projectes.

El licitador en aquest apartat haurà de Presentar la proposta de Metodologia del quadre de Comandament descrit en l'apartat 4.1.2, els processos de govern definits en l'apartat 4.1.3 i els mecanismes de coordinació i comunicació necessaris per garantir una alineació estratègica segons es detalla a l'apartat 4.1.4. Es valorarà la metodologia proposada i els portals i eines resultants restin a disposició de l'Ajuntament/IMI així com la definició d'un pla d'implantació viable amb referències a la obtenció de objectius i resultats efectius i reals en el temps

4.- Elaboració de l'Anàlisi d'Impacte de Negoci (BIA) (màxim 10 pàgines)

En aquesta secció, el licitador haurà de presentar detalladament la metodologia proposada per identificar els processos de negoci crítics de l'Ajuntament. Això inclourà una descripció exhaustiva dels passos metodològics que seguirà per avaluar els diferents tipus d'impacte — operacional, econòmic, de reputació, legal i contractual— i la manera en què establirà els objectius temporals de recuperació (RTO, MTD, RPO) per a cada procés identificat.

A més, el licitador haurà de detallar el procés de coordinació i execució de les entrevistes amb els stakeholders claus. Es preveu que inclogui el format i estructura de les entrevistes, les preguntes estàndard que plantejarà, i els mecanismes que implementarà per assegurar que la informació recollida sigui completa, precisa i fiable.

El licitador també descriurà com desenvoluparà el pla de prioritat de recuperació, basant-se en els RTO i MTD prèviament identificats. Haurà d'exposar com aquest pla assignarà els recursos de l'Ajuntament per atendre les necessitats més crítiques en situacions d'interrupció, garantint una resposta efectiva i coordinada.

Addicionalment, cal que proposi un protocol per a les revisions periòdiques i actualitzacions del BIA. Això haurà d'incloure la freqüència amb què es realitzaran les actualitzacions, els factors

desencadenants per a una revaluació, i com s'integraran els canvis en l'entorn operacional o estratègic de l'Ajuntament.

Per acabar, el licitador haurà de detallar els materials de formació i les iniciatives de sensibilització que desenvoluparà per a educar al personal de l'Ajuntament sobre la importància del BIA i les millors pràctiques en gestió de la continuïtat del negoci. Aquesta formació haurà de fomentar una cultura de preparació i resiliència dins de l'organització.

5.- Elaboració del Mapa de Riscos de Seguretat Integral (màxim 6 pàgines)

En aquesta secció el licitador haurà de presentar la proposta de identificació i avaluació del risc de seguretat integral a totes les Gerències i organismes de l'Ajuntament de Barcelona incloses en l'abast del contracte. Haurà de detallar la seva metodologia d'anàlisi de riscos i la resta de punts sol·licitats a l'apartat 4.2. Es valorarà especialment les millores que l'oferta del licitador aporti a la metodologia descrita així com la presentació d'exemples gràfics per aclarir l'abast de la proposta.

El licitador haurà de presentar també la proposta d'enfoc i com es realitzaran les auditories necessàries de determinar el nivell de risc, descrivint com gestionarà aspectes de continguts, metodologia, sessions, evidències i no conformitats i proposta de millores. També es descriuran les eines que es posen a disposició per aquest servei amb les funcionalitats que incorporen, així com totes aquelles condicions que es considerin distintives.

6.- Control de Proveïdors (màxim 4 pàgines)

En aquesta secció el licitador haurà de presentar la proposta de metodologia per planificar, executar i fer el seguiment dels diferents tipus de proveïdor de l'Ajuntament, millorant i detallant el que s'explicita en l'apartat 4.3.2, tot identificant explícitament les propostes de millora respecte del que s'ha descrit en aquest apartat.

7.- Metodologia de Seguretat en el Disseny (màxim 4 pàgines)

En aquesta secció el licitador haurà de presentar la proposta de plantejament del servei de la metodologia de Seguretat en Projectes millorant i detallant el descrit en l'apartat 4.3.2, plantjeant l'enfoc general porposada així com detallant les tasques i activitats proposades en les diferents fases (disseny, desenvolupment, pas a producció,..) d'un projecte de desenvolupament.

8.- Determinació del Nivell de Maduresa Objectiu (màxim 6 pàgines)

En aquesta secció el licitador ha d'exposar la metodologia que seguirà per definir el Nivell de Maduresa Objectiu en seguretat integral per a l'Ajuntament de Barcelona. El licitador ha de proporcionar evidències de que disposa de dades per realitzar el benchmark sol·licitat i ha de donar resposta als punts plantejats en l'apartat 4.4. Es requerirà una explicació detallada de les estratègies per assolir els estàndards desitjats.

El licitador haurà de presentar també la proposta d'enfoc i com es realitzaran les auditories necessàries de determinar el nivell de maduresa objectiu, descrivint com gestionarà aspectes de continguts, metodologia, sessions, evidències i no conformitats i proposta de millores. També es descriuran les eines que es posen a disposició per aquest servei amb les funcionalitats que incorporen, així com totes aquelles condicions que es considerin distintives.

9.-Elaboració d'Auditories Tècniques (màxim 8 pàgines)

En aquesta secció, el licitador haurà de presentar la metodologia per a la realització d'auditories tècniques en xarxes IT i OT, seguint enfocaments avançats de pentesting i anàlisi de vulnerabilitats. L'objectiu és garantir que l'avaluació de la seguretat dels sistemes i infraestructures de l'Ajuntament sigui basada en proves pràctiques i efectives, que permetin validar la resiliència dels entorns municipals davant possibles amenaces.

El licitador haurà de descriure amb detall les proves que es realitzaran sobre els diferents entorns tecnològics, incloent la identificació de superfícies d'atac, l'execució de simulacions d'intrusió controlades i la validació de mecanismes de defensa implantats. Es valorarà la inclusió de metodologies que cobreixin les particularitats de les infraestructures OT, tenint en compte les tecnologies de ciutat i les xarxes industrials.

A més, haurà de descriure els criteris per a la selecció de sistemes a auditar, així com els mecanismes per assegurar que l'execució d'aquestes proves es realitzi de manera segura, sense afectar la disponibilitat dels serveis municipals.

10 Elaboració d'un Pla Plurianual de Tractament del Risc 2025-2028 (màxim 10 pàgines)

En aquesta secció el licitador ha de descriure la metodologia per determinar els projectes de tractament del risc més adients i tota la informació sol·licitada en l'apartat 4.5. El licitador haurà de realitzar una proposta dels perfils de l'ajuntament que voldrà entrevistar tenint en compte l'organigrama de la Figura 1.

De forma específica, el licitador haurà de presentar una proposta per abordar la certificació de l'ENS en l'Ajuntament. Presentar l'enfoc i l'abast de la certificació proposats, així com el desglossament de les tasques del pla de certificació indicant les tasques a executar per a la certificació de conformitat de l'ENS, d'acord amb el que es preveu en l'article 34 i en l'annex III de l'ENS.

11.- Actualització del Cos Normatiu de Seguretat Integral (màxim 8 pàgines)

Presentar la proposta de plantejament per a la construcció del Cos Normatiu de Seghuretat amb especial atenció en els llibres blanc d'arquitectures de seguretat millorant i detallant el descrit en l'apartat 4.7. Es valorarà la inclussió d'un pla d'implementació detallat de les Normatives i Procediments proposats.

12.- Model de relació (màxim 3 pàgines)

En aquesta secció el licitador ha d'exposar el seu enteniment i la seva proposta de models de relació entre l'IMI, l'equip del licitador adscrit al contracte i els equips especialitzats que el licitador proposi posar a disposició del contracte, segons està descrit a l'apartat 4.2, fent especial incís amb el model de relació amb els serveis experts que es demana disposar en el marc dels serveis d'aquest contracte.

13.- Pla de devolució del servei (màxim 3 pàgines)

En aquesta secció el licitador ha de detallar la proposta del pla de devolució del contracte, indicant les accions que assegurin el tancament de totes les tasques correctament, la qualitat dels lliurables finals, i de traspassar completament tota la informació a l'IMI, en base al que està descrit a l'apartat 6.4. El Pla es presentarà amb el detall suficient per tal de garantir la seva viabilitat, coherència, realisme, estructura organitzativa i previsible de la seva realització material.

14.- Pla de Qualitat (màxim 3 pàgines)

En aquesta secció el licitador ha de detallar la proposta del Pla de Qualitat, indicant el conjunt de documentació tècnica que es detalla en la "Proposta Tècnica" amb el detall suficient que permeti la valoració de la seva viabilitat, coherència, realisme, estructura organitzativa, en base al que està descrit a l'apartat 8.6.

10.2.CONTINGUT DEL SOBRE ELECTRÒNIC C

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

11. CLÀUSULES GENERALS DE SEGURETAT

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

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

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

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

311/2022 de 3 de maig pel que es regula l'Esquema Nacional de Seguretat (ENS) així com la Directiva NIS2 i la legislació que la desenvolupa.

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

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

11.2.CONFORMITAT AMB L'ESQUEMA NACIONAL DE SEGURETAT

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

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

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

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

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

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

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

11.3.CLÀUSULA DE PROPIETAT INTEL·LECTUAL

Tot i reconeixent l'autoria de les persones que els hagin elaborat, la propietat intel·lectual dels treballs realitzats a l'empara d'aquest contracte pertany a l'Ajuntament de Barcelona de forma exclusiva. Els productes o subproductes derivats, no podran ser utilitzats sense la deguda autorització prèvia.

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

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

11.4.RESPONSABLE DE SEGURETAT

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

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

11.5.CONFIDENCIALITAT

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

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

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

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

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

11.6.CLÀUSULA PER ACCESSOS POTENCIALS

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

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

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

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

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

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

11.7.CLÀUSULA DE PERSONAL EXTERN

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

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

12.CLÀUSULES D'ACCÉS ALS SISTEMES D'INFORMACIÓ

12.1.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.

12.2.GESTIÓ D'INCIDENTS

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

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

12.3.DIMENSIONAMENT/GESTIÓ DE CAPACITATS

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

12.4.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.

12.5.ANÀLISIS FORENSES

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

12.6.CONTROL D'ACCÉS

12.6.1.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.

12.6.2.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.

12.7.GESTIÓ DEL PERSONAL

12.7.1.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.

12.7.2.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.

12.8.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.

12.9.PROTECCIÓ DEL LLOC DE TREBALL

12.9.1.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.

12.9.2.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.

12.9.3.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.

12.9.4.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.

12.10.GESTIÓ D'EXCEPCIONS

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

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

13.CLÀUSULES DE SEGURETAT PER A L'IMPLANTACIÓ DE PRODUCTES

13.1.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·licitadors.

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

Autenticació interna

Els usuaris interns (de gestió Municipal) hauran d'autenticar-se amb els mecanismes d'autenticació definits per l'IMI basats en protocols estàndards de seguretat. L'empresa proveïdora haurà

d'assegurar que s'utilitzi el proveïdor d'identitats corporatiu (en endavant, IDP) per a l'autenticació dels usuaris.

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

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

Autenticació externa

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

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

13.2.AUTORITZACIÓ DELS USUARIS ALS SISTEMES

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

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

Aquesta integració podrà ser de dos tipus:

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

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

Perfilat d'usuaris
Les autoritzacions han de seguir un model RBAC (Role Based Access Control) que haurà de ser validat pels responsables tecnològics de la plataforma i pel Departament de Seguretat de l'IMI.
El model proposat haurà de complir amb els següents principis:

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

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

Per facilitar l'administració s'hauran de poder gestionar els permisos mitjançant rols de seguretat, entenent com a rol una entitat que dona accés a una sèrie d'operacions.
Sota la premissa d'aquests criteris generals, l'adjudicatari haurà de dissenyar el joc de permisos i autoritzacions requerits pels sistemes d'informació implementats, en base al document 'Pla d'Autoritzacions'. Aquest document serà revisat i actualitzat per l'adjudicatari per incloure nous punts a tractar o adaptacions dels punts existents.

14. 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 l' 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.

Barcelona,

Álex Collado Costa

Cap de Departament de Govern de Seguretat

David Esteban Haro

Direcció de Serveis de Seguretat de la Informació

15.ANNEXOS

15.1.ANNEX 1: ABAST A ORGANITZACIÓ MUNICIPAL

Per a establir el govern de la seguretat de la informació a nivell estratègic de tot l'Ajuntament, l'abast arriba a tot el "grup Municipal" incloent les entitats públiques empresarials i Societats Municipals Mercantils i tenir en compte la existència de Societats Mercantils amb participació minoritària, Consorcis, Fundacions i Associacions, essent cada entitat la que implementi el govern de la seguretat però de manera pautada i coordinada per tal d'obtenir un nivell de seguretat i de risc municipal.

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

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

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

Volumetria aproximada dels SISTEMES D'INFORMACIÓ	
Núm. de SI categoritzats per ENS	115 Sistemes d'Informació categoritzats 85 Sistemes d'Informació pendents de categoritzar (estimatiu).
Protecció de Dades Tractaments Municipals	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.

15.3.ANNEX 3: INFORMACIÓ ADDICIONAL / ACLARIMENTS

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

En l'assumpte del correu indicar:

*Contracte Pla Director de Seguretat: [**Número d'expedient del contracte**]*

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

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

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

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

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