



POLÍTICA DE SEURETAT DE LA INFORMACIÓ I DE DADES PERSONALS

- 1. *Introducció***
 - 1.1 Abast**
 - 1.2 Àmbit la política**
 - 1.3 Missió**
 - 1.4 Aprovació i entrada en vigor**

- 2. *Marc legislatiu***

- 3. *Principis de compliment de la política de seguretat***
 - 3.1 Dades personals**
 - 3.2 Gestió de riscos**
 - 3.3 Prevenció i reacció davant incidències**
 - 3.3.1 Prevenció**
 - 3.3.2 Detecció**
 - 3.3.3 Resposta**
 - 3.3.4 Recuperació**

- 4. *Dades personals***
 - 4.1 Protocols per a la creació, modificació i supressió de tractaments**
 - 4.2 Principis de protecció de dades**
 - 4.3 Drets dels interessats**
 - 4.4 Aplicació del principi de responsabilitat proactiva i demostrable**

- 5. *Organització de la seguretat***
 - 5.1 Funcions i responsabilitats**
 - 5.2 Procediments de designació**

- 6. *Obligacions del personal***

- 7. *Terceres parts***

- 8. *Gestió i desenvolupament de la política de seguretat de la informació***
 - 8.1 Revisió de la política de seguretat de la informació**
 - 8.2 Revisió de la política de seguretat de la informació**

- 9. *Glossari***

1. Introducció

El present document respon a la necessitat de l'Ajuntament de Montmeló de complir amb els requisits expressats en la legislació de protecció de dades i serveis per mitjans electrònics.

La finalitat de la present **Política de Seguretat de les dades personals i de la Informació** és la definició dels components i els processos necessaris per complir amb la legislació vigent en l'àmbit de la seguretat de les Dades de Personals (Reglament (UE) 2016/679 del Parlament 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- RGPD i la Llei Orgànica 3/2018, de 5 de desembre de Protecció de Dades Personals i Garantia dels Drets Digitals) i serveis per mitjans electrònics (Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat, modificat pel RD 951/2015 de 23 d'octubre - ENS). Així mateix aquest document també té com a finalitat la recopilació de totes les referències als principals requisits de protecció dels mitjans físics que continguin Dades Personals, serveis i informació responsabilitat de l'Ajuntament.

D'aquesta manera, el seu propòsit és el foment de la millora ens els processos desenvolupats a l'entitat de forma que es garanteixin els principis bàsics que han de regir qualsevol tractament de dades especialment el principi de privacitat en el disseny, responsabilitat proactiva i garantir una gestió adient dels riscos associats als tractaments de dades personals.

L'Ajuntament de Montmeló com a Administració Pública al servei de la ciutadania disposa d'una infraestructura de Tecnologies d'Informació i Comunicacions (TIC) per a desenvolupar les seves competències i assolir els seus objectius.

La gestió de la documentació i de les TIC ha de ser portada a terme aplicant les mesures necessàries que li permetin garantir la protecció davant de les possibles incidències (accidentals o deliberades) que es puguin produir, de forma que es puguin minimitzar les afectacions sobre la disponibilitat, integritat o confidencialitat de la informació relacionada amb els serveis prestats i les dades personals.

La qualitat de la informació i la prestació continuada de serveis hauran de ser garantits actuant de forma preventiva, mitjançant una adequada supervisió periòdica i constant, tenint com a objectiu final la seguretat de la informació com a cultura general a l'entitat.

D'acord amb allò que s'estableix a l'article 11.1 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (ENS) i la legislació vigent en matèria de protecció de dades, la política de seguretat ha de ser aprovada pel titular de l'òrgan superior corresponent i s'ha de desenvolupar aplicant els requisits mínims següents:

- a) Organització i implantació del procés de seguretat.
- b) Avaluació d'Impacte
- c) Anàlisi i gestió dels riscos.
- d) Gestió de personal.
- e) Professionalitat i deure de secret
- f) Protocols per a la creació, modificació i supressió de tractaments
- g) Drets dels interessats
- h) Autorització i control dels accessos.
- i) Protecció de les instal·lacions.
- j) Adquisició de productes.
- k) Seguretat per defecte.
- l) Integritat i actualització del sistema.
- m) Protecció de la informació emmagatzemada i en trànsit.
- n) Prevenció davant altres sistemes d'informació interconnectats.
- o) Registre d'activitat.
- p) Incidents de seguretat.
- q) Continuitat de l'activitat.
- r) Millora contínua del procés de seguretat.

Així mateix, l'article 11.2 de l'ENS indica que, als efectes que indica l'apartat anterior, es consideren òrgans superiors els responsables directes de l'execució de l'acció del Govern, central, autonòmic o local, en un sector d'activitat específic, d'acord amb el que estableix la Llei 6/1997, de 14 d'abril, d'organització i funcionament de l'Administració General de l'Estat, i la Llei 50/1997, de 27 de novembre, del Govern; els estatuts d'autonomia corresponents i normes de desplegament; i la Llei 7/1985, de 2 d'abril, reguladora de les bases del règim local, respectivament.

La present **Política de Seguretat de les dades personals i de la Informació** defineix el marc tècnic, organitzatiu i jurídic que ha de complir tot el personal de l'Ajuntament de Montmeló.

1.1 Abast

L'Ajuntament de Montmeló és una Administració Pública que està composta i organitzada en diferents àrees i serveis administratius orientats per al desenvolupament de la seva activitat.

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions,...), sistemes d'informació i tractaments de dades personals de l'Ajuntament de Montmeló, sense excepcions.

La Política de Seguretat afecta les polítiques, les estructures organitzatives, les responsabilitats, els procediments, els processos i els recursos emprats per l'Ajuntament de Montmeló.

1.2 Àmbit la política

La present **Política de Seguretat** s'aplicarà a tots els tractaments de dades personals i serveis TIC que siguin responsabilitat de l'Ajuntament de Montmeló.

Els tractaments amb Dades Personals estan detallats al document denominat al **REGISTRE D'ACTIVITATS DE TRACTAMENT**.

Els serveis àmbit de l'Esquema Nacional de Seguretat estan detallats a la classificació d'actius de l'**Anàlisi de Riscos de l'Ajuntament**.

Aquesta **Política de Seguretat de les dades personals i de la Informació** contempla les normes organitzatives i tècniques establertes a l'entitat, i és d'obligat compliment per a tot el personal de l'Ajuntament de Montmeló.

Les normes internes contingudes en el present document s'han de posar en coneixement del personal de l'Ajuntament de Montmeló, amb l'objectiu de garantir el correcte coneixement d'aquesta política per part de tot el personal.

1.3 Missió

Mitjançant la present Política de Seguretat l'Ajuntament de Montmeló expressa el seu compromís amb l'administració de la seguretat de la seva informació, d'acord amb els requeriments propis, així com amb les lleis i normatives vigents.

1.4 Aprovació i entrada en vigor

Aquesta política de seguretat de la Informació és efectiva des de la data d'aprovació mitjançant Junta de Govern, fins que sigui reemplaçada per una nova política.

2. Marc legislatiu

L'ús de les TIC i les dades personals per part de l'Ajuntament de Montmeló es troba regulat per les següents normes jurídiques:

ESTATAL

- Reglament (UE) 2016/679 del Parlament 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 (RGPD).
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals (LOPDGDD)
- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Reial decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat, modificat pel RD 951/2015 de 23 d'octubre.
- Reial decret 951/2015, de 23 d'octubre, de modificació del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica.
- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Reial decret 1671/2009, de 6 de novembre, pel que es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic.
- Instruccions del Centre Criptogràfic Nacional, CCN-STIC.

AUTONÒMICA

- Llei 26/2010, de 3 d'agost, de règim jurídic i de procediment de les administracions públiques de Catalunya.
- Llei 29/2010, de 3 d'agost, d'ús dels mitjans electrònics al sector públic de Catalunya.

3. Principis de compliment de la política de seguretat

Les TIC utilitzades per l'Ajuntament de Montmeló per donar suport als serveis i tractament de dades personals han de disposar d'elements que en garanteixin una protecció adient contra amenaces que, degut a la seva constant evolució, tenen un gran potencial per a produir afectacions en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació, les dades personals i els serveis.

Amb l'objectiu de disposar d'elements per a la defensa d'aquestes amenaces, l'Ajuntament necessita disposar d'una estratègia que s'adapti als canvis constants que es produeixen a l'entorn per garantir la prestació contínua dels serveis. Això implica que l'Ajuntament ha d'aplicar les mesures mínimes de seguretat exigides pel Reial decret 3/2010, de 8 de gener, que regula l'ENS, i les derivades de l'avaluació d'impacte sobre els tractaments de dades així com realitzar un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Les àrees funcionals de l'Ajuntament de Montmeló han de garantir que la seguretat TIC esdevingui un element integral del sistema, des del seu disseny inicial fins a la retirada de servei, passant per les decisions de desenvolupament o adquisició de programari i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació de l'àrea, en la sol·licitud de propostes de serveis, i en la elaboració dels plecs per a la licitació de projectes relacionats amb les TIC.

Els procediments i normatives aplicables als sistemes informàtics i organització es recull als *Procediments tècnics TIC*.

3.1 Gestió de riscos

Tots els sistemes d'informació i tractaments de dades subjectes a aquesta política hauran de ser objecte d'una anàlisi de riscos, on s'avaluïn les amenaces i els riscos a què estan exposats.

Aquesta anàlisi es portarà quan es produeixin les següents circumstàncies:

- Regularment, almenys un cop l'any.
- Quan es produeixin canvis en la informació tractada.
- Quan es produeixin canvis en els serveis prestats.
- Quan es detecti una incidència de seguretat greu.
- Quan es detectin vulnerabilitats greus.
- Quan es determini un nou tractament de dades personals que requereix un Avaluació d'Impacte.

Per a l'harmonització dels anàlisis de riscos, la Comissió de Seguretat establirà una valoració de referència per als diferents tipus d'informació tractats i els diferents serveis prestats. La Comissió de Seguretat dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat, promovent inversions de caràcter horitzontal.

El procediment per desenvolupar l'anàlisi de riscos es pot trobar als Procediments Tècnics RGPD de l'Ajuntament de Montmeló.

3.2 Prevenció i reacció davant incidències

El Personal de l'Ajuntament de Montmeló han d'estar preparats per a la prevenció, detecció, reacció i recuperació davant de possibles incidents, d'acord amb l'article 7 de l'ENS, i l'article 33 de l'RGPD si afecta dades personals.

3.2.1 Prevenció

El Personal de l'Ajuntament de Montmeló han d'evitar, o almenys prevenir en la mesura del possible, que la informació, les dades personals o els serveis es vegin perjudicats per incidents de seguretat. Per això, les àrees han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat del personal, estaran definits i documentats.

Per garantir el compliment de la política, els responsables funcionals de cada àmbit han de:

- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent avaluacions dels canvis de configuració
- Demanar la revisió periòdica per part de tercers amb la finalitat d'obtenir una avaluació independent.

3.2.2 Detecció

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració fins a la seva detenció, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies en els

nivells de prestació dels serveis i actuar en conseqüència segons el que estableix l'article 9 de l'ENS i donar compliment a les exigències de l'article 33 de l'RGPD si afecta dades personals.

El monitoratge és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i informe que arribin als responsables regularment i quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com normals.

3.2.3 Resposta

L'Ajuntament de Montmeló per donar resposta als incidents ha definit un procediment que estableix:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres àrees o en altres organismes.
- Establir protocols per l'intercanvi d'informació relacionada amb l'incident; inclouen comunicacions amb l'Equip de Resposta d'Incidents del Centre de Seguretat de la Informació de Catalunya (CESICAT-CERT) o organisme competent.

3.2.4 Recuperació

Per garantir la disponibilitat dels serveis crítics, les àrees de l'Ajuntament de Montmeló han de desenvolupar plans de continuïtat dels sistemes TIC com a part del seu pla general de continuïtat de negoci i activitats de recuperació.

4. Dades personals

L'Ajuntament de Montmeló, en el desenvolupament de les seves competències, tracta dades personals de ciutadans, personal, contribuents i tercers. El Registre d'Activitats de Tractament - que es pot trobar al Portal de Transparència a disposició dels interessats - recull la relació de tractaments de dades existents amb la identificació dels responsables corresponents i les mesures aplicades.

Els sistemes d'informació i documents de l'Ajuntament de Montmeló han d'aplicar les mesures de seguretat adients per garantir la seva confidencialitat i integritat.

Els procediments aplicats sobre el tractament de dades personals estan definits en la present política a continuació i desenvolupades amb procediments recollits als **Procediments RGPD**.

4.1 Protocols per a la creació, modificació i supressió de tractaments

Es considera tractament qualsevol conjunt organitzat de Dades Personals que siguin objecte d'un processament a una entitat, independentment de la forma o modalitat de la seva creació, emmagatzematge, organització i accés.

Al document **Registre d'Activitats de Tractaments** es relacionen tots el tractaments que han estat identificats per cadascun dels diferents àmbits de responsabilitat de L'Ajuntament de Montmeló.

Aquest document conté, a més, les estructures dels tractaments que han estat inventariats a L'Ajuntament de Montmeló.

L'Ajuntament de Montmeló ha definit un procediment denominat Gestió del Registre d'Activitats de Tractament on es descriu la metodologia a seguir per a la gestió i actualització del Registre d'Activitats de Tractament.

Aquest procediment es pot trobar als Procediments Tècnics RGPD de L'Ajuntament de Montmeló.

4.2 Principis de protecció de dades

Els tractaments de dades personals desenvolupats a L'Ajuntament de Montmeló es regiran pels següents principis:

- Licitud, lleialtat i transparència, en relació a portar a terme un tractament lícit, lleial i transparent respecte a l'interessat i que aquest conegui de forma precisa quins usos donarem a les seves dades personals.
- Limitació de les finalitats, en relació als usos que es donaran als tractaments de dades personals.
- Minimització de dades, de forma que es portin a terme tractaments de dades proporcionals a les finalitats que n'hagin motivat la seva creació.
- Exactitud, de forma que s'habilitin els mecanismes d'actualització necessaris per tal de garantir que reflecteixin informació precisa sobre l'interessat.
- Limitació de terminis de conservació, garantint que les dades es conservin únicament els terminis que defineixi la normativa reguladora de cada tractament.
- Integritat i confidencialitat, de forma que s'estableixin aquelles mesures que siguin necessàries per tal de garantir que no es produeixin accessos no autoritzats i s'eviti la pèrdua d'informació.
- Responsabilitat proactiva i demostrable, realitzant aquelles accions que siguin necessàries per al compliment dels principis anteriors i documentant totes les accions portades a terme.

4.3 Drets dels interessats

El dret dels interessats són personals i seran exercits per l'afectat enfront de l'Ajuntament en tant que **Responsable de Tractament**. Per a aquest fi, serà necessari que l'afectat acrediti la seva identitat.

Podrà, no obstant això, actuar el representant legal de l'interessat quan aquest es trobi en situació de discapacitat o minoria d'edat que li impossibiliti l'exercici personal dels seus drets. En aquest cas serà necessari que el representant legal acrediti aquesta condició.

L'Ajuntament de Montmeló ha definit un procediment denominat Gestió dels drets de l'interessat on es descriu la metodologia per a gestionar cada un dels drets que la legislació reconeix als interessats.

Aquest procediment es pot trobar als Procediments Tècnics RGPD de l'Ajuntament de Montmeló.

4.4 Aplicació del principi de responsabilitat proactiva i demostrable

El Principi de Responsabilitat Proactiva i Demostrable recull el compromís efectiu amb els drets i llibertats de les persones per part de l'Ajuntament de Montmeló, de manera que es garanteixi que totes les accions que es portin a terme respecte als tractaments de dades personals aniran sempre encaminades a complir de la forma més efectiva possible les obligacions establertes per la legislació.

Les accions que es portaran a terme seran les següents:

- Accions orientades a la protecció de dades en el disseny, de forma que es garanteixi que davant d'un nou tractament de dades personals s'hagi tingut en compte els principis de la legislació de protecció de dades.
- Avaluacions d'impacte sobre dades personals, tenint en compte l'impacte que els tractaments de dades puguin tenir a l'organització des de les dimensions tècniques, organitzatives i jurídiques.
- Anàlisi i gestió dels riscos associats als tractaments de dades personals.
- Creació d'un Registre d'Activitats de Tractament on L'Ajuntament de Montmeló identificarà tots els tractaments de dades que porti a terme en el desenvolupament de la seva activitat.

Per tal de garantir la realització de les accions descrites i la seva constància documental a efectes de requeriments per part dels Supervisors, l'Ajuntament de Montmeló designarà un Delegat de Protecció de Dades.

5. Organització de la seguretat

5.1 Funcions i responsabilitats

L'organització de la seguretat de l'Ajuntament de Montmeló, es concreta en una Comissió de Seguretat.

Els rols i les funcions de l'organització de la seguretat establerts a l'Esquema Nacional de Seguretat seran assumits per la Comissió de Seguretat i el rol d'Administrador de seguretat del sistema que serà assumit pel Responsable d'Informàtica.

Les Responsabilitats dels Òrgans de Direcció de L'Ajuntament de Montmeló respecte al compliment de la legislació són:

1. Nomenar els membres de la **Comissió de Seguretat** encarregats de coordinar i controlar les mesures definides en a la present Política **de Seguretat**.
2. Nomenar el **Delegat de Protecció de Dades**.
3. Nomenar el **Responsable de Seguretat ENS**, tasca assumida per la **Comissió de Seguretat**.
4. Nomenar el **Responsable de Sistemes**, tasca assumida pel Director de Sistemes d'informació.
5. Donar el suport i dotar dels recursos necessaris a la **Comissió de Seguretat** i al Delegat de Protecció de Dades per a poder portar a terme les seves funcions.

La Organització per a la gestió de la protecció de dades i seguretat de la informació és:

Comissió de Seguretat

Responsable	Comissió de Seguretat
Composició	President/a Secretari/a Quatre Vocals entre els quals haurà d'estar el responsable de seguretat i el responsable de sistema
Funcionament	<ul style="list-style-type: none">• 1 reunió trimestral, amb caràcter ordinari• Extraordinàriament, aquesta Comissió es reuniria per tractar temes urgents i/o de necessitat
Funcions de la Secretària	<ul style="list-style-type: none">• <i>Convocatòria de les reunions ordinàries i extraordinàries.</i>• <i>Elaborar actes de les reunions ordinàries i extraordinàries</i>• <i>Elaborar informes, instruccions, circulars, enviar comunicacions, etc.</i>• <i>Gestió administrativa de la documentació emesa per la Comissió de Seguretat.</i>
Relació amb la les dades personals	La Comissió de Seguretat implanta les mesures per a la protecció de les dades i dona suport al DPD
Funcions	1. Establir les polítiques de seguretat a l'Ajuntament.

	<ol style="list-style-type: none"> 2. Validar i aprovar la documentació relacionada amb la seguretat de la informació i les dades personals. 3. Impulsar les polítiques de seguretat a l'Ajuntament. 4. Validar la documentació de seguretat i el Registre d'Activitats de Tractament per a la seva aprovació per part del Responsable de Tractament, l'Ajuntament. 5. Aprovar l'anàlisi i gestió de riscos en el sistema i assignar els recursos necessaris. 6. Analitzar semestralment la situació de l'Ajuntament i validar i aprovar la planificació a portar a terme en cada període. 7. Aprovar els resultats de les auditories de seguretat de la informació i dades personals. 8. Establir plans de formació, conscienciació i divulgació de les normes, les obligacions i els procediments de seguretat a l'Ajuntament. 9. Establir les accions a aplicar en cas d'incompliment de la normativa estipulada pels usuaris de l'Ajuntament. 10. Prestar col·laboració amb el Responsable de Seguretat, el Responsable del Sistema i el Delegat de Protecció de Dades en tot allò que requereixi per tal de facilitar el desenvolupament de les seves funcions.
--	---

Responsable	Responsable de Seguretat
Funcions delegades	<ol style="list-style-type: none"> 1. Definir i proposar a la Comissió de Seguretat la documentació relacionada amb la seguretat de la informació i les dades personals. 2. Garantir l'aplicació i el compliment de la Política, normativa, procediments i instruccions de Seguretat de la informació i dades personals. 3. Dur a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema. 4. Investigar i fer el seguiment dels incidents de seguretat que hagin ocorregut 5. Avaluar els informes emesos en relació als controls, les anomalies i les deficiències que, en matèria de seguretat, es detectin, i proposar al Responsable del Tractament les mesures que cal implantar. 6. Redactar les normes internes corresponents als usuaris. 7. Promoure les auditories i controls regulars que permetin verificar el compliment de les obligacions de l'Ajuntament en seguretat de la informació i dades personals. 8. Adoptar o proposar l'adopció de les mesures correctores adequades en funció de l'anàlisi dels informes realitzats pels Administradors de Seguretat. 9. L'anàlisi de riscos i l'aplicació de les mesures tècniques i organitzatives es farà amb la implicació i la responsabilitat de les àrees afectades.

Responsable	Responsable del Sistema
Funcions delegades	<ol style="list-style-type: none"> 1. Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa. 2. Assegurar que els controls de seguretat establerts són complerts estrictament. 3. Assegurar que són aplicats els procediments aprovats per maneig del sistema. 4. Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta. 5. Establir procediments de seguiment i reacció davant alarmes i situacions imprevistes. 6. La gestió, configuració i actualització, si s'escau, del maquinari i programari en què es basen els mecanismes i serveis de seguretat del sistema. 7. Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema. 8. Donar d'alta nous rols d'accés als programes, aplicacions corporatives.

Responsable	Delegat de Protecció de Dades
Funcions delegades	<ol style="list-style-type: none"> 1. Supervisió del compliment del RGPD a l'Ajuntament. 2. Assessorar el conjunt de l'organització sobre qualsevol aspecte relacionat amb el compliment de la normativa de protecció de dades: aplicació de mesures tècniques, definició de textos legals, ... 3. Registre d'Activitats de Tractament: <ul style="list-style-type: none"> · Determinar les activitats de tractament i mantenir actualitzat el Registre d'Activitats de Tractament.. · Analitzar i comprovar la conformitat amb la normativa de les activitats. · Informar i assessorar el responsable o l'encarregat del tractament. 4. Anàlisi d'impacte: <ul style="list-style-type: none"> · Assessorar i aprovar l'avaluació d'impacte relativa a la protecció de dades. · Determinar la metodologia a emprar en l'Anàlisi d'Impacte, si cal realitzar-se internament o externament. · Establir les salvaguardes jurídiques, tècniques i organitzatives segons els resultats del mateix.. · Si l'avaluació s'ha dut a terme correctament o no i si les seves conclusions són conformes amb el RGPD. 5. Resolució i resposta als interessats que exerceixin els seus drets davant l'Ajuntament. 6. Formar i informar el personal de l'organització sobre les seves tasques i obligacions en el tractament de dades personals. 7. Enfocament basat en el risc: assessorar, assumir la realització i supervisió d'Auditories d'interne o coordinació d'auditories externes, formació, determinar quins recursos es deuen destinar a quines operacions de tractament, etc. 8. Elaborar i mantenir actualitzats aquells procediments i normatives internes que siguin necessàries per a garantir el correcte compliment de la legislació. 9. Exercitar com a interlocutor del Responsable de Tractament davant els interessats (gestió de sol·licituds de drets) així com davant l'Organisme Regulador. 10. Cooperació amb l'autoritat de control i actuació com a punt de contacte davant els interessats. 11. Assistir a les reunions de la Comissió de Seguretat així com a les convocatòries realitzades per la més alta autoritat de l'Ajuntament. <p>Així com a totes les funcions que quedin determinades per la legislació.</p>

Responsable	Responsables Funcionals / Responsables de Serveis
Funcions delegades	<ol style="list-style-type: none"> 1. Definir els serveis necessaris per portar a terme les competències de l'Ajuntament. 2. Vetllar pel compliment de les polítiques i normes de seguretat determinades per l'Ajuntament en el tractament dels fitxers de l'àmbit de responsabilitat. 3. Implementar totes les mesures de seguretat definides a la documentació de seguretat per a fitxers no automatitzats (arxiu i emmagatzematge de documentació). 4. Definir els perfils i criteris d'accés a la documentació i aplicacions informàtiques sota l'àmbit de responsabilitat. 5. Concedir o denegar l'autorització d'accés als usuaris a les dades personals sota el seu àmbit de responsabilitat. 6. Descriure l'estructura dels sistemes i de dades del fitxer i notificar a la Comissió de Seguretat qualsevol modificació que es produeixi. 7. Aplicació de llegendes sobre els formularis de recollida de dades. 8. Informar a la Comissió respecte a les demandes de cessió de dades per part de Tercers. 9. Garantir que els contractes de serveis comptin amb clàusules de confidencialitat.

5.2 Procediments de designació

El responsable de Seguretat i el Delegat de Protecció de Dades serà nomenat per Decret d'Alcaldia o Junta de Govern de local. El nomenament s'ha de revisar cada 2 anys o quan el lloc quedi vacant.

Si un servei es desenvolupa fora de l'àmbit competencial del servei TIC, l'àrea responsable del servei que es presti electrònicament haurà de designar el Responsable del Sistema, prèvia autorització i validació expressa de la Comissió de Seguretat.

6. Obligacions del personal

Tots els membres de l'Ajuntament de Montmeló tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat de la Comissió de Seguretat disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'Ajuntament de Montmeló atendran a una sessió de conscienciació en matèria de seguretat TIC i de protecció de dades personals com a mínim un cop l'any. S'establirà un programa de conscienciació contínua per atendre tots els membres de l'Ajuntament de Montmeló, en particular als de nova incorporació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al tractament segur dels sistemes en la mesura que la necessitin per realitzar-la. La formació és obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

La Normativa de Seguretat que defineix les obligacions del personal es troben recollides al Manual d'usuari dels sistemes d'informació.

7. Terceres parts

7.1 Serveis que presten altres entitats (Encarregats de tractament).

Quan l'Ajuntament de Montmeló utilitzi serveis de tercers o cedeixi informació a tercers, hauran d'acomplir amb els principis i mesures de seguretat definides per l'Ajuntament.

En el supòsit que aquestes entitats tractin dades personals seran considerades Encarregats de Tractament.

Aquests tercers quedaran subjectes a les obligacions establertes en aquesta normativa i hauran d'aplicar els principis i mesures tècniques definides per l'Ajuntament, especialment s'establiran procediments específics d'informe i resolució d'incidències.

En el cas que l'entitat apliqui altres mesures diferents de les establertes, es requerirà un informe del Responsable de Seguretat (Comissió de Seguretat) amb l'assessorament del Delegat de Protecció de Dades que precisi els riscos en què s'incorre i la forma de tractar-lo. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

7.2 Serveis prestats a tercers parts

Quan l'Ajuntament presti serveis o tracti informació o dades personals d'altres entitats haurà d'aplicar les mesures de seguretat requerides en quant al tractament de les dades i la informació, establint canals per informe i coordinació dels respectius òrgans i interlocutors de Seguretat i procediments d'actuació per a la reacció davant incidents de seguretat.

En el cas que aquestes entitats requereixin altres mesures addicionals diferents de les definides a aquesta Política de Seguretat de la Informació haurà de ser comunicat a l'Ajuntament per a avaluar la idoneïtat d'aplicar aquestes mesures addicionals o bé comunicar a aquestes entitats que l'Ajuntament no està en disposició de realitzar el tractament de la informació i les dades personals a fi i efecte que les entitats tercers prenguin les opcions i alternatives alienes per al tractament.

8. Gestió i desenvolupament de la política de seguretat de la informació

Aquesta política s'ha de desenvolupar per mitjà de normativa de seguretat que afronti aspectes específics. La normativa de seguretat estarà a disposició de tots els membres de l'organització que necessitin conèixer-la, en particular per aquells que utilitzin, operin o administrin els sistemes d'informació i comunicacions.

La normativa de seguretat estarà disponible a la xarxa corporativa, d'accés al personal de l'Ajuntament.

8.1 Revisió de la política de seguretat de la informació

Serà missió de la Comissió de Seguretat la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. La política serà aprovada per Decret d'Alcaldia o Junta de Govern local i difosa perquè la coneguin totes les parts afectades.

8.2 Revisió de la política de seguretat de la informació

Per verificar que s'acompleix amb tot allò que queda establert en aquesta **Política de Seguretat**, es realitzaran els controls interns que determini el Delegat de Protecció de Dades, en el referent a dades personals, i el Responsable de Seguretat, en el referent als sistemes informàtics.

La periodicitat d'aquests controls serà definida també per aquestes figures, existint també la possibilitat de portar a terme altres controls que pugui determinar en funció del desenvolupament de les operacions.

L'objectiu de les auditories serà el de verificar la possibilitat que els controls establerts a través de les mesures de seguretat siguin efectius; i que sigui possible garantir la integritat, la confidencialitat i la disponibilitat de les Dades Personals i els serveis TIC.

Serà missió de la Comissió la revisió anual d'aquesta Política de Seguretat de la Informació i la proposta de revisió o manteniment de la mateixa. Les modificacions a la Política de Seguretat seran aprovades per Decret de l'Alcaldia o Junta de Govern Local i difoses pel seu coneixement a tota l'organització.

9. Glossari

Anàlisi de riscos: Utilització sistemàtica de la informació disponible per a identificar perills i estimar els riscos.

Dades personals: Qualsevol informació concernent a persones físiques identificades o identificables.

Gestió d'incidents: Pla d'acció per atendre les incidències que es donin. A més de resoldre-les ha d'incorporar mesures d'acompliment que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos: Activitats coordinades per dirigir i controlar una organització pel que fa als riscos.

Incident de seguretat: Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació.

Política de seguretat: Conjunt de directrius plasmades en document escrit, que regeixen la forma en que una organització gestiona i protegeix la informació i els serveis que considera crítics.

Principis bàsics de seguretat: Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Responsable de la informació: Persona que té la potestat d'establir els requisits d'una informació en matèria de seguretat.

Responsable de la seguretat: El responsable de seguretat ha de determinar les decisions per satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei: Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema: Persona que s'encarrega de l'explotació del sistema d'informació.

Servei: Funció o prestació exercida per alguna entitat oficial destinat a tenir cura interessos o satisfer necessitats dels ciutadans.

Sistema d'informació: Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, fer servir, compartir, distribuir, posar a disposició, presentar o transmetre.