INFORMACIÓ CONFIDENCIAL

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Adequació dels Serveis Informàtics del Consorci Servei de Recaptació Cerdanya-Ripollès a l'Esquema Nacional de Seguretat

CONSORCI SERVEI DE RECAPTACIÓ
CERDANYA-RIPOLLÈS

Govertis Advisory Services, SL
Av. Corts Valencianes, 58 - desp. 806 46015 – València.
Passeig de la Castellana, 153 – baix. 28046 Madrid
Telèfon: 963531910 – 902012150
Fax: 96 353 19 09
Correu Electrònic: info@govertis.com

INFORMACIÓ CONFIDENCIAL

Govertis Advisory Services, SL
Av. Corts Valencianes, 58 - desp. 806 46015 – València.
Passeig de la Castellana, 153 – baix. 28046 Madrid
Telèfon: 963531910 – 902012150
Fax: 96 353 19 09
Correu Electrònic: info@govertis.com

CONTROL D'EDICIÓ

DATA	EDICIÓ	REVISIÓ	RESPONSABLE	DESCRIPCIÓ DE CANVIS
09-09-2022	01	01	Responsable del sistema.	Edició inicial.

ÍNDEX

01 INTRODUCCIÓ

1..1 JUSTIFICACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Consorci Servei de Recaptació Cerdanya-Ripollès (d'ara endavant, CSRCR) necessita els sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els seus objectius. 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 qualitat de la informació i la prestació continuada dels serveis, actuant preventivament, supervisant l'activitat diària i reaccionant amb rapidesa quan hi ha incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial d'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 de les condicions de l'entorn per garantir la prestació continuada dels serveis. És per això que l'Esquema Nacional de Seguretat (Reial Decret 311/2022, de 3 de maig, ENS en endavant), a l'article 12 estableix que "Cada administració pública comptarà amb una política de seguretat formalment aprovada per l'òrgan competent".

Això implica que les diferents àrees del Consorci han d'aplicar les mesures mínimes de seguretat exigides per l'ENS i fer un seguiment continuat dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per tal de garantir la continuïtat dels serveis prestats.

Totes les àrees 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 les necessitats de finançament, 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. Les diferents àrees han d'estar preparades per prevenir, detectar, reaccionar i recuperar-se d'incidents d'acord amb l'article 8 de l'ENS.

1..2 MISSIÓ I SERVEIS PRESTATS

De conformitat amb l'article 3 dels seus Estatuts (BOP de Girona núm. 10, de 15 de gener de 2019), el Consorci Servei de Recaptació Cerdanya-Ripollès tindrà els objectius següents:

> *"3.1 El Consorci tindrà els objectius següents:*
>
> *a) La gestió, liquidació i recaptació dels tributs i de les quantitats que com ingressos de dret públic -tals com prestacions patrimonials de caràcter públic no tributàries, preus públics, multes i sancions pecuniàries-, hagin de percebre les hisendes de les entitats locals dels àmbits territorials de la Cerdanya i del Ripollès, quan tinguin delegades aquestes competències a favor del Consorci.*

b) La recaptació de qualsevol tipus d'ingrés de dret públic de les administracions públiques, dels seus ens o empreses públiques dependents i de qualsevol altra corporació de dret públic, que es trobin dins de l'àmbit territorial de les comarques de la Cerdanya i del Ripollès, sempre que prèviament ho hagin sol·licitat al Consorci i aquest hagi acceptat l'encàrrec.

c) Les funcions de gestió cadastral referents a la tramitació dels expedients d'alteracions d'ordre físic, jurídic i econòmic que afectin als béns immobles de naturalesa urbana ubicats en els municipis que tenen delegada la facultat de gestió tributària de l'IBI a favor de cada consell comarcal.

3.2 La recaptació dels conceptes referenciats abastarà els períodes voluntari i executiu, si procedeix.

3.3 La facultat d'emetre providències de constrenyiment i altres tràmits necessaris per a la gestió recaptadora, en aquells supòsits en què el Consorci tingui delegada la gestió, liquidació i recaptació o únicament la recaptació.

3.4 Efectuar la devolució als contribuents de les quantitats que s'hagin de reintegrar, en aquells supòsits en què el Consorci tingui delegada la gestió, liquidació i recaptació, mitjançant deducció de la primera liquidació que s'efectuï.

3.5 Per acord de la Junta de Govern podran ampliar-se els objectius del Consorci a altres operacions."

El Consorci Servei de Recaptació Cerdanya-Ripollès, per a la gestió dels seus interessos, en l'àmbit de les seves competències i com a Administració pública, serveix amb objectivitat els interessos generals i actua d'acord amb els principis d'eficàcia, jerarquia, descentralització i coordinació , promou diferents activitats i presta els serveis públics que contribueixen a satisfer les necessitats i aspiracions dels habitants dels municipis als que presta els serveis.

Aquesta Política de Seguretat aplica a les diferents activitats en què participa el Consorci a través de mitjans electrònics, en concret:

- Les relacions de caràcter juridicoeconòmiques entre els ciutadans i el Consorci.
- La consulta per part dels ciutadans de la informació pública administrativa i de les dades administratives que estiguin en poder del Consorci.
- La realització dels tràmits i procediments administratius incorporats per tramitar-los a través de la Seu Electrònica del Consorci, de conformitat amb el que preveu l'Ordenança d'Administració Electrònica del Consell Comarcal del Ripollès.
- El tractament de la informació obtinguda pel Consorci en l'exercici de les seves potestats.

02 MARC NORMATIU

Com a base normativa per realitzar aquesta guia de seguretat, s'ha analitzat la legislació vigent, que afecta el desenvolupament de les activitats de l'Administració local pel que fa a administració electrònica i que implica la implantació de forma explícita de mesures de seguretat per als sistemes d'informació. El marc legal en matèria de seguretat de la informació ve establert per la següent legislació:

- Llei 29/2010, del 3 d'agost, de l'ús dels mitjans electrònics al sector públic de Catalunya, que regula el procés de transformació de les administracions públiques catalanes en base a l'ús dels mitjans electrònics.
- Llei 32/2010, de l'1 d'octubre, de l'Autoritat Catalana de Protecció de Dades, que vetlla per la garantia del dret a la protecció de dades en l'àmbit de les administracions públiques de Catalunya.
- Decret 76/2020, de 4 d'agost, d'Administració digital.
- Decret 124/2019, de 4 de juny, de reestructuració del Departament de Polítiques Digitals i Administració Pública, pel qual es crea la Direcció General d'Administració Digital.
- Decret 232/2013, de 15 d'octubre, pel qual es crea la seu electrònica, amb l'objectiu de posar a disposició de la ciutadania, empreses i entitats un espai electrònic únic de relació amb l'Administració de la Generalitat.
- Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, que assenyala a l'art. 17.3 que els mitjans o suports en què s'emmagatzemin documents hauran de comptar amb les mesures de seguretat que estableix l'Esquema Nacional de Seguretat, que garanteixin una sèrie de principis (com integritat, autenticitat, confidencialitat, qualitat, protecció i conservació dels documents emmagatzemats); i, estableix també, al seu art. 27.3 que les administracions públiques hauran de complir amb l'Esquema Nacional de Seguretat per garantir la identitat i el contingut de les còpies electròniques o en paper, és a dir, el caràcter de còpies autèntiques. Finalment, disposa a la seva Disposició Addicional segona que, tant les Comunitats Autònomes, com les Entitats Locals, hauran de garantir la seva compatibilitat informàtica i interconnexió, així com la transmissió telemàtica de les sol·licituds, escrits i comunicacions que es realitzin en els seus registres i plataformes corresponents. mitjançant el compliment, igualment, de l'Esquema Nacional de Seguretat. I que, a més, deroga la Llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als serveis públics.
- 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, la finalitat de la qual és la creació de les condicions necessàries per garantir el nivell d'interoperabilitat tècnica, semàntica i organitzativa adequat. dels sistemes i aplicacions emprats per les administracions públiques, que permeti l'exercici de drets i el compliment de deures a través de l'accés electrònic als serveis públics, alhora que redunda en benefici de l'eficàcia i l'eficiència.
- Reglament (UE) 2016/679, del Parlament Europeu i del Consorci, 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 (d'ara endavant RGPD).

03 ORGANITZACIÓ DE LA SEGURETAT

2

3

3.1 DEFINICIÓ DE ROLS

L'organització de la Seguretat de la Informació en el Consorci Servei de Recaptació Cerdanya-Ripollès s'estableix en la forma que s'indica a continuació.

3.1.1. Responsable de la informació

S'ha designat responsable de la informació a la **Presidència del Consorci Servei de Recaptació Cerdanya-Ripollès** o òrgan en qui es delegui, a qui corresponen les funcions següents:

- Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat dels tractaments de dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat, tenint en compte l'estat de la tecnologia, la naturalesa de les dades emmagatzemades i els riscos a què estan exposats, ja provinguin de l'acció humana o del medi físic o natural.

- Té la responsabilitat última de l'ús que se'n faci d'una certa informació i, per tant, de la seva protecció.

- El Responsable de la Informació és el responsable últim de qualsevol error o negligència que porti a un incident de confidencialitat o integritat.

- Estableix els requisits de la informació en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.

- Determinarà els nivells de seguretat en cada dimensió dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.

- Encara que l'aprovació formal dels nivells correspongui al Responsable de la Informació, podrà demanar una proposta al Responsable de la Seguretat i convé que escolti l'opinió del Responsable del Sistema.

3.1.2. Responsable del servei

S'han designat responsables del Servei a cadascun dels responsables d'unitats funcionals amb serveis a la Seu electrònica (Direcció, Secretaria, Intervenció, Tresoreria, Recaptació i caps d'àrea de les diferents unitats del CSRCR, si existeixen), a qui correspon les funcions següents:

- Pel que fa a l'RGPD, per delegació del Responsable del tractament s'encomana al Responsable del Servei el desenvolupament de les tasques relacionades amb la gestió dels fitxers i tractaments de dades personals que es realitzen a la seva àrea en concret. Aquesta figura en terminologia de protecció de dades de caràcter personal s'anomena Gestor de Fitxers Concrets.

- Estableix els requisits dels serveis en matèria de seguretat. En el marc de l'ENS, equival a la potestat de determinar els nivells de seguretat de la informació.

- Té la responsabilitat última de l'ús que se'n faci de determinats serveis i, per tant, de la seva protecció.

- El Responsable del Servei és el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis.

- Determinarà els nivells de seguretat en cada dimensió del servei dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.

- Encara que l'aprovació formal dels nivells correspongui al Responsable del Servei, podrà demanar una proposta al Responsable de la Seguretat i convé que escolti l'opinió del Responsable del Sistema.

- La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que vinculada a aquest servei, de manera que es poden heretar els requisits de seguretat d'aquesta, afegint-hi requisits de disponibilitat, així com altres com accessibilitat, interoperabilitat, etc.

3.1.3. Responsable de seguretat de la informació

S'ha designat com a responsable de Seguretat de la Informació a la **Secretaria del Consorci Servei de Recaptació Cerdanya-Ripollès**, a qui correspondran les funcions següents:

- Coordinarà i controlarà les mesures definides al Registre d'Activitats del Tractament i en general s'encarregarà del compliment de les mesures de seguretat que detalla l'informe d'avaluació d'impacte a la protecció de dades.

- Reportarà directament al Comitè de Seguretat de la Informació.

- Actuarà com a secretari del Comitè de Seguretat de la Informació.

- Convocarà el Comitè de Seguretat de la Informació, recopilant la informació pertinent.

- Mantindrà la seguretat de la informació i dels serveis prestats pels sistemes d'informació en el seu àmbit de responsabilitat, d'acord amb allò establert a la Política de Seguretat de l'Organització.

- Promourà la formació i la conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.

- Recopilarà els requisits de seguretat dels Responsables d'Informació i del Servei i determinarà la categoria del Sistema.

- Realitzarà l'Anàlisi de Riscos.

- Elaborarà una Declaració d'Aplicabilitat a partir de les mesures de seguretat requerides d'acord amb l'Annex II de l'ENS i el resultat de l'Anàlisi de Riscos.

- Facilitarà als Responsable d'Informació i als Responsables de Servei informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades a l'anàlisi de riscos i les mesures de seguretat requerides per l'ENS.

- Coordinarà l'elaboració de la documentació de seguretat del sistema.

- Participarà en l'elaboració, en el marc del Comitè de Seguretat de la Informació, la Política de Seguretat de la Informació, per aprovar-la per Direcció.

- Participarà en l'elaboració i aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de seguretat de la informació.

- Elaborarà i aprovarà els procediments operatius de seguretat de la informació.

- Facilitarà periòdicament al Comitè de Seguretat un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i de l'estat de la seguretat del sistema (en particular del nivell de risc residual a què està exposat el sistema).

- Elaborarà, juntament amb els Responsables de Sistemes, Plans de Millora de la Seguretat, per a la seva aprovació pel Comitè de Seguretat de la Informació.

- Elaborarà els plans de formació i conscienciació del personal en seguretat de la informació, que hauran de ser aprovats pel Comitè de Seguretat de la Informació.

- Validarà els Plans de Continuïtat de Sistemes que elabori el Responsable de Sistemes, que hauran de ser aprovats pel Comitè de Seguretat de la Informació i provats periòdicament pel Responsable de Sistemes.

- Aprovarà les directrius proposades pels Responsables de Sistemes per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos: especificació, arquitectura, desenvolupament, operació i canvis.

Com a Secretària del Comitè de Seguretat de la Informació li correspon:

- Convocar les reunions del Comitè de Seguretat de la Informació.
- Preparar els temes a tractar a les reunions del Comitè, aportant informació puntual per a la presa de decisions.
- Elaborar l'acta de les reunions.
- És responsable de l'execució directa o delegada de les decisions del Comitè.

3.1.4. Responsable del sistema

S'ha designat com a responsable del Sistema al **Tècnic/a d'Administració Electrònica i Transparència del Consell Comarcal del Ripollès**, al qual corresponen les funcions següents:

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, de les especificacions, instal·lació i verificació del funcionament correcte.
- Definir la topologia i el sistema de gestió del sistema d'informació establint els criteris d'ús i els serveis disponibles en aquest.
- Assegurar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- El Responsable del Sistema pot acordar la suspensió del tractament d'una certa informació o la prestació d'un determinat servei si és informat de deficiències greus de seguretat que poguessin afectar al compliment dels requisits establerts. Aquesta decisió ha de ser acordada amb els Responsables de la Informació afectada, el Servei afectat i amb el Responsable de la Seguretat abans de ser executada.
- Aplicar els procediments operatius de seguretat elaborats i aprovats pel responsable de seguretat.
- Monitoritzar l'estat de la seguretat del Sistema d'Informació i reportar-lo periòdicament o davant d'incidents de seguretat rellevants al Responsable de Seguretat de la Informació.
- Elaborar els Plans de Continuïtat del Sistema perquè siguin validats pel Responsable de Seguretat de la Informació, i coordinats i aprovats pel Comitè de Seguretat de la Informació.
- Realitzar exercicis i proves periòdiques dels Plans de Continuïtat del Sistema per mantenir-los actualitzats i verificar que són efectius.
- Elaborarà les directrius per considerar la Seguretat de la Informació durant tot el cicle de vida dels actius i processos (especificació, arquitectura, desenvolupament, operació i canvis) i les facilitarà al Responsable de Seguretat de la Informació per aprovar-la.

- Dur a terme el registre, la comptabilitat i la gestió dels incidents de seguretat en els sistemes sota la seva responsabilitat.

3.1.5. Administrador de la seguretat del sistema

S'ha designat com a Administrador de la Seguretat del Sistema al **Tècnic/a informàtic designat en el marc del contracte formalitzat per la prestació d'assistència i manteniment informàtic al Consorci Servei de Recaptació Cerdanya-Ripollès**, al qual, com a tal, li corresponen les funcions següents:

- La implementació, la gestió i el manteniment de les mesures de seguretat aplicables al Sistema d'Informació.
- Assegurar que els controls de seguretat establerts són estrictament complerts.
- Assegurar que la traçabilitat, pistes d'auditoria i altres registres de seguretat requerits estiguin habilitats i es registrin amb la freqüència desitjada, d'acord amb la política de seguretat establerta per l'Organització.
- Aplicar als sistemes, usuaris i altres actius i recursos relacionats amb aquest, tant interns com externs, els procediments operatius de seguretat i els mecanismes i serveis de seguretat requerits.
- Assegurar que són aplicats els procediments aprovats per operar el sistema d'informació i els mecanismes i serveis de seguretat requerits.
- La gestió, configuració i actualització, si escau, del maquinari i programari en què es basen els mecanismes i els serveis de seguretat del Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per assegurar que la seguretat no està compromesa.
- Aprovar els canvis en la configuració vigent del sistema d'informació, garantint que segueixin operatius els mecanismes i els serveis de seguretat habilitats.
- Informar els Responsables de la Seguretat i del Sistema de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Monitoritzar l'estat de seguretat del sistema.

En cas que es produeixin incidents de seguretat de la informació:

- Executar el pla de seguretat aprovat.
- Aïllar l'incident per evitar la propagació a elements aliens a la situació de risc.

- Prendre decisions a curt termini si la informació s'ha vist compromesa de manera que pogués tenir conseqüències greus (aquestes actuacions haurien d'estar reflectides en un procediment documentat per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).

- Assegurar la integritat dels elements crítics del Sistema si se n'ha vist afectada la disponibilitat (aquestes actuacions haurien d'estar reflectides en un procediment documentat per reduir el marge de discrecionalitat de l'Administrador de Seguretat del Sistema al mínim nombre de casos).

- Mantenir i recuperar la informació emmagatzemada pel sistema i els seus serveis associats.

- Investigar l'incident: Determinar el mode, els mitjans, els motius i l'origen de l'incident.

3.2 COMITÈ DE SEGURETAT DE LA INFORMACIÓ

S'ha creat el Comitè de Seguretat de la Informació que estarà compost pels membres següents:

PRESIDÈNCIA: Presidència o membre de la Junta de Govern en qui es delegui.

SECRETARIA: Secretària del CSRCR.

VOCALS: Direcció del CSRCR, Interventor/a del CSRCR, tresorer/a del CSRCR, el Recaptador/a del CSRCR, els Tècnics i tècniques d'Administració General del CSRCR, el Tècnic/a d'Administració Electrònica i Transparència del CCR i el Tècnic/a informàtic designat en el marc del contracte formalitzat per la prestació d'assistència i manteniment informàtic al Consorci Servei de Recaptació Cerdanya-Ripollès.

Poden acudir a requeriment del Comitè qualssevol altres caps de servei o àrea i responsables la intervenció dels quals sigui necessària per ser afectats per l'Esquema Nacional de Seguretat i per l'RGPD.

Les funcions del Comitè de Seguretat de la Informació són les següents:

- Atendre les inquietuds de l'Alta Direcció i dels diferents departaments.

- Informar regularment de l'estat de seguretat de la informació a l'Alta Direcció.

- Promoure la millora contínua del sistema de gestió de la seguretat de la informació.

- Elaborar l'estratègia d'evolució del Consorci pel que fa a la seguretat de la informació.

- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per assegurar que els esforços són consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.

- Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.

- Aprovar la normativa de seguretat de la informació.

- Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris des del punt de vista de seguretat de la informació.

- Monitoritzar els principals riscos residuals assumits pel Consorci i recomanar possibles actuacions respecte d'aquests.

- Monitoritzar l'exercici dels processos de gestió d'incidents de seguretat i recomanar possibles actuacions respecte d'aquests. En particular, vetllar per la coordinació de les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

- Promoure la realització de les auditories periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.

- Aprovar plans de millora de la seguretat de la informació de l'Ajuntament. En particular, vetllarà per la coordinació de diferents plans que es puguin fer en diferents àrees.

- Vetllar perquè la seguretat de la informació es tingui en compte en tots els projectes TIC 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.

- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees de l'Organització, elevant aquells casos en què no tingui prou autoritat per decidir.

- Demanarà regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions.

- S'assessorarà sobre els temes que hagi de decidir o emetre una opinió. Aquest assessorament es determinarà en cada cas, podent materialitzar-se de diferents formes i maneres:

    - Grups de treball especialitzats interns, externs o mixtos.
    - Assessoria interna i/o externa.
    - Assistència a cursos o altres tipus d'entorns formatius o d'intercanvi d'experiències.

En cas d'ocurrència d'incidents de seguretat de la informació:

- Aprovarà el Pla de Millora de la Seguretat, amb la dotació pressupostària corresponent.

3.3 JERARQUIA EN EL PROCÉS DE DECISIÓ I MECANISMES DE COORDINACIÓ

Els diferents rols de seguretat de la informació (autoritat principal i possibles delegades) es limiten a una jerarquia simple: el Comitè de Seguretat de la Informació dona instruccions al Responsable de la Seguretat de la Informació, supervisant que administradors i operadors implementen les mesures de seguretat segons el que estableix la política de seguretat aprovada per a l'Organització.

L'Administrador de la Seguretat del Sistema reporta el Responsable del Sistema:

- Incidents relatius a la seguretat del sistema.
- Accions de configuració, actualització o correcció.

El Responsable del Sistema informa al Responsable de la Informació de les incidències funcionals relatives a la informació que li competeix.

El Responsable del Sistema informa al Responsable del Servei de les incidències funcionals relatives al servei que li competeix.

El Responsable del Sistema reporta al Responsable de la Seguretat:

- Actuacions en matèria de seguretat, en particular pel que fa a decisions d'arquitectura del sistema.
- Resum consolidat dels incidents de seguretat
- Mesures de l'eficàcia de les mesures de protecció que cal implantar.

El Responsable de la Seguretat informa el Responsable de la Informació de les decisions i incidents en matèria de seguretat que afectin la informació que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

El Responsable de la Seguretat informa al Responsable del Servei de les decisions i incidents en matèria de seguretat que afectin el servei que li competeix, en particular de l'estimació de risc residual i de les desviacions significatives de risc respecte dels marges aprovats.

Quan hi hagi un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta a aquest comitè com a secretari:

- Resum consolidat d'actuacions en matèria de seguretat.
- Resum consolidat d'incidents relatius a la seguretat de la informació.
- Estat de la seguretat del sistema, en particular del risc residual a què el sistema està exposat.

El Responsable de la Seguretat informa a la Direcció de l'Organització, segons allò acordat al Comitè de Seguretat de la Informació.

Quan no hi hagi un Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta directament a la Direcció de l'Organització:

- Resum consolidat d'actuacions en matèria de seguretat.
- Resum consolidat d'incidents relatius a la seguretat de la informació.
- Estat de la seguretat del sistema, en particular del risc residual a què el sistema està exposat.

3.4 PROCEDIMENTS DE DESIGNACIÓ DE PERSONES

La Direcció de l'Organització nomenarà formalment mitjançant la seva publicació al Butlletí Oficial corresponent:

- Al Responsable de la Informació.
- Als Responsables del Servei.
- Al Responsable de la Seguretat, que ha de reportar directament a la Direcció o, quan n'hi hagi, al Comitè de Seguretat de la Informació.
- Al Responsable del Sistema, que ha de reportar directament a la Direcció o, quan n'hi hagi, al Comitè de Seguretat de la Informació.

La Direcció de l'Organització designa la persona Responsable del Sistema:

- A proposta del Responsable de la Informació tractada, quan el sistema d'informació tracti una única informació.
- A proposta del Responsable del Servei prestat, quan el Sistema d'informació presta un únic servei.
- Directament quan el sistema d'informació tracta diferents informacions o presta diferents serveis, escoltant els Responsables de les Informacions i dels Serveis afectats.

La Direcció de l'Organització designa l'Administrador de Seguretat del Sistema a proposta del Responsable del Sistema o del Responsable de Seguretat de la Informació.

3.5 DADES DE CARÀCTER PERSONAL

Per a la prestació dels serveis previstos cal tractar dades de caràcter personal. El Registre d'Activitats del Tractament detalla els tractaments afectats i els responsables corresponents, així com les mesures adoptades derivades de l'anàlisi de riscs feta sobre els tractaments de dades. Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollides a l'esmentat Registre d'Activitats del Tractament.

3.6 FIGURES VINCULADES A LA PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

1.

1.1.

1.2.

1.3.

1.4.

1.5.

1.6.

1.7.

3.6.1. Funcions i obligacions del responsable del tractament

El Responsable del tractament és la persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que decideix sobre la finalitat, contingut i ús del tractament.

A l'efecte de l'entitat local s'ha atribuït la condició de Responsable de Tractament a la persona jurídica-pública, és a dir, al mateix Consorci Servei de Recaptació Cerdanya-Ripollès. De manera que el Consorci és el Responsable del Tractament de les dades de caràcter personal, tractades pels sistemes d'informació, i que deriven de la prestació dels serveis públics atribuïts a nivell de competències.

Alhora, cal dir que la consideració de Responsable de Tractament no ha de ser associada a persona física representant del CSRCR, en qualitat del càrrec o lloc (com per exemple, Presidència o Secretaria).

Les funcions del Responsable del tractament són:

- Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat.

- Informar als titulars de les dades dels drets que els assisteixen i en els termes en què poden exercir-los.
- Excloure del tractament les dades relatives a l'afectat que s'oposi al tractament.
- Cessar en la utilització o cessió il·lícita de les dades quan així ho requereixi l'interessat.
- Obligació de fer efectiu el dret de rectificació o supressió de l'interessat en el termini màxim d'un mes.
- Notificar les rectificacions o cancel·lacions efectuades a les dades personals a qui s'hagi comunicat aquestes dades, en el cas que es mantingui el tractament per aquest últim, que també haurà de procedir a la cancel·lació.

3.6.2. Funcions i obligacions del delegat de protecció de dades (DPD)

El Ple del Consell Comarcal del Ripollès, en sessió de data 15 de març de 2022, va crear una central de contractació per a la licitació agregada del servei de delegat de protecció de dades i altres serveis connexos derivats de la normativa vigent en la matèria de protecció de dades, per al Consell Comarcal del Ripollès i tots els municipis i consorcis de la comarca que s'hi adhereixin. En aquesta mateixa sessió va aprovar el model de Conveni d'encàrrec de gestió a subscriure entre el Consell Comarcal i els ajuntaments i consorcis de la comarca per a la contractació agregada del servei de delegat de protecció de dades i altres serveis connexos derivats de la normativa vigent en la matèria de protecció de dades. Aquest Conveni ha estat aprovat pel CONSORCI SERVEI DE RECAPTACIÓ CERDANYA-RIPOLLÈS per acord de la Junta de Govern de data 29 de març de 2022. El conveni s'ha formalitzat en data 19 d'abril de 2022.

Mitjançant acord del Consell de Govern del Consell Comarcal del Ripollès, en sessió celebrada el 19 d'abril de 2022, va acordar adjudicar a l'empresa GLOBAL LEGAL DATA, S.L el contracte del servei de Delegat de Protecció de Dades i altres serveis connexos, contracte que es va acabar formalitzant el 7 de juny de 2022, a fi de desenvolupar les funcions previstes tant a la normativa nacional com a comunitària relatives al Delegat de Protecció de Dades així com totes aquelles qüestions relacionades amb el compliment de l'Esquema Nacional de Seguretat.

El contracte té caràcter administratiu i es regeix pels plecs de clàusules administratives i de prescripcions tècniques particulars que figuren al perfil del contractant del CSRCR, les clàusules dels quals es consideren part integrant del contracte. A més, es regeix per la normativa en matèria de contractació pública.

El termini de vigència del contracte és de 2 anys a partir del dia 1 de juny de 2022. El contracte es podrà prorrogar per dues anualitat més. Les pròrrogues s'hauran d'adoptar d'any en any, fina a un màxim de quatre anualitat, i són obligatòries per contractista sempre que s'hagi procedit al preavís amb una antelació mínima de 2 mesos abans de la finalització del contracte o de la pròrroga vigent. Un cop esgotat el termini de vigència i, si és el cas, les pròrrogues pertinent, el procés de renovació tornarà a activar en forma de licitació conjunta.

Els ens actualment adherits al contracte són, a banda del Consorci Servei de Recaptació Cerdanya-Ripollès,

el Consorci Servei de Recaptació Cerdanya-Ripollès, el Consorci de Benestar Social del Ripollès, el Consorci d'Espais d'Interès Natural del Ripollès i els ajuntaments de Campelles, Gombrèn, Llanars, Les Llosses, Planoles, Queralbs, Ribes de Freser, Ripoll, Sant Joan de les Abadesses, Sant Pau de Segúries, Setcases, Toses, Vallfogona del Ripollès i Vilallonga de Ter.

En aquest darrer terme, el Reglament General de Protecció de Dades estableix a l'article 37.3 "Quan el responsable o l'encarregat del tractament sigui una autoritat o organisme públic, es podrà designar un únic delegat de protecció de dades per a diverses d'aquestes autoritats o organismes, tenint en compte la seva estructura organitzativa i mida".

D'acord amb això, l'Agència Espanyola de Protecció de Dades (d'ara endavant, AEPD) assenyala a l'Informe del seu Gabinet Jurídic N/REF: 002995/2019 que, seguint el que disposa l'article 8.3 de la Llei 40/2015, de 1 d'octubre, de Règim Jurídic del Sector Públic - LRJSP, res no s'oposaria que un òrgan superior pogués desenvolupar orgànicament les normes competencials de què emani l'exercici de les competències del DPD, emmarcant-les en l'àmbit funcional d'una o altra Administració. Així, l'Agència assenyala, amb caràcter general, el nomenament del DPD d'una Administració pública, òrgan administratiu, o ens públic, o bé de diversos òrgans o entitats públiques,

El Gabinet Jurídic de l'AEPD assenyala que, "amb independència del criteri organitzatiu seguit en l'àmbit d'una determinada Administració pública, així com del nomenament únic o múltiple de diversos DPD, en cap cas la fórmula adoptada no podrà suposar una excusa per al compliment adequat del conjunt de les obligacions derivades de la normativa.

El DPD és un òrgan col·legiat les funcions del qual s'assenyalen a l'article 39 del Reglament (UE) 679/2016, així com els articles 36 i 37 de la Llei Orgànica 3/2018, i s'ocupa de l'aplicació de la legislació sobre privadesa i protecció de dades a l'entitat on desenvolupa les seves funcions. Cal designar un delegat de protecció de dades en els casos següents:

D'acord amb aquest Reglament i l'Autoritat Catalana de protecció de dades, el Delegat de Protecció de Dades pot formar part de la plantilla del responsable o l'encarregat o bé actuar en el marc d'un contracte de serveis.

- Quan el tractament el duu a terme una autoritat o un organisme públic (tret de jutjats i tribunals). En aquest cas, es pot designar un únic delegat de protecció de dades per a diverses d'aquestes autoritats o organismes.

- Quan el tractament requereix l'observació habitual i sistemàtica d'interessats a gran escala.

- Quan el tractament té per objecte categories especials de dades personals o dades relatives a condemnes o infraccions penals.

Un cop designat el delegat, les entitats incloses dins l'àmbit d'actuació de l'APDCAT han de comunicar aquesta designació a l'Autoritat Catalana de Protecció de Dades. Així mateix, cal que mantinguin actualitzades les dades comunicades.

El Delegat de Protecció de Dades tindrà com a mínim les funcions següents:

- Informar i assessorar el responsable o l'encarregat del tractament i els empleats que s'ocupin del tractament de les obligacions que els incumbeixen en virtut del present Reglament i d'altres disposicions de protecció de dades de la Unió o dels Estats membres;
- Supervisar el compliment del que disposa aquest Reglament, d'altres disposicions de protecció de dades de la Unió 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 demani sobre l'avaluació d'impacte relativa a la protecció de dades i supervisar-ne l'aplicació de conformitat amb l'article 35;
- Cooperar amb l'autoritat de control;
- Actuar com a punt de contacte de l'autoritat de control per a qüestions relatives al tractament, inclosa la consulta prèvia a què fa referència l'article 36, i fer consultes, si escau, sobre qualsevol altre assumpte.

  El Delegat de Protecció de Dades exercirà les seves funcions prestant la deguda atenció als riscos associats a les operacions de tractament, tenint en compte la naturalesa, l'abast, el context i les finalitats del tractament.

  Per això haurà de ser capaç de:

  - Demanar informació per determinar les activitats de tractament,
  - Analitzar i comprovar la conformitat de les activitats de tractament, i
  - Informar, assessorar i emetre recomanacions al Responsable o Encarregat del Tractament.
  - Recollir informació per supervisar el registre de les operacions de tractament.
  - Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.
  - Assessorar sobre:
    - Si cal dur a terme una avaluació d'impacte de la protecció de dades o no.
    - Quina metodologia s'ha de seguir per fer una avaluació d'impacte de la protecció de dades.
    - Si cal dur a terme l'avaluació d'impacte de la protecció de dades amb recursos propis o amb contractació externa.

- Quines salvaguardes (incloses les mesures tècniques i organitzatives) aplicar per mitigar qualsevol risc per als drets d'interessos dels afectats.
- Si s'ha dut a terme correctament o no l'avaluació d'impacte de la protecció de dades, i
- si les seves conclusions (si continuar endavant o no amb el tractament i quines salvaguardes aplicar) són conformes al Reglament.

- Prioritzar les seves activitats i centrar els seus esforços en aquelles qüestions que presentin més riscos relacionats amb la protecció de dades.
- Assessorar el responsable del tractament sobre:
  - Quina metodologia aplicar en dur a terme una avaluació d'impacte de la protecció de dades,
  - Quines àrees s'han de sotmetre a auditoria de protecció de dades interna o externa,
  - Quines activitats de formació internes proporcionar al personal o als directors responsables de les activitats de tractament de dades i a quines operacions de tractament dedicar més temps i recursos.

El DPD haurà de reunir coneixements especialitzats del dret i la pràctica en matèria de protecció de dades. S'han identificat, en conseqüència, aquells coneixements, habilitats o destreses necessàries que ha de saber o posseir el Delegat de Protecció de Dades per dur a terme una de les funcions pròpies del seu lloc.

Aquestes funcions genèriques del DPD es poden concretar en tasques d'assessorament i supervisió, entre d'altres, a les àrees següents:

- Compliment de principis relatius al tractament, com ara els de limitació de finalitat, minimització o exactitud de les dades.
- Identificació de les bases jurídiques dels tractaments.
- Valoració de compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.
- Determinació de l'existència de normativa sectorial que pugui determinar condicions de tractament específiques diferents de les establertes per la normativa general de protecció de dades.
- Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.
- Establiment de mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.
- Valoració de les sol·licituds d'exercici de drets per part dels interessats.

- Contractació d'encarregats de tractament, inclòs el contingut dels contractes o actes jurídics que regulin la relació responsable-encarregat.
- Identificació dels instruments de transferència internacional de dades adequades a les necessitats i les característiques de l'organització i de les raons que justifiquin la transferència.
- Disseny i implantació de polítiques de protecció de dades.
- Auditoria de protecció de dades.
- Establiment i gestió dels registres d'activitats de tractament.
- Anàlisi de riscos dels tractaments realitzats.
- Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequades als riscos i naturalesa dels tractaments.
- Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.
- Establiment de procediments de gestió de violacions de seguretat de les dades, inclosa l'avaluació del risc per als drets i les llibertats dels afectats i els procediments de notificació a les autoritats de supervisió i als afectats.
- Determinació de la necessitat de fer avaluacions d'impacte sobre la protecció de dades.
- Realització d'avaluacions d'impacte sobre la protecció de dades.
- Relacions amb les autoritats de supervisió.
- Implantació de programes de formació i sensibilització del personal en matèria de protecció de dades.

3.6.3. Funcions i obligacions d'usuaris amb accés a dades

Tots els empleats de l'entitat estan subjectes a funcions i obligacions. Tot el personal de l'entitat que disposi d'accés a les dades de caràcter personal ha de complir les obligacions següents:

- No es permet la difusió de dades de caràcter personal ni confidencial pertanyent a l'entitat. Estant obligat a guardar secret de la informació fins i tot acabada la relació laboral.
- L'usuari es responsabilitzarà de notificar tota incidència segons el procediment de gestió d'incidències; no notificar una incidència serà considerada una omissió del deure del treballador.
- L'usuari es responsabilitzarà de tots els accessos que es facin sota el vostre identificador i contrasenya, per tant, no haurà de revelar la contrasenya.
- L'usuari es responsabilitza sempre que abandoni el lloc de treball de tancar la sessió o bloquejar l'equip amb contrasenya.

- No es podran instal·lar aplicacions als sistemes de l'entitat sense el consentiment del delegat de protecció de dades.
- No es permet la còpia de dades de caràcter personal, en suports, sense l'autorització expressa del delegat de protecció de dades.
- L'usuari es responsabilitzarà de desar còpies de tots els correus que incloguin annexos amb dades personals vinculades a l'entitat.

3.6.4. Funcions i obligacions de l'encarregat del tractament

Els encarregats del tractament tenen com a missió fer les tasques ordinàries per al desenvolupament efectiu de les funcions per a les quals ha estat creat el tractament per compte del Responsable del tractament.

En aquest sentit, l'apartat 8 de l'article 4 del RGPD defineix l'encarregat de tractament com "la persona física o jurídica, autoritat pública, servei o altre organisme que tracti dades personals per compte del responsable del tractament".

L'encarregat del tractament ha d'aplicar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i n'evitin l'alteració, la pèrdua, el tractament o l'accés no autoritzat.

Igualment haurà d'implementar les mesures de seguretat a què es refereix el paràgraf anterior i que apareixeran estipulades al contracte amb el Responsable del Tractament.

En concret, les seves funcions són les de:

- Tractar les dades del tractament.
- Realitzar el control de tractament, qualitat i seguretat de les dades.
- Controlar la forma i els requisits per procedir a les addicions i cancel·lacions.
- Controlar els suports de seguretat.
- Control i accés de contrasenyes.
- Manteniment del registre d'incidències.
- Crear una llista per a les situacions en què un afectat no vulgui que les dades personals s'emmagatzemin en el tractament.
- Traslladar al responsable del tractament les sol·licituds d'exercici de dret que es rebin per part dels interessats.

En conseqüència, **GLOBAL LEGAL DATA, S.L** haurà de dur a terme un document actualitzat on

s'identificaran els encarregats de tractament que estan prestant serveis a l'Administració, així com la indicació de la formalització del contracte pertinent amb aquests prestadors de serveis amb accés a dades.

04 GESTIÓ DE RISCOS

4

4.1 JUSTIFICACIÓ

Tots els sistemes subjectes a aquesta Política hauran de fer una anàlisi de riscos, avaluant les amenaces i els riscos a què estan exposats.

L'anàlisi de riscos serà la base per determinar les mesures de seguretat que s'han d'adoptar a més dels mínims establerts per l'Esquema Nacional de Seguretat, segons el que preveu l'article 7 de l'ENS.

4.2 CRITERIS D'AVALUACIÓ DE RISCOS

Per a l'harmonització de les anàlisis de riscos, el Comitè de Seguretat de la Informació establirà una valoració de referència per als diferents tipus d'informació i els diferents serveis prestats.

Els criteris d'avaluació de riscos detallats s'especificaran a la metodologia d'avaluació de riscos que elaborarà l'organització, basant-se en estàndards i en bones pràctiques reconegudes.

S'han de tractar, com a mínim, tots els riscos que puguin impedir la prestació dels serveis o el compliment de la missió de l'organització de manera greu.

Es prioritzaran especialment els riscos que impliquin un cessament en la prestació de serveis als ciutadans.

4.3 DIRECTRIUS DE TRACTAMENT

El Comitè de Seguretat de la Informació dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, promovent inversions de caràcter horitzontal.

4.4 PROCÉS D'ACCEPTACIÓ DEL RISC RESIDUAL

Els riscos residuals seran determinats pel Responsable de Seguretat de la Informació.

Els nivells de risc residuals esperats sobre cada informació després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat previstes a l'annex II de l'ENS) hauran de ser acceptats prèviament pel Responsable d'aquesta Informació.

Els nivells de Risc residuals esperats sobre cada Servei després de la implementació de les opcions de tractament previstes (incloent-hi la implantació de les mesures de seguretat previstes a l'Annex II de l'ENS) hauran de ser acceptats prèviament pel Responsable d'aquest Servei.

Els nivells de risc residuals seran presentats pel Responsable de Seguretat de la Informació al Comitè de Seguretat de la Informació, perquè aquest procedeixi, si és el cas, a avaluar, aprovar o rectificar les opcions de tractament proposades.

4.5 NECESSITAT DE REALITZAR O ACTUALITZAR LES AVALUACIONS DE RISCOS

- L'anàlisi dels riscos i el seu tractament han de ser activitats repetides regularment, segons el que estableix l'article 10 de l'ENS. Aquesta anàlisi es repetirà:
- Regularment, si més no una vegada a l'any.
- Quan es produeixin canvis significatius a la informació tractada.
- Quan es produeixin canvis significatius als serveis prestats.
- Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
- Quan es produeixi un incident greu de seguretat.
- Quan es reportin vulnerabilitats greus.

05 GESTIÓ D'INCIDENTS DE SEGURETAT

5

5.1 PREVENCIÓ D'INCIDENTS

Els Departaments han d'evitar, o almenys prevenir en la mesura que sigui possible, que la informació o els serveis es vegin perjudicats per incidents de seguretat.

Per això, els departaments han d'implementar les mesures mínimes de seguretat determinades per l'ENS, així com qualsevol control addicional identificat mitjançant una avaluació d'amenaces i riscos. Aquests controls, i els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Per garantir el compliment de la política, els Departaments han de:

- Establir àrees segures per als sistemes d'informació crítica o confidencial.
- Autoritzar els sistemes abans d'entrar en operació.
- Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de forma rutinària.

- Sol·licitar la revisió periòdica per part de tercers per obtenir una avaluació independent.

5.2 MONITORITZACIÓ I DETECCIÓ D'INCIDENTS

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple disminució del rendiment fins a la seva detenció, els serveis han de monitoritzar l'operació de manera contínua per detectar anomalies en els nivells de prestació dels serveis i actuar en conseqüència segons allò establert a l'article 10 de l'ENS.

La monitorització és especialment rellevant quan s'estableixen línies de defensa d'acord amb l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i notificació que arribin als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

Els sistemes de detecció d'intrusos compleixen fonamentalment una tasca de supervisió i auditoria sobre els recursos de l'Organització, verificant que la Política de Seguretat no és violada i intenta identificar qualsevol tipus d'activitat maliciosa d'una manera primerenca i eficaç.

S'hauran d'establir, en funció de les necessitats, les classificacions següents:

- Sistemes de detecció d'intrusos a nivell de xarxa.
- Sistemes de detecció d'intrusos a nivell sistema.

5.3 RESPOSTA DAVANT D'INCIDENTS

Els Departaments han de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar un punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o altres organismes.
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els Equips de Resposta a Emergències (CERT).

5.4 RECUPERACIÓ DAVANT D'INCIDENTS I PLANS DE CONTINUÏTAT

Per garantir la disponibilitat dels serveis crítics, els Departaments han de desenvolupar plans de continuïtat dels sistemes TIC com a part del pla general de continuïtat de negoci i activitats de recuperació.

06 OBLIGACIONS DEL PERSONAL

Tots els membres de l'organització tenen l'obligació de conèixer i complir aquesta Política de Seguretat de la Informació i la Normativa de Seguretat, i és responsabilitat del Comitè de Seguretat de la Informació disposar els mitjans necessaris perquè la informació arribi als afectats.

Tots els membres de l'organització assistiran a una sessió de conscienciació en matèria de seguretat TIC almenys una vegada cada dos anys. S'establirà un programa de conscienciació continuada per atendre tots els membres de l'organització, en particular els de nova incorporació.

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

El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos l'organització, constituint el seu incompliment infracció greu a efectes laborals.

07 TERCERES PARTS

Quan es prestin serveis o es gestioni informació d'altres organitzacions, se'ls farà partícip d'aquesta Política de Seguretat de la Informació, s'establiran canals per reportar i coordinar els Comitès de Seguretat de la Informació respectius i s'establiran procediments d'actuació per a la reacció. davant d'incidents de seguretat.

Quan s'utilitzin serveis de tercers o cedeixi informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la Normativa de Seguretat que afecta aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, i podrà desenvolupar els seus propis procediments operatius per satisfer-la.

S'establiran procediments específics de notificació i resolució d'incidències.

Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que el que estableix aquesta Política.

Quan algun aspecte de la Política no pugui ser satisfet per una tercera part segons l'indicat en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat sobre els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels Responsables de la Informació i els Serveis afectats abans de seguir endavant.

08 REVISIÓ I APROVACIÓ DE LA POLITICA DE SEGURETAT

La Política de Seguretat de la Informació serà revisada pel Comitè de Seguretat de la Informació a intervals planificats, que no podran excedir l'any de durada, o sempre que es produeixin canvis significatius, per assegurar que se'n mantingui la idoneïtat, l'adequació i eficàcia.

Els canvis sobre la política de seguretat de la informació han de ser aprovats per l'òrgan superior competent que correspongui, d'acord amb l'article 12 de l'ENS.

Qualsevol canvi sobre aquesta haurà de ser difós a totes les parts afectades.

09 DOCUMENTACIÓ COMPLEMENTÀRIA

La Política de Seguretat de la Informació s'emplenarà amb documents més precisos que ajudin a dur a terme allò proposat. Per això s'utilitzaran:

- Normes de seguretat (*security standards*).
- Guies de seguretat (*security guides*).
- Procediments de seguretat (*security procedures*).

Les normes uniformitzen l'ús d'aspectes concrets del sistema. Indiquen l'ús correcte i les responsabilitats dels usuaris. Són de caràcter obligatori.

Les guies tenen un caràcter formatiu i busquen ajudar els usuaris a aplicar correctament les mesures de seguretat proporcionant raonaments on no hi ha procediments precisos. Per exemple, hi sol haver una guia sobre com escriure procediments de seguretat. Les guies ajuden a prevenir que es passin per alt aspectes importants de seguretat que es poden materialitzar de diverses maneres.

Els procediments [operatius] de seguretat afronten tasques concretes, indicant què cal fer, pas a pas. Són útils en tasques repetitives.

ANNEX I: RELACIÓ DE RESPONSABLES DEL SERVEI

SERVEI	RESPONSABLE DEL SERVEI
Direcció	Director/a
Secretaria i serveis generals	Secretari/ària
Serveis econòmics	Interventor/a
Serveis econòmics	Tresorer/a
Recaptació	Recaptador/a

Font: Portal de transparència.

ANNEX II: GLOSSARI DE TERMES

Anàlisi de riscos
Utilització sistemàtica de la informació disponible per identificar perills i estimar-ne els riscos.

Dades de caràcter personal
Qualsevol informació concernent persones físiques identificades o identificables.

Gestió d'incidents
Pla d'acció per atendre les incidències que es donin. A més de resoldre-les, ha d'incorporar mesures de compliment que permetin conèixer la qualitat del sistema de protecció i detectar tendències abans que es converteixin en grans problemes.

Gestió de riscos
Activitats coordinades per dirigir i controlar una organització pel que fa als riscos.

Incident de seguretat
Succés inesperat o no desitjat amb conseqüències en detriment de la seguretat del sistema d'informació.

Informació
Cas concret d´un cert tipus d´informació.

Política de seguretat
Conjunt de directrius plasmades en document escrit, que regeixen la manera com una organització gestiona i protegeix la informació i els serveis que consideren crítics.

Principis bàsics de seguretat
Fonaments que han de regir tota acció orientada a assegurar la informació i els serveis.

Responsable de la informació
Persona que té la potestat d'establir els requisits duna informació en matèria de seguretat.

Responsable de la seguretat
El responsable de seguretat determinarà les decisions per satisfer els requisits de seguretat de la informació i dels serveis.

Responsable del servei
Persona que té la potestat d'establir els requisits d'un servei en matèria de seguretat.

Responsable del sistema
Persona que s'encarrega de l'explotació del sistema d'informació.

Servei
Funció o prestació exercida per alguna entitat oficial destinada a cuidar interessos o satisfer necessitats dels ciutadans.

Sistema d'informació
Conjunt organitzat de recursos perquè la informació es pugui recollir, emmagatzemar, processar o tractar, mantenir, fer servir, compartir, distribuir, posar a disposició, presentar o transmetre.