



**Ajuntament
d'Aldover**

Esquema Nacional de Seguretat

**Política de Seguretat de la
Informació**



Aquest document conté **informació confidencial** propietat de l'Ajuntament de l'Ajuntament d'Aldover. Es permet l'ús en l'àmbit intern i del personal autoritzat definit a l'abast del document.

La metodologia, estructura i procediments de treball recollits al present document són propietat i d'ús restringit d'Objetivo Tarsys SL.



VERSIÓ	DATA	CANVIS REALITZATS	RESPONSABLE
1.0	Setembre de 2020	DOCUMENT INICIAL	Ajuntament d'Aldover



Índex

1. Introducció	5
1.1 Abast	6
1.2 Missió	6
1.3 Aprovació i entrada en vigor	6
2. Marc legislatiu	7
3. Principis de compliment de la política de seguretat	8
3.1 Dades de caràcter personal	8
3.2 Gestió de riscos	8
3.3 Prevenció i reacció davant incidències	9
3.3.1 Prevenció	9
3.3.2 Detecció	9
3.3.3 Resposta	9
3.3.4 Recuperació	9
4. Organització de la seguretat	10
4.1 Funcions i responsabilitats	10
4.1.1 Responsable de les Dades	10
4.1.2 Responsable de Seguretat	10
4.1.3 Responsable del Sistema	11
4.2 Procediments de designació	11
5. Obligacions del personal	12
6. Terceres parts	13
7. Gestió i desenvolupament de la política de seguretat de la informació	14
7.1 Revisió de la política de seguretat de la informació	14

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

1. Introducció

L'Ajuntament d'Aldover, d'ara endavant l'Ajuntament, en tant que 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 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.

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), la política de seguretat s'ha d'establir sobre la base dels principis bàsics en l'àmbit de l'Administració electrònica i estableix que tots els òrgans superiors de les administracions públiques han de disposar formalment de la seva política de seguretat, que ha de ser aprovada pel titular de l'òrgan superior corresponent indicats i s'ha de desenvolupar aplicant els requisits mínims següents:

- a) Organització i implantació del procés de seguretat.
- b) Anàlisi i gestió dels riscos.
- c) Gestió de personal.
- d) Professionalitat.
- e) Autorització i control dels accessos.
- f) Protecció de les instal·lacions.
- g) Adquisició de productes.
- h) Seguretat per defecte.
- i) Integritat i actualització del sistema.
- j) Protecció de la informació emmagatzemada i en trànsit.
- k) Prevenció davant altres sistemes d'informació interconnectats.
- l) Registre d'activitat.
- m) Incidents de seguretat.
- n) Continuitat de l'activitat.
- o) 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.

Per tot el que s'exposa anteriorment, en aquest document es defineix la política de seguretat de la informació de l'Ajuntament.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

1.1 Abast

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions,...) de l'Ajuntament i a tots els seus membres, sense excepcions.

1.2 Missió

Mitjançant la present Política de Seguretat l'Ajuntament d'Aldover 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.

1.3 Aprovació i entrada en vigor

Aquesta política de seguretat de la Informació és efectiva des de la data d'aprovació mitjançant Decret d'Alcaldia i fins que sigui reemplaçada per una nova política.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

2. Marc legislatiu

L'ús de les TIC per part de l'Ajuntament d'Aldover es troba regulat per les següents normes jurídiques:

ESTATAL

- 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.
 - Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Reglament (UE) 679/2016, del Parlament Europeu i del Consell, relatiu a la protecció de les dades personals de les persones físiques
- Llei orgànica 3/2018, de 5 de desembre, de protecció de les dades personals i garantia de drets digitals.

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.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

3. Principis de compliment de la política de seguretat

Les TIC utilitzades per l'Ajuntament 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 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, 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.

L'Ajuntament ha 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.

3.1 Dades de caràcter personal

L'Ajuntament, en el desenvolupament de les seves competències, tracta dades de caràcter personal de ciutadans. La Documentació que regula el tractament de dades de caràcter personal a l'Ajuntament es troba al repositori documental dels servidors corporatius.

Els sistemes d'informació de l'Ajuntament han d'aplicar les mesures de seguretat adients en funció dels nivells de seguretat requerits per la normativa en funció de la de les dades de caràcter personal identificades en l'esmentat document de seguretat.

3.2 Gestió de riscos

Tots els sistemes subjectes a aquesta política hauran de ser objecte d'un anàlisi de riscos, on s'avaluin les amenaces i els riscos a què estan exposats. Aquest anàlisi es portarà a terme anualment.

A més de l'anàlisi anual també caldrà portar a terme l'anàlisi quan es produeixin les següents circumstàncies:

- 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.

Per a l'harmonització dels anàlisis de riscos, l'Ajuntament establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

L'Ajuntament garantirà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

3.3 Prevenció i reacció davant incidències

L'Ajuntament ha d'estar preparat per a la prevenció, detecció, reacció i recuperació davant de possibles incidents, d'acord amb l'article 7 de l'ENS.

3.3.1 Prevenció

L'Ajuntament ha d'evitar, o almenys prevenir en la mesura del possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat. Per això ha d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat a través d'una avaluació d'amenaques i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política, l'Ajuntament ha de:

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

3.3.2 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.

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.

3.3.3 Resposta

L'Ajuntament ha de:

- 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 departaments o en altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en ambdós sentits, amb el Centre de Seguretat de la Informació de Catalunya.

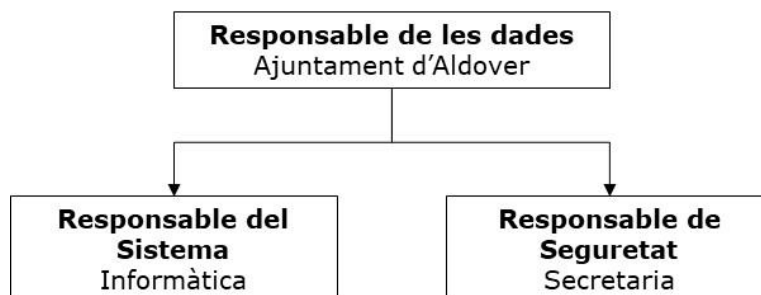
3.3.4 Recuperació

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

4. Organització de la seguretat

4.1 Funcions i responsabilitats

L'organització de la seguretat de la informació de l'Ajuntament es concreta en la següent estructura.



4.1.1 Responsable de les Dades

Responsable	Alcaldia
Funcions	<ol style="list-style-type: none"> 1. Nomenar el Responsable de Seguretat ENS, tasca assumida per Secretaria. 2. Nomenar el Responsable del Sistema, tasca assumida per Informàtica. 3. Donar el suport i dotar dels recursos necessaris al Responsable de Seguretat i al Responsable del Sistema per a poder portar a terme les seves funcions.

4.1.2 Responsable de Seguretat

Responsable	Secretaria
Funcions	<ol style="list-style-type: none"> 1. Establir, impulsar i garantir l'aplicació i el compliment de les polítiques i procediments de Seguretat aprovats per l'Ajuntament. 2. Validar i tramitar l'aprovació de la documentació relacionada amb la seguretat de la informació (Política de Seguretat, Reglaments Interns,...). 3. Promoure les auditories i controls regulars que permetin verificar el compliment de les obligacions de l'Ajuntament en seguretat de la informació. 4. Promoure la formació i conscienciació de la seguretat de la informació al personal de l'Ajuntament. 5. Garantir, amb el suport del Responsable del Sistema, la implantació i control de les mesures de seguretat de manera que aquestes s'integrin adequadament a l'operativa d'Administració Electrònica. 6. Garantir la correcta regulació legal dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. 7. Vetllar per tal que es dugui a terme el preceptiu procés d'anàlisi i gestió de riscos en el sistema.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

	8. Fer el seguiment dels incidents de seguretat que hagin ocorregut relatius a la seguretat de la informació, amb el suport del Responsable del Sistema.
--	--

4.1.3 Responsable del Sistema

Responsable	Informàtica
Funcions delegades	<ol style="list-style-type: none"> 1. Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar el seu correcte funcionament i operativitat. 2. Gestió, configuració i actualització, del maquinari i programari sota el seu àmbit de gestió en què es basen els mecanismes i serveis de seguretat del sistema. 3. Implementació, gestió i manteniment de les mesures de seguretat aplicables al sistema que es trobi sota el seu àmbit de gestió. 4. Interlocució amb dels proveïdors de tecnologies d'informació que suportin els serveis vinculats a l'ENS. 5. Assegurar que la traçabilitat, auditoria i altres registres de seguretat es duen a terme sovint, d'acord amb la política de seguretat establerta. 6. Establir procediments de seguiment i reacció davant incidències. 7. Donar d'alta nous rols d'accés als programes i aplicacions corporatives que es trobin sota el seu àmbit de gestió.

4.2 Procediments de designació

El responsable de Seguretat serà nomenat per Decret d'Alcaldia. El nomenament s'ha de revisar cada 2 anys o quan el lloc quedi vacant.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

5. Obligacions del personal

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

Tots els membres de l'Ajuntament atendran a una sessió de conscienciació en matèria de seguretat TIC quan el Responsable de Seguretat ho estimi necessari. Igualment s'establirà un programa de conscienciació contínua per atendre tots els membres de l'Ajuntament.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al maneig 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.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

6. Terceres parts

Quan l'Ajuntament presti serveis a altres organismes o gestioni informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, s'establiran canals per informe i coordinació dels respectius Responsables de Seguretat i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan l'Ajuntament utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat que pertoqui a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i poden desenvolupar els seus propis procediments operatius per satisfer-la. S'establiran procediments específics d'informe i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta política.

Quan algun aspecte de la política no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

	Política de Seguretat	Versió 1.0
--	------------------------------	------------

7. 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 l'Unitat de servidor definida per als documents a compartir entre el personal de l'Ajuntament.

7.1 Revisió de la política de seguretat de la informació

Serà missió del Responsable 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 i difosa perquè la coneguin totes les parts afectades.