



Reglament per a l'ús i governança de la intel·ligència artificial (IA) a l'Ajuntament d'Olot

Títol: Reglament per a l'ús i governança de la intel·ligència artificial (IA) a l'Ajuntament d'Olot.

Òrgan d'aprovació: Ple de l'Ajuntament d'Olot.

Data d'aprovació: 19 de març de 2026.

Publicació oficial: Portal de transparència.

1. Introducció

En el context actual, en què la introducció de noves tecnologies està transformant la societat a tots els nivells, les Administracions Públiques —i especialment les entitats locals— estan vivint un procés de canvi continu, profund i estructural que proporcionen oportunitats per millorar l'eficiència, agilitzar processos i oferir serveis més personalitzats, facilitant noves tipologies de relació de l'Administració amb la ciutadania. En aquest sentit, s'ha produït la progressiva inclusió en les agendes tradicionals de gestió pública de múltiples reptes en diverses matèries d'acord amb l'impacte de la revolució digital en la forma en què les persones viuen, treballen i interactuen.

Aquesta nova realitat digital condueix a una reflexió necessària des del sector públic, que inclou l'impacte que tindrà, en efecte, la intel·ligència artificial (IA) en la gestió pública pel que fa a extrems com ara els usos que podrà tenir —i que té ara ja— aquesta tecnologia en l'Administració Pública, qui s'ha d'ocupar de la seva gestió, i de quina manera s'ha de gestionar la seva utilització. A aquests efectes, és essencial per a l'Administració dissenyar un full de ruta clar a efectes de començar a integrar de forma ordenada la IA en la gestió pública com una eina de millora clau en la consecució dels objectius de l'administració, entre els quals es pretén, precisament, la simplificació administrativa i la reducció de càrregues.

A aquest respecte, l'ús de les tecnologies basades en sistemes algorísmics i intel·ligència artificial ofereix l'oportunitat per a l'Ajuntament de transformar els serveis municipals perquè siguin més eficients, proactius i adaptats a les necessitats de la ciutadania, així com també per agilitzar els processos interns i donar suport a la presa de decisions. Així, la introducció de la IA presenta la possibilitat de fer un salt qualitatiu en la gestió dels serveis públics, contribuint en la seva transformació i impactant directament en el seu funcionament i la prestació de serveis.

Essent precisament la gestió basada purament en dades —i que aquestes dades siguin de qualitat— un dels reptes encara pendents de la *transformació digital* pautaada per la Llei 39/2015, d'1 d'octubre, de Procediment Administratiu Comú de les Administracions Públiques i a la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic (així com al seu desenvolupament per Reial decret 203/2021, de 30 de març, pel qual s'aprova el Reglament d'actuació i funcionament del sector públic per mitjans electrònics), és essencial donar prioritat a l'abordament d'aquesta qüestió amb totes les garanties; sobretot pel que respecta a la introducció de sistemes algorísmics basats en IA, tenint en compte que el desplegament d'aquest tipus de sistemes comporta múltiples riscos.

A tot això, és imprescindible tenir sempre present que no es pot abordar la IA sense plantejar qüestions fonamentals sobre la seva aplicació responsable, l'ètica o la transparència, i sempre des d'un punt de partida basat en els potencials riscos, tal com els classifica el Reglament d'Intel·ligència Artificial europeu¹ (en endavant, RIA). Per aquesta raó esdevé imperatiu assegurar que la seva implementació introdueix mecanismes de salvaguarda i garantia dels drets fonamentals; que es duu a terme de manera proporcionada, supervisada i fonamentada d'acord amb la legislació vigent i els estàndards ètics i tècnics adequats; i, finalment, que el procés afavoreix la participació i deliberació constants amb la ciutadania i les comunitats impactades.

Per tot l'anterior, l'objectiu de la governança intel·ligent ha de ser que totes les Administracions públiques puguin servir els ciutadans d'una manera més ràpida i precisa, a partir d'un model de gestió pública que permeti millorar les seves actuacions i establir nous canals de relació amb la ciutadania i les empreses i facilitar la tramitació de procediments; tot això a partir de l'ús de dades i a través d'algorismes que facilitin tant la presa de decisions públiques com l'avaluació de l'efectivitat de les normes i de l'eficàcia de les polítiques públiques, així com la prestació dels serveis públics. I, en aquest sentit, es fa palesa la necessitat d'establir les bases per a una política institucional d'implementació i ús responsable de serveis d'Intel·ligència Artificial (IA) i d'Intel·ligència Artificial Generativa (IAG) en els processos administratius, plasmats en un instrument que actuï com a marc dels principis i garanties per a l'ús de la IA a l'Ajuntament d'Olot de forma transparent, ètica, sostenible, responsable i respectuosa amb els drets humans, la igualtat la privacitat i la no discriminació, i que permeti enumerar i classificar els riscos i les oportunitats que presenten aquestes eines en l'àmbit de la gestió pública.

Aquesta política complementa la normativa interna d'aquest Ajuntament per orientar la institució cap a una organització *'data driven'* a efectes de d'augmentar l'eficiència en la gestió i la millora dels serveis públics a partir d'una presa de decisió basada en dades de qualitat, elaborant-se en un moment en què l'Ajuntament d'Olot es troba

en ple procés de definició de la seva estratègia institucional en matèria d'intel·ligència artificial. Així les coses, el contingut d'aquesta política ha de considerar-se un marc inicial flexible i revisable, susceptible d'actualització per a adaptar-se a les evolucions i concrecions d'aquesta estratègia.

2. Aspectes generals

2.1. Objecte

Aquesta política general té per objecte assegurar un ús ètic, segur, transparent i responsable de la intel·ligència artificial en els serveis i processos de l'Ajuntament d'Olot. Per aquest motiu ha d'alinejar-se amb els drets fonamentals, els principis de transparència, seguretat i bon govern, i basar-se en la confiança ciutadana en la implementació d'aquesta tecnologia; prenent en consideració la necessitat d'adoptar les garanties adequades quant al tractament de dades —personals, no personals, o una combinació d'ambdues—, i amb un enfocament global i conforme a dret en el seu ús, tenint en compte l'impacte sobre els drets fonamentals en el disseny, desenvolupament i desplegament dels sistemes i models d'IA.

2.2. Àmbit d'aplicació

Aquesta política serà aplicable a totes les activitats, funcions i processos que dugui a terme l'Ajuntament d'Olot en què es faci ús de sistemes basats en IA, bé siguin desenvolupats per l'Ajuntament o bé siguin contractats a través de tercers.

Aquesta política és d'obligat compliment per a:

- Els òrgans, serveis i unitats que integren l'Ajuntament, incloent-hi totes les seves àrees i departaments
- Els organismes públics i entitats de dret públic vinculats o dependents de l'Ajuntament, que facin ús de sistemes d'intel·ligència artificial en l'exercici de les seves funcions
- Les entitats privades, contractistes, proveïdors i persones físiques o jurídiques que desenvolupin, implantin, gestionin i prestin serveis relacionats amb sistemes d'IA per l'Ajuntament o per als seus organismes dependents.

Aquesta política serà revisada i actualitzada periòdicament d'acord amb l'evolució i concreció dels sistemes d'IA.

2.3. Principis generals

Els sistemes d'IA que siguin utilitzats en l'àmbit municipal hauran de seguir els següents principis generals:

Seguretat i protecció de dades	Els sistemes d'IA utilitzats han de ser fiables, resistents a fallades i segurs davant ciber-amenaces. Per altra banda, les dades han de ser de qualitat, legals i protegides segons RGPD i altres normatives.
Principi de traçabilitat	L'Ajuntament ha de vetllar per a la incorporació dels mecanismes de seguretat que permetin la traçabilitat i l'eventual auditoria de les accions dutes a terme pel personal de la institució i de tercers en l'ús dels sistemes i serveis digitals.
Principi de confiança	L'Ajuntament ha de garantir que l'ús d'aquests sistemes i la prestació de serveis digitals assegurin la identitat, integritat, conservació i, si escau, la confidencialitat de la informació i les transaccions que es duguin a terme mitjançant mitjans electrònics, especialment en relació amb la protecció de dades personals.
Principi d'igualtat i legalitat i no discriminació	La IA ha d'evitar biaixos i garantir un tracte just i inclusiu per a tothom. Els sistemes han de garantir els principis de no discriminació, igualtat d'oportunitats i equitat, evitant biaixos algorísmics que puguin generar desigualtats. A més, han de garantir el compliment de la legislació vigent, especialment en matèria de protecció de dades, drets fonamentals i contractació pública.
Principi d'usabilitat,	Les eines i dispositius que s'emprin per a la comunicació per mitjans electrònics, així com la prestació de serveis públics digitals han d'estar

accessibilitat, no discriminació i reducció de la bretxa digital	focalitzades en les persones usuàries de manera que resultin intuïtius per a aquestes, minimitzant així el grau de coneixement necessari per a l'ús del servei, amb especial atenció a la reducció de la bretxa digital prestant consideració a les persones grans, amb dificultats d'accés als mitjans electrònics o amb discapacitats.
Principi de transparència	L'Ajuntament ha de garantir que els sistemes d'IA siguin explicables i comprensibles per a la ciutadania, permetent saber quan s'interactua amb la IA i assegurant l'accés a informació clara sobre el seu funcionament, criteris de decisió i fonts de dades utilitzades, així com la finalitat de l'ús de les dades.
Principi de responsabilitat	L'Ajuntament ha de vetllar perquè l'ús dels sistemes d'IA impliqui una rendició de comptes clara sobre les decisions automatitzades, establint mecanismes per a la supervisió i revisió de possibles errors i assegurant una capacitat de demostrar, i justificar l'ús i els resultats de la IA. Així mateix, cal definir clarament qui assumeix el control i les conseqüències del sistema, i la possibilitat de presentació de reclamacions per part de la ciutadania.
Principi d'explicabilitat i supervisió humana	Els sistemes d'IA han de permetre comprendre com es prenen les decisions automatitzades, facilitant la interpretació dels resultats i garantint la intervenció humana quan sigui necessari per evitar errors o decisions no justificades.
Solidaritat, autonomia, i benestar social i mediambiental	Els sistemes d'IA s'han de desenvolupar respectant l'autonomia de les persones per a que disposin d'un major control sobre la seva vida i allò que les envolta, preservant-se els vincles entre les persones i sense substituir-les en aquelles tasques que requereixin relacions humanes de qualitat. L'ús de la IA també ha de beneficiar la societat i reduir l'impacte ambiental.

Els principis d'aquesta política s'alineen amb els principis recollits en el RIA i en la normativa de protecció de dades, que en conjunt constitueixen el marc de referència ètic i jurídic per al desenvolupament i ús responsable dels sistemes d'IA.

3. Usos admesos, prohibicions i casos d'ús.

3.1. Usos admesos

L'Ajuntament només implementarà i/o utilitzarà sistemes d'intel·ligència artificial (IA) que s'ajustin a la normativa vigent (inclosa aquesta política) i que, de forma efectiva, contribueixin a la millora de la prestació dels serveis públics.

Aspectes a tenir en compte:

1. En qualsevol cas, serà obligatori motivar la necessitat d'implantar el sistema i definir prèviament els mecanismes de seguiment que permetin valorar el seu funcionament i la millora que aporta al servei.
2. La responsabilitat de l'ús dels resultats generats pel sistema correspon a la persona usuària designada, que té l'obligació de supervisar-los i validar-los abans de la seva aplicació.
3. Els sistemes d'IA es podran utilitzar, de manera justificada i prèviament autoritzada, exclusivament per a funcions de suport o assistència en la prestació de serveis públics (actuacions assistides). L'ús de l'IA als dispositius de la Corporació s'ha de limitar a finalitats de l'activitat professional. Està prohibit l'ús d'eines IA en dispositius personals o comptes personals per realitzar activitats relacionades amb l'Ajuntament.

Els usos admesos inclouen però no es limiten a:

- a) Suport a processos administratius

- Generació automatitzada de documents esborranys (informes, actes, certificats, etc.) que després són validats per una persona funcionària.
 - Classificació, indexació i arxiu de documents administratius, incloent correu electrònic, registres i expedients.
 - Traducció automàtica assistida per facilitar la redacció en diferents llengües oficials.
- b) Anàlisi i explotació de dades
- Identificació de patrons, anomalies o riscos a partir de conjunts de dades (per exemple, en serveis socials, inspecció o manteniment).
 - Elaboració de prediccions o escenaris per a la planificació de serveis públics (per exemple, ocupació d'aparcaments, demanda de serveis, etc.).
 - Generació de dashboards o quadres de comandament per monitorar indicadors clau (KPIs) de l'activitat municipal.
- c) Comunicació i atenció a la ciutadania
- Assistents virtuals o xatbots informatius que donin suport a preguntes freqüents o guiïn tràmits sense emetre resolucions.
 - Recomanadors personalitzats d'informació o tràmits basats en el perfil de l'usuari, sempre sense efectes jurídics.
- d) Gestió interna i suport operatiu
- Planificació automatitzada de torns o tasques, sota supervisió humana.
 - Extracció automatitzada d'informació rellevant de documents.
- e) Detecció i correcció d'errors habituals en formularis.
- f) Millora de l'accessibilitat
- Conversió de text a veu o veu a text per facilitar l'accés als continguts a persones amb discapacitat.
 - Resums automàtics o simplificació de textos administratius per fomentar el llenguatge planer i la comprensió general.
- g) Suport a la presa de decisions
- Sistemes de suport a la decisió que aportin informació addicional o valoracions estadístiques per facilitar la valoració tècnica d'expedients (sense substituir-la).
 - Modelatge de simulacions per a l'avaluació d'escenaris (per exemple, en urbanisme o planificació estratègica).

Atès que aquesta relació no inclou tots els casos d'ús possibles, si un cas d'ús no figura específicament a la llista, l'usuari haurà de sol·licitar autorització mitjançant el formulari habilitat a l'efecte (annex 3).

3.2. Prohibicions

D'altra banda, queda terminantment prohibit l'ús de sistemes d'IA que incorporessin alguna de les pràctiques següents, tal com estableix l'article 5 del Reglament (UE) 2024/1689:

- Manipulació subliminal o enganyosa: Prohibida la utilització de tècniques subliminals o manipulatives que alterin significativament el comportament de les persones i afectin negativament la seva capacitat per prendre decisions informades.
- Explotació de vulnerabilitats: No es permet l'ús de sistemes que aprofitin situacions de vulnerabilitat —per raó d'edat, discapacitat o condició socioeconòmica— per influir en el comportament de les persones i generar-les perjudicis.
- Sistema de puntuació social (social scoring): Queda prohibit classificar persones o col·lectius segons el seu comportament social o trets personals, especialment si comporta un tracte discriminatori, desproporcionat o perjudicial.
- Predicció de delictes basada en perfils: No es poden utilitzar sistemes d'IA per predir la probabilitat que una persona cometi un delictes només a partir de perfils o característiques personals, sense evidències objectives.
- Extracció indiscriminada d'imatges per reconeixement facial: Prohibida la creació de bases de dades biomètriques a partir de la recollida massiva d'imatges facials d'internet o de sistemes de videovigilància.
- Inferència d'emocions en entorns laborals o educatius: No es pot fer servir IA per detectar emocions en escoles o llocs de treball, excepte en casos degudament justificats per raons mèdiques o de seguretat.
- Categorització biomètrica sensible: Prohibida la classificació de persones mitjançant dades biomètriques per inferir trets sensibles com la raça, creences religioses, afiliació política o orientació sexual.

- Identificació biomètrica remota en temps real en espais públics: Només es permet l'ús d'aquests sistemes amb finalitats de seguretat pública en supòsits molt concrets i degudament regulats (com la recerca de persones desaparegudes o la prevenció de delictes greus), i sempre amb les garanties legals corresponents.

A més, no es permetrà l'ús de sistemes d'IA que automatitzin la presa de decisions amb efectes directes sobre procediments administratius o ciutadans sense supervisió humana.

3.3. Casos d'ús

A continuació s'identifiquen escenaris on la implementació d'un o més sistemes d'IA o IAG poden aportar valor i eficiència en els processos administratius (casos d'ús). Cadascun requereix analitzar l'impacte d'aquests sistemes en tot el procés, tant si tracten dades personals com si no, així com la interacció amb sistemes no basats en IA o IAG (sistemes de recollida, processament, transmissió, i emmagatzematge de dades, i fins i tot ajuda en la presa de decisions), els recursos humans i materials i els procediments organitzatius de tals processos. Aquests casos d'ús i similars poden presentar un risc o impacte significativament menor quan no incorporen informació amb dades personals, informació sensible o confidencial.

CASOS D'ÚS	DESCRIPCIÓ
<i>Estructuració, gestió o resum de documents generals i oberts (documents públics)</i>	Aplicació de models intel·ligents per resumir, extreure informació clau i transformar documents de caràcter públic o no confidencial en formats estructurats que facilitin el seu anàlisi o reutilització. Poden generar-se versions de classificació o anàlisis automatitzat amb fins d'estudi o divulgació, garantint en tot cas l'anonimat i l'exclusió de dades personals.
<i>Traducció de documents públics</i>	Facilitar la traducció de documents públics en diferents idiomes. Permet traduir documents redactats en llengües estrangeres (per exemple, resolucions d'autoritats europees) a l'espanyol i al català o viceversa, adaptant l'estil de la traducció segons el públic objectiu.
<i>Generació de contingut de comunicació institucional</i>	Assistència integral en la producció i revisió de materials de comunicació institucional
<i>Generació d'esquemes, mapes conceptuals i infografies per la comunicació</i>	Creació d'esquemes, mapes conceptuals i infografies explicatives elaborades a partir d'informació pública o de fonts obertes, per fer suport al a comprensió i difusió de continguts.
<i>Generació material i continguts multimèdia interactiu i de comunicació</i>	Desenvolupament de contingut multimèdia interactiu destinat a l'educació i divulgació ciutadana, així com composició automàtica de música o so ambiental per acompanyar vídeos o actes públics institucionals o promocionals.
<i>Generació d'àudios o vídeos a partir de continguts i documentació oberta</i>	Generació de locucions o vídeos sintètics, obtingudes exclusivament a partir de documentació pública o no confidencial i sense dades personals, aplicables a audio-guides, serveis telefònics o materials accessibles.
<i>Elaboració de continguts divulgatius o formatius</i>	Suport en la creació de materials de sensibilització i formació interna o externa sobre protecció de dades, accessibles i adaptats a diferents perfils.
<i>Identificació de tendències o patrons a partir de fonts obertes</i>	Identificació de tendències o patrons mitjançant l'anàlisi automatitzat d'informació oberta per al suport a la presa de decisions.
<i>Elaboració de gràfiques, taules i informes a partir d'informació d'accés públic o no confidencial</i>	Elaboració automàtica de gràfiques, taules i informes financers o pressupostaris basats en dades d'accés públic o no confidencials, garantint l'exclusió d'informació personal o sensible.

<i>Assistència en l'aproximació i preparació general d'arguments, estudis jurídics i tècnics</i> + <i>Assistència en la redacció inicial d'elements generals i aïllats, les idees dels quals després podran incorporar-se a resolucions, informes o guies tècniques.</i>	Utilització de sistemes IAG per a l'anàlisi i contrast de fonts jurídiques, doctrinals o tècniques de caràcter públic o no confidencial, amb el fi d'elaborar marcs argumentals, estudis comparats, notes tècniques o hipòtesis interpretatives. Aquestes eines recolzen la preparació d'estratègies o enfocaments jurídics sense substituir la valoració professional ni implicar la presa de decisions automatitzades. Així mateix, poden utilitzar-se per l'anàlisi exploratòria i sistemàtica de fonts jurídiques obertes, la comparació de marcs normatius doctrinals i l'elaboració d'estudis generals que no involucrin informació confidencial ni dades personals.
<i>Assistència en tasques de desenvolupament i configuració de sistemes</i>	Realització de tasques tècniques (<i>scripting</i>, generació de consultes SQL, construcció d'expressions regulars i resolució de dubtes sobre software específic), per facilitar que els usuaris s'enfoquin en la revisió i ajustament del contingut; essent especialment útil en entorns en què s'utilitzen múltiples tecnologies i configuracions avançades de sistemes
<i>Assistència interna normativa o doctrinal</i>	Desenvolupament d'assistents virtuals interns que facilitin la consulta ràpida de legislació, resolucions, informes jurídics, criteris interpretatius de l'Ajuntament d'Olot etc., millorant l'accés al coneixement organitzatiu. Poden servir de suport per a la inspecció en relació a les diverses fases de tramitació e sol·licituds d'aprovació de codis de conducta i els de sol·licituds d'acords de transferències internacionals, o per l'elaboració de resums anonimitzats pel suport a la divulgació de continguts, entre d'altres.
<i>Transcripció d'àudio i vídeo procedent de fonts obertes sense informació confidencial</i>	Transcripció de continguts multimèdia de fonts obertes o no confidencials per a la seva incorporació a diversos fluxos de treball o estudis. Podria contenir dades personals.
<i>Transcripció d'àudio i vídeo que contingui informació interna, privada o confidencial, en els eu cas de reunions i suport a la generació d'actes</i>	Transcripció de reunions internes, en el seu cas per fer suport a la generació d'actes. Així com d'arxius d'àudio particulars d'entrevistes concedides o intervencions realitzades pel personal de l'Ajuntament d'Olot en actes o esdeveniment, i elaboració del resum de text resultant.
<i>Estructuració, gestió o resums de documents administratius interns o amb dades personals.</i>	Aplicació de models intel·ligents per resumir, extreure informació clau i convertir documents administratius interns en estructures normalitzades que millorin la seva tramitació o anàlisi automatitzat. En aquests casos, ha d'aplicar-se una anonimització completa o parcial de les dades personals i limitar el tractament a entorns segurs i autoritzats, per exemple, per elaborar versions anonimitzades destinades a consultes de transparència o informes interns.
<i>Redacció d'esborranys, cartes, correus o notes internes amb to institucional</i>	Utilització de sistemes intel·ligents per elaborar propostes inicials de resposta a la ciutadania o organismes, o escrits agilitzant temps de tramitació i garantint coherència en els missatges institucionals.
<i>Generació d'esborranys de resposta a consultes per a canals d'atenció al ciutadà, canal DPD i jove</i>	La utilització de RAGs i sistemes ben afinats permetran accedir a informació actualitzada en temps real sobre tot el material produït per l'Ajuntament d'Olot per produir esborranys de respostes a consultes específiques dels canals d'atenció al ciutadà, etc.
<i>Classificació d'instàncies i altres entrades</i>	Aplicació de models de processament de llenguatge natural (PLN) per facilitar el tractament inicial de la informació que

	arriba a l'Ajuntament d'Olot permetent la seva categorització, indexació i anàlisi preliminar.
<i>Suport en l'anàlisi d'EIPD (valuació d'impacte en Protecció de Dades)</i>	Utilització de models experts per realitzar un primer triatge o suport documental en els informes d'avaluació d'impacte, proporcionant plantilles, criteris comuns o guies d'anàlisi.
Gestió pública basada en dades	Les dades esdevenen un recurs fonamental per a la millora de la política i la gestió pública. L'aplicació de sistemes d'intel·ligència artificial en la gestió pública permeten impulsar processos més eficients i transparents, facilitant la presa de decisions basada en evidències i l'optimització contínua dels recursos. Així, es poden identificar tendències i patrons en grans volums d'informació, fet que afavoreix la planificació estratègica i la capacitat d'adaptació de les polítiques públiques a les necessitats reals de la societat. Aquesta anàlisi avançada no només reforça la confiança de la ciutadania en les institucions, sinó que també contribueix a una administració més àgil, sostenible i orientada als resultats.
<i>Assistència en la redacció de resolucions, informes o guies tècniques</i>	Ús de l'eina d'IAG com a suport a l'elaboració inicial d'esborranys de documents normatius i doctrinals, facilitant l'estructuració de continguts i augmentant l'eficiència en la producció documental relativa a casos específics.
<i>Sistemes d'alertes intel·ligents (priorització de denúncies, reclamacions, notificacions i altres entrades)</i>	Desenvolupament de sistemes d'IA o RPA que permetin detectar i prioritzar denúncies, bretxes de dades o comunicacions sensibles, incloent alertes automàtiques per casos d'alt impacte, col·lectius vulnerables o situacions que requereixin una atenció prioritària a criteri de l'Ajuntament d'Olot, permetent així una gestió àgil o focalitzada.
<i>Suport a la tramitació d'expedients i notificacions de bretxes de dades</i>	La tramitació d'expedients i/o notificacions de bretxes de dades personals són processos manuals assistits per diverses eines corporatives. La IAG permet accelerar tasques, des de la classificació inicial de les entrades per registre, la seva categorització i extracció d'informació estructurada, fins l'elaboració de resums i esborranys.
<i>Anàlisi de dades per la presa de decisions</i>	Ajuda en l'anàlisi de grans volums de dades i identificació de patrons i tendències que poden ajudar en la presa de decisions informades per implementar les metes de l'Agenda 2030. Això pot incloure l'anàlisi de dades socio-econòmiques, demogràfiques i ambientals per a la planificació i l'avaluació de polítiques.
<i>Gestió eficient dels recursos</i>	Optimització de l'ús dels recursos naturals i energètics, ajudant a reduir el consum i impacte ambiental (per exemple, per al control intel·ligent de la xarxa elèctrica, la gestió eficient de l'aigua o la planificació del transport sostenible).
<i>Atenció ciutadana</i>	Xatbots basats en IA desplegats en llocs web municipals per respondre preguntes freqüents dels ciutadans, proporcionant assistència ràpida i millorant l'accessibilitat a la informació
<i>Gestió del registre d'entrada</i>	L'administració electrònica ha portat a que el procediment administratiu estigui digitalitzat gairebé en la seva totalitat i des del seu començament. Les sol·licituds dels ciutadans a través de mitjans electrònics permeten que una IA entrenada llegeixi les sol·licituds i estableixi el departament al qual s'ha

	de dirigir, realitzant la distribució dels assumptes automàticament.
<i>Ciutats intel·ligents i sostenibles</i>	Gestió eficient de ciutats, reducció de contaminació i optimització de serveis urbans per exemple, per al control del trànsit, gestió intel·ligent de residus (optimitzar les rutes de recollida de residus, prevenint la saturació de contenidors i reduint els costos operatius) o millora de l'eficiència energètica en els edificis.
<i>Optimització del transport públic</i>	Algorismes per optimitzar els horaris de transport públic i ajustar-los segons la demanda en temps real, millorant l'eficiència i la satisfacció dels usuaris.

La menció dels anteriors casos d'ús no esgota el potencial de l'aplicació d'aquestes tecnologies a l'Ajuntament d'Olot, podent-se ampliar progressivament i incorporar-se a la present política un cop s'identifiquin. La implementació de qualsevol sistema requerirà el seguiment dels criteris i especificacions establerts en aquesta política.

4. Instruments i procediments de governança

4.1. Òrgans i responsabilitats

Amb l'objectiu de garantir els mecanismes definits en aquest protocol l'Ajuntament reestructurarà o crearà comissions, oficines o grups de treball per tal d'afavorir el desplegament ètic dels sistemes d'intel·ligència artificial.

Les estructures seran les següents:

- a) **Òrgan de direcció estratègica:** L'òrgan de direcció estratègica serà la Comissió de seguretat, ja existent a l'Ajuntament d'Olot, encarregada de definir l'estratègia, supervisar el seu desplegament a tota l'organització i garantirà els recursos necessaris per al desenvolupament i ús responsable de la IA.
 - Assegurar que els sistemes d'IA s'alineïn amb aquesta política
 - Desenvolupar protocols per a ús ètic i responsable de la IA alineats amb els principis.
 - Coordinar la capacitat del personal i la ciutadania, per a l'ús responsable i ètic de la IA
 - Garantir la transparència sobre els casos d'ús de la IA
 - Establir el règim d'auditories i revisions de compliment de polítiques.
 - Garantir sistemes de control d'accés i mesures de seguretat per evitar l'accés no autoritzat a les dades.
 - Revisar i actualitzar periòdicament les polítiques de privadesa i protecció de dades.
 - Identificar i mitigar els riscos de biaix, discriminació o altres danys no desitjats provinents dels sistemes de IA.
 - Elaborar el pla estratègic
- b) **Responsable de desplegament:** A més a més, per a cada desplegament es designarà un responsable. El responsable defineix els objectius i garanteix l'ús ètic i adequat del sistema d'IA dins del servei públic i autoritza l'accés a les dades necessàries per al seu funcionament i també que la implantació compleixi els requisits de qualitat, seguretat, traçabilitat i conformitat normativa.
- c) **Oficina de la dada i intel·ligència artificial:** Aquesta Oficina de treball s'encarrega de definir, a nivell tècnic, els estàndards, eines, ús i implementació de tecnologies de IA sobre els projectes desenvolupats/implantats a l'Ajuntament; desenvolupar projectes pilot d'IA; donar suport per conceptualitzar les solucions a nivell tecnològic, metodològic i ètic i avaluar-ne els riscos. L'Oficina de la Dada lidera el govern, la qualitat i la gestió de les dades i vetlla per l'accés adequat i segur a les dades necessàries. Assumirà també funcions d'impuls i supervisió de l'ús de la IA a l'organització per garantir una estratègia coherent i coordinada amb la política de govern de la dada.
- d) **Delegat/da de protecció de dades:** El/la Delegat/da de Protecció de Dades exerceix les funcions pròpies per garantir la protecció de dades personals.

- e) **L'Àrea de Govern Digital i Ciutadania a través de la Secció de Tecnologia i Dades:** responsable de garantir la ciberseguretat dels sistemes d'IA, controlar l'accés als sistemes, i proporcionar la infraestructura i les solucions tecnològiques necessàries per al seu desplegament.

5. Mitjans d'adquisició, procediment i obligacions

5.1. Mitjans per a l'adquisició dels algorismes i sistemes d'IA

L'Ajuntament d'Olot pot adquirir i utilitzar sistemes d'IA mitjançant alguna de les següents modalitats:

- Desenvolupament de sistemes d'IA mitjançant recursos propis o a través de convenis de col·laboració amb altres administracions, entitats o institucions públiques o privades.
- Subscripció a plataformes d'IA de propòsit general, generalment ofertes com a serveis al núvol, o adquisició de llicències d'ús de sistemes d'IA desenvolupats per tercers, sempre que el proveïdor faciliti informació completa sobre el funcionament, l'entrenament i els criteris de presa de decisions dels sistema, tal i com s'estableix al RIA.
- Contractació, adquisició i ús de sistemes d'IA existents al mercat, sempre que aquests compleixin amb els requisits legals, tècnics i ètics establerts en el RIA; ja sigui com a productes tancats o serveis configurables.

En tots els casos, l'Ajuntament ha de garantir que els sistemes d'IA adquirits compleixen amb els principis generals establerts en aquesta política i en el RIA.

5.2. Procediment

Qualsevol ús de sistema d'IA per part de l'Ajuntament requerirà una avaluació prèvia del nivell de risc i una autorització expressa abans de la seva implementació o posada en funcionament.

El cap de l'àrea que vulgui adquirir o utilitzar un sistema d'IA haurà de completar la **fitxa d'autorització d'ús d'eines basades en IA** (Annex 2) i, caldrà adjuntar-hi tota la informació tècnica i contextual necessària per valorar els riscos associats, en especial els que afectin drets fonamentals, seguretat, privacitat i no discriminació.

Caldrà que el cap d'àrea emeti l'informe amb la documentació anteriorment detallada a través del sistema de gestió d'expedients de l'organització dirigida a l'Àrea de Govern Digital i Ciutadania – Secció de Tecnologia i Dades

La oficina de la dada i IA serà l'encarregada de realitzar:

- Anàlisi de riscos i emissió d'un informe tècnic.
- Resolució d'autorització o denegació d'ús

L'autorització atorgada podrà incloure condicions o limitacions d'ús, mecanismes de control periòdic i obligacions de transparència i rendició de comptes.

Qualsevol modificació substancial del sistema d'IA autoritzat (canvis d'algorisme, dades d'entrenament, ús previst, etc.) requerirà una nova avaluació i autorització.

5.3 Obligacions

5.3.1 Obligacions en el desenvolupament de sistemes d'IA

Quan l'Ajuntament participi en el desenvolupament de sistemes d'IA, ja sigui de manera directa o mitjançant acords de col·laboració amb tercers haurà de garantir:

- La definició clara dels objectius i requisits del sistema, incloent-hi els criteris de qualitat, seguretat i protecció de dades establerts a aquesta política.
- La participació activa dels departaments i unitats afectades en el disseny i implementació del sistema.

- c) El desenvolupament de protocols de validació i auditoria contínua, per assegurar-ne el correcte funcionament.
- d) Mecanismes per detectar i corregir errors, biaixos o riscos emergents

Requisits específics per a sistemes d'alt risc

En el cas de sistemes d'alt risc, l'Ajuntament haurà de realitzar una avaluació exhaustiva abans de la seva posada en marxa, incloent-hi la revisió dels requisits de l'apartat per part de l'òrgan de supervisió establert en aquesta política:

- a) Realitzar una avaluació d'impacte sobre drets fonamentals i riscos associats
- b) Implantar un sistema de gestió de riscos durant tot el cicle de vida del sistema
- c) Assegurar la qualitat de les dades d'entrenament, validació i prova mitjançant pràctiques de governança de dades
- d) Elaborar i mantenir la documentació tècnica del sistema i proporcionar instruccions d'ús clares
- e) Garantir una supervisió humana efectiva, amb personal qualificat per intervenir si cal
- f) Assegurar un nivell adequat de precisió, robustesa i ciberseguretat.

5.3.2. Obligacions a l'hora de contractar/adquirir una IA.

En els casos en què es contracti un proveïdor extern o es desenvolupi un règim de col·laboració, el document que reculli els termes del servei o la col·laboració ha de preveure els següents elements:

- a) Una avaluació prèvia del nivell de risc del sistema i el seu impacte potencial sobre els drets fonamentals.
- b) Detall dels termes i serveis oferts pel proveïdor per garantir que s'ajustin als principis ètics, de transparència i als requisits establerts en aquesta política i a la normativa vigent.
- c) Inclusió de disposicions contractuals que assegurin la supervisió contínua, la possibilitat d'auditoria independent i al responsabilitat del proveïdor respecte al funcionament, als resultats i als possibles impactes del sistema.
- d) Implementació de mesures rigoroses de confidencialitat, seguretat i protecció de les dades, incloent-hi mecanismes per garantir-ne la integritat, l'accés restringit i al seva eliminació segura un cop finalitzat el contracte.
- e) Definició de les condicions per a l'actualització i el manteniment del sistema d'IA, garantint que continuï complint amb els requisits normatius i els estàndards tècnics vigents.
- f) Determinar clarament les responsabilitats del proveïdor en cas d'errors, decisions indegudes o impactes negatius derivats de l'ús del sistema.
- g) Establiment d'indicadors i procediments per monitorar el rendiment del sistema d'IA durant tot el període de contractació, assegurant-ne el compliment dels criteris de qualitat, ètica i no discriminació.

A més, s'hauran d'incorporar les clàusules tipus incloses a l'Annex 3 d'aquesta política, les quals proporcionen una base per garantir el compliment normatiu i hauran de ser adaptades a la naturalesa concreta de cada contracte.

Els proveïdors tecnològics que subministren sistemes d'intel·ligència artificial a l'Ajuntament hauran de complir amb una sèrie de requisits específics, amb l'objectiu de garantir la transparència, la traçabilitat i la seguretat dels sistemes implantats. En particular, es requerirà que els sistemes disposin d'un registre automàtic d'esdeveniments (logs) al llarg de tot el seu cicle de vida, per assegurar la traçabilitat de la seva lògica operativa i dels resultats generats. A més, hauran d'estar dissenyats de manera que la seva lògica sigui prou transparent per tal que els usuaris puguin interpretar-ne els resultats i, alhora, permetre la supervisió humana durant el seu ús, mitjançant interfícies adequades. En aquells casos en què la supervisió en temps real no sigui viable, caldrà implementar mecanismes alternatius que assegurin una supervisió efectiva. Finalment, s'exigirà que els sistemes incorporin mesures específiques de ciberseguretat per evitar alteracions malicioses del funcionament o ús per part de tercers no autoritzats. Aquest conjunt de mesures serà d'obligat compliment en qualsevol procés de contractació o adquisició de tecnologia basada en IA.

Aquestes obligacions s'aplicaran directament als proveïdors o desenvolupadors dels sistemes, i hauran de quedar garantides contractualment en el cas de contractacions externes.

En proposaran clàusules contractuals tipus que proporcionin una base per garantir el compliment normatiu i hauran de ser adaptades a la naturalesa concreta de cada contracte.

5.3.3. Obligacions durant el desplegament i ús de la IA.

Quan l'Ajuntament desplegui sistemes d'IA (propis o de tercers), com a responsable de la seva implementació haurà de:

- Utilitzar-los d'acord amb les seves especificacions i instruccions
- Garantir la supervisió humana per part de persones competents
- Verificar que les dades d'entrada són rellevants i representatives, en la mesura que en tingui control
- Monitorar el funcionament dels sistemes i informar de riscos, incidents i anomalies als proveïdors i autoritats competents.
- Conservar els fitxers de registre sota el seu control, quan sigui aplicable
- Informar les persones treballadores i els seus representants abans d'implantar un sistema d'IA que afecti l'àmbit laboral
- Informar les persones afectades per decisions automatitzades o processos assistits per IA, de manera clar i comprensible.
- Assegurar que el personal responsable del maneig de sistemes d'IA disposa d'un nivell adequat d'alfabetització digital i competències en IA

Qualsevol modificació substancial del sistema d'IA autoritzat (canvis d'algoritme, dades d'entrenament, ús previst, etc.) requerirà una nova avaluació.

5.5 Classificació del nivell de risc del sistema

Els sistemes d'IA es classifiquen segons el seu nivell de risc en funció del seu potencial impacte en seguretat, drets fonamentals i altres àmbits d'especial sensibilitat; i tenint en compte el context d'aplicació del sistema i la seva finalitat. En aquest sentit, d'acord amb el RIA existeixen quatre nivells de risc:

Risc inacceptable	Sistemes prohibitius per l'amenaça clara que suposen als drets i llibertats fonamentals.
Risc alt	Sistemes subjectes a requisits estrictes, tant pel seu impacte en drets fonamentals com la llibertat, la privacitat o la no discriminació, com en la salut, la seguretat o els drets laborals de les persones o per la presa de decisions automatitzades amb conseqüències jurídiques o efectes significatius per a les persones físiques o jurídiques.
Risc limitat	Sistemes que poden influir en les persones i que han de complir amb certes obligacions, per exemple, de transparència.
Risc mínim o nul	Sistemes amb escàs impacte. Sense requisits específics segons el RIA.

Cap sistema d'intel·ligència artificial podrà ser implementat ni entrar en funcionament sense la valoració prèvia del seu nivell de risc i la corresponent autorització formal per part de l'òrgan competent designat per l'Ajuntament.

5.2.1. Risc inacceptable

Es prohibiran tots els sistemes d'IA que es considerin una clara amenaça per a la seguretat i els drets de les persones, des del "social scoring" dels governs fins a les joguines que fan servir assistència de veu i que fomenten comportaments perillosos. Es prohibiran també els sistemes d'identificació biomètrica remota en espais públicament accessibles.

5.2.2. Risc alt

Aquests inclouen la tecnologia d'IA utilitzada en:

- Identificació biomètrica remota en temps real o en diferit de persones físiques;
- Infraestructures crítiques (per exemple, el transport), que podrien posar en risc la vida i la salut de les persones

- La formació educativa o professional, que pot determinar l'accés a l'educació i el desenvolupament professional d'algú (per exemple, l'avaluació dels exàmens);
- Els components de seguretat dels productes (per exemple, l'aplicació de la IA en la cirurgia assistida per robots);
- L'ocupació, la gestió dels treballadors i l'accés a l'autoocupació (per exemple, programari de classificació de CV per als procediments de contractació);
- Serveis privats i públics essencials (per exemple, la qualificació de crèdits que nega als ciutadans l'oportunitat d'obtenir un préstec);
- Aplicació de la llei que pot interferir amb els drets fonamentals de les persones (per exemple, avaluació de la fiabilitat de les proves);
- Gestió de la migració, l'asil i el control de fronteres (per exemple, verificació de l'autenticitat dels documents de viatge);
- L'administració de justícia i els processos democràtics (per exemple, l'aplicació de la llei a un conjunt concret de fets).

Els sistemes de IA d'alt risc estaran subjectes a estrictes obligacions abans de poder comercialitzar-se o implementar-se:

- Sistemes adequats d'avaluació i mitigació de riscos;
- Alta qualitat dels conjunts de dades que alimenten el sistema per a minimitzar els riscos i els resultats discriminatoris;
- Registre de l'activitat per a garantir la traçabilitat i transparència dels resultats;
- Documentació detallada que proporcioni tota la informació necessària sobre el sistema i la seva finalitat perquè les autoritats puguin avaluar la seva conformitat;
- Informació clara i adequada a l'usuari;
- Mesures adequades de supervisió humana per a minimitzar el risc;
- Alt nivell de solidesa, seguretat i precisió;
- Tots els sistemes d'identificació biomètrica a distància es consideren d'alt risc i estan subjectes a requisits estrictes. L'ús de la identificació biomètrica a distància en espais d'accés públic amb finalitats policials està, en principi, prohibit.

Es defineixen i regulen estrictament algunes excepcions, com quan és necessari buscar un nen desaparegut, prevenir una amenaça terrorista específica i imminent o detectar, localitzar, identificar o processar a un autor o sospitós d'un delictes greu.

Aquesta utilització està subjecta a l'autorització d'un òrgan judicial o un altre òrgan independent i a uns límits adequats quant a temps, abast geogràfic i bases de dades consultades.

Requisits específics per a sistemes d'alt risc

En el cas de sistemes d'alt risc, l'Ajuntament haurà de realitzar una avaluació exhaustiva abans de la seva posada en marxa, incloent-hi la revisió dels requisits de l'apartat per part de l'òrgan de supervisió establert en aquesta política:

- a) Realitzar una avaluació d'impacte sobre drets fonamentals i riscos associats i, si s'escau, l'avaluació ètica.
- b) Implantar un sistema de gestió de riscos durant tot el cicle de vida del sistema.
- c) Assegurar la qualitat de les dades d'entrenament, validació i prova mitjançant pràctiques de governança de dades.
- d) Elaborar i mantenir la documentació tècnica del sistema i proporcionar instruccions d'ús clares.
- e) Garantir una supervisió humana efectiva, amb personal qualificat per intervenir si cal.
- f) Assegurar un nivell adequat de precisió, robustesa i ciberseguretat.

5.2.3. Risc limitat

El risc limitat es refereix als sistemes d'IA amb obligacions específiques de transparència. Quan s'utilitzen sistemes d'IA, com els xatbots, els usuaris han de ser conscients que estan interactuant amb una màquina per a poder prendre una decisió informada de continuar o retrocedir.

5.2.4. Risc mínim o cap risc

La proposta permet l'ús lliure de la IA de risc mínim. Això inclou aplicacions com els videojocs amb IA o els filtres d'*spam*. La gran majoria dels sistemes d'IA utilitzats actualment a la UE entren en aquesta categoria.

6. Aplicació de la IA en el procediment administratiu

6.1. Requisits per a l'automatització d'actuacions

La decisió que un àmbit d'actuació o una funció de l'Ajuntament incorpori l'ús d'IA s'ha d'adoptar seguint els criteris que s'estableixen en aquest article i en la resta d'aquesta política.

Les actuacions susceptibles d'automatització mitjançant sistemes basats en IA es poden classificar en alguna de les següents tipologies:

- a) Actuacions administratives automatitzades definides a l'article 41 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, en els quals hi pot haver algun element de presa de decisió que utilitzi IA.
- b) Actes preparatoris d'una actuació administrativa que impliquen l'elaboració d'informes o la formulació de propostes de resolució que eventualment seran revisades per part d'un òrgan de l'Ajuntament.
- c) Explotació de dades o extracció d'informació per generar indicadors, detectar riscos o d'alguna altra forma identificar la necessitat d'actuar per part de l'Ajuntament.
- d) Actuacions que impliquin l'ús de sistemes d'IA, per oferir informació o assessorament a ciutadans o a tercers, sense que es generi una resolució o una actuació administrativa per part de l'Ajuntament.

L'actuació administrativa automatitzada, en els termes regulats al a normativa bàsica reguladora del règim jurídic del sector públic vigent, permet la realització, per mitjans electrònics, de qualsevol acte o actuació administrativa mitjançant l'ús d'un sistema d'informació sense necessitat d'intervenció de personal empleat públic.

Adicionalment, quan per desenvolupar actuacions administratives automatitzades s'utilitzin algorismes involucrats en la presa de decisions basats en IA caldrà tenir en compte criteris d'eliminació de biaixos, transparència i retiment de comptes en la seva fase de disseny i d'entrenament de l'algorisme, tal i com estableix aquesta política. Per altra banda, s'haurà de promoure la realització d'avaluacions per a identificar l'existència de biaixos discriminatoris en els sistemes que ja estiguin en funcionament.

1. Quan en un procediment administratiu es prevegi l'ús de sistemes basats en IA per a l'elaboració d'esborranys, propostes o documents preparatoris, serà necessari identificar prèviament els aspectes següents:
 - a) Les fonts d'informació i els conjunts de dades (*datasets*) que s'utilitzin per l'entrenament del sistema, incloent-hi les plantilles o models preexistents.
 - b) Les persones responsables de la revisió i validació dels resultats generats pel sistema.
 - c) La fase o moment concret del procediment en què es farà ús de la IA i quin serà el grau d'intervenció.
2. Quan es prevegi l'ús de sistemes destinats a l'explotació o extracció d'informació per generar indicadors, detectar riscos o identificar la necessitat d'actuar per part de l'Ajuntament, serà necessari acordar prèviament els aspectes següents:
 - a) L'origen de les dades, incloent-hi la seva disponibilitat, titularitat, compliment de la normativa de protecció de dades i altres aspectes relatius a la privacitat.
 - b) La viabilitat de l'automatització en aquells casos en què les decisions derivades de l'explotació de dades puguin tenir un impacte sobre els drets de la ciutadania, garantint que es respectin els principis de transparència i no discriminació.

6.2. El cicle de vida d'un sistema algorísmic (TIC)

Per garantir que els sistemes algorísmics contractats per l'Ajuntament compleixen amb els principis rectors, cal alinear el cicle de vida d'un servei TIC i els procediments de contractació pública amb les particularitats del cicle de vida dels sistemes algorísmics i introduir, en cadascuna d'aquestes fases, totes les salvaguardes necessàries.

Tot producte o servei TIC té un cicle de vida: introducció, creixement, maduresa i declivi. A continuació es descriuen les fases del cicle de vida que haurà de seguir qualsevol aplicació que incorpori un sistema d'IA, ja sigui adquirida o desenvolupada internament. Tot cicle de vida haurà d'estar degudament documentat, i aquesta documentació s'haurà d'incloure al Registre Municipal d'Algorismes i Sistemes d'IA.

6.2.1. Identificació d'oportunitats

Abans d'iniciar qualsevol projecte basat en intel·ligència artificial, cal identificar de manera proactiva aquells àmbits o processos de l'organització en què l'ús de la IA pugui aportar un valor afegit tangible, ja sigui millorant l'eficiència, la capacitat predictiva, la qualitat del servei, la presa de decisions o la personalització de l'atenció ciutadana.

Aquesta fase inicial ha d'incloure:

- L'anàlisi de serveis que presentin colls d'ampolla, càrregues administratives recurrents o una elevada demanda ciutadana.
- La revisió de processos que generen grans volums de dades o que poden ser automatitzats parcialment.
- La detecció de necessitats estratègiques en què el coneixement generat per sistemes d'IA pot anticipar riscos o millorar la planificació.

A mesura que l'organització avanci en la maduresa digital, aquesta identificació puntual d'oportunitats s'ha d'integrar dins d'una visió més àmplia i sistemàtica d'intel·ligència de processos. Això implica analitzar de manera estructurada el funcionament de l'organització per detectar patrons, correlacions i indicadors rellevants que permetin reconfigurar serveis, millorar la gestió del canvi i establir una cultura de millora contínua basada en dades i evidències.

En aquest sentit, la implantació d'IA no ha de ser només una resposta tecnològica, sinó una palanca per transformar la manera com es dissenyen i executen les polítiques públiques i els serveis.

6.2.2 Planificació i definició de l'abast

En aquesta fase s'han de definir de manera clara els objectius i requisits del sistema d'intel·ligència artificial, garantint que compleixi els criteris de qualitat, seguretat i protecció de dades establerts en aquesta política.

Les principals actuacions seran:

- Justificar l'ús de la IA, identificant-ne els beneficis esperats i l'impacte en la prestació de serveis a la ciutadania
- Determinar les fonts de dades i informació que s'utilitzaran.
- Realitzar un anàlisi previ de riscos.
- Dissenyar el sistema d'acord amb els principis ètics i normatius establerts.
- Definir indicadors que permetin avaluar la millora en els serveis o processos.
- Establir protocols de validació i supervisió que assegurin un ús responsable.
- Garantir la participació activa dels departaments i unitats implicades en el disseny i la implementació, així com de la ciutadania.

6.2.3. Recopilació de dades i informació

En aquesta fase es duu a terme la recollida, neteja i preparació de dades d'alta qualitat, representatives i lliures de biaixos. Es definirà el sistema de control d'accés necessari per garantir la protecció i seguretat de les dades, establint limitacions específiques per a l'accés a dades històriques i incorporant mecanismes d'accés ètic, d'acord amb el que s'estableixi en la Política de Govern de la Dada.

Es valorarà la idoneïtat de les dades destinades a l'entrenament del sistema, així com la necessitat d'utilitzar dades sintètiques.

En cas de dades personals, s'empraran tècniques d'emascarament (ofuscació o anonimització) o de tokenització per protegir la informació identificable. Si es tracten dades confidencials, es podran inserir marques d'aigua digitals en els textos per facilitar-ne el rastreig i la detecció d'usos no autoritzats.

6.2.4. Desenvolupament i entrenament

En aquesta fase es durà a terme la selecció del model d'IA més adequat i el seu entrenament amb dades de qualitat, representatives i mitigar biaixos. Es realitzaran processos de validació i ajust continu per garantir la robustesa, la fiabilitat i el compliment dels requisits essencials de seguretat, transparència i governança de dades.

S'habilitarà un entorn de proves que repliqui fidelment les condicions de producció, incloent les mateixes mesures de seguretat i controls d'accés, per tal de verificar el comportament del sistema abans del desplegament real.

Es definiran i implementaran mecanismes sistemàtics per a la detecció i correcció proactiva d'errors, biaixos, al·lucinacions i altres riscos emergents, assegurant una supervisió humana adequada i una traçabilitat completa de les decisions i resultats generats pel sistema.

6.2.5. Avaluació i aprovació prèvia al desplegament

La definició del nivell de risc del sistema d'IA permetrà determinar en quins casos és exigible l'avaluació d'impacte en drets fonamentals. Addicionalment, quan la naturalesa del sistema o el seu potencial impacte sobre les persones o els processos públics així ho requereixin, s'hi haurà d'incorporar l'avaluació ètica corresponent.

a) Avaluació d'impacte sobre Drets Fonamentals

La metodologia d'avaluació d'impacte definida per l'Autoritat Catalana de Protecció de Dades s'ha d'aplicar en tots els sistemes d'IA que puguin afectar drets, persones o processos rellevants de l'Administració, especialment quan es tracti de sistemes d'alt risc segons el RIA, quan s'utilitzin dades personals sensibles o quan la IA tingui un paper en la presa de decisions automatitzades o semiautomatitzades.

Aquesta avaluació permet identificar i minimitzar riscos que puguin afectar la privacitat, la protecció de dades i altres drets fonamentals de les persones.

Guia i formulari disponibles a: FRIA – AcdPD

b) Avaluació ètica

L'avaluació ètica es realitzarà mitjançant el model d'autoavaluació PIO (Principis, Indicadors i Observables) de l'Observatori d'Ètica en Intel·ligència Artificial de Catalunya (OEIAC). Aquesta eina actua com un mecanisme de verificació prèvia que permet identificar i analitzar els riscos ètics associats als sistemes d'IA.

L'autoavaluació s'aplicarà en aquells sistemes d'IA que, per la seva naturalesa o pel potencial impacte sobre les persones o els processos públics, requereixin una valoració específica en termes d'ètica, transparència i no-discriminació. El seu objectiu és assegurar que el sistema s'alinea amb els principis ètics establerts, garantint la justícia, la igualtat de tracte i l'absència de biaixos indeguts.

L'eina està disponible a: OEIAC

La Comissió tècnica executiva analitzarà cada cas i podrà proposar elevar el projecte a la Comissió Ètica quan consideri necessària una revisió específica.

6.2.6. Desplegament i operació

Un cop licitat el servei, el proveïdor passarà a desenvolupar i posar en funcionament el sistema algorímic. En aquestes fases del cicle de vida (desenvolupament, producció i explotació) caldrà garantir que el sistema funciona segons el seu objectiu inicial i que els riscos que emergeixen són mitigats. En el cas que el sistema incorpori l'aprenentatge automàtic, caldrà vetllar perquè les operacions dutes a terme per aquest continuïn sent explicables i el sistema no incorpori biaixos.

El desplegament dels sistemes d'IA es realitzarà de manera planificada i controlada, assegurant-ne la correcta integració en els serveis municipals. Aquest procés inclourà:

- Formació específica de l'equip, assegurant que el personal implicat disposi dels coneixements tècnics i procedimentals necessaris per utilitzar el sistema de manera eficient, segura i ètica.
- Posada en marxa controlada (fase pilot), amb monitoratge intensiu del rendiment i comportament del sistema per detectar i corregir possibles incidències abans del seu ús generalitzat.

6.2.7. Monitoratge i supervisió continuats

Es garantirà una vigilància constant del rendiment, la seguretat, el compliment ètic i la detecció d'incidències o desviacions no desitjades en el funcionament dels sistemes d'IA.

En particular, s'hauran de definir i aplicar els elements següents:

- Procediment de verificació periòdica dels resultats generats pel sistema, amb especial atenció a la identificació de biaixos, errors en la comunicació i altres anomalies.
- Mecanisme de reavaluació contínua, que determini com es revisaran i ajustaran els criteris de funcionament tant abans de la posada en marxa com durant l'operació ordinària.
- Condició prèvia per a sistemes que informen la ciutadania: no es podrà posar en servei cap sistema d'IA destinat a proporcionar informació pública sense haver establert prèviament el procediment formal de supervisió i millora contínua.

L'Ajuntament no haurà d'abonar un import addicional al contractista pels treballs que es derivin de les accions descrites anteriorment.

OBLIGATORI	Risc Alt	Risc Mitjà	Risc mínim o nul
------------	----------	------------	------------------

L'Ajuntament o entitat local posarà a disposició de la ciutadania i de totes les parts interessades la informació pública relacionada amb els sistemes algorísmics que liciti al Registre Públic d'Algoritmes que es crearà a aquests efectes. De manera preliminar i no restrictiva², es preveu que es publiquin:

- Informació bàsica sobre el sistema algorísmic:
 - Finalitat del sistema algorísmic
 - Àrea municipal que l'impulsa
 - Actors implicats en les decisions del sistema
 - Abast del sistema algorísmic
 - Dades que es faran servir
 - Incorporació d'aprenentatge automàtic
 - Política d'utilització
 - Calendari d'aplicació
 - Riscos que podrien aparèixer i estratègia de gestió d'aquests
 - Legitimació de la finalitat en el cas de tractament de dades personals, prèviament alineat al RAT
- Els estudis d'impacte algorísmic (només dels sistemes que acabin sent licitats)
- El model de Clàusules Tipus per la Contractació de Sistemes d'IA Fiables
- Els informes d'auditoria algorísmica
- Informe de balanç final
- Informació clara i detallada dels mecanismes de comunicació ciutadana disponibles per tramitar peticions d'informació o consultes, incidències, queixes i suggeriments en relació al funcionament dels sistemes algorísmics

A banda del Registre d'Algoritmes, aquells sistemes que incorporin tractament de dades personals hauran d'incorporar-se al RAT.

6.2.8. Actualització i manteniment

Es garantirà la revisió i evolució periòdica dels sistemes d'IA per assegurar-ne la vigència, la qualitat i el compliment normatiu. Les actuacions inclouran:

- Reajustament del model per optimitzar-ne el rendiment davant canvis en les dades o en l'entorn operatiu.
- Re-entrenament amb noves dades per mantenir la precisió, reduir biaixos i incorporar millores detectades durant el monitoratge.

² Vegeu el punt 6.2.7.2 de l'Annex 1.

- Millora de processos associats a la utilització de la IA, aprofitant els aprenentatges obtinguts durant l'operació.
- Adequació a noves normes i estàndards, garantint el compliment permanent amb el Reglament Europeu d'IA i altres regulacions aplicables.

6.2.9. Desactivació o retirada

Quan un sistema d'IA arribi al final de la seva vida útil, presenti obsolescència o es decideixi la seva substitució, es durà a terme un procés ordenat i segur que inclourà:

- Tancament controlat i sistemàtic del sistema, garantint la interrupció segura de totes les seves funcions.
- Esborrat segur i verificat de totes les dades, models i configuracions associades, d'acord amb les polítiques de protecció de dades i seguretat de la informació.
- Documentació i arxiu de tot el procés per a la seva consulta futura i per complir amb les obligacions de traçabilitat establertes.

S'establirà un protocol específic per a la desactivació immediata del sistema en cas que es detectin canvis de comportament que puguin afectar la seva fiabilitat, seguretat o compliment normatiu.

7. Entrenament dels sistemes de protecció de dades

7.1. Propietat i ús de les dades en l'entrenament dels sistemes

En qualsevol dels escenaris previstos en la present política l'Ajuntament ha de tenir en compte les consideracions següents:

- a) Si l'Ajuntament és propietari de les dades, pot fer ús d'aquesta informació per a l'entrenament dels sistemes d'IA, sempre que es garanteixi el compliment de la normativa vigent en matèria de protecció de dades.
- b) Si l'Ajuntament no és la propietari de les dades, cal verificar si es disposa dels requisits necessaris per al seu ús. En cas afirmatiu, cal obtenir les autoritzacions pertinents dels titulars o responsables de les dades. Si no es compleixen els requisits legals o no es disposa de les autoritzacions corresponents, les dades no es podran utilitzar per a l'entrenament o millora dels sistemes.
- c) Que no es tracti de dades personals, a efectes de garantir la privacitat i la protecció dels drets de les persones titulars de les dades, d'acord amb la normativa vigent.

En projectes col·laboratius es poden establir acords per compartir les dades propietat de l'Ajuntament amb tercers per l'entrenament dels sistemes, sempre que aquests acords incloguin garanties adequades de seguretat, protecció de dades i benefici mutu, com el dret a utilitzar el sistema resultant per part de l'Ajuntament.

Així mateix, es pot autoritzar la cessió de dades per al 'entrenament d'eines desenvolupades per tercers, sempre que es prenguin les mesures necessàries per garantir la protecció, anonimització i ús adequat de la informació.

7.2. Qualitat de les dades

Les dades utilitzades per a l'entrenament, validació i prova dels sistemes d'IA han de ser precises, completes, actualitzades i representatives de la realitat que pretenen modelar.

Per garantir la qualitat de les dades abans del seu ús en sistemes d'IA s'ha de verificar que:

- a) Siguin veraces, consistents i lliures d'errors, evitant informació incompleta o contradictòria
- b) No continguin biaixos que puguin afectar el funcionament o els resultats del sistema i als drets de les persones interessades
- c) Reflecteixin el context en què s'implementaran
- d) Disposin de traçabilitat, documentant-ne l'origen i les transformacions aplicades.

La supervisió i manteniment continuat de la qualitat de les dades es regirà pel sistema de governança i gestió de dades establert a l'Ajuntament.

7.3. Protecció de dades personals

El tractament de dades personals en l'entrenament, desenvolupament i ús dels sistemes d'IA ha de complir amb el que estableix la normativa vigent en matèria de protecció de dades personals.

La protecció de dades personals s'ha de garantir al llarg de tot el cicle de vida del sistema d'IA, aplicant els següents principis:

- a) Minimització de dades: només es poden tractar les dades estrictament necessàries per a la finalitat prevista
- b) Limitació de la finalitat: les dades personals només es poden utilitzar per al es finalitats determinades, explícites i legítimes per les quals van ser recollides. No obstant això, la normativa vigent permet utilitzar dades recavades per finalitats diferents per tal d'utilitzar-les en entorns de prova de cara a millorar l'aprenentatge i el resultat del sistema d'IA.
- c) Exactitud: s'han de prendre mesures per assegurar que les dades siguin precises i actualitzades
- d) Integritat i confidencialitat: s'ha d'assegurar un tractament segur, incloent-hi mesures de protecció contra accessos no o autoritzats, pèrdues o alteracions de dades.
- e) Protecció de dades des del disseny i per defecte: els sistemes d'IA han d'incorporar mecanismes per garantir la privacitat en totes les fases del seu desenvolupament i ús.

Quan el tractament de dades personals sigui realitzat per un tercer per compte de l'Ajuntament, caldrà formalitzar el corresponent contracte d'encarregat del tractament, d'acord amb l'article 28 del Reglament General de Protecció de Dades. Si el tercer no actua com a encarregat del tractament però té accés a informació confidencial, es requerirà la formalització d'un acord de confidencialitat.

En cas de sistemes considerats d'alt risc cal realitzar una avaluació d'impacte en drets fonamentals per identificar i mitigar possibles riscos abans de la seva implementació³.

Ús de dades sintètiques

Amb caràcter general, l'Ajuntament fomentarà l'ús de dades sintètiques en aquells casos on el tractament de dades reals comporti riscos per a la privacitat, limitacions legals o dificultats tècniques. L'objectiu és garantir el desenvolupament de sistemes d'IA responsables, segurs i respectuosos amb la normativa vigent.

L'ús de dades sintètiques és especialment recomanable en els següents supòsits:

- Protecció de dades personals: quan l'ús de dades reals pugui comprometre la privacitat de les persones o vulnerar el Reglament General de Protecció de Dades (RGPD) i altra normativa aplicable.
- Manca de dades reals o dades escasses: quan no hi ha prou informació per entrenar o validar un sistema d'IA de manera adequada.
- Equilibri i no discriminació: per corregir desequilibris en els conjunts de dades que puguin generar biaixos o discriminacions no desitjades.
- Simulació d'escenaris: per provar sistemes d'IA amb situacions hipotètiques, infreqüents o d'alt risc sense posar en perill dades reals.
- Desenvolupament i proves: per validar funcionalitats durant el desenvolupament tècnic en entorns de test, evitant l'exposició de dades reals.

Les dades sintètiques utilitzades han de generar-se mitjançant mètodes tècnicament sòlids que assegurin una representació fidel dels patrons i distribucions de les dades originals, evitant la introducció de biaixos artificials o resultats enganyosos. El seu ús no eximeix de complir amb els principis establerts a la normativa d'IA ni amb els criteris d'explicabilitat, responsabilitat i traçabilitat.

7.4. Detecció, correcció i mitigació de biaixos

Tot i les mesures preventives establertes anteriorment, l'Ajuntament ha de garantir la detecció, mitigació i correcció de possibles biaixos que puguin aparèixer durant el desenvolupament i ús dels sistemes d'IA.

- a) En les auditories periòdiques es realitzaran anàlisis comparatives per identificar biaixos i avaluar-ne l'impacte.

³ [Guia d'avaluació d'impacte en drets fonamentals](#)

- b) En cas de detectar biaixos, s'adoptaran mesures de mitigació com l'ajust d'algorismes, la millora de les dades d'entrenament i la intervenció humana.
- c) Si la mitigació no és suficient, es prendran mesures correctores immediates, incloent-hi la revisió del sistema o la seva suspensió si cal.

8. Garanties. Mecanismes de supervisió i control

8.1. Garantia de supervisió humana

L'Ajuntament ha de garantir la intervenció i supervisió humana en les actuacions automatitzades mitjançant sistemes d'IA per revisar, modificar o revertir decisions; especialment en casos complexos, errors tècnics o impugnacions formulades pels usuaris.

8.2. Auditories i informes periòdics

Els sistemes d'IA implementats per l'Ajuntament s'han de sotmetre a auditories sistemàtiques i periòdiques per identificar riscos, possibles biaixos i verificar el compliment dels requisits ètics, tècnics i legals establerts en aquesta política.

Les auditories han de tenir en compte, sense caràcter limitatiu, els següents elements:

- a) Anàlisi de biaixos algorísmics: avaluació de possibles discriminacions i impacte en diferents col·lectius.
- b) Verificació dels tractaments de dades personals: assegurant el compliment de la normativa de protecció de dades.
- c) Revisió de l'impacte del sistema. Valoració dels seus efectes en els drets dels ciutadans, la seguretat i la qualitat dels serveis públics.
- d) Avaluació del rendiment i fiabilitat. Identificació d'errors, limitacions i possibles millores tècniques i anàlisi sobre la viabilitat de l'automatització.

Els resultats d'aquestes auditories es documentaran en informes periòdics que han de ser accessibles, quan escaigui, per a la ciutadania mitjançant el Portal de Transparència.

L'Ajuntament ha de garantir l'existència de mecanismes de correcció i millora contínua derivats de les auditories, incloent-hi la revisió i ajust dels algorismes quan sigui necessari.

8.3. Propietat intel·lectual

L'Ajuntament garantirà el respecte als drets de propietat intel·lectual en totes les fases del cicle de vida dels sistemes d'IA, assegurant que l'ús, adquisició o desenvolupament d'aquests sistemes no vulneri els drets de tercers, i preservant, si escau, els drets sobre els actius propis generats.

Per assolir aquest objectiu, s'adoptaran les mesures següents:

- Verificació de llicències i drets d'ús: en la contractació de solucions d'IA desenvolupades per tercers, es verificarà que el proveïdor disposa dels drets d'explotació corresponents i que la llicència cobreix l'ús previst per part de l'Ajuntament.
- Protecció de les dades i resultats: s'establiran clàusules contractuals que regulin la titularitat i l'ús dels resultats generats pels sistemes d'IA (textos, informes, codis, models, etc.), especialment quan aquests resultats puguin ser objecte de protecció per drets d'autor.
- Desenvolupament propi o col·laboratiu: en els projectes propis o en col·laboració amb altres entitats, es definirà de manera explícita qui és el titular dels drets sobre els models, algorismes o dades generats, mitjançant convenis o acords específics.
- Evitar l'ús indegut d'obres protegides: es vetllarà perquè els sistemes d'IA no s'entrenin amb dades o materials protegits per drets d'autor sense la correspon.

8.4. Òrgans de supervisió i control

L'oficina de la dada o Equip tècnic serà l'òrgan encarregat de la supervisió i control de la implementació i ús de l'IA a l'Ajuntament.

En concret, els seves funcions són, sense caràcter limitatiu:

- a) Definir i impulsar la implementació de l'Agenda Digital i fer-ne el seguiment.
- b) Impulsar la configuració d'una administració àgil orientada a donar els millors serveis mitjançant l'acompanyament i assessorament en la transformació digital i, en particular, en l'ús dels sistemes d'intel·ligència artificial.
- c) Portar a terme projectes multidisciplinaris que puguin actuar com a palanca de canvi en aquest procés de transformació, dels quals se'n deriven:
 - i. El desplegament d'accions de formació del personal al servei de l'Ajuntament.
 - ii. La Gestió del Registre Municipal de sistemes d'intel·ligència artificial i d'avaluació de l'impacte en els drets fonamentals.
 - iii. Avaluacions periòdiques
 - iv. Elaboració d'informes sobre l'ús dels sistemes d'intel·ligència artificial
- d) Vetllar per al correcte ús dels sistemes d'intel·ligència artificial.

En paral·lel, la Comissió de seguretat creada a l'Ajuntament d'Olot, incorporarà noves funcions en matèria de la definició i l'impuls de la política de dades municipal, el desenvolupament del model de governança de la dada, i el compliment estricte de la normativa, en particular pel que fa a un desplegament ètic, responsable, inclusiu i transparent del sistemes d'IA.

8.5. Traçabilitat

La traçabilitat és un principi essencial per garantir l'ús responsable i segur dels sistemes d'intel·ligència artificial. Implica la capacitat de rastrejar les dades utilitzades, els processos seguits, les decisions preses i les versions dels models implementats, al llarg de tot el cicle de vida del sistema. Aquesta traçabilitat ha de permetre auditories internes o externes, facilitar la comprensió dels resultats obtinguts i identificar possibles errors, biaixos o desviacions. Per fer-ho possible, cal establir registres detallats i sistemàtics de les accions i canvis produïts, tant en l'entrenament del model com en la seva execució operativa. Això contribueix a reforçar la confiança, la responsabilitat i el compliment normatiu en l'ús de la IA.

Per garantir la traçabilitat a l'usuari, s'estableix que tot contingut sintètic creat amb IA (text, imatge, àudio, vídeo,...) haurà d'incloure:

- Una etiqueta visible per a l'usuari
- Una marca tècnica oculta incrustada en les metadades

8.6. Ciberseguretat

La ciberseguretat és un requisit essencial en el desplegament de qualsevol sistema d'intel·ligència artificial. Aquests sistemes han de protegir-se de manera efectiva contra atacs, manipulacions o accessos no autoritzats que puguin comprometre la integritat de les dades, la confidencialitat de la informació o el correcte funcionament dels algorismes.

Caldrà aplicar mesures de seguretat específiques i adequades durant tot el cicle de vida del sistema —des del desenvolupament fins a la retirada incloent la posada en producció, la monitorització contínua i la gestió d'incidents.

Totes aquestes actuacions es duran a terme d'acord amb els estàndards reconeguts de seguretat de la informació, el Reglament Europeu d'IA, la normativa vigent en matèria de protecció de dades i l'Esquema Nacional de Seguretat.

Així mateix, caldrà aplicar mesures específiques, entre les quals:

- a) **Detecció i prevenció d'atacs específics a sistemes d'IA:** El sistema haurà d'incorporar mesures per prevenir i detectar atacs dirigits. Per a la detecció i classificació d'aquestes amenaces, es recomana l'ús de MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems), que proporciona un marc de referència internacional amb tècniques, tàctiques i procediments documentats per identificar, comprendre i mitigar atacs contra sistemes d'IA.
- b) **Protocol de resposta davant canvis de comportament:** Si la monitorització detecta variacions significatives en les dades que provoquin errors, biaixos, al·lucinacions o altres resultats incompatibles amb els requisits establerts, el sistema serà desactivat temporalment.

9. Gestió del canvi i adopció de la IA a l'Ajuntament

9.1. Formació i capacitat del personal

El pla de formació i capacitat del l'Ajuntament ha d'incorporar accions formatives específiques en matèria d'IA, adaptades a les necessitats dels diferents àmbits i departaments de l'entitat. L'objectiu és minimitzar els riscos derivats de l'ús indegut de sistemes d'IA i garantir una aplicació ètica, responsable i segura.

Caldrà identificar els col·lectius de l'organització que requereixen formació específica en l'ús de la IA i en els aspectes establerts per aquesta política.

A efectes de garantir el que disposa l'apartat anterior, les competències professionals que l'Ajuntament identifiqui s'han d'incorporar, en funció del perfil professional, als processos de selecció i provisió de personal.

El personal de nova incorporació haurà de rebre formació específica en IA seguint els criteris establerts en els apartats anteriors.

9.2. Comunicació i difusió interna

L'Ajuntament ha d'establir una estratègia de comunicació i difusió interna per garantir que tot el personal conegui la present política i les guies pràctiques corresponents i compregui l'abast i les implicacions de l'ús de la IA dins l'organització.

L'Ajuntament ha d'establir mecanismes per verificar que els treballadors han rebut i comprès aquesta informació, així com per resoldre possibles dubtes sobre la seva aplicació.

10. Publicitat i transparència

10.1. Transparència i accés a la informació

L'Ajuntament ha de garantir la transparència en l'ús de la IA en la seva gestió i presa de decisions, assegurant que la ciutadania i les persones afectades estiguin informades de manera clara i accessible sobre les actuacions automatitzades, quan estiguin interactuant amb un sistema d'IA, quan es generi contingut sintètic o quan s'utilitzin tecnologies de reconeixement d'emocions o categorització biomètrica; així com de les conseqüències associades i l'accés a l'espai on l'Ajuntament difon la relació d'actuacions.

S'informarà de manera explícita i comprensible a la ciutadania en qualsevol interacció on rebi informació o assistència per part d'un sistema d'IA. Això inclou, en particular:

- Actuacions administratives automatitzades definides a l'article 41 de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, en les quals hi pot haver algun element de presa de decisió que utilitzi IA.
- Actuacions que impliquin l'ús de sistemes d'IA, per oferir informació o assessorament a ciutadans o a tercers, sense que es generi una resolució o una actuació administrativa per part de l'Ajuntament.

La informació que ha de difondre l'Ajuntament es correspon amb una descripció del disseny i funcionament, les dades utilitzades en la configuració i entrenament, mecanismes de rendició de comptes i de transparència, recursos que procedeixen contra l'actuació i els informes periòdics previstos en aquesta política.

10.2. Explicabilitat

L'explicabilitat és un element clau per generar confiança en l'ús de la IA. Les decisions, recomanacions o resultats generats hauran de ser comprensibles, expressats en un llenguatge clar i adaptat a l'usuari, especialment quan puguin tenir un impacte rellevant sobre drets o interessos. Caldrà oferir explicacions transparents sobre el funcionament del sistema, els factors que han determinat la seva sortida i les dades utilitzades, afavorint així una supervisió humana significativa i la possibilitat d'impugnar resultats.

La transparència serà obligatòria, amb independència del nivell de risc, en els casos següents:

- Sistemes d'IA destinats a interactuar amb persones físiques: cal informar-les de manera explícita que estan interactuant amb un sistema d'IA.

- Sistemes que generin contingut sintètic (àudio, imatge, vídeo o text): s'hauran de marcar en un format llegible per màquina que permeti detectar que el contingut ha estat generat o manipulat artificialment.
- Sistemes de reconeixement d'emocions o categorització biomètrica: s'haurà d'informar les persones exposades sobre el funcionament del sistema.
- Sistemes que generin o manipulin imatges, àudio o vídeo constituint ultrafalsificacions, o continguts sobre assumptes d'interès públic: s'haurà d'indicar que el contingut ha estat generat o manipulat artificialment.

10.3. Publicitat dels sistemes d'IA

A més, l'Ajuntament publicarà de manera proactiva al Portal de Transparència la informació clau recollida al Registre municipal d'algoritmes i sistemes d'IA, que haurà d'incloure com a mínim:

- a) L'inventari actualitzat de sistemes d'IA utilitzats i la seva finalitat.
- b) L'impacte potencial i les implicacions en la presa de decisions administratives.
- c) Els criteris de funcionament, l'origen de les dades i els mètodes d'entrenament.
- d) Els biaixos detectats i les limitacions conegudes, així com els riscos associats.
- e) Els resultats d'avaluacions d'impacte i altres mecanismes de supervisió d'especial rellevància.

Tota aquesta informació s'expressarà en un llenguatge clar i entenedor, explicant el disseny, la lògica de funcionament i les dades utilitzades en el desenvolupament, entrenament i ús del sistema.

Finalment, es garantirà que qualsevol persona afectada per decisions, recomanacions o continguts generats per sistemes d'IA disposi de vies de reclamació clares, accessibles i adaptades al canal utilitzat per interactuar amb el sistema. Aquestes reclamacions hauran de ser ateses en un termini raonable, amb possibilitat de revisió i, si escau, correcció dels resultats.

10.4. Registre municipal d'algoritmes i sistemes d'intel·ligència artificial

Es crearà el Registre Municipal d'Algoritmes i Sistemes d'Intel·ligència Artificial que actuarà com a instrument centralitzat per a la gestió, seguiment i supervisió de tots els sistemes d'IA utilitzats per l'Ajuntament.

Aquest registre recollirà tant la informació necessària per al control intern i la gestió operativa, com aquella que, d'acord amb la normativa vigent, hagi de ser publicada al Portal de Transparència.

S'hi inscriuran obligatòriament totes les aplicacions, serveis i usos que incorporin funcionalitats d'IA, tant si han estat desenvolupats internament com adquirits a tercers. El registre inclourà, com a mínim, la informació següent:

Descripció general:

- Nom del sistema
- Estat
- Problemàtica que es vol resoldre
- Àmbit d'ús
- Beneficis esperats
- Data d'alta i baixa

Dades tècniques

- Tipus d'informació i dades
- Tipus algorisme utilitzat
- Consideracions sobre el tractament i conservació de les dades
- Responsables del desplegament
- Proveïdor

Riscos i seguretat

- Classificació del risc
- Gestió de riscos
- Supervisió humana
- És actuació administrativa automatitzada (AAA)
- Avaluació d'impacte sobre els drets fonamentals
- Avaluació ètica

Seguiment i millora

- Sistemes de monitoratge
- Mesures d'avaluació de la millora

Aquest registre es mantindrà permanentment actualitzat i serà la referència oficial per al seguiment de l'ús de la intel·ligència artificial dins la corporació municipal.

Annex 1. Classificació del nivell de risc del sistema

Seguint un enfocament basat en el risc potencial en l'ús de la IA, el RIA estableix majors restriccions i obligacions com més gran és el risc, distingir entre risc inacceptable, alt risc, risc limitat i mínim risc:

RISC INNACCEPTABLE

Des del 2 de febrer de 2025, ja és d'aplicació l'article 5 del RIA, que estableix les pràctiques d'IA prohibides per considerar-se el risc inacceptable. En concret:

- a) L'ús de tècniques subliminals, manipuladores o enganyoses per distorsionar el comportament d'una persona o un grup de persones, fent-los prendre una decisió que altrament no haurien pres, d'una manera que probablement els causi un perjudici considerable.
- b) L'explotació de les vulnerabilitats d'una persona física o un grup de persones derivades de l'edat o la discapacitat, o d'una situació social o econòmica, amb la finalitat o l'efecte d'alterar-ne substancialment el comportament amb una probabilitat raonable de causar-los perjudicis considerables.
- c) Puntuació ciutadana (*social scoring*) – Sistemes d'IA per a l'avaluació o classificació de persones físiques o grups de persones durant un període determinat en funció del seu comportament social o les seves característiques personals, que poden donar lloc a un tracte perjudicial o desfavorable en contextos socials no relacionats amb aquells en què es van demanar les dades, o a un tracte injustificat o desproporcionat.
- d) Sistemes d'IA per avaluar o predir el risc que una persona física cometi un delictes, basant-se únicament en el perfil o els trets de personalitat.
- e) Sistemes d'IA que creïn o amplii bases de dades de reconeixement facial mitjançant l'extracció no selectiva d'imatges facials d'internet o circuits tancats de televisió.
- f) Sistemes d'IA per inferir les emocions d'una persona física als llocs de treball i als centres educatius, excepte quan el seu ús estigui destinat a fins mèdics o de seguretat.
- g) Sistemes d'IA de categorització biomètrica que classifiquen individualment les persones físiques basant-se en les dades biomètriques per deduir o inferir determinades dades sensibles.
- h) Sistemes d'identificació biomètrica remota en temps real en espais d'accés públic amb fins de garantia del compliment de la llei, amb certes excepcions subjectes a condicions i garanties.

RISC ALT

Sistemes que plantegen un risc significatiu de dany per a la salut, la seguretat o els drets fonamentals (article 6 RIA). En aquest cas, s'estableixen un conjunt d'obligacions que caldrà tenir presents en tot moment, en particular pel que fa a la traçabilitat i explicabilitat adequades, garantint que la ciutadania en té el control i és conscient que està interactuant amb un sistema d'IA.

RISC LIMITAT

El *Considerant 53* del RIA es refereix a casos específics en què els sistemes d'IA no comporten un risc considerable de causar un perjudici als interessos jurídics, ja que no influeixen en la presa de decisions o no perjudiquen aquests interessos substancialment. Es tracta doncs d'un sistema d'IA que no afecta el fons —ni consegüentment al resultat— de la presa de decisions, ja sigui humana o automatitzada; sempre que es compleixin determinades condicions.

Alguns exemples poden ser:

- sistemes d'IA que transformen dades no estructurades en dades estructurades;
- que classifiquen en categories els documents rebuts;
- que detecten duplicats;
- que milloren el llenguatge utilitzat en documents;
- la indexació, la cerca, el tractament de text i de la parla;
- la vinculació de dades a altres fonts de dades;
- o bé els sistemes d'IA utilitzats per a la traducció de documents.

En aquests casos, també s'ha de garantir la traçabilitat i la transparència, i els proveïdors han d'elaborar la documentació de l'avaluació prèviament a la introducció al mercat o l'entrada en servei del sistema IA esmentat i facilitar-la a les autoritats nacionals competents quan aquestes ho sol·licitin. Igualment, els proveïdors tenen l'obligació de registrar el sistema a la base de dades de la UE.

RISC MÍNIM

Tots els altres sistemes d'IA poden desenvolupar-se i utilitzar-se conforme a la legislació vigent sense obligacions addicionals. Els proveïdors d'aquests sistemes poden optar voluntàriament per aplicar les directrius per a una IA digna de confiança i adherir-se a codis de conducta voluntaris.

Annex 2. Fitxa d'autorització d'ús d'eines basades en IA

1. Informació General

1	Nom del treballador/treballadora	
2	Àrea responsable	
3	Data (en què es preveu utilitzar l'eina d'IA)	
4	Nom de l'eina basada en IA proposada	
5	Descripció de l'eina	

2. Descripció de les necessitats i objectiu de l'ús del sistema

6	Tipus d'iniciativa	<i>Especificar si es tracta d'una prova pilot, d'una prova de concepte o d'una posada en marxa definitiva del sistema.</i>
7	Necessitats i finalitat específica de l'ús de l'eina	<i>Descriure les necessitats que motiven la proposta i l'ús previst del sistema, especificant la finalitat perseguida.</i>
8	Beneficis esperats	<i>Descriure els beneficis esperats (funcions i utilitats) amb la implementació del sistema (per exemple, reducció de tràmits o automatització de tasques repetitives).</i>

3. Impacte en els drets i llibertats de la ciutadania

9	Impacte directe previst en el ciutadà	<i>Especificar si l'ús del sistema tindrà un impacte directe en el ciutadà i en què consistirà. Per exemple, l'eina d'IA interactuarà directament amb el ciutadà?</i>
10	S'utilitzarà el sistema d'IA per a la presa de decisions administratives? Com s'integrarà en els processos de treball intern?	<i>Especificar si el sistema d'IA s'utilitzarà per a la presa de decisions administratives i com s'integrarà en els processos de treball intern de l'Ajuntament, indicant el nivell d'accessorietat previst de sistema d'IA. Es tracta d'analitzar l'impacte en la presa de decisions administratives i integració en processos de treball interns.</i>
11	En el cas que SÍ, hi ha supervisió humana abans de la presa d'aquesta decisió?	<i>Descriure les mesures de revisió i supervisió humanes previstes per l'Ajuntament i la possibilitat de modificar o revertir els resultats de la decisió presa per l'algorisme.</i>
12	L'ús del sistema d'IA té algun impacte en els drets i llibertats de la ciutadania? ☐ SÍ ☐ NO ☐ NSNC En cas afirmatiu, quins?	<i>El RIA fa molt d'èmfasi en el respecte absolut dels drets fonamentals i llibertats reconeguts a la Carta Europea. Es tracta de reflexionar prèviament a l'ús d'aquesta tecnologia sobre el possible impacte. Per a més informació, es pot consultar la metodologia publicada per l'APDCAT. Si no es coneix el possible impacte, es pot marcar NSNC.</i>

4. Protecció de dades personals

13	Tipus de dades personals tractades: ☐ Dades identificatives	<i>Indicar els tipus de dades personals identificades a les quals tindrà accés el</i>
----	---	---

	☐ Dades especialment protegides (ideologia, afiliació sindical, religió o creences, origen racial, dades de salut, vida sexual, genètiques i biomètriques, comissió d'infraccions penals o administratives) ☐ Altres (especificar)	<i>sistema d'IA. Alguns exemples de dades especialment protegides són: dades mèdiques i de salut, afiliació sindical, dades genètiques o relatives a l'orientació sexual. Alguns exemples d'altres dades són: dades econòmiques i financeres, ocupació professional, estat civil, edat, dades de contacte).</i>
14	Base jurídica per al tractament de dades ☐ Consentiment ☐ Execució d'un contracte ☐ Obligació legal ☐ Interès públic ☐ Interès legítim	<i>Per donar compliment al 'article 6 del Reglament General de Protecció de Dades, que parla de la licitud del tractament de les dades.</i>
15	Es preveuen mesures tècniques i organitzatives de control previ? ☐ SÍ ☐ NO Si és que SÍ, descripció de les mesures adoptades	<i>Descriure les mesures de control i supervisió prèvies previstes per l'Ajuntament (per exemple, proves del sistema, formació als usuaris sobre els usos de la IA)</i>
16	S'ha fet o es té prevista fer formació i capacitatció de l'usuari en l'ús d'aquesta eina? ☐ SÍ ☐ NO	<i>Marcar nomes SÍ o NO.</i>

