El Ple del Consell de Garanties Estatutàries, en la seva sessió de data 31 de juliol de 2024, ha aprovat la política de seguretat de la informació de la institució i ha disposat la seva publicació en el lloc web oficial del Consell.

Així mateix, en compliment de l'autorització del Ple, i en ús de les atribucions conferides per l'article 7.3 de la Llei 2/2009, de 12 de febrer, i l'article 12./ del Reglament d'organització i funcionament del Consell, el president del Consell de Garanties Estatutàries ha signat la política de seguretat de la informació en data 31 de juliol de 2024.

PALAU CENTELLES
Baixada de Sant Miquel, 8 - 08002 Barcelona
Tel. + 34 933 176 268 Fax + 34 933 181 720
consell@cge.cat

CONSELL DE GARANTIES ESTATUTÀRIES
DE CATALUNYA

Política de seguretat de la informació del Consell de Garanties Estatutàries

Versió aprovada el dia 31 de juliol de 2024

Contingut

1. Introducció

Aquest document exposa la política de seguretat de la informació del Consell de Garanties Estatutàries de Catalunya (en endavant, "CONSELL"), com el conjunt de principis bàsics i línies d'actuació als quals l'organització es compromet, en el marc de l'Esquema Nacional de Seguretat (ENS).

La informació és un actiu crític, essencial i d'un gran valor per al desenvolupament de l'activitat del CONSELL. Aquest actiu ha de ser adequadament protegit, mitjançant les necessàries mesures de seguretat, davant les amenaces que puguin afectar-lo, independentment dels formats, suports, mitjans de transmissió, sistemes, o persones que intervinguin en el seu coneixement, processament o tractament.

La seguretat de la informació és la protecció d'aquest actiu, amb la finalitat d'assegurar la qualitat de la informació i la continuïtat de les funcions de la institució i minimitzar el risc.

La seguretat de la informació és un procés que requereix mitjans tècnics i humans i una adequada gestió i definició dels procediments i en el qual és fonamental la màxima col·laboració i implicació de tot el personal i membres del CONSELL.

El Ple del CONSELL, conscient del valor de la informació, està profundament compromès amb la política descrita en aquest document.

2. Definicions

- **Sistema d'informació:** conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, utilitzar, compartir, distribuir, posar a disposició, presentar o transmetre.
- **Risc:** estimació del grau d'exposició perquè una amenaça es materialitzi sobre un o més actius i causi danys o perjudicis a l'organització.
- **Gestió de riscos:** activitats coordinades per dirigir i controlar una organització respecte als riscos.
- **Sistema de gestió de seguretat de la informació (SGSI):** sistema de gestió que, basat en l'estudi dels riscos, s'estableix per crear, implementar, fer funcionar, supervisar, revisar, mantenir i millorar la seguretat de la informació. El sistema de gestió inclou l'estructura organitzativa, les polítiques, les activitats de planificació, les responsabilitats, les pràctiques, els procediments, els processos i els recursos.
- **Disponibilitat:** És necessari garantir que els recursos del sistema es trobaran disponibles quan es necessitin, especialment la informació crítica.
- **Integritat:** La informació del sistema ha d'estar disponible tal com es va emmagatzemar per un agent autoritzat.

- **Confidencialitat:** La informació només ha d'estar disponible per a agents autoritzats, especialment el seu propietari.
- **Autenticitat**: S'ha d'assegurar la identitat o origen de la informació.
- **Traçabilitat**: S'ha d'assegurar per a certes dades qui va fer què i en quin moment.

3. Propòsit

El propòsit d'aquesta política de seguretat de la informació és protegir els actius d'informació del CONSELL, tot assegurant la disponibilitat, integritat, confidencialitat, autenticitat i traçabilitat de la informació i de les instal·lacions, sistemes i recursos que la processen, gestionen, transmeten i emmagatzemen, sempre d'acord amb els requeriments de la seva activitat i la legislació vigent.

4. Abast

La present política de seguretat de la informació és d'aplicació a totes les persones, sistemes i mitjans que accedeixin, tractin, emmagatzemin, transmetin o utilitzin la informació coneguda, gestionada o propietat del CONSELL per als processos descrits.

El personal subjecte a aquesta política inclou totes les persones amb accés a la informació descrita, independentment del suport automatitzat o no en el que es trobi aquesta i de si l'usuari és o no empleat del CONSELL. Per tant, també s'aplica a qualsevol tercer que tingui accés a la informació o als sistemes del CONSELL.

Per garantir que el procés de seguretat implementat sigui actualitzat i millorat de forma contínua, s'implantarà i documentarà un sistema de gestió de la seguretat de la informació. Així, el contingut de la política de seguretat de la informació serà desenvolupat en normes i procediments complementaris de seguretat.

5. Objectius o missió de la institució

El Consell de Garanties Estatutàries és la institució de la Generalitat que vetlla per l'adequació de les normes amb rang de llei del Govern i del Parlament a l'Estatut i a la Constitució. Així mateix, també és responsable d'identificar, amb caràcter previ a la presentació dels recursos corresponents davant el Tribunal Constitucional, els possibles motius d'inconstitucionalitat i de conflicte de competències que puguin afectar l'autogovern català o l'autonomia local a conseqüència de la normativa d'origen estatal.

El CONSELL exerceix la seva funció consultiva mitjançant dictàmens jurídics sol·licitats pel Parlament, el Govern, el Síndic de Greuges o les institucions locals. Així mateix, compleix un paper d'especial tutela dels drets estatutaris d'acord amb l'article 38.1 de l'Estatut d'autonomia de Catalunya.

6. Fonaments d'aquesta política

L'objectiu últim de la seguretat de la informació és garantir que una organització pugui complir els seus objectius, desenvolupar les seves funcions i exercir les seves competències utilitzant sistemes d'informació. Per tant, en matèria de seguretat de la informació s'hauran de tenir en compte els següents principis bàsics:

Seguretat com a procés integral

La seguretat s'ha d'entendre com un procés integrat per tots els elements tècnics, humans, materials i organitzatius, relacionats amb el sistema.

Es promourà la conscienciació de les persones que intervenen en el procés i els seus responsables jeràrquics perquè ni la ignorància, ni la falta d'organització i coordinació, ni instruccions inadequades no siguin font de risc per a la seguretat.

Gestió de la seguretat basada en els riscos

L'anàlisi dels riscos és part essencial i contínua del procés de seguretat. La gestió d'aquests riscos permetrà el manteniment d'un entorn controlat, amb els esmentats riscos a nivells acceptables, i es realitzarà mitjançant l'aplicació de mesures de seguretat de manera proporcionada a la naturalesa de la informació tractada i dels serveis prestats.

Prevenció, detecció, resposta i conservació

La seguretat del sistema preveu mesures que implementin els aspectes de prevenció, detecció i resposta davant d'incidents de seguretat, i de conservació de la informació i dels serveis en cas que l'incident es produeixi.

Existència de línies de defensa

El CONSELL implementa una estratègia de protecció basada en múltiples capes, constituïdes per mesures organitzatives, físiques i lògiques, de tal manera que quan una de les capes falli, el sistema permeti:

- Guanyar temps per a una reacció adequada davant els incidents que no han pogut evitar-se.
- Reduir la probabilitat que el sistema sigui compromès en el seu conjunt.
- Minimitzar l'impacte final sobre el sistema.

Les línies de defensa han d'estar constituïdes per mesures de naturalesa organitzativa, física i lògica.

Vigilància contínua i reavaluació periòdica

La vigilància contínua permetrà la detecció d'activitats o comportaments anòmals i la seva resposta oportuna.

El CONSELL implementa controls i avaluacions regulars de la seguretat (incloses avaluacions dels canvis de configuració de forma rutinària) per

conèixer en tot moment l'estat de la seguretat dels sistemes en relació amb les especificacions dels fabricants, les vulnerabilitats i les actualitzacions que els afectin, tot reaccionant amb diligència per gestionar el risc en vista del seu estat de seguretat. L'entrada de nous elements, ja siguin físics o lògics, requerirà una autorització formal prèvia.

Així mateix, sol·licitarà la revisió periòdica per part de tercers a fi d'obtenir una avaluació independent.

Les mesures de seguretat s'avaluaran i actualitzaran periòdicament i s'adequarà la seva eficàcia a l'evolució dels riscos i els sistemes de protecció, fins al punt d'arribar a un replantejament de la seguretat, si fos necessari.

Diferenciació de responsabilitats

El CONSELL ha organitzat la seva seguretat amb el compromís de tots els membres i el personal de la institució mitjançant la designació de diferents rols de seguretat amb responsabilitats clarament diferenciades, tal com es recull més endavant en aquest document.

En els sistemes d'informació es diferenciarà entre el responsable de la informació, que determina els requisits de la informació tractada; el responsable del servei, que determina els requisits dels serveis prestats; el responsable del sistema, que s'encarregarà de desenvolupar la forma concreta d'implementar la seguretat en el sistema i de la supervisió de la seva operació diària; i el responsable de seguretat, que determina les decisions per a satisfer els requisits de seguretat de la informació i els serveis. El Comitè de Seguretat de la Informació (o Comitè de Seguretat), ateses les característiques del CONSELL, assumeix, en aquest cas, les funcions del responsable de seguretat. En els supòsits de tractament de dades personals s'identificarà, a més, el responsable de tractament i, si escau, l'encarregat de tractament.

7. Requisits de seguretat

Aquesta política de seguretat es desenvoluparà aplicant els següents requisits:

Organització i implantació del procés de seguretat

La seguretat de la informació compromet tots els membres de l'organització. El CONSELL identifica els responsables i estableix les seves responsabilitats en els apartats de "Rols, responsabilitats i deures" i "Terceres parts" d'aquest document. Les persones compreses en l'àmbit d'aplicació d'aquest document coneixeran aquesta política de seguretat i la normativa.

Anàlisi i gestió dels riscos. Inclusió dels riscos amb dades personals

Conèixer els riscos i elaborar una estratègia per gestionar-los adequadament és primordial per al CONSELL, ja que únicament si es coneix l'estat de

seguretat podran prendre's les decisions adequades per mitigar els riscos a què s'enfronta.

Quan un sistema d'informació tracti dades personals s'aplicarà allò previst en el Reglament General de Protecció de Dades (RGPD) i en la LOPDGDD o, en el seu cas, la Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractats per a finalitats de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals. El responsable o l'encarregat del tractament, assessorat pel delegat/a de protecció de dades, realitzarà una anàlisi de riscos conforme a l'article 24 del RGPD i, en els supòsits del seu article 35, una avaluació d'impacte en la protecció de dades. Del resultat d'aquesta anàlisi poden derivar-se mesures addicionals per implantar.

El CONSELL utilitza la metodologia Magerit per analitzar els riscos i realitza una anàlisi detallada dels que afectin els actius recollits en un inventari d'actius, que queda documentat en un document d'anàlisi de riscos.

L'entitat determina els nivells de risc a partir dels quals pren accions de tractament sobre aquests. Un risc es considera acceptable quan implementar més controls de seguretat s'estima que consumiria més recursos que el possible impacte associat.

El Comitè de Seguretat, que assumeix les funcions del responsable de seguretat, serà l'encarregat de que es realitzi l'anàlisi de riscos, així com d'identificar mancances i debilitats i d'informar-ne el Ple del CONSELL.

Aquesta anàlisi es repetirà:

- Regularment, almenys una vegada cada any.
- Quan canviïn la informació tractada i/o els serveis prestats de manera significativa.
- Quan es produeixi un incident greu de seguretat o es detectin vulnerabilitats greus.

Una vegada dut a terme el procés d'avaluació de riscos, el Ple del CONSELL és el responsable d'aprovar els riscos residuals i els plans de tractament de risc.

En el cas de les mesures implantades segons l'ENS, si l'anàlisi de riscos estableix mesures més importants, aquestes s'afegiran a les descrites a l'ENS.

Gestió de personal

Tot el personal del CONSELL relacionat amb la informació i els sistemes és format i informat sobre els seus deures i obligacions en matèria de seguretat, essencialment mitjançant els procediments de seguretat que en cada cas siguin procedents i mitjançant la normativa d'ús dels actius. Les seves actuacions són supervisades segons els rols establerts per verificar que se segueixen els procediments definits.

Els accessos dels usuaris són únics i els seus drets i les activitats que tenen a veure amb la seguretat de la informació per corregir o exigir responsabilitats, si escau, es verifiquen de forma periòdica.

Professionalitat, conscienciació i formació

La seguretat dels sistemes és gestionada i revisada per personal del CONSELL qualificat i personal extern especialitzat, que rep i actualitza la formació necessària per garantir la seguretat de la informació en tot el cicle de vida dels sistemes d'informació: planificació, disseny, adquisició, construcció, desplegament, explotació, manteniment, gestió d'incidències i desmantellament. Els requisits de qualificació (formació i experiència) seran sempre establerts pel CONSELL.

Aquesta política de seguretat de la informació ha de ser coneguda per tots els usuaris interns i externs i per les empreses que accedeixin, gestionin o tractin dades del CONSELL.

El conjunt de polítiques, normes i procediments complementaris a aquesta política de seguretat de la informació també haurà de ser adequadament comunicat a les persones, empreses i institucions afectades o implicades en cada cas.

Es definiran, periòdicament, programes de comunicació, conscienciació i formació i es posarà a disposició dels usuaris la normativa d'ús dels actius d'informació.

El CONSELL promourà la formació tècnica en seguretat de la informació necessària, especialment per als membres del Comitè de Seguretat, atesa l'assumpció de les funcions del responsable de seguretat per part d'aquest Comitè, i per al responsable de sistemes.

Autorització i control dels accessos

L'accés als sistemes d'informació és controlat, monitoritzat i limitat als usuaris, processos, dispositius i sistemes d'informació amb les mínimes funcionalitats permeses i/o autoritzades.

S'establiran i gestionaran les autoritzacions necessàries per a les tasques crítiques.

Protecció de les instal·lacions

Els sistemes del CONSELL i la seva infraestructura de comunicacions estan situats en àrees degudament protegides, dotades de mesures de seguretat físiques, de redundància, continuïtat i ambientals, i amb un procediment de control d'accés físic.

Adquisició de productes de seguretat i contractació de serveis de seguretat

Per a l'adquisició de productes, el CONSELL tindrà en compte que aquests tinguin certificada la funcionalitat de seguretat relacionada amb l'objecte de

la seva adquisició, tret d'aquells casos en què les exigències de proporcionalitat quant als riscos assumits no ho justifiquin, segons el parer Comitè de Seguretat, actuant com a responsable de seguretat.

Per a la contractació de serveis de seguretat s'aplicarà allò previst en els apartats anteriors i en l'apartat "Terceres parts" més endavant en aquest document.

Mínim privilegi i seguretat des del disseny

En el CONSELL els sistemes es dissenyen i configuren sempre pensant en la seguretat per defecte. El sistema proporciona la funcionalitat mínima requerida perquè les funcions d'operació, administració i registre d'activitat siguin les mínimes necessàries, i el CONSELL s'assegura que només són accessibles per a les persones i des d'emplaçaments o equips autoritzats.

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

Tots els projectes relacionats o que afectin els sistemes d'informació hauran d'incloure, en el seu procés d'anàlisi, una avaluació dels requisits de seguretat i definir un model de seguretat consensuat amb el Comitè de Seguretat en la seva actuació com a responsable de seguretat de la informació.

En el disseny, desenvolupament, instal·lació i gestió dels sistemes d'informació i en els projectes es tindran en compte i aplicaran els conceptes de seguretat des del disseny, codificació segura i els controls i mesures de seguretat que siguin procedents segons el document d'aplicabilitat aprovat pel CONSELL.

Integritat i actualització del sistema

En el CONSELL els sistemes s'avaluen de manera periòdica per conèixer en tot moment el seu estat de seguretat, prenent en consideració les especificacions dels fabricants, les vulnerabilitats, les deficiències de la seva configuració, les actualitzacions que siguin procedents i la detecció primerenca d'incidents, i gestionant d'aquesta manera la seva integritat.

Tots els elements dels sistemes requereixen autorització prèvia a la seva instal·lació.

Protecció de la informació emmagatzemada i en trànsit

La informació es classifica d'acord amb la sensibilitat requerida en el seu tractament i segons els nivells de seguretat i protecció exigibles.

El CONSELL para especial atenció a la informació emmagatzemada o en trànsit a través d'entorns insegurs. Això inclou la informació emmagatzemada

o tractada en equips portàtils, tauletes, telèfons intel·ligents, dispositius perifèrics, suports d'informació, així com les comunicacions sobre xarxes obertes o amb xifratge feble, on s'apliquen les mesures de seguretat que garanteixin que la informació es tracta conforme a la seva classificació.

S'aplicaran procediments que garanteixin la recuperació i conservació a llarg termini dels documents electrònics produïts pels sistemes d'informació.

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

Prevenció davant d'altres sistemes d'informació interconnectats

El CONSELL protegeix el perímetre d'accés al seu sistema, en particular en les connexions a través d'internet, analitza sempre els riscos derivats de la interconnexió amb altres sistemes, i estableix les mesures que garanteixin el nivell de seguretat necessari.

Registre d'activitat i detecció de codi nociu

El CONSELL ha habilitat registres de l'activitat dels usuaris que permeten retenir la informació necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, i identificar en cada moment la persona que actua. Tot això 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 i altres disposicions que resultin d'aplicació.

El CONSELL implementa un procés integral de detecció, reacció i recuperació davant codi nociu mitjançant el desenvolupament de procediments que cobreixen els mecanismes de detecció, els criteris de classificació, els procediments d'anàlisi i resolució, així com les vies de comunicació a les parts interessades i el registre de les actuacions.

Amb la finalitat de preservar la seguretat dels sistemes d'informació i garantir el rigorós compliment dels principis d'actuació de les administracions públiques, i de conformitat amb les disposicions del RGPD i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació enunciats a l'esmentat Reglament, es podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, únicament per a les finalitats de seguretat de la informació, de manera 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 nociu així com altres danys a les dites xarxes i sistemes d'informació.

Per corregir o, si 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.

Incidents de seguretat

Per tal que la informació i/o els serveis no es vegin perjudicats per incidents de seguretat, el CONSELL implementa les mesures de seguretat establertes, així com qualsevol altre control addicional, que hagi identificat com a necessari, a través d'una avaluació d'amenaces i riscos. Aquests controls, així com els rols i responsabilitats de seguretat de tot el personal, estan clarament definits i documentats.

Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals, s'establiran els mecanismes de detecció, anàlisis i report necessaris perquè arribin als responsables regularment.

El CONSELL establirà les següents mesures de reacció davant d'incidents de seguretat:

- Mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions respecte 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 els Equips de Resposta a Emergències.
- Per garantir la disponibilitat dels serveis, el CONSELL disposa dels mitjans i tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

Els usuaris disposen de canals establerts per informar de forma immediata de qualsevol incident o anomalia detectada.

Continuïtat de l'activitat

El CONSELL realitza les còpies de seguretat que garanteixen la recuperació de la informació i estableix els mecanismes adequats per garantir la continuïtat de les operacions en cas de pèrdua dels mitjans habituals.

En aquest sentit s'han desenvolupat procediments que asseguren la recuperació i conservació a llarg termini dels documents i dades electròniques produïdes en l'àmbit de les seves competències.

Millora contínua del procés de seguretat

El sistema de gestió de seguretat implantat és actualitzat i millorat de manera contínua, segons estableixen les certificacions, tal com està descrit més endavant en aquest document.

8. Requisits legals i marc normatiu

A més de la normativa general en matèria de contractació, funció pública, procediment administratiu i règim jurídic del sector públic, així com de transparència i societat de la informació, i de la normativa reguladora de la institució, la política de seguretat de la informació del CONSELL es regeix pel següent marc normatiu específic en la seva versió vigent en cada moment:

- Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 abril de 2016 relatiu a la protecció de les persones físiques respecte al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (RGPD)
- Llei orgànica 3/2018, de 5 de desembre, de protecció de dades i garantia dels drets digitals (LOPDGDD)
- Reial decret legislatiu 1/1996, de 12 d'abril, pel qual s'aprova el text refós de la Llei de propietat intel·lectual, regularitzant, aclarint i harmonitzant les disposicions legals vigents sobre la matèria
- Llei 37/2007, de 16 de novembre, sobre reutilització de la informació del sector públic
- Reial decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional 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
- 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
- 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 d'Informe de l'Estat de la seguretat
- UNE-ISO/IEC 27001:2023 Seguretat de la informació, ciberseguretat i protecció de la privacitat. SGSI. Requisits
- UNE-ISO/IEC 27002:2023 Seguretat de la informació, ciberseguretat i protecció de la privacitat. Control de Seguretat de la Informació

Així mateix, el Comitè de Seguretat, actuant com a responsable de seguretat, serà responsable d'identificar les guies de seguretat del Centre Criptològic

Nacional (CCN), que seran d'aplicació per millorar el compliment del que estableix l'Esquema Nacional de Seguretat.

9. Rols, responsabilitats i deures

Usuaris

Tota persona o sistema que accedeixi a la informació tractada, gestionada o propietat del CONSELL es considerarà un usuari. Els usuaris són responsables de la seva conducta quan accedeixen a la informació o utilitzin els sistemes informàtics del CONSELL. L'usuari és responsable de totes les accions realitzades utilitzant els seus identificadors o credencials personals.

Els usuaris tenen l'obligació de:

- Complir la política de seguretat de la informació i les normes, procediments i instruccions complementàries.
- Protegir i custodiar la informació del CONSELL, evitant la revelació, emissió a l'exterior, modificació, esborrament o destrucció accidental o no autoritzada o el mal ús independentment del suport o mitjans pel qual hagi estat accedida o coneguda.
- Conèixer i aplicar la política de seguretat de la informació, les normes d'ús dels sistemes d'informació i la resta de polítiques, normes, procediments i mesures de seguretat aplicables.

Els usuaris que incompleixin la política de seguretat de la informació o les normes i procediments complementaris podran ser sancionats d'acord amb el règim disciplinari aplicable al personal al servei del CONSELL i, en el cas d'usuaris externs, de conformitat amb l'establert als contractes que emparin la seva relació amb la institució i amb la legislació vigent i aplicable.

Responsable de la informació (Esquema Nacional de Seguretat)

El responsable de la informació és qui determina els requisits de la informació tractada.

El responsable de la informació té les següents responsabilitats:

- Vetllar pel bon ús de la informació i, per tant, de la seva protecció.
- Establir els requisits de la informació en matèria de seguretat.
- Determinar els nivells de seguretat de la informació tractada, valorant les conseqüències d'un impacte negatiu.

Responsable del servei (Esquema Nacional de Seguretat)

El responsable del servei tindrà les següents responsabilitats generals:

- Establir els requisits del servei en matèria de seguretat, inclosos els requisits d'interoperabilitat, accessibilitat i disponibilitat.

- Determinar els nivells de seguretat del servei, d'acord amb el responsable de seguretat i el responsable del sistema.
- Mantenir la seguretat de la informació tractada i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat.

Direcció

El Ple del CONSELL està profundament compromès amb la política descrita en aquest document i és conscient del valor de la informació i del greu impacte econòmic i d'imatge que pot produir un incident de seguretat.

El Ple del CONSELL és, per tant, propietari dels actius d'informació propis del CONSELL, i també és responsable dels riscos.

El Ple del CONSELL assumeix a més les següents responsabilitats:

- Vetllar pel compliment del sistema de gestió de seguretat de la informació.
- Assegurar que s'estableix la política i els objectius de seguretat de la informació i que aquests són compatibles amb la direcció estratègica de l'organització.
- Aprovar i comunicar la política de seguretat de la informació, les normes d'ús dels sistemes d'informació i la importància del seu compliment a tots els usuaris, interns o externs, i als proveïdors.
- Convocar una sessió almenys una vegada a l'any i quan qualsevol esdeveniment o sol·licitud extraordinària ho requereixin, per ser informat pel president/a del Comitè de Seguretat sobre el SGSI i actualitzar l'estratègia en matèria de seguretat de la informació.
- Fomentar una cultura corporativa de seguretat de la informació.
- Donar suport a la millora contínua dels processos de seguretat de la informació.
- Assegurar que estiguin disponibles els recursos necessaris per al compliment de la política de seguretat de la informació, de les normes d'ús dels sistemes i per al funcionament del sistema de gestió de seguretat de la informació.
- Definir l'enfocament per a l'anàlisi i la gestió dels riscos de seguretat de la informació i els criteris per assumir els riscos i assegurar la seva avaluació almenys amb una periodicitat anual.
- Assegurar que es realitzen auditories internes de seguretat de la informació i que es revisen els seus resultats per identificar oportunitats de millora.
- Definir i controlar el pressupost per a la seguretat de la informació.
- Aprovar els plans de formació i les millores i projectes relacionats amb la seguretat de la informació.

- Aprovar la documentació fins al seu segon nivell de normes i procediments.
- Determinar les mesures, siguin disciplinàries o de qualsevol altre tipus, que poguessin aplicar-se als responsables de violacions de seguretat.

Responsable de seguretat

El Comitè de Seguretat, actuant com a responsable de la seguretat, determina les decisions per satisfer els requisits de seguretat de la informació i dels serveis i supervisa la implantació de les mesures necessàries per garantir que se satisfan els requisits i reportarà sobre aquestes qüestions.

En conseqüència assumirà les següents funcions:

- Promoure la seguretat de la informació tractada i dels serveis electrònics prestats pels sistemes d'informació, amb la responsabilitat i autoritat per assegurar-se que el sistema de gestió de la seguretat de la informació compleix els requisits de l'ENS.
- Supervisar el compliment de la present política, de les seves normes, procediments derivats i de la configuració de seguretat dels sistemes.
- Establir les mesures de seguretat, adequades i eficaces per complir els requisits de seguretat establerts pels responsables del servei i de la informació, seguint en tot moment l'exigit a l'annex II de l'ENS, i declarar l'aplicabilitat de les esmentades mesures.
- Promoure les activitats de conscienciació i formació en matèria de seguretat en el seu àmbit de responsabilitat.
- Realitzar la coordinació i seguiment de la implantació dels projectes d'adequació a les normes especificades en col·laboració amb el responsable de sistemes.
- Realitzar, amb la col·laboració del responsable del sistema, les preceptives anàlisis de riscos, seleccionar les salvaguardes a implantar i revisar el procés de gestió del risc. Així mateix, juntament amb el responsable del sistema, acceptar els riscos residuals calculats en l'anàlisi de riscos.
- Promoure auditories periòdiques per verificar el compliment de les obligacions en matèria de seguretat de la informació i analitzar els informes d'auditoria i elaborar les conclusions a presentar al responsable del sistema perquè adopti les mesures correctores adequades.
- Coordinar el procés de gestió de la seguretat, en col·laboració amb el responsable de sistemes.
- Firmar la declaració d'aplicabilitat, que comprèn la relació de mesures de seguretat seleccionades per a un sistema.
- Elaborar informes diaris de seguretat que incloguin els incidents més rellevants en cada període, en coordinació amb el responsable de sistemes.

- Determinar la categoria del sistema segons el procediment descrit a l'annex I de l'ENS i les mesures de seguretat que s'han d'aplicar d'acord amb el previst a l'annex II de l'ENS.
- Verificar que les mesures de seguretat són adequades per a la protecció de la informació i els serveis.
- Executar directament o de manera delegada les decisions del Ple del CONSELL i exposar-hi, a través del seu president/a, l'estratègia per assegurar-les.

Respecte a la documentació, i amb el suport del responsable del sistema, són funcions del Comitè de Seguretat com a responsable de seguretat:

- Proposar al Ple, per a la seva aprovació, la documentació de seguretat de segon nivell (normes de seguretat TIC —STIC— i procediments generals del sistema de gestió de la seguretat de la informació —SGSI—) i firmar l'esmentada documentació.
- Aprovar la documentació de seguretat de tercer nivell (procediments operatius STIC i instruccions tècniques STIC).
- Mantenir la documentació organitzada i actualitzada, gestionant els mecanismes d'accés a la mateixa.

El responsable de la seguretat serà diferent del responsable del sistema, i no existirà dependència jeràrquica entre ambdós.

Delegat/ada de protecció de dades

Seguint el que estableix el RGPD i la LOPDGDD, el/la delegat/ada de protecció de dades tindrà com a mínim les següents funcions:

- Informar i assessorar el responsable del tractament i els seus empleats de les obligacions que els corresponen en relació amb el RGPD i altres disposicions de protecció de dades.
- Supervisar el compliment d'allò previst en el RGPD, d'altres disposicions de protecció de dades de la Unió Europea o dels estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- Oferir l'assessorament que se li sol·liciti sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar la seva aplicació de conformitat amb l'article 35 RGPD.
- Cooperar amb l'autoritat de control en matèria de protecció de dades.
- Actuar com a punt de contacte de l'autoritat de control en matèria de protecció de dades per a qüestions relatives al tractament, inclosa la consulta prèvia a què es refereix l'article 36 RGPD, i realitzar consultes, si escau, sobre qualsevol altre assumpte.

Responsable del sistema

El responsable del sistema, per si o a través de recursos propis o contractats, s'encarrega de desenvolupar la forma concreta d'implementar la seguretat en el sistema i de la supervisió de la seva operació diària, i pot delegar en administradors o operadors sota la seva responsabilitat.

Seran funcions del responsable del sistema les següents:

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, de les seves especificacions, instal·lació i verificació del seu correcte funcionament.
- Definir la topologia i el sistema de gestió del sistema d'informació i establir els seus criteris d'ús i els serveis disponibles.
- Assegurar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Realitzar exercicis i proves sobre els procediments operatius de seguretat i els plans de continuïtat existents.
- Seguiment del cicle de vida dels sistemes: especificació, arquitectura, desenvolupament, operació, canvis.
- Implantar les mesures necessàries per garantir la seguretat del sistema durant tot el seu cicle de vida, d'acord amb el Comitè de Seguretat.
- Aprovar tota modificació substancial de la configuració de qualsevol element del sistema.
- Realitzar en el si del Comitè de Seguretat i amb la seva col·laboració les preceptives anàlisis de riscos, seleccionar les salvaguardes a implantar i revisar el procés de gestió del risc. Així mateix, juntament amb el Comitè de Seguretat, acceptar els riscos residuals calculats en l'anàlisi de riscos.
- Elaborar en el si del Comitè de Seguretat i amb la seva col·laboració, la documentació de seguretat de tercer nivell (procediments operatius STIC i instruccions tècniques STIC).

Comitè de Seguretat de la Informació

El Comitè de Seguretat de la Informació està format per un representant del Ple del CONSELL, que actuarà com a president/a, un representant dels Serveis Jurídics, que actuarà com a secretari/ària, un representant de l'àrea de Recursos Econòmics i Gestió dels Serveis Generals i el responsable de sistemes, que actuaran com a vocals.

Així mateix, assistirà a les reunions del Comitè, quan l'assumpte a tractar ho requereixi, el/la delegat/a de protecció de dades del CONSELL, que actuarà amb veu però sense vot.

Igualment, el Comitè podrà incorporar altres experts externs en qualitat d'assessors, que actuaran amb veu però sense vot.

El Ple del CONSELL designarà els membres del Comitè de Seguretat de la informació. Així mateix, també designarà, si escau, els substituts que actuaran en casos de vacant, absència o malaltia dels membres titulars.

El Comitè de Seguretat s'haurà de reunir una vegada al mes.

Les seves funcions 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. Amb aquest objectiu s'encarregarà de:
    - 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.
    - 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.
    - 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 funcionament. 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.
    - Realitzar un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'aquests.
    - Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'aquests.
    - Revisar regularment la present política de seguretat de la informació per a la seva aprovació per l'òrgan competent.
    - Elaborar la normativa de seguretat de la informació per a la seva aprovació en coordinació amb la direcció.
    - Verificar els procediments de seguretat de la informació i altra 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 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 de l'ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'organització en matèria de seguretat de la informació.

Procediment de designació i resolució de conflictes

El Ple del CONSELL assigna, renova i comunica les responsabilitats, autoritats i rols relatius a la seguretat de la informació, i determina en cada cas els motius i el termini de vigència. També s'assegurarà que els usuaris coneixen, assumeixen i exerceixen les responsabilitats, autoritats i rols assignats, i resoldrà els conflictes que es generin en relació amb cada responsabilitat en matèria de seguretat de la informació.

Dades de caràcter personal

L'organització només recollirà dades de caràcter personal quan siguin adequades, pertinents i no excessives i aquestes es trobin en relació amb l'àmbit i les finalitats per als quals s'hagin obtingut. De la mateixa manera, adoptarà les mesures d'índole tècnica i organitzatives necessàries per al compliment de la normativa de protecció de dades vigent en cada cas.

D'aquesta manera, amb la LOPDGDD s'han adaptat les mesures oportunes com ara l'anàlisi de legitimitat jurídica de cada un dels tractaments de dades que es duguin a terme, l'anàlisi de riscos, l'avaluació d'impacte si el risc és alt, el registre d'activitats i el nomenament de qui exerceixi les funcions de delegat/ada de protecció de dades.

Terceres parts

Quan l'organització presti serveis a altres organismes, o tracti informació d'altres organismes, se'ls farà partícips d'aquesta política de seguretat de la informació. El CONSELL definirà i aprovarà els canals per a la coordinació de la informació i els procediments d'actuació per a la reacció davant d'incidents de seguretat, així com la resta d'actuacions que el CONSELL dugui a terme en matèria de seguretat en relació amb altres organismes.

Quan el CONSELL utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta política de seguretat i de la normativa de seguretat existent que incumbeix als esmentats serveis o informació. La dita tercera part quedarà subjecta a les obligacions establertes en l'esmentada normativa i podrà 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.

Quan algun aspecte d'aquesta política de seguretat no pugui ser satisfet per una tercera part segons s'estableix 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. Serà necessària l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de seguir endavant.

10. Terceres parts com a serveis externalitzats de seguretat

En el cas de serveis externalitzats, excepte per causa justificada i documentada, l'organització prestatària dels esmentats serveis haurà de designar un punt o persona de contacte (POC) per a la seguretat de la informació tractada i el servei prestat, que compti amb el suport dels òrgans de direcció i que canalitzi i supervisi tant el compliment dels requisits de seguretat del servei que presta o de la solució que proveeixi, com les comunicacions relatives a la seguretat de la informació i la gestió dels incidents per a l'àmbit de l'esmentat servei.

L'esmentat POC de seguretat serà el mateix responsable de seguretat de l'organització contractada, formarà part de la seva àrea o tindrà comunicació directa amb aquesta.

11. Desenvolupament del SGSI, revisió i auditories

El Ple del CONSELL ha aprovat el desenvolupament d'un sistema de gestió de seguretat de la informació (SGSI) que és establert, implementat, mantingut i millorat conforme als estàndards de seguretat. Aquest sistema s'adequarà i servirà de gestió dels controls de l'ENS. El sistema serà documentat i permetrà generar evidències dels controls i del compliment dels objectius marcats. Existeix un procediment de gestió documental que estableix les directrius per a l'estructuració de la documentació de seguretat del sistema, la seva gestió i accés.

La política i les normes de seguretat de la informació s'adaptaran a l'evolució dels sistemes i de la tecnologia i als canvis organitzatius i s'alinearan amb la legislació vigent i amb els estàndards i millors pràctiques de l'ENS, amb especial atenció a les guies publicades pel Centre Criptològic Nacional com a desenvolupament de les mesures i controls de seguretat.

Les mesures de seguretat i els controls físics, administratius i tècnics aplicables es detallaran en el document d'aplicabilitat, i seran proporcionals a la criticitat de la informació a protegir i a la seva classificació.

El Comitè de Seguretat de la Informació revisarà aquesta política anualment o quan hi hagi canvis significatius que així ho aconsellin, i la sotmetrà de nou a l'aprovació pel Ple del CONSELL. Les revisions comprovaran l'efectivitat de la política, valorant els efectes dels canvis tecnològics i de les activitats.

El Ple del CONSELL serà responsable d'aprovar les modificacions necessàries en el text quan es produeixi un canvi que afecti les situacions de risc establertes al present document.

El sistema de gestió de seguretat s'auditarà anualment segons un pla d'auditories desenvolupat pel Comitè de Seguretat.