SEGURdades

Consultors en protecció de dades personals

PLS-ENS-001

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

PÚBLIC

Esquema Nacional de Seguridad

ordisa s.a.

CONTROL DEL DOCUMENT

Nom del document: **ENS-001-Política General de Seguretat-V01.docx** Nombre de Pàgines: **14**	
Autor: SEGURdades SL	
Aprovat per:	Firma:
Classificació de la informació: **PÚBLIC**	
Llista de distribució: SENSE RESTRICCIONS	

Aquest document està dirigit EXCLUSIVAMENT a les persones nomenades a la llista de distribució, les quals podran, en base al seu criteri, divulgar-lo als que considerin oportú. Es recomana encaridament una divulgació controlada on tots els cessionaris del document coneguin inequívocament la seva CLASSIFICACIÓ i es comprometin a mantenir la conseqüent confidencialitat en tot el cicle d'ús i, si escau, arxiu i/o destrucció.

CONTROL DE VERSIONS

Núm. Versió	Autor	Data	Canvis realitzats	Comentaris
1.0	SEGURdades	25/05/2023	Versió Inicial	Sense Comentaris
2.0	David Masgrau Haro	20/11/2024	Versió adaptada al CASG	

ordisa s.a.

POLÍTICA DE SEGURETAT

Índex

ordisa s.a.

1) APROVACIÓ I ENTRADA EN VIGOR

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

2) INTRODUCCIÓ

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

L'objectiu de la seguretat de la informació és garantir la confidencialitat, integritat, autenticitat i traçabilitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb pretesa 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, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació continuada dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per a garantir la continuïtat dels serveis prestats.

Els diferents departaments han d'assegurar-se que la seguretat TIC és una part integral de cada etapa del cicle de vida del sistema, des de la 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 la valoració del seu cost, han de ser identificats i inclosos a la planificació, a la sol·licitud d'ofertes, i en plecs de licitació per a projectes de TIC.

3) MISSIÓ

L'entitat, per a la gestió dels seus interessos i de les funcions i competències que té atribuïdes en diferents normes o convenis, promou els serveis necessaris a les persones i a la comunitat, per millorar el benestar i contribuir a la cohesió social a la comarca de la Garrotxa.

4) ABAST

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

5) MARC NORMATIU

Els marcs normatius referencials es troben al Registre Corporatiu de Marcs Normatius:

CASG-RGS-GLB-002-Normativa Aplicable

ordisa s.a.

Contenint els marcs normatius aplicables al CASG

6) COMPLIMENT DELS REQUISITS MÍNIMS DE SEGURETAT

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

La seguretat com un procés integral i mínim privilegi

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

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

Els sistemes d'informació s'han de dissenyar i configurar atorgant els mínims privilegis necessaris per a l'exercici correcte, cosa que implica incorporar els aspectes següents:

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

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

c) En un sistema d'explotació s'eliminaran o desactivaran, mitjançant el control de la configuració, les funcions que siguin innecessàries o inadequades per tal 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.

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

Vigilància contínua, re-avaluació periòdica i Integritat, actualització del sistema i millora contínua del procés de seguretat

La vigilància contínua per part del CASG permetrà la detecció d'activitats o comportaments anòmals i la resposta oportuna.

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

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

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

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

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

Gestió de personal i professionalitat

ordisa s.a.

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

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

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

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

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

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

La gestió dels riscos permetrà mantenir un entorn controlat i minimitzar els riscos a nivells acceptables. La reducció a aquests nivells es realitzarà mitjançant una aplicació apropiada de mesures de seguretat, de manera equilibrada i proporcionada a la naturalesa de la informació tractada, dels serveis a prestar i dels riscos a què estiguin exposats.

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

Incidents de seguretat, prevenció, detecció, reacció i recuperació

El CASG disposa de procediments de gestió d'incidents de seguretat d'acord amb allò previst a l'article 33, la Instrucció Tècnica de Seguretat corresponent, i de mecanismes de detecció, criteris de classificació, procediments d'anàlisi i resolució, així com de les vies de comunicació a les parts interessades.

La seguretat del sistema contemplarà les accions relatives als aspectes de prevenció, detecció i resposta, a fi de minimitzar-ne les 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 podran incorporar components orientats a la dissuasió o a la reducció de la superfície d'exposició, han d'eliminar o reduir la possibilitat que les amenaces arribin a materialitzar-se.

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

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

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

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

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

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

Es protegirà el perímetre del sistema d'informació, especialment, quan el sistema del CASG es connecta a xarxes públiques, tal com es defineixen a la legislació vigent en matèria de telecomunicacions, reforçant-se les tasques de prevenció, detecció i resposta a incidents de seguretat.

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

ordisa s.a.

Diferenciació de responsabilitats, organització i implantació del procés de seguretat

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

Autorització i control dels accessos

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

Protecció de les instal·lacions

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

Adquisició de productes de seguretat i contractació de serveis de seguretat

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

Per a la contractació de serveis de seguretat s'atendrà a allò que s'ha assenyalat quant a la professionalitat.

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

El CASG prestarà especial atenció a la informació emmagatzemada o en trànsit a través dels equips o dispositius portàtils o mòbils, els dispositius perifèrics, els suports d'informació i les comunicacions sobre xarxes obertes, que s'hauran d'analitzar especialment per aconseguir-ne una adequada protecció.

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

Tota informació en suport no electrònic que hagi estat causa o conseqüència directa de la informació electrònica a què fa referència aquest Reial decret, ha 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 siguin aplicables.

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

Registre d'activitat i detecció de codi nociu

El CASG, amb el propòsit de satisfer l'objecte d'aquest Reial decret, amb garanties plenes 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, registrarà les activitats dels usuaris, retenint la informació estrictament necessària per monitoritzar, analitzar, investigar i documentar activitats indegudes o no autoritzades, permetent identificar en cada moment la persona que actua.

A fi de preservar la seguretat dels sistemes d'informació, garantint la rigorosa observança dels principis d'actuació de les administracions públiques, i de conformitat amb el que disposa el Reglament General de Protecció de Dades i el respecte als principis de limitació de la finalitat, minimització de les dades i limitació del termini de conservació allí enunciats, el CASG podrà, en la mesura estrictament necessària i proporcionada, analitzar les comunicacions entrants o sortints, i únicament per als fins 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 xarxes i sistemes d'informació esmentades.

Per corregir o, si escau, exigir responsabilitats, cada usuari que accedeixi al sistema d'informació haurà d'estar identificat de manera única, de manera que se sàpiga, en tot moment, qui rep drets d'accés, de quina mena són aquests, i qui ha realitzat una determinada activitat.

ordisa s.a.

Infraestructures i serveis comuns

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

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

El CASG tindrà en compte l'aplicació dels perfils de compliment específics per a Entitats Locals que siguin d'aplicació.

ordisa s.a.

7) MODEL DE GOVERNANÇA

Per garantir el compliment de l'Esquema Nacional de Seguretat i establir l'organització de la seguretat de la informació al CASG, es designarà rols de seguretat i es constituirà un Comitè de Seguretat de la informació.

7).1 Rols o perfils de seguretat

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

- **Responsable/s d'informació:** Direcció de Suport i Acompanyament d'equips i professionals
- **Responsable dels Serveis:** Direcció de Suport i Acompanyament d'equips i professionals
- **Responsable de Seguretat:** Responsable del Departament d'Informàtica
- **Responsable del Sistema:** Responsable del Departament d'Informàtica

7).2 Comitè de Seguretat de la Informació

S'ha constituït un Comitè de Seguretat de la Informació, com a òrgan col·legiat, i està format pels membres següents:

- **President/a:** Gerència del Consorci d'Acció Social de la Garrotxa
- **Secretari/ària:** Responsable de Seguretat i sistemes
- **Vocals:**
  - **Responsable/s d'informació:** Directora de suport i acompanyament a equips o professionals
  - **Responsable/s de Serveis:** Directora de suport i acompanyament a equips o professionals
  - **Responsable de Seguretat:** Administratiu informàtic (C1)
  - **Responsable del Sistema:** Administratiu informàtic (C1)
- **Delegat de Protecció de dades (DPD):** Amb funcions d'assessorament i supervisió en matèria de protecció de dades.

Els responsables de la informació i dels serveis seran convocats en funció dels assumptes a tractar.

Així mateix, i amb caràcter opcional, es poden incorporar a les tasques del Comitè grups de treball especialitzats, ja siguin de caràcter intern, extern o mixt.

Els membres del Comitè seran renovats cada quatre anys o amb motiu de vacant.

7).3 Responsabilitats associades a l'Esquema Nacional de Seguretat

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

7).3.1 Funcions del Responsable de la Informació i dels Serveis

- Establir i aprovar els requisits de seguretat aplicables al servei i la informació dins el marc establert a l'annex I del Reial decret de l'Esquema Nacional de Seguretat.

ordisa s.a.

- Acceptar els nivells de risc residual que afectin el Servei i la Informació.

7).3.2 Funcions del Responsable de Seguretat

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

7).3.3 Funcions del Responsable del Sistema

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

ordisa s.a.

7).4 Funcions del Comitè de Seguretat de la Informació

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

- Atendre les sol·licituds, en matèria de Seguretat de la Informació, de l'administració i dels diferents rols de seguretat i/o àrees informant regularment de l'estat de la Seguretat de la Informació.
- Assessorar en matèria de seguretat de la informació.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre les diferents unitats administratives.
- Promoure la millora contínua del sistema de gestió de la seguretat de la informació. Per això 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 dotació pressupostària corresponent, i prioritzar 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 posada en operació. En particular haurà de vetllar per la creació i utilització de serveis horitzontals que redueixin duplicitats i donin suport a un funcionament homogeni de tots els sistemes TIC.
    - Realitzar un seguiment dels principals riscos residuals assumits per l'Administració i recomanar-ne possibles actuacions.
    - Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'aquests.
    - Elaborar i revisar regularment la Política de Seguretat de la Informació per aprovar-la l'òrgan competent.
    - Elaborar la normativa de Seguretat de la Informació per aprovar-la en coordinació amb la Direcció General.
    - Verificar els procediments de seguretat de la informació i la resta de documentació per a la seva aprovació.
    - Elaborar programes de formació destinats a formar i sensibilitzar el personal en matèria de seguretat de la informació i en particular en matèria de protecció de dades de caràcter personal.
    - Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de Seguretat de la Informació.
    - Promoure la realització de les auditories periòdiques ENS i de protecció de dades que permetin verificar el compliment de les obligacions de l'administració en matèria de seguretat de la Informació.

7).5 Procediments de designació

La designació dels Responsables identificats en aquesta Política ha estat realitzada per **presidència** del Consorci d'Acció Social de la Garrotxa, i comunicada a les parts afectades **convocant una sessió**.

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

7).6 Resolució de conflictes

Si hi ha conflicte entre els responsables, serà resolt pel Comitè de Seguretat de la Informació.

ordisa s.a.

8) DADES DE CARÀCTER PERSONAL

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

En desenvolupament dels principis de la vigent normativa de protecció de dades, entre d'altres, els de minimització, confidencialitat o proactivitat, el Consorci d'Acció Social de La Garrotxa ha definit un marc d'actuació a la Política de Protecció de Dades, aprovada per Decret 2024/560 de 13 de novembre de 2024.

9) DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

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

La revisió anual de la present Política correspon al Comitè de Seguretat de la Informació proposant en cas que calgui millores de la mateixa, per a la seva aprovació per part del mateix òrgan que la va aprovar inicialment.

10) TERCERES PARTS

Quan es presta serveis a altres organismes, o manegi informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació. El CASG 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 de les actuacions que el CASG dugui a terme en matèria de seguretat en relació amb altres organismes.

Quan el CASG utilitzi serveis de tercers o cedeixi informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la Normativa de Seguretat existent que afecta aquests serveis o informació. Aquesta tercera part queda subjecta a les obligacions establertes en la normativa esmentada, i poden 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 el que estableix aquesta Política de Seguretat.

De la mateixa manera, tenint en compte l'obligació de complir amb el que disposen les Instruccions Tècniques de Seguretat recollida a la Disposició addicional segona (Desenvolupament de l'Esquema Nacional de Seguretat) del Reial Decret Reial Decret 311/2022, de 3 de maig, pel que es regula l'Esquema Nacional de Seguretat, i en consideració a la Instrucció Tècnica de Seguretat de conformitat amb l'Esquema Nacional de Seguretat, on s'estableix que els operadors del sector privat que prestin serveis o proveeixin solucions a les entitats públiques, als quals resulti exigible el compliment de l'Esquema Nacional de Seguretat, hauran d'estar en condicions d'exhibir la corresponent Declaració de Conformitat amb l'Esquema Nacional de Seguretat quan es tracti de sistemes de categoria BÀSICA, o la Certificació de Conformitat amb l'Esquema Nacional de Seguretat, quan es tracti de sistemes de categories MITJANA o ALTA.

Quan algun aspecte d'aquesta Política de Seguretat no pugui ser satisfet per una tercera part segons es requereixi en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que necessiti els riscos en què

s'incorre i la manera de tractar-los. Aquest informe haurà de ser aprovat pels responsables d'informació i els serveis, amb caràcter previ a l'inici de la relació amb la tercera part.