Consell Comarcal del Segrià

Esquema Nacional de Seguretat

Política de Seguretat de la Informació

Aquest document conté **informació confidencial** propietat del Consell Comarcal del Segrià. 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	Març de 2024	DOCUMENT INICIAL	Consell Comarcal del Segrià

Índex

1. Introducció

El Consell Comarcal del Segrià, d'ara endavant el Consell Comarcal, 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 adecuada 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 12.6 del Reial decret 311/2022, de 3 de maig, 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 corresponentindicats i s'ha de desenvolupar aplicant els requisits mínims següents en proporció als riscos identificats en cada sistema:

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 de seguretat i contractació de serveis de seguretat.

h) Mínim privilegi.

i) Integritat i actualització del sistema.

j) Protecció de la informació emmagatzemada i en trànsit.

k) Prevenció davant d'altres sistemes d'informació interconnectats.

l) Registre de l'activitat i detecció de codi nociu.

m) Incidents de seguretat.

n) Continuïtat de l'activitat.

o) Millora contínua del procés de seguretat.

Així mateix, l'article 12.2 de l'ENS indica que la política de seguretat ha de ser formalment aprovada per l'òrgan competent

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

1.1 Abast

Aquesta política s'aplica a tots els sistemes TIC (infraestructures, programari, comunicacions,...) del Consell Comarcal i a tots els seus membres, sense excepcions.

1.2 Missió

Mitajnçant la present Política de Seguretat el Consell Comarcal del Segrià 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 el mecanisme determinat pel Consell i fins que sigui reemplaçada per una nova política.

2. Marc legislatiu

L'ús de les TIC per part del Consell Comarcal del Segrià 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 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat.
- Reial decret 4/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional d'Interoperabilitat.
- Reglament (UE) 2016/679 del Parlament i del Consell Comarcal, 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)
- 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 el Consell Comarcal 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, el Consell Comarcal 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 el Consell Comarcal ha d'aplicar les mesures mínimes de seguretat exigides pel Reial decret 311/2022, de 3 de maig, 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.

El Consell Comarcal 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 deprojectes relacionats amb les TIC.

3.1 Dades de caràcter personal

El Consell Comarcal, 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 al Consell Comarcal es troba al respositori documental dels servidors corporatius.

Els sistemes d'informació del Consell Comarcal 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, el Consell Comarcal establirà una valoració de referència per als diferents tipus d'informació manejats i els diferents serveis prestats.

El Consell Comarcal garantirà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

3.3 **Prevenció i reacció davant incidències**

El personal del Consell Comarcal ha ha de disposar dels mecanismes per a la prevenció, detecció, resposta i conservació per a minimitzar les vulnerabilitats, evitar que les amenaces es materialitzin i – en cas contrari - reaccionar davant de possibles incidents, d'acord amb l'article 8 i 25 de l'ENS, i l'article 33 de l'RGPD si afecta dades personals.

La seguretat del sistema ha de contemplar les accions relatives als aspectes de prevenció, detecció i resposta, a fi de 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 als serveis que presta.

Les mesures de prevenció, que poden 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 incident de seguretat.

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

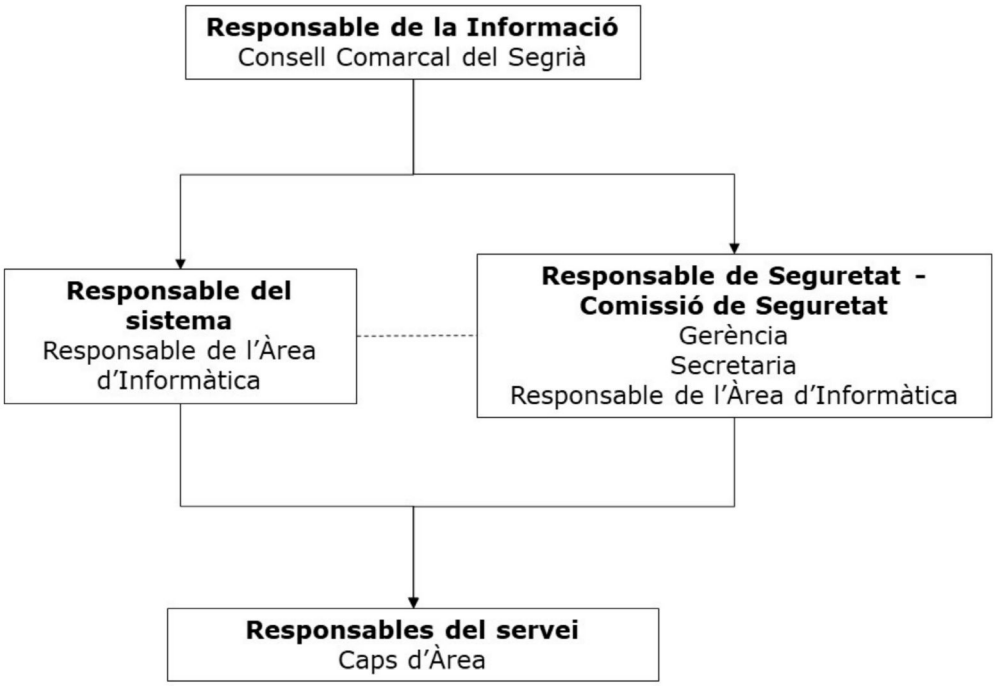
El sistema d'informació garantirà la conservació de les dades i informació en suport electrònic, garantint que la seva aplicació no suposi una reducció en l'aplicació principis bàsics i requisits mínims establerts,.

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

4. Organització de la seguretat

4.1 Funcions i responsabilitats

L'organització de la seguretat de la informació del Consell Comarcal es concreta en la següent estructura.



4.1.1 Responsable de les Dades

Responsable	Presidència
Funcions	1. Nomenar el Responsable de Seguretat ENS, tasca assumida per la Comissió de Seguretat. 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	Comissió de Seguretat
Components de la Comissió	Gerència Secretaria Responsable de l'Àrea d'Informàtica
Funcions	1. Establir, impulsar i garantir l'aplicació i el compliment de les polítiques i procediments de Seguretat aprovats per el Consell Comarcal. 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 del Consell Comarcal en seguretat de la informació.

	4. Promoure la formació i conscienciació de la seguretat de la informació al personal del Consell Comarcal. 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. 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	Responsable de l'Àrea d'Informàtica
Funcions delegades	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.

4.1.4 Responsables dels Serveis

Responsable	Caps d'Àrea
Funcions delegades	1. Definir els serveis necessaris per portar a terme les competències del Consell. 2. Vetllar pel compliment de les polítiques i normes de seguretat determinades pel Consell en el tractament dels fitxers de l'àmbit de responsabilitat.

4.2 Procediments de designació

El responsable de Seguretat serà nomenat pel mateix procediment pel qual s'aprovi la present Política de Seguretat.

5. Obligacions del personal

Tots els membres del Consell Comarcal 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 del Consell Comarcal 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 del Consell Comarcal.

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.

6. Terceres parts

Quan el Consell Comarcal 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 el Consell Comarcal 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.

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 del Consell Comarcal.

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 de Presidència i difosa perquè la coneguin totes les parts afectades.

DILIGÈNCIA: *document aprovat per acord de Ple del Consell en sessió de 21 de juny de 2024*

La secretària