2021

POLÍTICA DE SEGURETAT

Política de seguretat de la informació del Consell Comarcal de l'Alt Penedès en compliment de l'Esquema Nacional de Seguretat (ENS)

Consell Comarcal de l'Alt Penedès

PS000-Política de Seguretat- CCAlt Penedès
15/07/2021

Política de Seguretat

Control de Versions

CONTROL DEL DOCUMENT

Nom del document: PS000 - Política de Seguretat - CC Alt Penedès **Nombre de pàgines:** 17	
Autor: Segurdades (empresa externa)	**Revisat per:** Xavier Reina, responsable de sistemes
Data: octubre 2020	**Data:** abril de 2021
Aprovat per: Junta de Govern del Consell Comarcal de l'Alt Penedès **Data d'aprovació:** 15/07/2021	
Classificació de la informació: ÚS INTERN	
Distribució: Personal del Consell i empreses prestadores de serveis.	

CONTROL DE VERSIONS

Núm Versió	Autor	Data	Canvis realitzats	Comentaris
02	Xavier Reina	22/04/2021	Versió per aprovar.	
01	Jordi Vidal (extern)	21/09/2020	Versió inicial	Pendent de revisió

1. APROVACIÓ I ENTRADA EN VIGOR

Aquesta Política de Seguretat de la Informació serà efectiva des de la seva aprovació i fins que sigui reemplaçada o derogada.

2. INTRODUCCIÓ

El Consell Comarcal de l'Alt Penedès depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els seus objectius. Aquests sistemes han d'administrar-se amb diligència, prenent les mesures adequades per protegir-los enfront de danys accidentals o deliberats que puguin afectar la disponibilitat, la integritat o la confidencialitat de la informació tractada i els serveis prestats.

L'objectiu de la seguretat de la informació és garantir la qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa als incidents.

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

Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat. I també, realitzar un seguiment continu dels nivells de prestació dels serveis, seguir i analitzar les vulnerabilitats reportades i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

Els serveis i departaments del Consell Comarcal han d'assegurar-se 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 retirada de servei, passant per les decisions de desenvolupament o adquisició i les activitats d'explotació. Els requisits de seguretat i les necessitats de finançament han de ser identificats i inclosos en la planificació, en la sol·licitud d'ofertes i en els plecs de licitació per a projectes de TIC.

Conseqüentment, el Consell Comarcal ha d'estar preparat per prevenir, detectar, reaccionar i recuperar-se d'incidents, d'acord amb l'article 7 de l'ENS, per tal de poder prestar serveis als municipis i a la ciutadania.

3. ABAST

La Política de Seguretat del Consell Comarcal de l'Alt Penedès és d'obligat compliment per a tot el personal del Consell, independentment del tipus de relació contractual; tots els sistemes TIC i el personal d'empreses externes en allò que els sigui d'aplicació.

4. MISSIÓ

El Consell Comarcal de l'Alt Penedès té la missió principal d'Impulsar la qualitat de vida a la comarca, d'acord amb les seves competències establertes pel Decret Legislatiu 4/2003, pel qual s'aprova el text refós de la Llei de l'organització comarcal de Catalunya.

5. MARC NORMATIU

Per a l'execució d'aquesta política de seguretat s'ha tingut en compte la legislació que afecta el sistema d'informació objecte d'aquest document, que és:

- Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques.
- Llei 40/2015, d'1 d'octubre, de règim jurídic del Sector Públic.
- Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'administració electrònica, modificat pel Reial Decret 951/2015, de 23 d'octubre.
- Resolució de 13 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat.
- Resolució de 7 d'octubre de 2016, de la Secretaria d'Estat d'Administracions Públiques, per la qual s'aprova la Instrucció Tècnica de Seguretat de l'Informe de l'Estat de la Seguretat.
- Resolució de 27 de març de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat d'Auditoria de la Seguretat dels Sistemes d'Informació.
- Resolució de 13 d'abril de 2018, de la Secretaria d'Estat de Funció Pública, per la qual s'aprova la Instrucció Tècnica de Seguretat de Notificació d'Incidents de Seguretat.
- Reial Decret 4/2010, de 8 de gener, pel qual es regula l'Esquema Nacional d'Interoperabilitat en l'àmbit de l'Administració Electrònica.
- Reial Decret 1671/2009, de 6 de novembre, pel qual es desenvolupa parcialment la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

- Articles 23 i 24 de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal.
- Reglament (UE) 2016/679 del Parlament Europeu i de Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa a el tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46 / CE (Reglament general de protecció de dades, RGPD).
- Llei 34/2002, de 11 de juliol, de serveis de la societat de la informació i de comerç electrònic.
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic.
- Llei 19/2013, de 9 de desembre, de transparència, accés a la informació pública i bon govern.
- Llei 25/2007, de 18 d'octubre, de conservació de dades relatives a les comunicacions electròniques i a les xarxes públiques de comunicacions.
- Llei 56/2007, de 28 de desembre, de mesures d'impuls de la Societat de la Informació.
- Llei 9/2014, de 9 de maig, general de telecomunicacions.
- Llei 7/1985, de 2 d'abril, Reguladora de les Bases de Règim Local, modificada per la llei 11/1999, de 21 d'abril.
- Reial Decret Legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el Text refós de la Llei de Propietat Intel·lectual.
- Reial Decret Legislatiu 5/2015, de 30 d'octubre, pel qual s'aprova el text refós de la Llei de l'Estatut Bàsic de l'Empleat Públic.
- Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Reial Decret 1553/2005, de 23 de desembre, pel qual es regula el document nacional d'identitat i els seus certificats de signatura electrònica.
- Text refós de la Llei de Contractes de Sector Públic, aprovat per Reial Decret Legislatiu 3/2011, de 14 de novembre, i la normativa de desenvolupament.
- Reial decret llei 14/2019, de 31 d'octubre, pel qual s'adopten mesures urgents per raons de seguretat pública en matèria d'administració digital, contractació del sector públic i telecomunicacions.

6. OBJECTIUS

El Consell Comarcal de l'Alt Penedès, per assolir el compliment dels articles 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), que recullen els principis bàsics i els requisits mínims de la Seguretat de la Informació, ha implementat diverses mesures de seguretat proporcionals a la naturalesa de la informació i dels serveis a protegir, i tenint en compte la categoria dels sistemes afectats.

La seguretat com un procés integral (*article 6*) i la seguretat per defecte (*article 19*)

La seguretat constitueix un procés integrat per tots els elements tècnics, humans, materials i organitzatius relacionats amb el sistema. L'aplicació de l'Esquema Nacional de Seguretat al Consell Comarcal de l'Alt Penedès 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, perquè ni el desconeixement, ni la manca d'organització i coordinació, ni les instruccions inadequades, siguin font de risc per a la seguretat.

Els sistemes es dissenyaran de manera que garanteixin la seguretat per defecte:

a) El sistema proporcionarà la mínima funcionalitat requerida perquè l'organització assoleixi els seus objectius.
b) Les funcions d'operació, administració i registre d'activitat seran les mínimes necessàries, i s'ha de garantir que només són accessibles per a les persones autoritzades o des d'emplaçaments i equips autoritzats; podent-se exigir, si 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 no siguin d'interès, les que siguin innecessàries o inadequades.
d) 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 la persona usuària.

Reavaluació periòdica (article 9) i integritat i actualització de sistema (article 2)

El Consell Comarcal ha implementat controls i avaluacions regulars de la seguretat (incloent avaluacions dels canvis de configuració de forma rutinària) per conèixer, en tot moment, l'estat de la seguretat dels sistemes amb relació a les especificacions dels fabricants, les vulnerabilitats i les actualitzacions que els puguin afectar, i ha reaccionat amb diligència per gestionar el risc a la vista del seu estat de seguretat.
Abans de la introducció de nous elements, ja siguin físics o lògics, caldrà una autorització formal.

També es sol·licitarà l'auditoria periòdica dels sistemes, per part de tercers, amb la finalitat d'obtenir una avaluació independent.

Gestió del personal (article 14) i professionalitat (article 15)

Com a mínim un cop l'any, tot el personal del Consell Comarcal de l'Alt Penedès, dins l'àmbit de l'ENS, assistirà a una sessió de conscienciació en matèria de seguretat. Aquesta

sessió s'integrarà també en la política de benvinguda del nou personal del Consell Comarcal.

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

Incidents de seguretat (article 24), prevenció, reacció i recuperació (article 7)

El Consell Comarcal ha implementat un procés integral de detecció, reacció i recuperació davant de codi nociu, mitjançant el desenvolupament de procediments que cobreixen tant els mecanismes de detecció, els criteris de classificació i els procediments d'anàlisi i resolució, com les vies de comunicació a les parts interessades i el registre de les actuacions. Aquest registre es farà servir per a la millora contínua de la seguretat de sistema.

Per tal que la informació i els serveis es vegin perjudicats el mínim possible per incidents de seguretat, el Consell Comarcal de l'Alt Penedès ha implementat les mesures de seguretat establertes per l'ENS, i qualsevol altre control addicional que hagi identificat com a necessari a través d'una avaluació d'amenaces i riscos. Aquests controls, i també els rols i les responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Quan es produeixi una desviació significativa respecte dels paràmetres preestablerts com a normals, s'establiran els mecanismes de detecció, anàlisi i informe necessaris perquè arribin regularment a les persones responsables.

El Consell Comarcal de l'Alt Penedès ha d'establir les mesures de reacció següents davant d'incidents de seguretat:

- Mecanismes per respondre eficaçment als incidents de seguretat.
- Designació d'un mecanisme per comunicar els incidents detectats per part dels departaments o altres organismes.
- Establiment de protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou les comunicacions (en ambdós sentits) amb els Equips de Resposta a Emergències (CERT).
- Determinar mitjans i tècniques necessaris per garantir la recuperació i la disponibilitat dels serveis més crítics.

Línies de defensa (article 8) i prevenció davant altres sistemes interconnectats (article 22)

El Consell Comarcal de l'Alt Penedès ha d'implementar una estratègia de protecció basada en múltiples capes, constituïdes per mesures organitzatives, físiques i lògiques, de manera que, quan una de les capes falli, el sistema implementat permeti:

- Guanyar temps per reaccionar adequadament davant els incidents que no s'han pogut evitar.
- Reduir la probabilitat que el sistema quedi compromès en el seu conjunt.
- Minimitzar l'impacte final sobre el mateix.

Aquesta estratègia ha de protegir especialment el perímetre, en particular si es connecta a xarxes públiques. En tot cas s'analitzaran els riscos derivats de la interconnexió del sistema amb altres sistemes a través de xarxes, i es controlarà el seu punt d'unió.

Funció diferenciada (article 10) i organització i implantació del procés de seguretat (article 12)

El Consell Comarcal de l'Alt Penedès organitzat la seguretat de 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 "ORGANITZACIÓ DE LA SEGURETAT" d'aquest document.

Autorització i control dels accessos (article 16)

El Consell Comarcal de l'Alt Penedès ha implementat mecanismes de control d'accés al sistema d'informació, limitant els accessos als estrictament necessaris i degudament autoritzats.

Protecció de les instal·lacions (article 17)

El Consell Comarcal de l'Alt Penedès ha implementat mecanismes de control de l'accés físic per prevenir els danys a la informació i als recursos, impedint els accessos físics no autoritzats mitjançant perímetres de seguretat, controls físics i proteccions generals en àrees.

Adquisició de productes de seguretat i contractació de serveis de seguretat (article 18)

Per a l'adquisició de productes, el Consell Comarcal de l'Alt Penedès ha de valorar que aquests tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de la seva

adquisició; excepte en aquells casos en què les exigències de proporcionalitat, pel que fa als riscos assumits, no ho justifiquin a criteri del responsable de Seguretat.

Protecció de la informació emmagatzemada i en trànsit (article 21) i continuïtat de l'activitat (article 25)

El Consell Comarcal de l'Alt Penedès ha implementat mecanismes per protegir la informació emmagatzemada o en trànsit, especialment quan aquesta es troba en entorns insegurs (portàtils, tauletes, suports d'informació, xarxes obertes, etc.).
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 de treball.

S'ha de disposar de procediments que assegurin la recuperació i la conservació a llarg termini dels documents electrònics produïts en l'àmbit de les competències del Consell Comarcal de l'Alt Penedès. De la mateixa manera, s'han implementar mecanismes de seguretat d'acord amb la naturalesa del suport en què es trobin els documents, per garantir que tota la informació en suport no electrònic estigui protegida amb el mateix grau de seguretat que l'electrònica.

Registres d'activitat (article 23)

El Consell Comarcal de l'Alt Penedès ha habilitat registres de l'activitat dels usuaris (*logs*), retenint la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, i permetent identificar en cada moment a la persona que actua. Tot això amb la finalitat exclusiva d'aconseguir el compliment de 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 siguin aplicables.

7. DADES DE CARÀCTER PERSONAL

Des de la seva condició de Responsable de Tractament, el Consell Comarcal de l'Alt Penedès dona compliment a la normativa de protecció de dades per a les dades dels ciutadans a les quals els Encarregats de Tractament accedeixen, visionen i tracten en el marc de la prestació de serveis que realitzen.

Per aquest motiu, disposa d'un registre d'activitats de tractament (RAT) actualitzat que defineix i analitza els riscos que el tractament de dades pot significar. També realitza les pertinents avaluacions d'impacte sobre les dades personals i aplica les mesures tècniques I organitzatives necessàries per realitzar un tractament de dades de conformitat amb els

requisits reglamentaris i legals, amb la qual cosa dona compliment a les notes de confidencialitat, disponibilitat i integritat exigides per la normativa de protecció de dades en el marc de la seva responsabilitat proactiva.

8. COMPROMÍS DE LA DIRECCIÓ

El Govern del Consell Comarcal de l'Alt Penedès expressa el seu compromís total amb aquesta política de seguretat, per la qual cosa mantindrà les directrius fixades en aquest document i proporcionarà els recursos adequats.

9. ORGANIZACIÓ DE LA SEGURETAT

L'organització de la Seguretat de la Informació del Consell Comarcal de l'Alt Penedès s'estableix de la manera que s'indica tot seguit:

9.1. ROLS O PERFILS DE SEGURETAT

Per garantir el compliment i l'adaptació de les mesures exigides s'han creat rols o perfils de seguretat i s'han designat els càrrecs o òrgans que els ocuparan, de la forma següent:

- Delegat de Protecció de Dades (DPD)
- Responsable de la Informació i Serveis
- Responsable de Seguretat (TIC)
- Responsable del Sistema

9.2. COMITÉ DE SEGURETAT TIC

El Consell Comarcal de l'Alt Penedès ha constituït un Comitè de Seguretat de la Informació, com a òrgan col·legiat, format pels membres següents:

- Presidència: la Gerència del Consell.
- Responsable de Manteniment.
- Responsable de RRHH
- Responsable TIC.
- Delegat de Protecció de Dades
- La cap de l'OAC i Consum.

El secretari del Comitè STIC serà el responsable de les TIC del Consell Comarcal i tindrà les funcions següents:

- Convocar per ordre del president les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes a tractar en les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de les reunions.

El Delegat de Protecció de Dades participarà, amb veu però sense vot, en les reunions de Comitè de Seguretat de la Informació quan s'hagin d'abordar qüestions relacionades amb el tractament de dades de caràcter personal, i també sempre que es requereixi la seva participació. Quan el DPD assisteixi a una reunió per tractar un assumpte sotmès a votació, es farà constar sempre en l'acta la seva opinió.

El Comitè podrà requerir l'assistència a les seves reunions d'altres membres del Consell Comarcal, inclosos grups de treball especialitzats.

La Comissió es reunirà en sessió ordinària, almenys un cop l'any, amb l'objecte d'elaborar un informe que remetrà a la direcció de l'entitat i que coincidirà amb el lliurament dels indicadors per a l'Informe Nacional de l'Estat de Seguretat (INES). Igualment, podrà reunir-se en sessió extraordinària sempre que els assumptes relacionats amb les seves competències ho requereixin.

Les reunions seran convocades per la Presidència de la Comissió, per pròpia iniciativa o a petició de qualsevol dels seus components. El seu quòrum mínim serà de 4 membres, sent necessària la presència de la gerència, el responsable de les TIC, el responsable de RRHH i el delegat de protecció de dades.

9.3. RESPONSABILITATS ASSOCIADES A L'ESQUEMA NACIONAL DE SEGURETAT

9.3.1. Responsable de la Informació i Serveis

El Responsable de la Informació i Serveis durà a terme les tasques següents amb relació a l'Esquema Nacional de Seguretat:

- Identificar, valorar i aprovar la informació i els serveis a ciutadans o d'altres administracions públiques que fossin tractats pel Consell Comarcal.
- Prèvia proposta al responsable de seguretat de l'ENS i/o al Comitè de Seguretat de la Informació, establir i aprovar els requisits de seguretat aplicables al servei i a la

informació dins el marc establert en l'annex I del Reial Decret 3/2010, de 8 de gener.
- Acceptar els nivells de risc residual que afectin al Servei i a la Informació.
- Conèixer l'estat de la seguretat de la informació tractada i dels serveis prestats.
- Comunicar al Govern de l'organisme la necessitat de suspendre un servei per violacions de la seguretat que afectin a la informació tractada o al mateix servei.

9.3.2. Responsable de Seguretat

El Responsable de Seguretat durà a terme les tasques següents amb relació a l'Esquema Nacional de Seguretat:

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

Quan la complexitat del sistema ho justifiqui, el Responsable de Seguretat podrà designar els responsables del sistema delegats que consideri necessaris, que tindran dependència funcional directa d'aquell i seran responsables en el seu àmbit de totes aquelles accions que els delegui. De la mateixa manera, també podrà delegar funcions concretes de les responsabilitats que se li atribueixen.

9.3.3. Responsable del Sistema IT

El Responsable del Sistema IT durà a terme les tasques següents amb relació a l'Esquema Nacional de Seguretat:

- Implementar les mesures de seguretat d'índole tècnica que hagués estipulat com a necessàries el Responsable de Seguretat.

- Posar en marxa els plans de continuïtat del servei, assessorat pel Responsable de Seguretat.
- Gestionar, configurar i actualitzar, si escau, el maquinari i el programari en els quals es basen els mecanismes i els serveis de seguretat del Sistema d'Informació.
- Gestionar les autoritzacions concedides als usuaris del sistema, en particular els privilegis concedits, incloent-hi el monitoratge que l'activitat desenvolupada en el sistema s'ajusta a l'autoritzada.
- Aplicar els Procediments Operatius de Seguretat.
- Aprovar els canvis en la configuració vigent del Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són assolits estrictament.
- Assegurar que són aplicats els procediments aprovats per gestionar el sistema d'informació.
- Supervisar les instal·lacions de maquinari i programari per garantir que la seguretat no queda compromesa i que s'ajusten a les autoritzacions pertinents.
- Monitoritzar l'estat de seguretat del sistema proporcionat per les eines de gestió d'esdeveniments de seguretat i pels mecanismes d'auditoria tècnica implantats.

9.3.4. Comitè de Seguretat TIC

El Comitè STIC tindrà les funcions següents:

- Divulgar la política i la normativa de seguretat.
- Revisar i actualitzar la normativa de seguretat.
- Desenvolupar el procediment de designació de rols.
- Designar rols i responsabilitats.
- Promocionar, supervisar i aprovar les tasques de seguiment de l'ENS:
    - Tasques d'adequació
    - Anàlisi de riscos
    - Plans de millora de la seguretat de la informació
- Elaborar l'estratègia d'evolució pel que fa a seguretat de la informació.
- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris, des del punt de vista de la seguretat de la informació.
- Promoure les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
- Monitoritzar els principals riscos residuals assumits pel seu organisme i recomanar possibles actuacions respecte d'aquests.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació per assegurar que els esforços són consistents i alineats amb l'estratègia decidida en aquesta matèria i per evitar duplicitats.
- Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats

9.4. ASSIGNACIÓ DE ROLS

Es designa com a Responsable de la Informació i Serveis el/la gerent del Consell Comarcal de l'Alt Penedès.

Es designa com a Responsable de la Seguretat i Responsable del Sistema, el Responsable TIC del Consell Comarcal de l'Alt Penedès.

9.5. PROCEDIMIENTS DE DESIGNACIÓ DE LES PERSONES

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels responsables identificats en aquesta Política ha estat realitzada per la Junta de Govern del Consell Comarcal de l'Alt Penedès.
Els membres de Comitè i els rols de seguretat seran revisats cada quatre anys o en ocasió de vacant.

9.6. RESOLUCIÓ DE CONFLICTES

El Comitè STIC, i en cas que no es constitueixi, la gerència del Consell, s'encarregarà de la resolució dels conflictes o diferències d'opinió que poguessin sorgir entre els rols de seguretat.

10. GESTIÓ DE RISCOS

Tots els sistemes subjectes a aquesta Política hauran de realitzar una avaluació de les amenaces i els riscos als quals estan exposats. Aquesta avaluació es repetirà:

- Regularment, almenys una vegada a l'any.
- Quan canviï la informació gestionada.
- Quan canviïn els serveis prestats.
- Quan ocorri un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

Per a l'harmonització de les avaluacions, el Comitè STIC establirà una valoració de referència per als diferents tipus d'informació manipulada i els diferents serveis prestats. El comitè STIC dinamitzarà la disponibilitat dels recursos per atendre les necessitats de seguretat dels diferents sistemes i promourà inversions de caràcter horitzontal.

11. DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Consell Comarcal ha de desenvolupar i implementar un sistema de gestió, que serà establert, implementat, mantingut i millorat, d'acord amb els estàndards de seguretat i els recursos disponibles.

Aquest sistema s'adequarà i servirà de gestió dels controls de l'Esquema Nacional de Seguretat. Serà documentat i permetrà generar evidències dels controls i de l'acompliment dels objectius marcats pel Comitè.

Haurà d'existir un procediment que estableixi les directrius per a l'estructuració de la documentació de seguretat del sistema, la seva gestió i el seu accés.

També s'establiran, com a mínim, les polítiques següents:

1. Ús dels sistemes TIC al Consell.
2. Ús de dispositius mòbils al Consell.
3. Accés d'externs als sistemes d'Informació del Consell.
4. Comunicació i resolució d'incidents de seguretat.
5. Còpies de seguretat.
6. Pla de recuperació d'incidents greus de seguretat.

Les polítiques 1, 2 i 3 les aprovarà l'òrgan competent, en tractar-se de matèries que afecten els drets i les obligacions del personal o les empreses externes. Les polítiques 4, 5 i 6 les aprovarà el Responsable de Seguretat, en tractar-se de documents interns.

Correspon al Comitè STIC la revisió anual d'aquesta Política de Seguretat de la Informació i, si és necessari, proposar millores i elevar-les al Ple del Consell Comarcal per a la seva aprovació.

12. OBLIGACIONS DEL PERSONAL

Tot el personal del Consell Comarcal de l'Alt Penedès i tot el personal que presti serveis al Consell Comarcal relacionats amb els sistemes d'informació té l'obligació de conèixer els principis de la Política de Seguretat de la Informació i complir la normativa d'ús de les TIC que se'n derivin.

El seu incompliment podrà implicar l'adopció de les mesures disciplinàries oportunes i, si escau, les responsabilitats legals corresponents.

13. TERCERES PARTS

Quan el Consell Comarcal de l'Alt Penedès presti serveis a municipis de la comarca o tingui accés a la seva informació, se'ls farà partícips de la normativa interna rellevant en matèria de TIC, inclosos els principis establerts en la Política de Seguretat de la Informació. Quan el personal del Consell Comarcal presti serveis en altres administracions i es produeixi un incident de seguretat relacionat amb les TIC, s'establiran canals de comunicació entre els ens afectats a fi i efecte de cooperar de bona fe per a la resolució del problema i per tal de minimitzar els efectes.

Quan el Consell Comarcal utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips de la Política de Seguretat o de la Normativa de Seguretat que pertoqui i hauran de complir els mateixos mínims que es determinin per al personal del Consell Comarcal (amb les particularitats pròpies de cada cas).

Quan algun aspecte de la 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 del Consell Comarcal que indiqui els riscos en què s'incorre i la forma d'afrontar-los. Es requerirà l'aprovació d'aquest informe per part dels responsables de la informació i dels serveis afectats abans de seguir endavant.