PLEC TÈCNIC PER LA CONTRACTACIÓ DELS SERVEIS DE DETECCIÓ, VALIDACIÓ, GESTIÓ I ASSESSORAMENT DE NARRATIVES DE DESINFORMACIÓ PER L'AJUNTAMENT DE BARCELONA

Índex

1. Antecedents i motivació del contracte 5
2. Objecte del contracte 6
3. Abast del contracte 7
4. Característiques del servei 8
4.1. Monitorització del servei 9
4.2. Classificació, valoració i clusterització de conceptes 10
4.3. Verificació, agregació de narratives i diagnòstics 12
4.4. Assessorament i propostes d'actuació 13
5. Volumetries 15
6. Organització del servei 15
6.1. Recursos humans 16
6.2. ANS's generals de la solució 18
6.3. Horari de servei 19
7. Fases d'execució del contracte 20
8. Regulació de la IA 22
9. Seguretat 23
9.1. Clàusules generals de seguretat en la prestació del servei 23
9.2. Clàusules generals de seguretat 36
9.3. Clàusules generals de seguretat en el desenvolupament 38

1. Antecedents i motivació del contracte

La transformació digital ha canviat profundament la manera com ens relacionem i participem en la vida comunitària . Avui, gran part de les experiències, aprenentatges i expressions passen per entorns digitals on la informació circula amb una immediatesa i intensitat sense precedents. En aquest escenari, la desinformació hi troba un terreny especialment fèrtil i condiciona la manera com construïm opinions, percebem el món i alhora ens vinculem amb la resta de la societat. L'exposició no es produeix només a través de continguts obertament falsos, sinó també mitjançant rumors, teories conspiratives, continguts descontextualitzats, manipulacions audiovisuals i missatges que adopten formes aparentment fiables o properes. Aquest tipus de continguts circulen especialment bé en plataformes de consum ràpid i en entorns de missatgeria interpersonal, on la confiança o la immediatesa afavoreixen la seva difusió.

La Comissió Europea ha definit la desinformació com "informació falsa, errònia o enganyosa dissenyada, presentada i promoguda intencionadament per causar danys públics o per a lucrar-se" (referència: Comissió Europea (2018). A multi-dimensional approach to disinformation. Report of the independendent High level Group onfake news and online desinformation https://bit.ly/37TYo2T). Amb la pràctica de la desinformació s'ataca els fonaments de la democràcia, es manipula a les persones, es vulneren drets fonamentals i s'expandeixen els discursos d'odi. Així, la desinformació és avui un problema greu que preocupa a la ciutadania i les institucions públiques.

Interès municipal en la licitació

L'Ajuntament de Barcelona s'ha dotat del *Pla de Foment del Pensament Crític i Sensibilització sobre la Desinformació entre els Infants, Adolescents i Joves de la Ciutat, 2026-2030*.Aquest pla pretén fomentar l'alfabetització mediàtica i informacional, impulsant el pensament crític i la verificació entre els seus ciutadans més joves.

Aquest pla es presenta com una resposta integral a un repte col·lectiu que afecta la qualitat democràtica i el futur de les noves generacions: garantir que els individus creixin amb la capacitat de comprendre, qüestionar i transformar l'entorn.

Tot i que aquest Pla posa un èmfasi especial en els infants, adolescents i joves, la necessitat de comprendre i abordar els impactes de la desinformació s'estén al conjunt de la ciutadania.

Per als ciutadans de Barcelona és important que l'Ajuntament disposi de mecanismes que permetin identificar, analitzar i comprendre els fenòmens de desinformació que es produeixen a les xarxes socials i als entorns digitals, atès que aquests poden tenir efectes directes sobre:

- La convivència. La desinformació a les xarxes socials afecta la convivència perquè altera la manera com les persones perceben la realitat i es relacionen entre elles. Quan circulen informacions falses, enganyoses o manipulades, es poden generar conflictes, desconfiances i divisions dins de la societat.

- La confiança en la *res pública*. La desinformació debilita els vincles de confiança que fan possible la vida democràtica i la bona governança dels assumptes públics.
- La reputació de la ciutat. En una ciutat global com Barcelona, la reputació és un actiu estratègic. Influeix en l'atracció de talent, d'inversions, de congressos internacionals, de turisme de qualitat i fins i tot en l'orgull de pertinença dels residents.

La desinformació no és només un problema comunicatiu, sinó també econòmic, social i democràtic que afecta tota la ciutadania.

Les administracions públiques han de disposar d'eines tecnològiques especialitzades per monitoritzar, analitzar i interpretar el món digital, identificar continguts enganyosos, interpretar el món digital, identificar continguts enganyosos que cerquen la desinformació i alhora fer un ús responsable de la tecnologia, per així enfortir els valors democràtics i consolidar un ecosistema digital que faciliti la cohesió social i la convivència.

Per tot el que s'ha exposat, es considera necessari disposar d'un servei estable de detecció, validació, gestió i assessorament d'aquelles narratives de desinformació. Aquest Plec Tècnic detalla els aspectes necessaris per posar en marxa aquest servei.

2. Objecte del contracte

El present contracte té per objecte la prestació del servei de detecció, validació, gestió i assessorament de narratives de desinformació.

Els objectius del present contracte són:

- El rastreig informàtic (també anomenat scrapping tecnològic) sostingut de les mencions a les xarxes socials i mitjans digitals relacionades amb l'activitat municipal
- La construcció d'un repositori de dades oficials públiques per al contrast de desmentits
- La càrrega en repositori de mencions de període anterior (12 mesos) abans de l'entrada en vigor del contracte.
- La construcció d'una base de dades (BBDD) de desinformació (dades del rastreig de les mencions, classificades i enriquides).
- La connectivitat via una interfície de programació d'aplicacions (API) de la BBDD de desinformació amb eines de Business Intelligence (BI) corporatiu ja que la informació obtinguda s'ha de poder treballar amb eines de tractament de dades corporatives de l'ecosistema d'aplicacions corporatives en el cas d'informes agregats on aquesta informació sigui rellevant

- L'anàlisi de les mencions.

- El diagnòstic de les mencions segons temàtica, sentiment, recurrència i tipologia de desinformació.

- La proposta de pla d'acció contra la desinformació, incloent l'eliminació automatitzada de les mencions o la sol·licitud de rectificació quan aquesta sigui viable.

L'aplicació dels objectius fixats anteriorment ha de proporcionar els següents resultats:

- Disposar d'un servei de detecció, validació, gestió i assessorament de les narratives de desinformació que vetlli per la qualitat de la informació que, vinculada a l'activitat municipal, es difon per les xarxes socials i mitjans digitals.

- Contribuir a combatre la desinformació mitjançant els següents propòsits:
  - Lluitar contra la vulneració de drets individuals i associats ja que "la desinformació vulnera el dret a rebre informació veraç i a formar-se una opinió de manera lliure" (Assemblea General de les Nacions Unides, art. 19).

  - Fomentar els valors democràtics a l'oposar-se a la degradació de la confiança en els mitjans de comunicació i les institucions.

  - Donar suport als col·lectius més vulnerables ja que els perjudicis causats per la desinformació no són homogenis entre la ciutadania i són diferents depenent de l'edat, dels gènere, de l'orientació sexual, de la religió, l'origen i/o el context socioeconòmic.

  - Deixar de ser reactius davant el fenomen de la desinformació i passar a tenir un paper més actiu davant aquelles activitats que pretenen erosionar els sistemes democràtics.

3. Abast del contracte

Estan inclosos en l'abast d'aquest servei durant tota la vigència del contracte i les seves pròrrogues, en el cas de que aquestes s'executin:

- Els serveis d'assessorament i anàlisi especialitzat per l'ús de la solució proposada d'acord amb el detall del punt 4 i els corresponents epígrafs d'aquest Plec Tècnic.

- 7 llicències/subscripcions pel número d'usuaris necessaris a la solució tecnològica proposada (en règim *Software as a Service*), composta pel programari/s i interfícies necessàries per dur a terme els diferents serveis descrits en el present plec i interconnectada amb les solucions corporatives existents a l'Ajuntament i la base de dades de desinformació.

- El manteniment correctiu i evolutiu de la solució tecnològica durant la vigència del contracte.

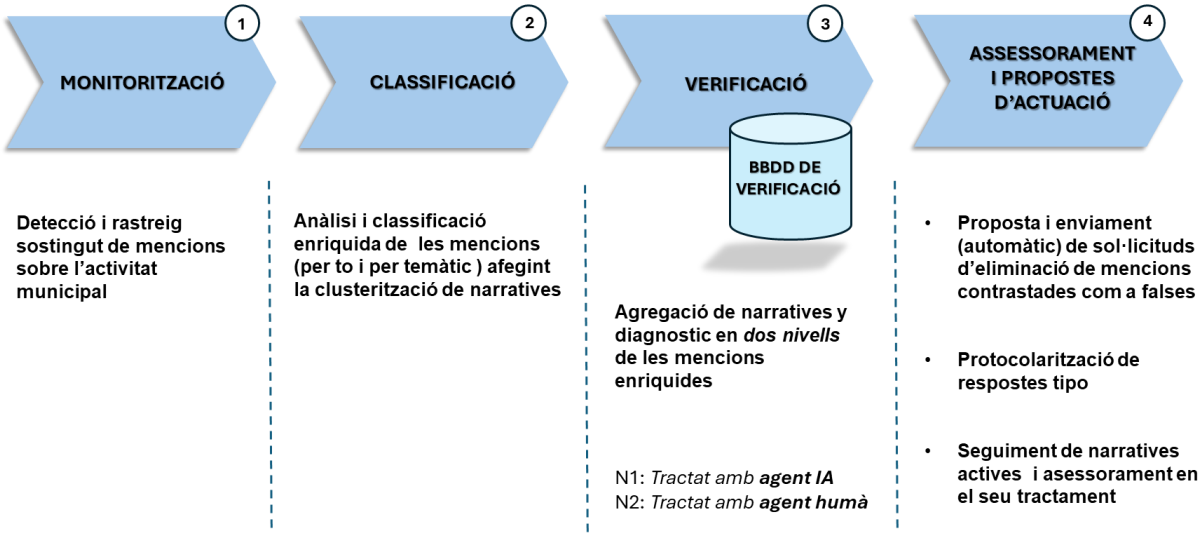
- Els recursos humans necessaris per a dur a terme el desplegament i la configuració de la solució tecnològica proposada i la formació a l'equip de l'Ajuntament en aquesta solució.

- La planificació de sessions de treball, *reporting* i presentacions a l'equip responsable de l'Ajuntament de Barcelona amb la finalitat d'obtenir una correcta operació de la solució, tant en la fase de desplegament com de manteniment.

4. Característiques del servei

L'empresa adjudicatària haurà d'oferir una solució tecnològica clau en mà composta per un o més programaris que, amb les seves interfícies i BBDD i d'acord amb el detall funcional que es detalla a continuació, donin resposta al següent plantejament representat en un diagrama de flux del servei.

El següent diagrama de flux representa les diferents fases del cicle de tractament d'una menció feta sobre l'activitat municipal en un mitjà o a les xarxes socials, des de de la seva detecció amb un procés de rastreig sostingut fins el seu tractament en la fase final del procés.
El gràfic detalla només les principals activitats de cada fase i aquest Plec Tècnic les detalla en el desenvolupament d'aquest punt 4 que s'estructura en quatre subapartats , un per cadascuna de les fases representades en el esquema conceptual:



La solució tecnològica ha d'estar estructurada modularment i relacionada amb els serveis professionals a partir del flux de treball expressat en el punt anterior on es relaciona, a alt nivell la funcionalitat sol·licitada que haurà de ser coberta amb una solució tecnològica i amb serveis professionals especialitzats.

El servei a prestar s'estructurarà en les següents fases:

1. Monitorització del servei: detecció i rastreig
2. Classificació, valoració i clusterització de conceptes
3. Verificació , agregació de narratives i diagnòstics
4. Assessorament i propostes d'actuació

4.1. Monitorització del servei

S'entén per Monitorització, el servei de detecció i rastreig continuat de mencions relacionades amb l'activitat municipal a les xarxes socials i suports digitals publicats en català i castellà amb un abast temporal 24/7 mitjançant l'ús d'una solució tecnològica.

Cal disposar d'aquesta detecció i rastreig sostingut de les mencions en un període de temps màxim de 15 minuts des de la seva publicació.

Requeriments funcionals associats

La solució tecnològica ha de disposar d'un seguit de funcionalitats associades al rastreig i la monitorització agrupades en un mòdul o conjunt de funcionalitats que permetin la cobertura de les següents necessitats:

- L'abast de xarxes socials i de suports digitals que s'haurà de rastrejar i dels quals s'ingesten continguts és el següent:
  - Instagram
  - Facebook
  - TikTok
  - X
  - Bluesky
  - Threads
  - Mitjans de comunicació

- Sistema d'alertes automatitzat que detecti i registri volums significatius de mencions genèriques i/o específiques en referència a una relació de paraules clau predefinida per part de l'equip de l'Ajuntament de Barcelona. Les quantitats -volumetries- a partir de les que es poden disparar les alertes han de poder ser parametritzables directament per part dels usuaris de la solució modificant aquells paràmetres que fan que una determinada quantitat es consideri susceptible de generar una alerta

- Funcionalitat de *dashboard* o quadre d'indicadors amb una representació numèrica i gràfica que ha permetre la visualització de continguts que s'han de poder classificar per

temàtica, font, sentiment – en aquest cas parametritzable directament per part de l'usuari- i per l'origen de les dades.

- Funcionalitat capaç de poder identificar els autors de les mencions per rellevància, entesa aquesta com el nombre de mencions adjudicables a un mateix autor d'acord amb la programació de les consultes o *queries* que es facin contra la BBDD.

- Sistema d'etiquetat que permeti classificar el contingut per temàtiques, possibilitant l'edició i/o introducció de noves temàtiques, subtemàtiques i paraules claus a suggeriment de l'equip de l'Ajuntament.

- Els continguts ingestats a la BBDD del programari han de poder ser cercats per un sistema de paraules clau amb un temps de resposta no superior a 5 segons .

- Existència d'una o més APIS que permetin la integració amb una o vàries fonts de continguts.

- Detecció d'imatges de marca (logotipat) en continguts visuals.

- Capacitat per monitoritzar (detectar, registrar i operar) contingut a les xarxes socials i suports digitals amb una retroactivitat de 12 mesos.

4.2. Classificació, valoració i clusterització de conceptes

Detectades les mencions associades a continguts de presumpta desinformació, el servei les ha d'analitzar i determinar d'acord als següents paràmetres:

- La categoria o temàtica a la que pertany
- La narrativa o subcategoria feta servir
- El sentiment d'aquesta menció en relació a l'activitat municipal, d'acord amb la tipologia predefinida

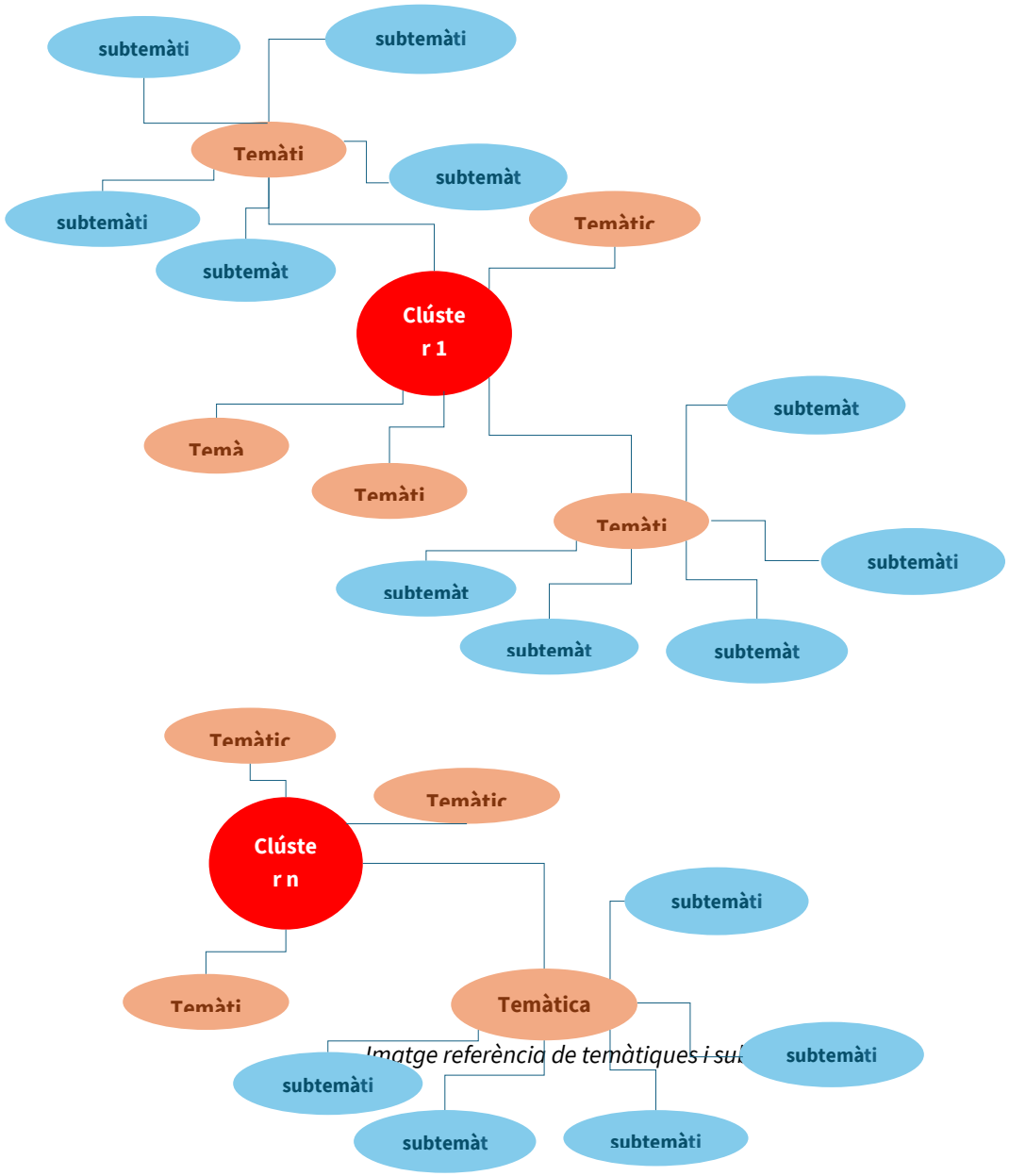
Requeriments funcionals associats

La funcionalitat bàsica de l'activitat de classificació, valoració i clusterització de conceptes és el processat i l'anàlisi de les mencions detectades en la fase prèvia.
Aquest processat té com a resultat principal un enriquiment de la informació associada a les mencions detectades que permetrà la gestió en fases posteriors.

La solució tecnològica ha de disposar d'un seguit de funcionalitats associades a aquesta activitat agrupades en un mòdul o conjunt de funcionalitats que permetin la cobertura de les següents necessitats :

- Classificació del contingut respecte a l'activitat municipal:
  - Segons la tipologia de desinformació: fals, enganyós, imatge falsa, descontextualitzada (poden introduir-se noves categories a futur).
  - Segons tipologia de sentiment: positiu, negatiu, neutre.
  - Segons temàtiques vinculables al context de l'activitat municipal (seguretat, polítiques i gestió pública, tramitació etc.)

- Detecció de narratives (subcategories) classificades com desinformació i que són transversals entre diferents tipologies de mencions no essent paraules clau i que s'entén com a clusterització de temàtiques. S'entén com a clúster temàtic una estructura de continguts que s'organitza a l'entorn d'un tema principal, que s'acostuma a composar d'un contingut que aborda el tema central de forma extensa i de diferents continguts satèl·lit que aprofundeixen en subtemes relacionats amb el principal.



Imatge referència de temàtiques i sub

4.3. Verificació, agregació de narratives i diagnòstics

L'objectiu de la detecció de mencions que contenen desinformació és poder abordar-les per part dels equips de l'Ajuntament.

Aquest tractament de la desinformació es farà mitjançant el contrast amb informacions oficials. Amb aquest objectiu cal explotar un repositori que, de manera centralitzada, agregui dades oficials de l'Ajuntament per permetre aquest contrast entre la informació oficial disponible i la que s'ha detectat i diagnosticat com a falsa o errònia en les mencions registrades públiques de l'activitat municipal.

Requeriments funcionals associats

La solució tecnològica ha de disposar d'un seguit de funcionalitats associades a aquesta activitat agrupades en un mòdul o conjunt de funcionalitats que permetin la cobertura de les següents necessitats:

- Repositori centralitzat de dades oficials de l'Ajuntament per a contrastar afirmacions detectades.
  La càrrega inicial d'aquest repositori s'haurà de construir, per una banda, a partir de fonts oficials existents, i, per altra banda, a partir de les narratives identificades en l'anàlisi de contingut retroactiu dels 12 mesos anteriors.

  Aquest repositori estarà configurat en una base de dades en la que s'haurà de poder carregar i estructurar, entre d'altres, la següent informació municipal oficial d'abast públic:
  - ✓ Estadístiques
  - ✓ Ordenances
  - ✓ Resolucions
  - ✓ Comunicats

  Aquesta informació oficial s'ha de poder:
  - ✓ Indexar
  - ✓ Cercar semànticament amb les mateixes taxonomies temàtiques del mòdul de monitorització.
  - ✓ Actualitzar periòdicament de manera automàtica i també manual

- Sistema de valoració de les mencions
  La solució tecnològica ha de permetre fer un diagnòstic en dos nivells diferents de profunditat:

  – **Diagnòstic preliminar**: consistent en una valoració inicial del contingut de la menció.

La funció d'aquest diagnòstic preliminar és el contrast d'informacions entre les mencions i el repositori de dades públiques oficials.

Es considera necessari l'actuació d'un **agent IA** en aquesta fase degut a l'alt volum de mencions detectades (estimades en 100.000 mencions anuals), fet que impossibilitaria dur a terme la tasca inicial amb agilitat i celeritat en cas de fer-se mitjançant recursos humans professionals.

Aquesta valoració s'haurà d'efectuar a partir d'un tipològic de l'estil:

- ✓ Enganyós
- ✓ Fals
- ✓ Imatge falsa
- ✓ Imatge descontextualitza
- ✓ Cert
- ✓ No es troben dades publicades

La valoració haurà d'anar acompanyada d'un indicador, aquest ha de poder generar una alerta de "verificació addicional necessària" perquè es pugui gestionar manualment.

– **Diagnòstic de verificació**: consistent en una valoració posterior a la feta per l'agent IA i en la que un/a consultor/a especialista en comunicació revisa el diagnòstic preliminar i l'eleva a definitiu abans de proposar qualsevol tipus d'actuació.

4.4. Assessorament i propostes d'actuació

Aquesta fase del procés consisteix en la presa de decisions en relació a totes les mencions identificades com a falses o enganyoses o descontextualitzades.

L'equip responsable de l'Ajuntament de Barcelona supervisarà la categorització dels continguts identificats com a desinformació i ho posarà en comú amb el servei d'assessorament proporcionat per l'empresa adjudicatària, qui serà l'encarregat de fer les propostes d'actuació demandades.

Requeriments funcionals associats

La solució tecnològica ha de disposar d'un seguit de funcionalitats associades a aquesta activitat agrupant les mencions detectades i classificades en un mòdul o conjunt de funcionalitats que permeti la cobertura de les següents necessitats:

- Fer un seguiment individualitzat de l'evolució de las narratives de desinformació detectades

- Disposar de *feeds* de continguts amb capacitat per filtrar per l'estat de la narrativa amb una tipologia de filtratge:
  - ✓ Identificada
  - ✓ Verificada
  - ✓ En monitoratge
  - ✓ Gestionada

- Disposar d'un sistema de permisos i regles que permetin la configuració dels usuaris en, com a mínim, els següents perfils: Editor, Lector, Gestor.

- Possibilitat d'enrutar o direccionar continguts directament adreçats als diferents perfils d'usuari donats d'alta en el sistema amb una tipologia de direccionalment de l'estil de:
  - ✓ Revisió
  - ✓ Validació
  - ✓ Decisió (actuació)

- Permetre que l'equip municipal a càrrec del projecte sol·liciti la eliminació o desindexació de continguts que han estat contrastats fefaentment com a desinformació en els mitjans de comunicació o xarxes/plataformes que els han publicat o que els hostatgen.

  Aquesta sol·licitud l'ha de fer la empresa adjudicatària amb programaris que executin aquesta funcionalitat en el cas de que l' eina proposada per a la detecció i tractament de mencions no contempli aquesta opció per defecte.

- Crear informes automàtics sobre la relació de continguts de desinformació, descàrrega en format Excel de mencions per temàtica, presentacions amb conclusions, aprenentatge i pla d'acció.

- Disposar de funcionalitats de *reporting* que permetin llistar i visualitzar per diferents criteris les mencions detectades, les mencions processades i les propostes d'actuació per menció, temàtica i narratives associades mitjançant la recerca de paraules clau.

- Disposar d'una interfície estàndard (API) que permeti el bolcatge dels informes anteriors en diferents nivells de detall a solucions de mercat específiques de tractament de dades.

<u>Servei d'assessorament</u>

L'empresa adjudicatària haurà de proporcionar serveis d'assessorament especialitzats basats en el suport a les recomanacions estratègiques de resposta i/o actuació comunicativa i al manteniment

de la BBDD de coneixement que s'actualitza periòdicament amb les mencions processades i gestionades per temàtic.

El servei d'assessorament ha de desenvolupar les següents activitats:

- Recomanació d'accions per a cada narrativa verificada
  - Seguiment
  - Opcions de resposta
  - Rectificació, eliminació amb justificació comunicativa i institucional /legal en aquells casos en els que es consideri pertinent

- Co-creació juntament amb l' equip de treball de protocols de resposta per agrupació de comunitat/canal i sensibilitat del contingut

- Proposta de redacció de resposta

- Reingesta del coneixement generat en la BBDD i en les funcionalitats d'ingesta per garantir la construcció de coneixement

- Seguiment periòdic del contracte amb reunions de periodicitat setmanal o quinzenal

- Enviament d'informes diaris sobre narratives actives i enviament sobre casos gestionats

5. Volumetries

Durant el segon semestre de 2025, l'Ajuntament de Barcelona va realitzar un estudi inicial de diagnòstic, en el que es va obtenir els següents resultats:

- 44.000 mencions en 6 mesos en les xarxes socials i publicacions digitals analitzades
- El 20% (8.800) de les mencions tenien sentiment negatiu
- Es van detectar 111 narratives diferents
- De les 111 narratives, 31 eren susceptibles de pla d'acció

L'estimació amb la que es treballa és la superació de les 100.000 mencions anuals de mitjana en el període de vigència del contracte.

6. Organització del servei

L'adjudicatari serà l'encarregat de:

- La direcció global extrem a extrem de les tasques del contracte de serveis tal i com ha estat definit en el punt 4 i els seus apartats d'aquest Plec Tècnic
- La interlocució amb els usuaris de l'equip de treball interdisciplinar que s'estableixin com interlocutors del contracte.
- La coordinació dels diferents actors que intervenen al contracte.
- La supervisió i seguiment de les tasques detallades en aquest plec.
- L'aprovisionament del programari en la modalitat de llicència o SaaS per el número d'usuaris sol·licitats (7 llicències)
- El manteniment correctiu i evolutiu de la solució tecnològica plantejada d'acord amb els ANS's o Acords de Nivell de Servei detallats en aquest Plec
- El compliment de les especificacions de seguretat per els subministrament de solucions tecnològiques d'acord amb l'Institut Municipal Barcelona Innovació i Tecnologia de l'Ajuntament de Barcelona (BIT en endavant) exposades en aquest Plec

L'adjudicatari haurà de posar a disposició del projecte una eina de seguiment del manteniment del projecte, sent el seu ús obligatori per part de l'adjudicatari i assumint l'adjudicatari els costos que se'n derivin.

Abans de l'inici de les tasques de manteniment, l'adjudicatari haurà de dur a terme una auditoria tècnica completa de la xarxa existent. i dels sistemes instal·lats, amb l'objectiu d'identificar l'estat actual dels equips, possibles deficiències i les necessitats d'adequació per garantir el correcte funcionament de la xarxa. Aquesta auditoria inclourà la revisió i anàlisi de la infraestructura de comunicacions

Els resultats d'aquesta auditoria serviran com a base per a l'elaboració del pla de manteniment, assegurant que les actuacions previstes responguin a la realitat operativa i tècnica de cada mercat.

També serà responsable de dotar el contracte amb els recursos necessaris, tant humans com materials, que permetin el correcte desenvolupament d'aquestes tasques, des de la direcció

6.1. Recursos humans

L'empresa adjudicatària haurà de comptar, com a mínim amb els següents perfils per dur a terme el present contracte:

Cap de Projecte – Service Manager

Titulacions:

- Grau en enginyeria electrònica industrial i automàtica, o Grau en ciència i enginyeria de dades o Grau en Enginyeria Informàtica, en Informàtica o en enginyeria superior de Sistemes de Telecomunicació o Grau en Enginyeria electrònica de Telecomunicació o equivalents.

Experiència professional: Mínim de 5 anys en gestió de projectes tecnològics.

L'empresa adjudicatària haurà de designar un Cap de projecte com a responsable directe de la gestió i seguiment del contracte. Aquesta figura actuarà com a punt únic de contacte amb l'Ajuntament (Gerència de recursos , Direcció de Comunicació i IMI/BIT) i serà l'encarregada de coordinar les actuacions, supervisar la correcta execució dels serveis i garantir el compliment dels terminis i nivells de qualitat establerts.

El Cap de projecte haurà de disposar dels coneixements tècnics i de gestió adequats, i haurà de participar activament en les reunions de seguiment i en la resolució d'incidències que puguin sorgir durant l'execució del contracte.

Enginyer/a especialitzat en IA

Titulacions:

- Grau en enginyeria electrònica industrial i automàtica, o Grau en ciència i enginyeria de dades o Grau en Enginyeria Informàtica, en Informàtica o en enginyeria superior de Sistemes de Telecomunicació o Grau en Enginyeria electrònica de Telecomunicació o equivalents
  i
- Màster en Big Data o en Intel·ligència Artificial

Experiència professional: Mínim de 5 anys d'experiència en la gestió de projectes d'anàlisi de dades que hagin comportat tractament estadístic d'aquestes on s'hagi fet servir IA .

Cal disposar en l'equip d'un/a enginyer/a especialitzat/da en intel·ligència artificial per tal de gestionar la part de la solució tecnològica que contempla l'ús d'aquesta tecnologia aplicada a la valoració inicial del contingut de la menció tal i com s'indica en el punt 4.3.

L'enginyer/a IA serà la persona encarregada de programar i gestionar les funcions atribuïdes a l'agent IA en la fase de diagnòstic preliminar de les mencions.

Analistes-Consultors digitals

Caldrà disposar de dos perfils de consultors-analistes diferents:

– **Analista consultor/a de l'activitat de monitorització**

  Titulació:
  - Grau en Sociologia, o Grau en Ciència i enginyeria de dades o Grau en Màrqueting i Investigació de Mercats.

  Experiència professional: Mínim de 5 anys en projectes d'investigació de mercats i/o d'anàlisi de dades en el context dels mitjans digitals i/o de comerç electrònic amb focus en els processos d'escolta digital o "social listening", entès aquest com el procés de monitoratge i anàlisi de converses i mencions produïdes en el context d'internet sobre una marca, persona o entitat.

Aquest perfil serà l'encarregat de l'operativa de monitorització, d'acord a les funcions que es descriuen a l'apartat 4.1 del present plec.

– **Analista consultor/a de propostes d'actuació**

Titulació:

- Grau en Sociologia, o Grau en Ciència i enginyeria de dades o Grau en Màrqueting i Investigació de Mercats o Grau en Periodisme.

Experiència professional: Mínim de 5 anys en projectes d'investigació de mercats i/o d'anàlisi de dades en el context dels mitjans digitals i/o de comerç electrònic amb focus en els processos d'escolta digital o "social listening", entès aquest com el procés de monitoratge i anàlisi de converses i mencions produïdes en el context d'internet sobre una marca, persona o entitat.

Es considera adient un perfil amb experiència en comunicació relacionada amb el fenomen de les *Fake news* i tendències del consum de xarxes socials des de la vessant de la sociologia, i també amb experiència acreditada en el tractament estadístic de dades.

Aquest perfil serà l'encarregat d'interpretar les mencions valorades, proporcionant assessorament i propostes d'actuació reflectides en protocols que podran ser diferents per tipologia, narrativa i/o col·lectiu, d'acord amb la informació recollida a l'apartat 4.4 del present plec.

6.2. ANS's generals de la solució

L'adjudicatari serà el responsable d'aplicar les mesures preventives i correctives necessàries per tal de subsanar qualsevol incidència en el funcionament del programari/s i les eines de gestió vinculades a aquest durant la vigència del contracte i la seva pròrroga si aquesta s'executa.

De la mateixa manera caldrà que l'adjudicatari disposi d'eines de monitorització contínua de l'estat de la solució tecnològica proposada.

Aquest manteniment inclourà la correcció d'errors detectats posteriorment per mal funcionament o perquè no s'han cobert les especificacions requerides, que es posin de manifest en el funcionament diari de solució o que es descobreixin posteriorment, així com la correcció de la que tingui deficiències.

L'adjudicatari també serà el responsable de realitzar els canvis de configuració necessaris per tal de donar nous serveis per noves versions del programari/s fent alhora les corresponents formacions si és pertinent i proporcionant sempre el material necessari perquè els usuaris disposin de la informació necessària sobre aquests canvis.

La resolució d'incidències relacionades amb el manteniment d'aquest contracte es farà segons els següents ANS's o Acords de Nivell de Servei:

Resolució d'incidències generals	Temps de resposta	Temps de diagnòstic	Temps de resolució
Incidència crítica	1 hora	4 hores	8 hores
Incidència greu	2 hores	8 hores	12 hores
Incidència normal	4 hores	16 hores	20 hores

Tipus d'incidències:

- **Incidència crítica**: El programari no funciona o una de les funcionalitats bàsiques no funciona. Implica una aturada en l'operativa normal de funcionament de la solució.
- **Incidència greu**: El programari o un dels seus components té una anomalia important però no impedeix l'operativa normal d'aquest.
- **Incidència normal**: El sistema o un dels seus components té una incidència però es pot treballar sense dificultats

Franges de temps:

- **Temps de resposta**. És el temps transcorregut des de que la incidència és comunicada a l'adjudicatari fins que un tècnic qualificat es posa en contacte amb el responsable de l'aplicació o la persona que es designi.
- **Temps de diagnòstic**. És el temps transcorregut des de que la incidència és comunicada a l'adjudicatari fins que l'adjudicatari fa un diagnòstic del problema.
- **Temps de resolució**. És el temps transcorregut des de que la incidència és comunicada a l'adjudicatari fins que es considera tancada pel responsable de l'aplicació o la persona que es designi.

El temps de resposta, diagnòstic i resolució es compta sobre l'horari de 00:00 a 24:00 de dilluns a diumenge, tots els dies de l'any. Es fa notar que en el cas de les incidències, el temps de resposta és acumulatiu: és a dir, que tots els temps comencen a comptar des de l'inici de la comunicació de la incidència. En aquest cas, una millor resposta en un temps, dona més marge en els temps de resposta posterior.

6.3. Horari de servei

De dilluns a divendres en horari laborable de 9.00 a 17.00 h.

Caps de setmana: servei remot de guàrdia(*) de 10.00 a 15.00 h.

(*)Aquesta persona tindrà accés a les solucions tecnològiques proposades per l'oferta de l'adjudicatari i a les que disposi l'Ajuntament per a detectar mencions que s'hagin considerat que requereixen de tractament immediat i activarà el protocol establert per aquestes situacions.

7. Fases d'execució del contracte

En referència al cicle d'execució del contracte, tal i com ha estat definit en el present Plec Tècnic, el procés de prestació del servei de detecció, validació, gestió i assessorament de narratives de desinformació consta d'una sèrie d'etapes caracteritzades per les grans activitats de:

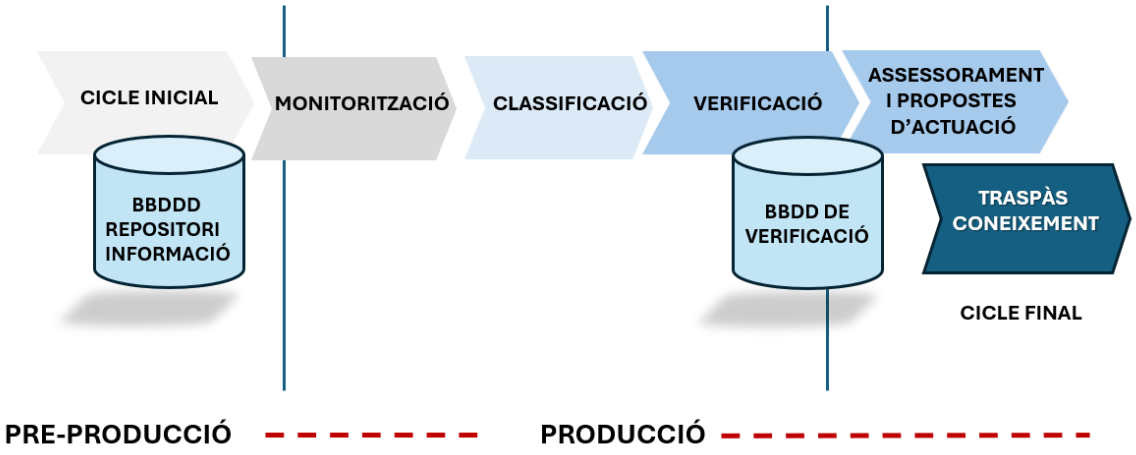
- Monitorització de les mencions objectes del servei
- Classificació d'aquestes mencions
- Verificació de la validesa/falsedat de les mencions
- Assessorament dei propostes d'actuació

Aquestes etapes alhora es corresponen amb un cicle temporal des de la seva vessant de projecte de desplegament d'una solució tecnologia i de l'ús d'aquesta solució per part dels usuaris i administradors assignats per part de l'Ajuntament de Barcelona.

Aquest cicle es divideix, entre d'altres classificacions possibles, en tres grans etapes:

- Cicle inicial: Pre-producció
- Cicle d'execució: Producció
- Cicle final: Traspàs del coneixement

A continuació es detallen les tasques i terminis clau per dur a termes cadascuna de les fases:



Cicle inicial de projecte: Pre-producció

Abans de que la solució tecnològica entri en funcionament i sigui visible i operativa públicament per part del seus públics, es considerarà en fase de pre-producció. Durant aquesta etapa caldrà que

l'empresa adjudicatària faci, de manera genèrica, un seguit de tasques per garantir que la solució tecnològica es desplegui adequadament per poder ser usada d'acord al funcionament acordat.

Construcció de la BBDD de repositori d'informació municipal

Tal i com es detalla a la clàusula 4.3 del Plec Tècnic, l'empresa adjudicatària haurà de construir una Base de Dades que actuarà com a repositori centralitzat de dades oficials de l'Ajuntament per a contrastar afirmacions detectades. La càrrega inicial d'aquest repositori s'haurà de construir a partir d'una relació d'informació de caràcter públic associada a l'Ajuntament de Barcelona.

L'empresa adjudicatària haurà d'elaborar aquesta base de dades en un període màxim d'un mes a partir de la data d'inici d'execució del contracte. Aquesta fita és clau per poder iniciar les tasques objectes del present contracte. Per tant, en cas que l'empresa adjudicatària no assoleixi aquest objectiu per fets no imputables a causes externes, podrà aplicar-se una penalitat d'acord amb que estableix la clàusula de Demora de les prestacions recollida al plec de clàusules administratives particulars del present contracte.

Cicle d'execució del projecte: Producció

Durant la fase d'execució del projecte, l'empresa adjudicatària haurà de dur a terme les diferents tasques associades a la detecció, validació, gestió i assessorament de narratives de desinformació, d'acord a les condicions i processos detallats a la clàusula 4 del present plec.

Tanmateix, serà l'encarregada del manteniment de la base de dades relativa a la informació de dades oficials de l'Ajuntament mitjançant l'actualització periòdica de noves informacions de les característiques que es defineixen en el present plec i/o a proposta de l'equip de treball de l'Ajuntament de Barcelona.

Cicle final de projecte: Traspàs del Coneixement

L'empresa adjudicatària haurà d'executar el pla de devolució durant l'últim mes del contracte, on haurà de preparar el traspàs de la informació i el coneixement del servei a l'Ajuntament de Barcelona o a qui aquest decideixi, mentre l'adjudicatari manté el nivell de servei de la fase d'execució.

El Pla de devolució del servei haurà de complir, com a mínim, els següents principis i continguts:

- Proporcionar els continguts de la BBDD de informació de l'Ajuntament en un format que permeti la càrrega d'aquesta informació per part del noi adjudicatari
- Proporcionar el contingut de les mencions i els seu tractament dels darrers 12 mesos de servei al nou adjudicatari en un format que permeti la càrrega d'aquesta informació per part del nou adjudicatari
- Proporcionar el contingut dels informes dels darrers 12 mesos de servei al nou adjudicatari en un format que permeti la consulta per part del nou adjudicatari

A més a més, l'empresa haurà de tenir disponible un servei de consulta via telèfon i correu electrònic sobre aspectes del servei durant un període d'un mes a partir de l'inici de la nova adjudicació i amb un compromís de resposta de màxim 24 hores.

L'incompliment d'aquesta condició serà considerat com incompliment greu, possibilitant l'aplicació de les penalitats corresponents recollides al plec de clàusules administratives particulars.

8. Regulació de la IA

Tal i com detalla *l' Estratègia per a l'adopció ètica, democràtica i sostenible de la intel·ligència artificial*[1] de l'Ajuntament de Barcelona: "La IA és una eina valuosa que pot ajudar els governs locals a afrontar els problemes complexos que han de gestionar en l'actualitat i, alhora, constitueix un instrument útil per facilitar el compliment dels objectius establerts a l'Agenda 2030, tal com ha reconegut l'Assemblea General de les Nacions Unides en diverses resolucions. Tanmateix, més enllà dels beneficis que se'n poden derivar, l'ús de la IA a les administracions públiques també pot generar nombrosos riscos i, eventualment, perjudicis en els interessos generals o els drets de les persones, per la qual cosa la seva utilització s'ha de fer amb garantia d'aquests drets, així com respecte als principis inherents a l'estat de dret la democràcia. La Unió Europea va reconèixer en el seu Llibre blanc sobre la intel·ligència artificial que la IA no es pot entendre com un fi en si mateix, sinó com un mitjà que ha de servir a les persones amb l'objectiu últim d'augmentar el seu benestar i, davant altres models, va apostar per la consolidació d'una IA fiable, ètica i plenament respectuosa dels drets fonamentals. El maig del 2024, aquest compromís s'ha concretat amb l'aprovació del Reglament d'intel·ligència artificial, el qual busca assegurar el respecte dels drets fonamentals de la ciutadania de la UE posant la persona en el centre, a la vegada que estimula la inversió i la innovació en IA a tot Europa. Amb aquesta finalitat, regula els requisits que han de complir els sistemes d'IA i determina les obligacions de persones proveïdores i usuàries dels sistemes d'IA. A més, la Unió Europea ha destacat el paper de les ciutats en aquest procés (a la Declaració sobre unir esforços per impulsar una transformació digital sostenible a les ciutats i comunitats de la UE). En aquest context, l'Ajuntament de Barcelona fa anys que s'ha posicionat a favor de l'humanisme tecnològic i aposta perquè el desenvolupament tecnològic se centri en l'ésser humà i la tecnologia estigui al servei de les persones i dels interessos generals".

En aquest sentit, l'ús de tecnologies IA en projectes desenvolupats i/o executats en l'Ajuntament de Barcelona s'ha d'adequar als principis generals d'ús d'aquesta tecnologia que en el context europeu estan regulats per el "Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia

1 Vegeu: https://ajuntament.barcelona.cat/institut-innovacio-tecnologia/sites/default/files/2026-03/AAFF-Mesura_Govern_IA_2026_web.pdf

artificial[2] (RIA)", a Catalunya per el marc definit per les polítiques digitals[3] promogudes per el Govern de la Generalitat de Catalunya i, en el cas de Barcelona per *l'Estratègia per a l'adopció ètica, democràtica i sostenible de la intel·ligència artificia*l assenyalada inicialment.

9. Seguretat

Aquest punt té com a principal objectiu establir les clàusules d'obligat compliment en termes de seguretat per part de l'adjudicatari que presta el servei utilitzant els sistemes de l'Institut Municipal Barcelona Innovació i Tecnologia de l'Ajuntament de Barcelona (BIT en endavant) i també des de les instal·lacions de l'empresa adjudicatària.

Aquestes clàusules generals tenen per objecte establir requeriments sobre qüestions transversals pel que fa a la seguretat d'un projecte.

9.1. Clàusules generals de seguretat en la prestació del servei

Auditoria

BIT auditarà que l'empresa adjudicatària vetlli per la qualitat del seu servei. Es contemplen dos tipus d'auditories:

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

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

L'empresa adjudicatària proporcionarà l'assistència i la informació que requereixin les auditories, sense càrrec addicional per BIT. La realització de l'auditoria en cap moment eximirà l'empresa adjudicatària 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.

[2] Vegeu: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-81079

[3] Vegeu https://politiquesdigitals.gencat.cat/web/.content/00-arbre/economia/IA/Estrategia-Catalunya-IA-2030.pdf

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

Gestió d'Incidents

L'empresa adjudicatària informarà a la Direcció de Seguretat de la Informació de BIT de qualsevol incident de seguretat, seguint el Procediment de Notificació i Gestió de Incidències de Seguretat TIC de l'Ajuntament de Barcelona establert per BIT.

L'empresa adjudicatària disposarà d'un procediment de notificació i gestió d'incidents de seguretat, que contempli aquells incidents en què es vegin afectades dades de caràcter personal.

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

En cas que l'incident afecti els sistemes i els recursos propietat de l' empresa adjudicatària, serà responsabilitat d'aquest realitzar les accions de contenció i resolució necessàries per restaurar el servei.

L'empresa adjudicatària haurà de documentar els incidents de seguretat i indicar el tipus d'incidència, moment en què es produeix, moment en què s'ha detectat, persona que fa la notificació, a qui es comunica, els efectes d'aquesta, moment en què se soluciona, descripció de la solució i persona que ho realitza. A l'esmentat registre s'han d'establir, a més, els procediments realitzats de recuperació de la informació, persona que executa el procés i la informació restaurada.

La documentació d'un incident de seguretat de la informació i la investigació i resposta consegüent s'han de preparar mitjançant informes de forma cronològica i lliurar-se a la Direcció de Serveis de Seguretat de la Informació, en el cas que hi hagi hagut, o pugui haver, afectació al servei prestat.

Confidencialitat

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

Un cop finalitzat el present contracte, l'empresa adjudicatària 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.

Dimensionament/gestió de capacitats

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

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'empresa adjudicatària 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 BIT.

Anàlisis forenses

L'execució d'anàlisis forenses és responsabilitat exclusiva de la Direcció de Seguretat de la Informació de BIT. L'empresa adjudicatària 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 la Direcció de Seguretat de la Informació de BIT i l'empresa adjudicatària.

Control d'accés

<u>Accés local</u>
L'empresa adjudicatària 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.

Accés remot

L'empresa adjudicatària 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 BIT per als sistemes de l'Ajuntament.

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'empresa adjudicatària.

L'empresa adjudicatària 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.

L'autenticació al sistema s'haurà de produir amb un segon factor d'autenticació (2FA), requerint així una verificació de la identitat de la persona usuària que sol·licita accés.

Certificació ISO/IEC 27001

Per tal de garantir la protecció de la confidencialitat, integritat i disponibilitat de les dades, és necessari que l'empresa adjudicatària disposi de la **certificació ISO/IEC 27001**, relacionada amb els sistemes de gestió de seguretat de la informació (SGSI).

La ISO/27001 és l'estàndard internacional en certificació per la seguretat de la Informació. Aquesta certificació defineix els requeriments para establir, implementar, mantenir i millorar de manera continuada un sistema de gestió de la seguretat de la informació . El seu objectiu principal és protegir la confidencialitat, integritat i disponibilitat de les dades d'una empresa o institució.de la següent manera:

- Confidencialitat: Només les persones autoritzades poden accedir a ella.
- Integritat: La informació és exacta i no ha estat alterada indegudament.
- Disponibilitat: Els usuaris autoritzats tenen accés a la informació i els seus actius sempre que els requereixin

L'empresa adjudicatària haurà de presentar la certificació ISO/IEC 27001 abans de l'adjudicació del contracte, atenent al requeriment corresponent. La data de certificació haurà de ser anterior a la data de finalització de presentació de les ofertes.

Gestió del Personal

Deures i obligacions del personal.
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.

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.

Formació i conscienciació

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

- Instrucció 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'empresa adjudicatària 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'empresa adjudicatària ha realitzat sobre el personal assignat a l'execució del contracte.

Clàusula de comunicacions externes

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

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

L'empresa adjudicatària 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 producte o servei.

Protecció del lloc de treball

Lloc de treball buit

L'empresa adjudicatària 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.

Bloqueig del lloc de treball

L'empresa adjudicatària 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.

Protecció d'equips

L'empresa adjudicatària 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'empresa adjudicatària 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 BIT.

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.

Mitjans alternatius

L'empresa adjudicatària 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.

Protecció dels Suports Informàtics

L'empresa adjudicatària haurà de gestionar els suports informàtics amb informació de l'Ajuntament de Barcelona seguint les següents pautes.

Etiquetat

L'empresa adjudicatària es compromet a etiquetar els suports d'informació de manera que, sense revelar el seu contingut, s'indiqui el nivell de seguretat de la informació continguda de major qualificació. Els usuaris han d'estar capacitats per entendre el significat de les etiquetes, bé mitjançant simple inspecció, bé mitjançant el recurs a un repositori que ho expliqui.

Criptografia

Qualsevol informació corporativa que requereixi ser xifrada a la seva ubicació d'emmagatzemament, en particular a tots els dispositius extraïbles del tipus CD, DVD, discos USB,

o uns altres de naturalesa anàloga, han de seguir els estàndards de seguretat, custòdia i protecció de les claus establerts per la Direcció de Seguretat de la Informació de BIT.

Qualsevol requeriment criptogràfic de plataformes que s'hagin de produir referents amb la informació municipal o corporativa, l'empresa adjudicatària haurà de presentar-les per ser validades per la Direcció de Seguretat de la Informació de BIT i/o seguir els estàndards i normes de BIT.

Transport

L'empresa adjudicatària garantirà que els dispositius romanen baix control i que satisfan els requisits de seguretat mentre estan sent desplaçats d'un lloc a un altre. L'empresa adjudicatària garantirà que es segueix el procediment de transport, de manera que s'haurà de disposar d'un registre de sortida que identifiqui al transportista que rep el suport per al seu trasllat i d'un registre d'entrada que identifiqui al transportista que el lliura, conjuntament amb un procediment rutinari que quadri les sortides amb les arribades i elevi les alarmes pertinents quan es detecti algun incident.

Esborrat i destrucció

L'empresa adjudicatària haurà de seguir els estàndards i normes de BIT respecte a l'esborrat i destrucció de suports d'informació. S'aplicarà a tot tipus d'equips susceptibles d'emmagatzemar informació, incloent mitjans electrònics i no electrònics. Els suports que hagin de ser reutilitzats per a una altra informació o alliberats a una altra organització hauran de ser objecte d'un esborrat segur del seu contingut. S'hauran de destruir de forma segura els suports en cas de que la naturalesa del suport no permeti un esborrat segur o quan així ho requereixi el procediment associat al tipus d'informació continguda, fent us dels productes certificats per BIT.

Periòdicament i segons les necessitats de recurrència d'aquestes activitats, s'haurà d'informar i lliurar al responsable del contracte el certificat de destrucció corresponent, on quedarà especificat com a mínim, el identificador dels actius, el mètode d'esborrat i/o destrucció emprat, la data de l'activitat i el destí dels actius.

Protecció de la Informació

Neteja de documents

L'empresa adjudicatària disposarà d'un procediment de neteja de documents, el qual retirarà d'aquests tota la informació addicional continguda en camps ocults, metadades, comentaris o revisions anteriors, excepte quan aquesta informació sigui pertinent per al receptor del document.

Aquesta mesura serà especialment rellevant quan el document es difongui àmpliament, com quan s'ofereix al públic en un servidor web o un altre tipus de repositori d'informació.

Protecció del correu electrònic

En el cas de que l'empresa adjudicatària faci ús del seu correu electrònic corporatiu per gestionar informació de l'Ajuntament, l'haurà protegir enfront d'amenaces que li són pròpies:

- La informació distribuïda per mitjà de correu electrònic, es protegirà, tant en el cos dels missatges, com en els annexos.
- Es protegirà la informació d'encaminament de missatges i establiment de connexions.
- No es permetrà la redirecció a dominis de correus públics fora del correu corporatiu de l'empresa adjudicatària.
- Es protegirà a l'organització enfront de problemes que es materialitzen per mitjà del correu electrònic, en concret:
    - Correu no sol·licitat (spam)
    - Programes nocius, constituïts per virus, cucs, troians, espies, o uns altres de naturalesa anàloga
    - Codi mòbil de tipus applet.

L'empresa adjudicatària establirà polítiques d'ús del correu electrònic que inclourà com a mínim:

- Limitacions a l'ús com a suport de comunicacions privades.
- Realitzar activitats de conscienciació i formació relatives a l'ús del correu electrònic per al seu personal, per exemple per detectar casos de malware o phishing.

El responsable del contracte de l'Ajuntament avaluarà si el contracte ha de gestionar informació sensible, especialment protegida en relació a la protecció de dades personals, confidencial de l'Ajuntament o de les tecnologies municipals (adreces IP, usuaris, credencials,...).

En cas afirmatiu, l'Ajuntament facilitarà a l'empresa adjudicatària un correu electrònic de l'Ajuntament (@ext.bcn.cat) el qual es convertirà en la via de comunicació entre l'empresa adjudicatària i l'Ajuntament.

Aquesta mesura vol evitar que les empreses externes retinguin informació confidencial de l'Ajuntament en servidors de correu aliens a l'entorn municipal, durant i sobretot, un cop finalitzat el contracte.

Protecció de les instal·lacions

Les instal·lacions de l'empresa adjudicatària hauran de disposar de certes condicions de seguretat física:

- En cas de emmagatzemar informació de l'Ajuntament de Barcelona, disposar de les mesures de seguretat pertinents per evitar els accessos físics als repositoris d'informació, segons la sensibilitat de dita informació.
- Garantir que la informació de l'Ajuntament de Barcelona no pugui ser visible i/o audible des de l'exterior de les instal·lacions.

Gestió d'excepcions

Qualsevol excepció al clausulat de seguretat no recollida en el present document en el moment de la contractació o que ocorri en el transcurs del servei, haurà de ser comunicada per mitjà dels canals oficials a la Direcció de Seguretat de la Informació de BIT per al seu corresponent tractament i valoració. S'haurà de presentar de forma clara i concisa l'objecte de l'excepció així com la modificació desitjada pel sol·licitant amb la seva deguda justificació.

Còpies de seguretat

L'empresa adjudicatària haurà de comptar amb procediments i mecanismes per fer còpies de seguretat de la informació. Aquests procediments han de tenir en compte els processos per fer les còpies de seguretat, la periodicitat, els mètodes d'emmagatzematge i custòdia, els processos de restauració, etc. de manera que garanteixin la recuperació de la informació davant d'una situació de pèrdua o destrucció d'aquesta.

L'empresa adjudicatària ha de garantir que les còpies de seguretat es facin com a mínim amb una periodicitat setmanal.

L'empresa adjudicatària ha d'emmagatzemar còpies de seguretat de la informació en una ubicació alternativa d'aquella en què es processa habitualment.

A més, l'empresa adjudicatària haurà de disposar de mecanismes per a la realització periòdica de proves de restauració de les dades i les aplicacions. Hauran de ser capaços de restaurar les dades a partir de la darrera còpia de seguretat i de fer de manera periòdica aquestes proves amb dades reals.

L'empresa adjudicatària serà responsable de realitzar còpies de seguretat als sistemes dels quals és administrador per tal de poder recuperar les dades en cas de pèrdua accidental o intencionada. La freqüència de les còpies de seguretat vindrà donada pel nivell de sensibilitat de les dades que conté, segons el recollit a les guies de BIT.

El nivell de seguretat d'aquestes dades ha de ser un reflex del de les dades originals a tots els nivells (integritat, confidencialitat, autenticitat y traçabilitat). Per tal de garantir la confidencialitat, BIT es reserva el dret de demanar el xifrat de les dades. L'abast de les còpies inclou:

Informació de treball de BIT.

- Aplicacions en explotació, incloent els sistemes operatius.
- Dades de configuració, serveis, aplicacions, equips o d'altres anàlegs.
- Claus emprades per conservar la confidencialitat de la informació.

Inventari d'actius

L'empresa adjudicatària haurà de mantenir un inventari actualitzat de tots els elements del sistema, detallant la seva naturalesa i identificant al seu responsable; és a dir, la persona que és responsable de les decisions relatives al mateix.

Configuració de seguretat

L'empresa adjudicatària haurà de configurar els equips prèviament a la seva entrada en operació, de manera que:

- Es retirin comptes i contrasenyes estàndard.
- S'aplicarà la regla de "mínima funcionalitat":
    - El sistema ha de proporcionar la funcionalitat requerida perquè l'organització aconsegueixi els seus objectius i cap altra funcionalitat.
    - No proporcionarà funcions gratuïtes, ni d'operació, ni d'administració, ni d'auditoria, reduint d'aquesta forma el seu perímetre al mínim imprescindible.
    - S'eliminarà o desactivarà mitjançant el control de la configuració, aquelles funcions que no siguin d'interès, no siguin necessàries, i fins i tot, aquelles que siguin inadequades al fi que es persegueix.
- S'aplicarà la regla de "seguretat per defecte":
    - Les mesures de seguretat seran respectuoses amb la persona usuària i protegiran a aquest, tret que s'exposi conscientment a un risc.
    - Per reduir la seguretat, la persona usuària ha de realitzar accions conscients.
    - L'ús natural, en els casos que la persona usuària no ha consultat el manual, serà un ús segur.

Manteniment

L'empresa adjudicatària haurà de mantenir l'equipament físic i lògic que constitueix el sistema i/o infraestructura administrada.

L'empresa adjudicatària haurà de mantenir actualitzats els productes utilitzats en l'abast del plec d'acord a la política acordada amb BIT.

La política d'actualitzacions està basada en el nivell de criticitat de la vulnerabilitat valorada segons l'última versió publicada de l'estàndard públic CVSS (Common Vulnerability Scoring System), segons el nivell de CVSS les actualitzacions per la correcció de vulnerabilitats s'hauran de produir dins d'uns terminis específics (en funció del nivell d'exposició, la criticitat de la vulnerabilitat i la criticitat de l'actiu afectat), detallats en la taula següent:

		Nivell d'exposició			
		Exposat a internet		No exposat a internet	
		Criticitat de l'actiu		**Criticitat de l'actiu**	
		Crític	No crític	Crític	No crític
Criticitat vulnerabilitat	CVSS <=3	20 dies	40 dies	40 dies	40 dies
	3 < CVSS <= 6	5 dies	1 mes	20 dies	20 dies
	6 < CVSS <=8	1 dia	5 dies	5 dies	5 dies
	CVSS > 8	1 dia	2 dies	1 dia	5 dies

El proveïdor s'haurà d'involucrar en tot el cicle de vida de les vulnerabilitats, des de la seva detecció fins a la mitigació d'aquesta. Haurà de tenir un seguiment proactiu de les vulnerabilitats que es puguin produir amb un seguiment continu del anunci de defectes, mantenint el contacte amb els fabricants per tenir coneixement de les possibles solucions que aquest proposin per corregir-les.

Antimalware

L'empresa adjudicatària serà responsable de la instal·lació i actualització de programes de protecció antimalware de les màquines que suporten serveis de BIT segons es recull al marc normatiu de BIT.

BIT obtindrà indicadors de la bona gestió de proteccions antimalware i en qualsevol moment tindrà accés i visió de l'estat de la seguretat global de les proteccions.

La Direcció de Seguretat de la Informació de BIT tindrà accés en consulta a la consola de gestió d'aquests programaris del proveïdor.

Control d'accés

Segregació de funcions i tasques

L'empresa adjudicatària s'encarregarà de que el sistema de control d'accés s'organitzi 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.

En concret, se separaran almenys les següents funcions:

- Desenvolupament d'operació. Garantint, com a mínim, que els desenvolupadors únicament disposin d'accés a l'entorn de preproducció i desenvolupament. La configuració dels entorns productius l'haurà de realitzar persones o equips diferents.

- Configuració i manteniment del sistema d'operació.
- Auditoria o supervisió de qualsevol altra funció.

Explotació

Gestió de la configuració

L'empresa adjudicatària s'encarregarà de gestionar de forma continua la configuració dels components del sistema de manera que:

- Es mantingui a tot moment la regla de "funcionalitat mínima".
- Es mantingui a tot moment la regla de "seguretat per defecte".
- El sistema s'adapti a les noves necessitats, prèviament autoritzades.
- El sistema reaccioni a vulnerabilitats reportades.
- El sistema reaccioni a incidents.

Gestió de canvis

L'empresa adjudicatària s'encarregarà de mantenir un control continu de canvis realitzats en el sistema, de manera que:

- Tots els canvis anunciats pel fabricant o proveïdor seran analitzats per determinar la seva conveniència per ser incorporats, o no.
- Abans de posar en producció una nova versió o una versió amb un pegat, es comprovarà en un equip que no estigui en producció, que la nova instal·lació funciona correctament i no disminueix l'eficàcia de les funcions necessàries per al treball diari. L'equip de proves serà equivalent al de producció en els aspectes que es comproven.
- Els canvis es planificaran per reduir l'impacte sobre la prestació dels serveis afectats.
- Mitjançant anàlisi de riscos es determinarà si els canvis són rellevants per a la seguretat del sistema. Aquells canvis que impliquin una situació de risc de nivell alt seran aprovats explícitament de forma prèvia a la seva implantació.

Protecció de claus criptogràfiques

- L'empresa adjudicatària utilitzarà programes avaluats o dispositius criptogràfics certificats.
- S'empraran algoritmes acreditats pel "Centre Criptològic Nacional".

Protecció dels serveis

Protecció enfront de la denegació de servei

L'empresa adjudicatària establirà mesures preventives i reactives enfront d'atacs de denegació de servei (DoS Denial of Service). Per tal de garantir-ho:

- Es planificarà i dotarà al sistema de capacitat suficient per atendre a la càrrega prevista sense posar en risc la disponibilitat del sistema.
- Es desplegaran tecnologies per prevenir els atacs coneguts.

9.2. Clàusules generals de seguretat

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

BIT 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.

BIT, 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 del 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 dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades) i la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, així com de la resta de l'ordenament jurídic que sigui d'aplicació.

Pel 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 qual es regula l'Esquema Nacional de Seguretat.

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

A les diferents clàusules d'aquesta secció es fa referència a Ajuntament de Barcelona, Administració Municipal i BIT indistintament. De conformitat amb els seus estatuts s'ha d'entendre que BIT 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.

Conformitat amb l'Esquema Nacional de Seguretat

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 qual es regula l'Esquema Nacional de Seguretat (en endavant ENS).

Donada la naturalesa del contracte, l'empresa adjudicatària 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'empresa adjudicatària haurà d'acreditar la conformitat amb l'ENS mitjançant alguna de les vies previstes a l'art. 38 de l'ENS, entre les que es troben les següents opcions:

- Certificació oficial d'una entitat de certificació acreditada.
- Informe d'auditoria de compliment. L'empresa adjudicatària 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'empresa adjudicatària garantirà l'accés per part de BIT 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'empresa adjudicatària dins de l'abast dels servis subcontractats. És responsabilitat de l'empresa adjudicatària 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.

Responsable de Seguretat

L'empresa adjudicatària 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 BIT 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 BIT.
- Assegurar que tot el personal de l'empresa adjudicatària 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.

Delegat de Protecció de Dades

Si l'empresa adjudicatària ha anomenat un delegat de protecció de dades, procedirà a comunicar les seves dades de contacte a l'Oficina del Delegat de Protecció de Dades de l'Ajuntament perquè es puguin establir els circuits de comunicació establerts en el Reglament General de Protecció de Dades. En cas de no haver definit aquesta figura, s'haurà de proporcionar el contacte de la persona encarregada del tractament de dades personals.

Clàusula programari i metodologia de desenvolupament

L'empresa adjudicatària, disposarà del programari necessari i farà servir la metodologia implantada per Barcelona Innovació i Tecnologia (BIT) per al desenvolupament dels serveis contractats.

Si l'Administració Municipal ho considera necessari, es podrà instal·lar programari en els equips de l'empresa adjudicatària, sempre sota la responsabilitat de l'empresa adjudicatària, amb la finalitat d'obtenir una correcta prestació dels serveis contractats. Les llicències de software necessàries per desenvolupar el servei correran a càrrec de l'empresa adjudicatària.

L'Administració Municipal continuarà essent la propietària o, en el seu cas, titular dels drets de propietat intel·lectual que el corresponen sobre el programari i bases de dades instal·lat en les màquines de l'empresa adjudicatària, sense que la corresponent llicència d'ús suposi transferència o cessió, total o parcial de la titularitat, ni autorització per la seva utilització amb una finalitat diferent a la definida en el contracte de prestació de serveis.

L'empresa adjudicatària donarà a conèixer a tot el personal adscrit a la prestació dels serveis, el contingut d'aquesta clàusula respecte al programari, sistemes operatius i bases de dades cedides per l'Administració Municipal, la seva obligació respecte a:

- No reproduir-los.
- No transmetre'ls a un altre sistema.
- No modificar, adaptar, cedir, ni realitzar qualsevol altre activitat sobre el programari cedit, sense l'autorització de l'Administració Municipal.
- No divulgar, publicar, ni posar a disposició d'altres persones diferents a les autoritzades.
- Fer ús única i exclusivament per les tasques encomanades, incloses en els serveis contractats.

9.3. Clàusules generals de seguretat en el desenvolupament

Desenvolupament segur

L'empresa adjudicatària es compromet a adequar les seves polítiques i procediments de desenvolupament de programari de tal forma que el seu cicle de desenvolupament de software garanteixi la seguretat en els productes desenvolupats al llarg de tot el cicle de vida, incloent normes de programació segura.

Els següents elements seran part integral del disseny del sistema:

- Els mecanismes d'identificació i autenticació.
- Els mecanismes de protecció de la informació.
- La generació i tractament de pistes d'auditoria.

El prestador està obligat a realitzar una revisió del codi font per a tots els desenvolupaments que siguin lliurats, ja sigui per al desenvolupament d'un aplicatiu, manteniment del mateix o desenvolupaments correctius, amb l'objecte de verificar si existeix alguna vulnerabilitat o amenaça en el desenvolupament realitzat, i si s'escau, procedir a la reparació de la mateixa.

BIT en qualsevol moment podrà realitzar una revisió del codi font. Si es detectés algun tipus de vulnerabilitat es comunicarà a l'empresa adjudicatària per tal que procedeixi a arreglar les mancances detectades.

Per a millorar el procés de desenvolupament segur d'aplicacions, l'empresa adjudicatària haurà de realitzar accions addicionals per a garantir la qualitat i seguretat del producte final. Aquestes accions són:

- Emprar una eina d'anàlisi de codi estàtic (SAST) per trobar vulnerabilitats de seguretat al codi font i garantir els bons estàndards de codificació. La periodicitat dels anàlisis hauran de ser acordats conjuntament amb el responsable del contracte. El software emprat al BIT correspon a l'eina SonarQube amb la modalitat OWASP, sent aquesta la tecnologia desitjable a emprar per l'empresa adjudicatària.

Per al cas particular d'aplicacions conteneritzades, l'empresa adjudicatària haurà de fer ús d'un software d'anàlisis d'imatges Docker. La tecnologia emprada al BIT i la preferent d'ús per part de l'empresa adjudicatària és Coreos Clair.

En cas de emprar softwares diferents als plantejats anteriorment, hauran de ser comunicats i justificats degudament al responsable del contracte.

Acceptació i posta en servei

Abans de passar a producció l'empresa adjudicatària comprovarà el correcte funcionament de l'aplicació es comprovarà que:

- Es compleixen els criteris d'acceptació en la matèria de seguretat.
- No es deteriora la seguretat d'altres components del servei.
- Addicionalment, l'empresa adjudicatària realitzarà les següents inspeccions prèvies a l'entrada en servei:
    - Anàlisis de vulnerabilitats.
    - Test de penetració.

Protecció de les aplicacions i serveis web

L'empresa adjudicatària garantirà que els subsistemes dedicats a la publicació de la informació hauran de ser protegits front a les amenaces que li siguin pròpies:

- Quan la informació tingui algun tipus de control d'accés, es garantirà la impossibilitat d'accedir a la informació obviant l'autenticació, en concret prenent mesures en els següents aspectes:
    - S'evitarà que el servidor ofereixi accés a documents per vies alternatives al protocol determinat.
    - Es previndran atacs de manipulació de URL.
    - Es previndran atacs de manipulació de fragments de la informació que s'emmagatzemin en el disc dur del visitant d'una pagina web a traves del seu navegador, a petició del servidor de la pagina, conegut en la terminologia anglesa com a "cookies".
    - Es previndran atacs d'injecció de codi.
- Es previndran intents d'escalat de privilegis.
- Es previndran atacs de "cross site scripting".
- Es faran servir certificats d'autentificació de llocs web d'acord amb les polítiques establertes per BIT-Seguretat.

Dades de proves

L'empresa adjudicatària es compromet a assumir tota la responsabilitat en la creació de dades de proves per testejar els serveis. En cap cas s'utilitzaran dades de l'entorn de producció per fer proves.

En cas que sigui necessari copiar dades de l'entorn productiu, aquestes seran les mínimes necessàries i hauran de ser sotmeses a un procés d'ofuscació. L'empresa adjudicatària es farà càrrec del desenvolupament dels procediments de tractament de dades (ofuscació, truncament, etc.) en cas que fossin necessaris.

Tota manipulació de dades de l'entorn de producció haurà de ser informada i aprovada pel propietari de les mateixes.

En cas que s'hagi de realitzar una migració de dades entre sistemes, l'empresa adjudicatària haurà de presentar un pla de migració de les dades on es detallin les operacions necessàries.

Aquest pla de migració s'adequarà al procediment establert per seguretat per tal de minimitzar l'exposició de les dades productives.

Signatura electrònica

Qualsevol requeriment de signatures digitals que s'hagin de produir referents amb la informació municipal o corporativa, el proveïdor haurà de presentar-les per ser valides per BIT-Seguretat i/o seguir els estàndards i normes de BIT.

Per la signatura electrònica s'empraran els mecanismes aprovats per BIT, en cas que hagin de ser uns altres, s'haurà de justificar, documentar tècnicament i haurà d'estar validat per BIT-Seguretat. En tot cas s'ha de complir la política de signatura electrònica de l'Ajuntament de Barcelona.

Pla de traces

Les aplicacions o productes que permeten realitzar operacions sobre les dades de negoci han de proporcionar informació sobre les accions i accessos realitzats en aquesta informació. Tant la criticitat de les dades i els criteris del negoci, com els requeriments legals marcaran la informació que cal recollir i el temps de retenció dels logs.

L'empresa adjudicatària haurà de dissenyar les traces necessàries en base al Document del 'Pla de Seguretat i Traces' que posarà a disposició BIT a l'inici del contracte.

Un cop dissenyades les traces s'haurà d'incorporar aquest disseny en els documents estàndards de seguretat: 'Pla mestre de Traces' (on s'avaluen els requeriments de les traces, el disseny i es determina l'inventari de traces necessàries) en la fase d'anàlisi i el document 'Pla de Traces' (on s'aporten detalls i mostres de cadascuna de les traces) en fase de proves i/o pas a producció.

BIT es reserva el dret de poder demanar en qualsevol moment del contracte la integrabilitat amb els sistemes corporatius destinats a la monitorització de traces, on actualment es contempla el sistema SIEM QRadar i/o ELK.

Informe de seguretat

El proveïdor elaborarà a petició de seguretat un informe on es detallaran tots els aspectes rellevants sobre Seguretat del seu contracte.

L'estructura d'aquest informe incloent la informació requerida es lliurarà al proveïdor durant les primeres etapes del contracte.

El document original ha estat signat electrònicament per:
Yolanda Agra Rustarazo el dia 13/10/2026 a les 11:08, que informa;
Pilar Roca Viola el dia 13/10/2026 a les 16:24, que dóna conformitat..