Ajuntament d'Argentona

Política de Seguretat segons el Model de Governança per Blocs de Responsabilitat de l'Ajuntament d'Argentona

Guía de Seguridad de las TIC
CCN-STIC 890
MAIG 2026

Ajuntament d'Argentona

1. APROVACIÓ I ENTRADA EN VIGOR

Política de seguretat v001.Text aprovat el dia 19 de Juny de 2025 per resolució del L'Alcaldia-Presidència de l'Ajuntament d'Argentona amb número 1349/2025.

Política de seguretat v002.Text aprovat el dia 14 de maig de 2026 per resolució del L'Alcaldia-Presidència de l'Ajuntament d'Argentona amb número 1290/2026.

Aquesta "Política de Seguretat de la Informació", en endavant Política, serà efectiva des de aquesta data i fins que sigui reemplaçada per una nova Política.

2. MODIFICACIONS

Es modifica la versió 001 de la política de seguretat de l'Ajuntament d'Argentona, traient el marc normatiu posant-lo com annex i no dins de la política de seguretat.

El decret 1349/2025 no conté el document política de seguretat v001 sencer, sinó un resum.

Modificació de possibles conflictes entre els responsable de sistemes i de seguretat, serà resolt per la Alcaldia-Presidència de l'Ajuntament d'Argentona, per la resta de conflictes seran resolts pel Comitè de Seguretat de la Informació.

3. INTRODUCCIÓ

L'Ajuntament d'Argentona, depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els seus objectius, exercir les seves competències i prestar els serveis que té atribuïts. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant danys accidentals o deliberats que puguin afectar la disponibilitat, integritat o confidencialitat de la informació tractada o els serveis prestats.

L' objectiu de la seguretat de la informació és garantir la confidencialitat, integritat, autenticitat i traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l' activitat diària i reaccionant amb prestesa als incidents.

Els sistemes TIC han d' estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, integritat, disponibilitat, ús previst i valor de la informació i els serveis. Per defensar-se d' aquestes amenaces, es requereix una estratègia que s' adapti als canvis en les condicions de l' entorn

per garantir la prestació contínua dels serveis. Això implica que els departaments han d' aplicar les mesures mínimes de seguretat exigides per l' Esquema Nacional de Seguretat, així com fer 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.

Els diferents departaments s' han de cerciorar que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d' explotació. Els requisits de seguretat i la valoració del seu cost, han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

4. MISIÓ DE L'AJUNTAMENT D'ARGENTONA

L' Ajuntament d' Argentona, per a la gestió dels seus interessos i de les funcions i competències que té atribuïdes en diferents normes o convenis, promou activitats i presta serveis públics que contribueixen a satisfer les necessitats i aspiracions de la població. Per a això posa a disposició d'aquesta la realització de tràmits online amb l'objectiu d'impulsar la tramitació electrònica dels procediments administratius, la millora en la prestació dels serveis i la participació de la ciutadania en els afers públics establint, d' aquesta manera, noves vies de participació que garanteixin el desenvolupament de la democràcia participativa i la millora de l' eficàcia i eficiència de l' acció pública.

Es vol potenciar d' altra banda l' ús de les noves tecnologies a l' Ajuntament i a la pròpia ciutadania. Els principals objectius que es persegueixen entre d' altres són: fomentar la relació electrònica de la ciutadania amb l' Ajuntament, crear la confiança necessària entre ciutadà i Ajuntament en aquesta relació.

5. ABAST

Aquesta Política s'aplicarà als sistemes d'informació de l'Ajuntament d' Argentona, que estan relacionats amb l'exercici de drets per mitjans electrònics, amb el compliment de deures per mitjans electrònics o amb l'accés a la informació o al procediment administratiu i que es troben dins l'àmbit d'aplicació de l'Esquema Nacional de Seguretat (ENS).

6. MARC NORMATIU

La base normativa que afecta el desenvolupament de les activitats i competències de l' Ajuntament d' Argentona, pel que fa a administració electrònica, i que implica la implantació de forma explícita de mesures de seguretat en els sistemes d' informació, està constituïda per la legislació que es troba en l'Annex 1 Marc normatiu.

El manteniment del marc normatiu serà responsabilitat de l' Ajuntament d'Argentona, i es mantindrà en un Annex a aquest document. Inclòs les instruccions tècniques de seguretat d' obligat compliment, publicades mitjançant resolució de la Secretaria d' Estat d' Administracions Públiques i aprovades pel Ministerio de Hacienda y Administraciones Públicas,a proposta del Comité Sectorial de Administració Electrónica i a iniciativa del Centro Criptológico Nacional (CCN) tal com s' estableix en el Reial decret.

Així mateix, l' Ajuntament d' Argentona, també serà responsable d' identificar les guies de seguretat del CCN, referenciades en l' esmentat article, que seran d' aplicació per millorar el compliment de l' establert a l' Esquema Nacional de Seguretat.

7. COMPLIMENT DELS REQUISITS MÍNIMS DE SEGURETAT

L'Ajuntament d'Argentona per aconseguir el compliment del Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, que recull els principis bàsics i dels requisits mínims, ha implementat diverses mesures de seguretat proporcionals a la naturalesa de la informació i els serveis a protegir i tenint en compte la categoria dels sistemes afectats.

La seguretat com un procés integral i mínim privilegi

La seguretat s' entén com un procés integral constituït per tots els elements tècnics, humans, materials, jurídics i organitzatius, relacionats amb el sistema. L' aplicació de l' Esquema Nacional de Seguretat a l ' Ajuntament d'Argentona, estarà presidida per aquest principi, que exclou qualsevol actuació puntual o tractament conjuntural.

Es prestarà la màxima atenció a la conscienciació de les persones que intervenen en el procés i als seus responsables jeràrquics, per evitar que, la ignorància, la manca d' organització i coordinació, o d' instruccions inadequades, constitueixin fonts de risc per a la seguretat.

Els sistemes d' informació s' han de dissenyar i configurar atorgant els mínims privilegis necessaris per al seu correcte acompliment, la qual cosa implica incorporar els aspectes següents:

a. El sistema proporcionarà la funcionalitat imprescindible perquè l' organització assoleixi els seus objectius competencials o contractuals.

b. Les funcions d' operació, administració i registre d' activitat seran les mínimes necessàries, i s' assegurarà que només són desenvolupades per les persones autoritzades, des d' emplaçaments o equips així mateix autoritzats; podent exigir-se, si s' escau, restriccions d' horari i punts d' accés facultats.

c. En un sistema d' explotació s' eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades a la fi que es persegueix. L' ús ordinari del sistema ha de ser senzill i segur, de manera que una utilització insegura requereixi d' un acte conscient per part de l' usuari.

S' aplicaran guies de configuració de seguretat per a les diferents tecnologies, adaptades a la categorització del sistema, a l' efecte d' eliminar o desactivar les funcions que siguin innecessàries o inadequades.

Vigilància contínua, reevaluació periòdica i Integritat, actualització del sistema i millora contínua del procés de seguretat

La vigilància contínua per part de l ' Ajuntament d'Argentona permetrà la detecció d' activitats o comportaments anòmals i la seva oportuna resposta.

L' avaluació permanent de l' estat de la seguretat dels actius permetrà mesurar la seva evolució, detectant vulnerabilitats i identificant deficiències de configuració.

Les mesures de seguretat es reavaluaran i actualitzaran periòdicament, adequant la seva eficàcia a l' evolució dels riscos i els sistemes de protecció, podent arribar a un replantejament de la seguretat, si fos necessari.

La inclusió de qualsevol element físic o lògic en el catàleg actualitzat d' actius del sistema, o la seva modificació, requerirà autorització formal prèvia.

L' avaluació i monitoratge permanents permetran adequar l' estat de seguretat dels sistemes atenent les deficiències de configuració, les vulnerabilitats identificades i les actualitzacions que els afectin, així com la detecció primerenca de qualsevol incident que tingui lloc sobre els mateixos.

El procés integral de seguretat implantat haurà de ser actualitzat i millorat de forma contínua. Per a això, s' aplicaran els criteris i mètodes reconeguts en la pràctica nacional i internacional relatius a la gestió de la seguretat de les tecnologies de la informació

Gestió de personal i professionalitat

Tot el personal, propi o aliè relacionat amb els sistemes d' informació de l' Ajuntament d'Argentona, dins l' àmbit de l' ENS, seran formats i informats dels seus deures, obligacions i responsabilitats en matèria de seguretat. La seva actuació serà supervisada per verificar que se segueixen els procediments establerts.

El significat i abast de l' ús segur del sistema es concretarà i plasmarà en unes normes de seguretat que seran aprovades per la direcció o l' òrgan superior corresponent. De la mateixa manera, es determinaran els requisits de formació i experiència necessària del personal per al desenvolupament del seu lloc de treball.

La seguretat dels sistemes d' informació estarà atesa i serà revisada i auditada per personal qualificat, dedicat i instruït en totes les fases del seu cicle de vida: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d' incidències i desmantellament.

De manera objectiva i no discriminatòria s' exigirà que les organitzacions que ens proporcionen serveis comptin amb professionals qualificats i amb uns nivells idonis de gestió i maduresa dels serveis prestats.

Gestió de la seguretat basada en els riscos, anàlisi i gestió de riscos

L' anàlisi i la gestió dels riscos serà part essencial del procés de seguretat i serà una activitat contínua i permanentment actualitzada.

La gestió dels riscos permetrà el manteniment d' un entorn controlat, minimitzant els riscos a nivells acceptables. La reducció a aquests nivells es realitzarà mitjançant una apropiada aplicació de mesures de seguretat, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis a prestar i dels riscos als quals estiguin exposats.

Aquesta gestió es realitzarà per mitjà de l' anàlisi i tractament dels riscos als quals està exposat el sistema. Sens perjudici del que disposa l' annex II, s' emprarà alguna metodologia reconeguda internacionalment. Les mesures adoptades per mitigar o suprimir els riscos hauran d' estar justificades i, en tot cas, existirà una proporcionalitat entre elles i els riscos.

Incidents de seguretat, prevenció, detecció, reacció i recuperació

L' Ajuntament d'Argentona, disposa de procediments de gestió d' incidents de seguretat acord amb el que preveu l' article 33, la Instrucció Tècnica de Seguretat corresponent, i de de mecanismes de detecció, criteris de classificació, procediments d' anàlisi i resolució, així com de les lleres de comunicació a les parts interessades.

La seguretat del sistema contemplarà les accions relatives als aspectes de prevenció, detecció i resposta, amb la qual cosa cal minimitzar les seves vulnerabilitats i aconseguir que les amenaces sobre aquest no es materialitzin o que, en el cas de fer-ho, no afectin greument la informació que maneja o els serveis que presta.

Les mesures de prevenció podran incorporar components orientats a la dissuasió o a la reducció de la superfície d' exposició, han d' eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se.

Les mesures de detecció aniran dirigides a descobrir la presència d'un ciberincident.

Les mesures de resposta es gestionaran en temps oportú, estaran orientades a la restauració de la informació i els serveis que poguessin haver-se vist afectats per un incident de seguretat.

El sistema d' informació garantirà la conservació de les dades i informació en suport electrònic.

De la mateixa manera, el sistema mantindrà disponibles els serveis durant tot el cicle vital de la informació digital, a través d' una concepció i procediments que siguin la base per a la preservació del patrimoni digital.

Existència de línies de defensa i prevenció davant d' altres sistemes d' informació interconnectats

L' Ajuntament d'Argentona ha implementat una estratègia de protecció del sistema d' informació constituïda per múltiples capes de seguretat, constituïdes per mesures organitzatives, físiques i lògiques, de tal manera que quan una capa ha estat compromesa permeti desenvolupar una reacció adequada davant els incidents que no s' han pogut evitar, reduint la probabilitat que el sistema sigui compromès en el seu conjunt i minimitzar-ne l' impacte final.

Es protegirà el perímetre del sistema d' informació, especialment, quan el sistema de l' Ajuntament es connecta a xarxes públiques, tal com es defineixen

en la legislació vigent en matèria de telecomunicacions, reforçant-se les tasques de prevenció, detecció i resposta a incidents de seguretat.

En tot cas, s' analitzaran els riscos derivats de la interconnexió del sistema amb altres sistemes i es controlarà el seu punt d' unió. Per a l' adequada interconnexió entre sistemes cal atenir-se al que disposa la Instrucció Tècnica de Seguretat corresponent.

Diferenciació de responsabilitats, organització i implantació del procés de seguretat

L'Ajuntament d'Argentona, ha organitzat la seva seguretat comprometent a tots els membres de la corporació mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal com es recull en l'apartat de "MODEL DE GOVERNANÇA" del present document.

Autorització i control dels accessos

L' Ajuntament d'Argentona ha implementat mecanismes de control d' accés al sistema d' informació, limitant-lo als usuaris, processos, dispositius i altres sistemes d' informació, degudament autoritzats, i exclusivament a les funcions permeses.

Protecció de les instal·lacions

L' Ajuntament d'Argentona, ha implementat mecanismes de control d' accés físic, prevenint els accessos físics no autoritzats, així com els danys a la informació i als recursos, mitjançant perímetres de seguretat, controls físics i proteccions generals en àrees.

Adquisició de productes de seguretat i contractació de serveis de seguretat

Per a l' adquisició de productes o contractació de serveis de seguretat l' Ajuntament d'Argentona, tindrà en compte la utilització de forma proporcionada a la categoria del sistema i el nivell de seguretat determinat, aquells que tinguin certificada la funcionalitat de seguretat relacionada amb l' objecte de la seva adquisició.

Per a la contractació de serveis de seguretat s' atendrà a l' assenyalat quant a la professionalitat.

Protecció de la informació emmagatzemada i en trànsit i continuïtat de l' activitat

L' Ajuntament d'Argentona prestarà especial atenció a la informació emmagatzemada o en trànsit a través dels equips o dispositius portàtils o mòbils,

els dispositius perifèrics, els suports d' informació i les comunicacions sobre xarxes obertes, que s' hauran d' analitzar especialment per aconseguir una adequada protecció.

S' aplicaran procediments que garanteixin la recuperació i conservació a llarg termini dels documents electrònics produïts pels sistemes d' informació compresos en l' àmbit d' aplicació d' aquest Reial decret, quan això sigui exigible.

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica a què es refereix aquest Reial decret, haurà d' estar protegida amb el mateix grau de seguretat que aquesta. Per a això, s' aplicaran les mesures que corresponguin a la naturalesa del suport, de conformitat amb les normes que resultin d' aplicació.

Els sistemes disposaran de còpies de seguretat i s' establiran els mecanismes necessaris per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

Registre d' activitat i detecció de codi danyós

L' Ajuntament amb el propòsit de satisfer l' objecte d' aquest Reial decret, amb plenes garanties del dret a l' honor, a la intimitat personal i familiar i a la pròpia imatge dels afectats, i d' acord amb la normativa sobre protecció de dades personals, de funció pública o laboral, i altres disposicions que resultin d' aplicació, registrarà les activitats dels usuaris, retenint la informació estrictament necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actua.

Per tal de preservar la seguretat dels sistemes d' informació, garantint la rigorosa observança dels principis d' actuació de les Administracions públiques, i de conformitat amb el que disposa el Reglament General de Protecció de Dades i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació allà enunciats, l' Ajuntament podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, i únicament per a les finalitats de seguretat de la informació, de forma que sigui possible impedir l' accés no autoritzat a les xarxes i sistemes d' informació, aturar els atacs de denegació de servei, evitar la distribució malintencionada de codi danyós així com altres danys a les esmentades xarxes i sistemes d' informació.

Per corregir o, si s' escau, exigir responsabilitats, cada usuari que accedeixi al sistema d' informació haurà d' estar identificat de forma única, de manera que

se sàpiga, en tot moment, qui rep drets d' accés, de quin tipus són aquests, i qui ha realitzat una determinada activitat.

Infraestructures i serveis comuns

L' Ajuntament d'Argentona, tindrà en compte que la utilització d' infraestructures i serveis comuns de les administracions públiques, inclosos els compartits o transversals, facilitarà el compliment del que disposa aquest Reial decret.

Perfils de compliment específics i acreditació d' entitats d' implementació de configuracions segures

L' Ajuntament d'Argentona, tindrà en compte l' aplicació d' aquells perfils de compliment específics per a Entitats Locals que siguin d' aplicació.

8. MODEL DE GOVERNANÇA

Per garantir el compliment de l' Esquema Nacional de Seguretat i establir l' organització de la seguretat de la informació adaptada a les necessitats i particularitat d' aquest Ajuntament, es proposa una designació de rols per blocs de responsabilitat: Govern, Supervisió i Operació.

D' acord amb aquesta estructura, s' han assignat les responsabilitats i funcions de seguretat següents:

Bloc de Govern:

1. **Responsable de Govern**, les funcions del qual exercita l' Alcaldia-Presidència de l' Ajuntament, que integra els següents rols i funcions ENS:
    1. Comitè de Seguretat de la Informació.
    2. Responsable de la Informació.
    3. Responsable del Servei.
2. L'Alcaldia-Presidència pot delegar aquests rols i/o funcions en un Regidor o Regidors.

Bloc Executiu/Supervisió:

1. **Responsable de Supervisió**, les funcions de la qual exercita la Secretaria-Intervenció de l' Ajuntament, i que integra el següent rol ENS:
    1. Responsable de la Seguretat.

1. **Delegat Protecció de Dades (DPD),** DIPUTACIÓ DE BARCELONA DSTSC-SAMSE, donant suport al Responsable de Supervisió, amb funcions d'assessorament i supervisió en matèria de protecció de dades.

Bloc d' Operació:

2. **Responsable d'Operació**, les competències del qual exercita un empleat municipal que ocupa el lloc com a tècnic del departament d'informàtica, i que integra el següent rol ENS:
    - Responsable del Sistema.

6.1 Responsabilitats associades a l' Esquema Nacional de Seguretat

A continuació, es detallen i s' estableixen les funcions i responsabilitats de cadascun dels rols de seguretat ENS:

Funcions del Responsable de la Informació i dels Serveis

- Establir i aprovar els requisits de seguretat aplicables al servei i la informació dins del marc establert a l' annex I del Reial decret de l' Esquema Nacional de Seguretat.
- Acceptar els nivells de risc residual que afectin el Servei i la Informació.

Funcions del Responsable de Seguretat

- Mantenir i verificar el nivell adequat de seguretat de la Informació manejada i dels serveis electrònics prestats pels sistemes d'informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la declaració d'aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, elaborar documentació del sistema.
- Proporcionar assessorament per a la determinació de la categoria del sistema, en col·laboració amb el Responsable del Sistema.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar a la Direcció l'aprovació de canvis i altres requisits del sistema.

Funcions del Responsable del Sistema

- Paralitzar o donar suspensió a l'accés a informació o prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida.
- Elaborar els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en el mateix.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Prestar al Responsable de Seguretat de la Informació assessorament per a la determinació de la Categoria del Sistema.
- Col·laborar, si així se li requereix, en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat.
- Dur a terme les funcions de l' administrador de la seguretat del sistema:
- La gestió, configuració i actualització, si s' escau, del maquinari i programari en els quals es basen els mecanismes i serveis de seguretat.
- La gestió de les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge de l'activitat desenvolupada en el sistema i la seva correspondència amb l'autoritzat.
- Aprovar els canvis en la configuració vigent del Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són complerts estrictament.
- Assegurar que són aplicats els procediments aprovats per manejar el Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitoritzar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.

8.2 Funcions del Comitè de Seguretat de la Informació

Les funcions pròpies d' un Comitè de Seguretat de la Informació són les següents:

- Atendre les sol·licituds, en matèria de Seguretat de la Informació, de l'Administració i dels diferents rols de seguretat i/o àrees informant regularment de l'estat de la Seguretat de la Informació.
- Assessorar en matèria de Seguretat de la Informació.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre les diferents unitats administratives.
- Promoure la millora contínua del sistema de gestió de la Seguretat de la Informació. Per a això s' encarregarà de:

o Coordinar els esforços de les diferents àrees en matèria de Seguretat de la Informació, per assegurar que aquests siguin consistents, alineats amb l' estratègia decidida en la matèria, i evitar duplicitats.

o Proposar plans de millora de la Seguretat de la Informació, amb la seva dotació pressupostària corresponent, prioritzant les actuacions en matèria de seguretat quan els recursos siguin limitats.

o Vetllar perquè la Seguretat de la Informació es tingui en compte en tots els projectes des de la seva especificació inicial fins a la seva posada en operació. En particular haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.

o Realitzar un seguiment dels principals riscos residuals assumits per l' Administració i recomanar possibles actuacions respecte d' ells.

o Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d' ells.

o Elaborar i revisar regularment la Política de Seguretat de la Informació per a la seva aprovació per l' òrgan competent.

o Elaborar la normativa de Seguretat de la Informació per a la seva aprovació en coordinació amb la Direcció General.

o Verificar els procediments de seguretat de la informació i la resta de documentació per a la seva aprovació.

- Elaborar programes de formació destinats a formar i sensibilitzar el personal en matèria de Seguretat de la Informació i en particular en matèria de protecció de dades de caràcter personal.
- Elaborar i aprovar els requisits de formació i qualificació d' administradors, operadors i usuaris des del punt de vista de Seguretat de la Informació.
- Promoure la realització de les auditories periòdiques ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l' Administració en matèria de seguretat de la Informació.

6.3 Procediments de designació

La designació dels Responsables identificats en aquesta Política ha estat realitzada Alcaldia-Presidència de l'Ajuntament d'Argentona i comunicada a les parts afectades decret 3531/2025 de la Constitució.

Els rols de seguretat seran revisats cada quatre anys, en el cas que existeixi una vacant la mateixa haurà de ser coberta en el termini d' un mes, seguint el mateix procediment.

6.4 Resolució de conflictes

Si hi hagués conflicte entre el responsable de sistemes i seguretat, serà resolt per la Alcaldia-Presidència de l'Ajuntament d'Argentona, per la resta de conflictes seran resolts pel Comitè de Seguretat de la Informació.

7. DATOS DE CARÁCTER PERSONAL

L' Ajuntament d'Argentona en el tractament de les dades personals, compleix amb els principis i obligacions de la normativa vigent, entre d' altres el Reglament 679/2016, del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la Protecció de les Persones Físiques pel que fa al tractament de dades personals i a la lliure circulació de aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament General de Protecció de Dades-RGPD-) i la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia de drets digitals, respectant, en tot cas, el dret fonamental a la protecció de dades personals, la intimitat i la resta dels drets fonamentals reconeguts tant en la legislació i tractats internacionals com en la Constitució vigent.

En desenvolupament dels principis de la vigent normativa de protecció de dades, entre d'altres, els de minimització, confidencialitat o proactivitat,

l'Ajuntament ha definit un marc d'actuació en la Política de Protecció de Dades, aprovada per Decret de xx/xx.

8.DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El compliment dels objectius marcats en aquesta Política de Seguretat es duu a terme mitjançant el desenvolupament de documentació que componen les normes i procediments de seguretat associats al compliment de l' Esquema Nacional de Seguretat. Per a la seva organització s' ha definit una Norma per a la Gestió de la Documentació, que estableix les directrius per a l' organització, gestió i accés.

La revisió anual de la present Política correspon al Responsable de Govern, proposant en cas que sigui necessari millores de la mateixa, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.

9.TERCERES PARTS

Quan el presti serveis a altres organismes, o manegi informació d' altres organismes, se'ls farà partícips d' aquesta Política de Seguretat de la Informació. L' Ajuntament d'Argentona, definirà i aprovarà els canals per a la coordinació de la informació i els procediments d' actuació per a la reacció davant incidents de seguretat, així com la resta de les actuacions que l' Ajuntament dugui a terme en matèria de Seguretat en relació amb altres organismes.

Quan l' Ajuntament, utilitzi serveis de tercers o cedeixi informació a tercers, se' ls farà partícip d' aquesta Política de Seguretat i de la Normativa de Seguretat existent que pertoca als esmentats serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en l' esmentada normativa, podent desenvolupar els seus propis procediments operatius per satisfer-la. S' establiran procediments específics de comunicació i resolució d' incidències.

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

De la mateixa manera, tenint en compte l' obligació de complir amb el que disposen les Instruccions Tècniques de Seguretat recollida en la Disposició addicional segona (Desenvolupament de l'Esquema Nacional de Seguretat) del

Ajuntament d'Argentona

Reial Decret Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat, i en consideració a la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, on s'estableix que els operadors del sector privat que prestin serveis o proveeixin solucions a les entitats públiques, als que resulti exigible el compliment de l' Esquema Nacional de Seguretat, hauran d' estar en condicions d' exhibir la corresponent Declaració de Conformitat amb l' Esquema Nacional de Seguretat quan es tracti de sistemes de categoria BÀSICA, o la Certificació de Conformitat amb l' Esquema Nacional de Seguretat, quan es tracti de sistemes de categories MITJANA o ALTA.

Quan algun aspecte d' aquesta Política de Seguretat 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. Aquest informe haurà de ser aprovat pels responsables d' informació i els serveis, amb caràcter previ a l' inici de la relació amb la tercera part.

Ajuntament d'Argentona

ANNEX 1, MARC NORMATIU

La base normativa que afecta el desenvolupament de les activitats i competències de l' Ajuntament d' Argentona, pel que fa a administració electrònica, i que implica la implantació de forma explícita de mesures de seguretat en els sistemes d' informació, està constituïda per la legislació següent:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).
- 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.
- Ordenança reguladora de l'Administració Electrònica de l'Ajuntament d'Argentona.
- Reglament pel qual s' estableix la Seu Electrònica de l' Ajuntament d'Argentona
- Reglament Orgànic Municipal (ROM).

També formen part del marc normatiu les restants normes aplicables a l' Administració Electrònica de l' Ajuntament d'Argentona, derivades de les anteriors i publicades a les seus electròniques compreses dins l' àmbit d' aplicació de la present Política, entre d' altres.

El manteniment del marc normatiu serà responsabilitat de l' Ajuntament d'Argentona, i es mantindrà en un Annex a aquest document. Inclòs les instruccions tècniques de seguretat d' obligat compliment, publicades mitjançant resolució de la Secretaria d' Estat d' Administracions Públiques i aprovades pel Ministerio de Hacienda y Administraciones Públicas,a proposta del Comité Sectorial de Administració Electrónica i a iniciativa del Centro Criptológico Nacional (CCN) tal com s' estableix en el Reial decret.

Així mateix, l' Ajuntament d' Argentona, també serà responsable d' identificar les guies de seguretat del CCN, referenciades en l' esmentat article, que seran d' aplicació per millorar el compliment de l' establert a l' Esquema Nacional de Seguretat.