



ENS-PLS-001-Política General de Seguretat de la  
Informació-V02

**DOCUMENT PÚBLIC**

#### CONTROL DEL DOCUMENT

Nom del document: ENS-PLS-001-Política General de Seguretat de la Informacio-V02.docx
Data creació: 11/10/2022
Classificació de la informació: <b>PÚBLIC</b>
Llista de Distribució: PERSONAL INTERN, EXTERN I TERCERS

*Aquest document està dirigit EXCLUSIVAMENT a les persones nomenades a la llista de distribució, les quals podran, en base al seu criteri, divulgar-ho als que considerin oportú. Es recomana una divulgació controlada en què 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

Nº Versió	Autor	Data	Canvis realitzats
V02	Manel Escatllar	05/10/2023	Correcció NC2 ENS. Apartat 7

---

*Material reservat. Està prohibit qualsevol ús, divulgació i/o transmissió en qualsevol forma o mitjà sense una autorització prèvia i per escrit de L CAT*

---

## INDEX

1	Contingut i Objectius del present document. ....	5
2	Justificació d'una política general de seguretat de la informació. ....	5
3	Àmbit objectiu de la PGSI. ....	5
4	Àmbit subjectiu de la PGSI.....	5
5	Missió i estratègia.....	6
6	Marc normatiu referencials de la PGSI.....	6
7	Compliment dels requisits mínims de seguretat.....	6
8	Òrgan Superior Competent. ....	10
9	Organització de la seguretat.....	10
9.1	Definició de rols. ....	10
9.2	Responsable de la Informació (RINF) .....	10
9.3	Responsable del Servei (RSIS) .....	10
9.4	Responsable de seguretat de la informació. (RSEG o CIS). ....	10
9.5	Responsable del sistema (RSIS o CIO). ....	11
9.6	Delegat de Protecció de Dades (DPD).....	11
9.7	Comitè de Seguretat Integral.....	12
9.7.1	Composició. ....	12
9.7.2	Funcions del Comitè de Seguretat Integral. ....	13
9.8	Jerarquia en el procés de decisions i mecanismes de coordinació.....	13
9.8.1	Comitè de Seguretat Integral.....	14
9.8.2	Responsable de seguretat de la informació. ....	14
9.8.3	Responsable del sistema.....	14
9.9	Procediments de designació de persones.....	14
9.10	Segregació de funcions. ....	14
9.11	Suplències i delegacions.....	15
10	Dades de caràcter personal.....	15
10.1	Tractament.....	15
10.2	Videovigilància. ....	15
11	Gestió de riscos.....	16
11.1	Justificació.....	16
11.2	Criteris d'avaluació de riscos.....	16
11.3	Directrius de tractament.....	16
11.4	Procés d'acceptació del risc residual. ....	16

11.5	Necessitat de fer o actualitzar les avaluacions de riscos. ....	16
12	Gestió d'incidents de seguretat.....	17
12.1	Prevenió.....	17
12.2	Detecció. ....	17
12.3	Resposta.....	17
12.4	Recuperació.....	18
12.5	Aprenentatge. ....	18
13	Gestió del personal.....	18
13.1	Obligacions del personal. ....	18
13.2	Caracterització del lloc de treball.....	18
13.3	Formació. ....	18
13.4	Conscienciació.....	19
14	Terceres parts.....	19
15	Revisió i aprovació de la Política de Seguretat.....	20
16	Documentació complementària.....	20
16.1	Normatives de seguretat.....	20
16.2	Procediments de seguretat.....	20
16.3	Instruccions de seguretat.....	20

## 1 Contingut i Objectius del present document.

Aquest document conté la Política General de Seguretat de la Informació (PGSI d'ara endavant) del Consorci d'aigües de Tarragona ("l'Organització" o "CAT", d'ara endavant).

L'objectiu fonamental d'aquesta Política es centra a definir les estructures organitzatives, els rols, les responsabilitats, els criteris i les iniciatives d'aquesta Organització respecte a la Seguretat de la Informació que emmagatzema i gestiona, així com el compliment dels diferents marcs normatius que la regulen.

## 2 Justificació d'una política general de seguretat de la informació.

Els marcs normatius vigents en matèria de seguretat de la informació requereixen la disponibilitat d'una política de seguretat corporativa que, aprovada per l'anomenat "Òrgan Superior Competent", representat en el cas del CAT pel seu Consell d'Administració, i adequadament difosa entre el personal i totes les entitats afectades, implementi els requeriments d'aquests Marcs per tal de preservar els drets i llibertats dels interlocutors socials amb els quals interactua el CAT, englobats en endavant sota la denominació genèrica "interlocutors", "interlocutors socials", "tercers" o "parts interessades".

La diversitat de marcs normatius, els seus diferents àmbits objectius i subjectius, així com l'evolució permanent dels mateixos, aconsellen desenvolupar una PGSI unificada i permetre amb això eliminar redundàncies en activitats, documents i controls, optimitzant amb això les actuacions corporatives i el nivell de compliment normatiu.

## 3 Àmbit objectiu de la PGSI.

La PGSI abasta tots els mitjans, automatitzats o no, que el CAT utilitza per al desenvolupament de les seves activitats, així com tots els mitjans pels quals opera internament amb altres entitats, públiques i/o privades. Les activitats inclouen:

- (1). Les relacions de caràcter juridicoeconòmic-administratiu entre els interlocutors socials i el CAT.
- (2). La realització de les funcions de negoci/servei per part del CAT, tant els desenvolupats per mitjans electrònics com els manuals.
- (3). El tractament de la informació gestionada per el CAT en l'exercici de les seues competències, especialment aquella relacionada amb dades personals.
- (4). Les relacions del CAT amb les administracions públiques.

## 4 Àmbit subjectiu de la PGSI.

La PGSI serà aplicada per tots els serveis, informacions, departaments, seccions, àrees, unitats administratives de l'Organització i, en general, per totes les entitats internes i externes de qualsevol tipus vinculades a aquesta entitat mitjançant qualsevol model de relació. Per tal d'unificar la terminologia les estructures organitzatives internes seran anomenades "departaments" en endavant.

La PGSI afecta tot el personal del CAT, sigui quina sigui la seva relació laboral amb aquesta. Així mateix, la PGSI afecta tot el personal que presta serveis a l'Organització a través d'empreses externes i que, per raó d'aquesta relació, accedeixi, emmagatzemi i/o tracti informació la competència i/o responsabilitat dels quals recaigui sobre l'Organització.

La PGSI serà aplicada en les relacions del CAT amb els interlocutors socials, empreses i entitats públiques i/o privades amb què interactuï, per la qual cosa les persones que intervinguin en aquestes relacions estan incloses en els subjectes a qui resulta de aplicació aquesta política.

## 5 Missió i estratègia

El Consorci d'Aigües de Tarragona té com a principal missió el subministrament d'aigua potable a municipis i indústries consorciades.

La seva estratègia es basa en la qualitat entesa com a producte i servei a un preu ajustat al cost, el respecte al medi ambient considerant el possible impacte de la seva activitat, el control dels riscos de seguretat i salut en el treball, el benestar i compromís amb l'entorn, la innocuïtat de l'aigua com a producte de consum humà, l'assegurament dels requisits i la competència tècnica en les activitats d'assaig, calibratge i presa de mostra, la seguretat de la informació en el context de l'organització i la responsabilitat social amb el desenvolupament sostenible i el territori.

## 6 Marcs normatius referencials de la PGSI.

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

***ENS-RGS-001-Normativa Aplicable***

Contenint els marcs normatius aplicables al CAT.

## 7 Compliment dels requisits mínims de seguretat

El CAT, 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 CAT, estarà presidida 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:

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

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.

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.

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 continua per part del CAT 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**

Tothom, propi o aliè relacionat amb els sistemes d'informació del CAT, 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 CAT 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 CAT, 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 de els 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 CAT es connecta a xarxes públiques, tal com es defineixen en la legislació vigent en matèria de telecomunicacions, reforçant 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 atènyer-se al que disposa la instrucció tècnica de seguretat corresponent.

### **Diferenciació de responsabilitats, organització i implantació del procés de seguretat**

El CAT ha organitzat la seva seguretat compromentent 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 CAT 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 CAT 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 CAT, 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 CAT 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 CAT 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, l'Ajuntament 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.

### **Infraestructures i serveis comuns**

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

## 8 Òrgan Superior Competent.

Als efectes de les actuacions previstes a l'SGSI i encomanades a l'anomenat "Òrgan Superior Competent", aquest Òrgan, al CAT, serà el seu Consell d'Administració i, si escau, en qui s'estableixi l'oportuna delegació.

## 9 Organització de la seguretat.

### 9.1 Definició de rols.

Tal com indiquen les normes de referència, la seguretat ha de comprometre tots els membres de l'organització. La Política de Seguretat ha d'identificar uns responsables clars per vetllar pel seu compliment i ser coneguda per tots els membres de l'Organització.

Adicionalment, altres marcs normatius requereixen així mateix la creació de rols específics, com ara el rol Delegat de Protecció de Dades al RGPD-LOPDGDD.

S'estableixen per tant els rols següents a l'Organització relacionats amb la Seguretat de la Informació:

### 9.2 Responsable de la Informació (RINF)

El Responsable de la Informació serà l'encarregat de dur a terme en relació amb l'Esquema Nacional de Seguretat les tasques següents:

- Establir i aprovar els requisits de seguretat aplicables a la informació dins de el marc establert en l'annex I de Reial Decret 311/2022, de 3 de maig, prèvia proposta a el responsable de seguretat i / o Comitè de Seguretat Integral
- Acceptar els nivells de risc residual que afectin a la Informació.

### 9.3 Responsable del Servei (RSIS)

El Responsable del Servei serà l'encarregat de dur a terme en relació amb l'Esquema Nacional de Seguretat les tasques següents:

- Establir i aprovar els requisits de seguretat aplicables al servei dins de el marc establert en l'annex I de Reial Decret 311/2022, de 3 de maig, prèvia proposta al responsable de seguretat i / o Comitè de Seguretat Integral
- Acceptar els nivells de risc residual que afectin el servei.

### 9.4 Responsable de seguretat de la informació. (RSEG o CIS).

El rol de Responsable de Seguretat ha d'assumir les funcions següents:

- Recopilar els requisits de seguretat del Responsable d'informació i Responsable del Servei i determinar la categoria del Sistema.
- Realitzar l'Anàlisi i la Gestió de Riscos.
- Elaborar i aprovar la Declaració d'Aplicabilitat.
- Facilitar al Responsable d'Informació i al Responsable del Servei informació sobre el nivell de risc residual esperat després d'implementar les opcions de tractament seleccionades a la declaració d'Aplicabilitat.

- Elaborar i revisar les Polítiques, Normatives i Procediments de Seguretat de la Informació.
- Facilitar periòdicament al Comitè de Seguretat Integral un resum d'actuacions en matèria de seguretat, d'incidents relatius a seguretat de la informació i de l'estat de la seguretat.
- Mantenir la seguretat de la informació gestionada i dels serveis prestats pels sistemes d'informació.
- Elaborar els plans de formació i conscienciació del personal en seguretat de la informació.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Elaborar, juntament amb el Responsable del Sistema, els Plans de Millora de la Seguretat.
- Elaborar, juntament amb el Responsable del Sistema, els Plans de Continuitat.
- Actuar en plena coordinació amb el delegat de protecció de dades (RGPD).
- Actuar com a punt de contacte amb les autoritats competents en matèria de seguretat (CNN-CERT, CESICAT, etc).
- Elaborar i reportar al CCN-CERT anualment l'informe d'Estat de la Seguretat (INES).

## 9.5 Responsable del sistema (RSIS o CIO).

El rol del Responsable del Sistema ha d'assumir les funcions següents:

- Paralitzar o donar suspensió a l'accés a informació o prestació de servei si es té 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-hi els criteris d'ús i els serveis disponibles.
- Assegurar que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Prestar al Responsable de Seguretat i/o al Comitè de Seguretat assessorament per a la determinació de la categoria del sistema.
- Elaborar, juntament amb el Responsable de Seguretat, els Plans de Millora de la Seguretat.
- Elaborar, juntament amb el Responsable de Seguretat, els Plans de Continuitat.
- 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.
  - Assegurar que els controls de seguretat establerts són estrictament complerts.
  - Assegurar que són aplicats els procediments aprovats per gestionar 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.

## 9.6 Delegat de Protecció de Dades (DPD).

El rol de Delegat de Protecció de Dades (DPD) és requerit pel RGPD en base al seu Art. 37:

*Article 37 Designació del delegat de protecció de dades*

*1. El responsable i l'encarregat del tractament designaran un delegat de protecció de dades sempre que:*

- a) El tractament el du a terme una autoritat o un organisme públic, excepte els tribunals que actuïn en exercici de la seva funció judicial.*
- b) Les activitats principals del responsable o de l'encarregat consisteixin en operacions de tractament que, per raó de la seva naturalesa, abast i/o fins, requereixin una observació habitual i sistemàtica d'interessats a gran escala.*
- c) Les activitats principals del responsable o de l'encarregat consisteixin en el tractament a gran escala de categories especials de dades personals d'acord amb l'article 9 RGPD i de dades relatives a condemnes i infraccions penals a què fa referència l'article 10 RGPD.*

Adicionalment, la LOPDGDD, en el seu article 76. Sancions i mesures correctives inclou com a punt a considerar en un possible procediment sancionador:

*g) Disposar, quan no sigui obligatori, un delegat de protecció de dades.*

En base a aquestes consideracions, el CAT assumeix la necessitat de disposar del rol delegat de protecció de dades.

Per tant, s'identificarà i nomenarà un delegat de protecció de dades corporatives, si bé aquest rol podrà ser assignat a personal intern o a un servei extern.

La titularitat concreta del DPD corporatiu es determina mitjançant designació de l'Òrgan Superior Competent, després d'un informe del Comitè de Seguretat Integral.

Les funcions del DPD estan definides al RGPD.

## 9.7 Comitè de Seguretat Integral.

### 9.7.1 Composició.

Es crea el Comitè de Seguretat Integral, que estarà compost pels membres següents:

<b>Càrrec al Comitè</b>	<b>Càrrec Corporatiu</b>
Presidència	Director i Gerent
Secretari	Responsable de Seguretat de la Informació
Vocal 1	Directora de Seguretat
Vocal 2	Delegat de Seguretat ETAP

El Comitè de Seguretat Integral podrà convocar responsables departamentals i/o altres persones la intervenció de les quals sigui requerida per al desenvolupament de les actuacions del Comitè. És obligatòria l'assistència de les persones convocades, l'aportació de tota la informació que els sigui sol·licitada i el compliment de les instruccions rebudes del Comitè de Seguretat Integral.

Correspon al secretari/ària del Comitè de Seguretat Integral:

- Convocar les reunions del Comitè de Seguretat Integral.

- 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.
- La responsabilitat de l'execució directa o delegada de les decisions del Comitè.

Tots els membres del Comitè actuaran amb veu i vot i els seus acords requeriran, com a mínim, el vot de la majoria simple dels membres.

### 9.7.2 Funcions del Comitè de Seguretat Integral.

Les competències i funcions del Comitè de Seguretat Integral són:

1. Atendre les inquietuds de la Direcció de l'entitat i dels diferents departaments.
2. Informar regularment de l'estat de la seguretat física i seguretat de la informació a la Direcció.
3. Promoure la millora continua del sistema de gestió de la seguretat física i seguretat de la informació.
4. Elaborar l'estratègia d'evolució de l'organització pel que fa a seguretat física i seguretat de la informació.
5. Coordinar els esforços de les diferents àrees en matèria de seguretat física i seguretat de la informació, per assegurar que els esforços són consistents, que estan alineats amb l'estratègia decidida en la matèria, evitant duplicitats.
6. Elaborar (i revisar regularment) la Política de Seguretat de la Informació per a aprovar-la per la Direcció.
7. Aprovar la Normativa, procediments i instruccions tècniques de seguretat necessàries per desenvolupar les polítiques i normatives existents en matèria de seguretat física i de la informació.
8. Elaborar i aprovar els requisits de formació i qualificació d'administradors, operadors i usuaris, des del punt de vista de seguretat de la informació.
9. Monitoritzar els riscos residuals principals assumits per l'organització i recomanar possibles actuacions.
10. 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 de tals incidents.
11. Aprovar plans de millora de la seguretat de la informació i seguretat física de l'organització. En particular, vetllarà per la coordinació de diferents plans que puguin realitzar-se en diferents àrees.
12. Prioritzar les actuacions en matèria de seguretat quan els recursos siguin limitats.
13. Vetllar perquè la seguretat de la informació i física es tingui en compte en tots els projectes relacionats amb les Tecnologies de la Informació i Comunicacions (TIC en endavant) des de la seva especificació inicial fins a la seva posada en operació, aplicant paral·lelament els principis de "privadesa per disseny i per defecte" en cas de tractament de dades personals. 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.
14. Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents àrees de l'organització, elevat aquells casos en què no tingui prou autoritat per decidir.
15. Articular i dur a terme els plans de modernització relacionats amb la millora de la seguretat física i de la informació
16. Vetllar pel compliment de la legislació vigent en matèria de seguretat de la informació, i en particular per que les exigències del Reglament General de Protecció de Dades i el RD 311/2022 del 3 de maig (ENS) siguin apropiadament satisfetes.
17. Vetllar pel compliment de la legislació vigent en matèria de seguretat privada i de protecció de les infraestructures crítiques.

## 9.8 Jerarquia en el procés de decisions i mecanismes de coordinació.

Els diferents rols de Seguretat de la Informació (autoritat principal i possibles delegades) es limiten a una jerarquia simple:

### 9.8.1 Comitè de Seguretat Integral.

El Comitè de Seguretat Integral dona instruccions al Responsable de Seguretat de la Informació, que s'encarrega d'emplenar-les, supervisant que administradors i operadors implementen les mesures de seguretat segons allò establert en aquesta PGSI.

### 9.8.2 Responsable de seguretat de la informació.

El Responsable de la Seguretat de la Informació:

1. Informa al 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.
2. 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.
3. Rendeix comptes al Comitè de Seguretat Integral, 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.
4. Rendeix comptes periòdicament a l'Òrgan Superior Competent, segons el que acorda el Comitè de Seguretat Integral; al Òrgan de Control Intern (OCI), que és l'encarregat d'impulsar i supervisar la implementació i eficàcia de Gestió de Compliance penal sigui conforme als requisits establerts a l'art. 31bis del Codi Penal, així com al Delegat de Protecció de Dades del CAT. .
  - 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.

### 9.8.3 Responsable del sistema.

El Responsable del Sistema:

1. Informa al Responsable de la Informació de les incidències funcionals relatives a la informació que li competeix.
2. Informa al Responsable de Servei de les incidències funcionals relatives al servei que li competeix.
3. Dona comptes 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.

## 9.9 Procediments de designació de persones.

L'Òrgan Superior Competent nomenarà formalment, mitjançant les resolucions pertinents:

- Comitè de Seguretat Integral.
- Delegat de protecció de dades.
- Responsable/s de la Informació
- Responsable/s del Servei/s
- Responsable/s de la Seguretat.
- Responsable/s dels sistemes d'informació.

## 9.10 Segregació de funcions.

L'ENS recull el principi de "seguretat com a funció diferenciada". Aquest principi exigeix:

- Responsable de Seguretat ha de ser independent del Responsable del sistema.
- Responsable de Servei o d'informació ha de ser independent del Responsable del Sistema.
- Les persones assignades a funcions de desenvolupament han de ser independents de les persones assignades als passis a producció.
- Les persones assignades a l'operació de sistemes hauran de ser independents de les persones assignades al manteniment de sistemes.
- Delegat de Protecció de Dades ha de ser independent de tota influència que pogués condicionar les seves actuacions, en base al que requereix el RGPD.

L'assignació de rols i responsabilitats tindrà en compte la preceptiva segregació de funcions, de manera que les actuacions de les persones titulars dels mateixos no comprometin la seguretat d'informacions i serveis en qualsevol de les seves dimensions (confidencialitat, integritat, disponibilitat, autenticitat i traçabilitat).

En casos excepcionals, sobretot quan no estan disponibles els recursos necessaris, es poden exceptuar aquestes regles de segregació de funcions i establir les mesures compensatòries apropiades per a la resolució dels conflictes d'interessos que puguin sorgir.

### 9.11 Suplències i delegacions.

Els rols requerits pels marcs normatius referencials d'aquesta PGSI han d'estar permanentment operatius. L'Organització establirà un procediment formal de suplències i/o delegacions de manera que l'absència d'una persona, per qualsevol motiu, no causi manca de les funcions i/o competències que desenvolupa.

## 10 Dades de caràcter personal.

### 10.1 Tractament.

Per a la prestació dels serveis corporatius han de ser demanats, tractats i emmagatzemats dades de caràcter personal. És compromís del CAT respectar i protegir els drets fonamentals recollits a la Constitució Espanyola respecte a la intimitat, privadesa, imatge i honor de les persones, per la qual cosa el compliment dels marcs normatius que els regulen i, per tant, la implementació de les mesures de seguretat i control requerides constitueix un objectiu prioritari d'aquesta Organització.

El compliment de RGPD, LOPDGDD i els seus marcs normatius que els desenvolupen serà una iniciativa prioritària. S'adoptaran les mesures necessàries perquè aquesta Organització compleixi en les dates d'entrada en vigor tots els preceptes dels nous marcs, sent un dels punts més importants el nomenament de la figura DPO/DPD (Data Protection Officer/Delegat de Protecció de Dades).

Així mateix, s'han de fer els cicles de formació i conscienciació específics perquè el personal conegui les mesures que han d'aplicar als seus llocs de treball i els mitjans disponibles per a la resolució de dubtes, problemes i incidents relacionats.

Serà prioritari implementar les mesures organitzatives i tècniques apropiades per protegir els drets i les llibertats de les persones físiques afectades pels tractaments de dades personals realitzats per l'Organització.

### 10.2 Videovigilància.

L'Organització observarà en tot moment la normativa vigent en matèria de videovigilància, respectant els drets de les persones captades i suprimint les imatges en els terminis establerts per aquest ordenament.

## 11 Gestió de riscos.

### 11.1 Justificació.

Tots els sistemes subjectes a aquesta PGSI hauran de fer una anàlisi de riscos, avaluant les amenaces a què estan exposats, les seves vulnerabilitats, l'impacte que suposaria la materialització de les amenaces i, per tant, el nivell de risc que suposa.

Pel que fa a tots els sistemes d'informació compresos a l'abast d'aquesta Política, caldrà fer anàlisis de riscos periòdics, avaluant les amenaces i els riscos a què estan exposats.

L'anàlisi de riscos serà una de les bases fonamentals per determinar les mesures de seguretat que cal adoptar, així com per als requeriments del RGPD relacionats sobre Anàlisi de Riscos i Avaluacions d'Impacte sobre Protecció de Dades (EIPD), quan siguin procedents.

### 11.2 Criteris d'avaluació de riscos.

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

Els criteris d'avaluació de riscos detallats s'especificaran a la metodologia d'avaluació de riscos que adoptarà l'Organització, basant-se en estàndards i bones pràctiques reconegudes. Aquesta metodologia serà MAGERIT V3 i les actualitzacions que pugueu incorporar en el futur.

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, en base a l'impacte que els esdeveniments analitzats suposin sobre aquests, així com aquells que afectin els drets i les llibertats de les persones físiques afectades pels tractaments de dades personals.

Es prioritzaran especialment els riscos que impliquin un cessament en la prestació de serveis als interlocutors socials i els associats als tractaments de dades de caràcter personal.

### 11.3 Directrius de tractament.

El Comitè de Seguretat Integral dinamitzarà la disponibilitat de recursos per atendre les necessitats de seguretat dels diferents sistemes, documentant, justificant i promovent les inversions adequades per a l'aprovació de l'Òrgan Superior Competent.

### 11.4 Procés d'acceptació del risc residual.

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

Els nivells de risc residual esperats sobre serveis i informacions després de la implementació de les opcions de tractament previstes (inclosa la implantació de les mesures de seguretat contingudes a l'Annex II de l'ENS i aquelles complementàries que siguin necessàries per al compliment de LOPDGDD) han de ser aprovats pel Comitè de Seguretat Integral, del qual forma part el Gerent del CAT, el seu Òrgan Superior Competent.

### 11.5 Necessitat de fer o actualitzar les avaluacions de riscos.

L'anàlisi dels riscos i el seu tractament han de ser una activitat repetida regularment, segons el que estableix l'article 9 de l'ENS. Aquesta anàlisi es repetirà:

- Regularment, si més no una vegada a l'any.
- Quan es produeixin canvis significatius a la informació manejada.

- 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.
- Quan es produeixin canvis normatius que així ho exigeixin o ho facin convenient.

## 12 Gestió d'incidents de seguretat

### 12.1 Prevenció.

EL CAT ha d'evitar, o, almenys, prevenir en la mesura que sigui possible, que la informació o els serveis es vegin afectats per incidents de seguretat. Per això, cal implementar les mesures de seguretat determinades per les normatives corporatives, així com qualsevol control addicional identificat a través d'una avaluació de riscos.

Aquests controls, així com els rols i les responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats, i hi ha una caracterització de llocs de treball on s'inclouin les qüestions relacionades amb la seguretat.

Per garantir el compliment de la política, i sota la supervisió del Comitè de Seguretat Integral, els departaments/unitats de negoci han de:

- Autoritzar els sistemes abans d'entrar en producció des del prisma de les prestacions, funcional i legal.
- Avaluar regularment la seguretat, incloent-hi apreciacions de riscos, impulsant les iniciatives necessàries per resoldre les situacions no conformes o fora dels marges de risc acceptables.
- Sol·licitar la revisió periòdica per part de tercers per obtenir una avaluació independent.
- Desenvolupar Plans de Formació per al personal, així com reciclatge periòdic i accions de conscienciació.

### 12.2 Detecció.

Atès que els serveis es poden degradar ràpidament a causa d'incidents, podent fins i tot provocar la seva detenció, el Responsable de Sistema i els Administradors de Seguretat del Sistema han de monitoritzar l'operació de manera contínua per detectar anomalies als nivells de prestació dels serveis i actuar a conseqüència, segons el que estableix l'article 9 de l'ENS.

La monitorització és especialment rellevant quan s'estableixen línies de defensa, pràctica requerida per les normatives de referència i l'article 8 de l'ENS. S'establiran mecanismes de detecció, anàlisi i reporti que arribin als responsables regularment i quan es produeixi una desviació significativa dels paràmetres que s'hagin preestablert com a normals.

### 12.3 Resposta.

L'equip de resposta davant d'incidents ha de:

- Establir mecanismes per respondre eficaçment als incidents de seguretat.
- Designar 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), autoritats competents i, si escau, als afectats. Aquest precepte està recollit explícitament a l'ENS i al RGPD (en aquest darrer cas, quan l'incident afecti dades de caràcter personal).

## 12.4 Recuperació.

Per garantir la disponibilitat dels serveis i les informacions corporatives, el CAT desenvolupa i manté iniciatives de continuïtat dels sistemes d'informació com a part del pla general de continuïtat de servei, així com activitats de recuperació en cas de caiguda total o parcial, afectant tant l'ENS com els preceptes de disponibilitat i resiliència de RGPD-LOPDGDD.

Aquestes iniciatives de continuïtat seran desenvolupades tenint en compte la categorització dels sistemes d'informació corporatius, segons el que preceptua l'Annex I – Categoria dels sistemes, de l'ENS, i aplicar les mesures corresponents del seu Annex II.

## 12.5 Aprenentatge.

Els incidents seran analitzats per determinar-ne la causa arrel, les actuacions desenvolupades en la seva resolució i recuperació i s'extrauran les conclusions apropiades per prevenir-ne la recurrència.

# 13 Gestió del personal.

## 13.1 Obligacions del personal.

El personal del CAT té l'obligació de conèixer i complir aquesta Política General de Seguretat de la Informació i les Normatives i Procediments de Seguretat, i és responsabilitat del Comitè de Seguretat Integral disposar els mitjans necessaris perquè la PGSI arribi a els afectats.

El personal de l'organització assistirà a sessions de formació o conscienciació en matèria de seguretat de la informació almenys un cop l'any, o quan es facin canvis significatius en mitjans i/o mètodes relacionats. S'establirà un programa de formació/conscienciació contínua per atendre el personal, en particular en els casos de nova incorporació.

El compliment de la present Política de Seguretat és obligatori per part de tot el personal intern o extern que intervingui en els processos de l'Organització, constituint-ne l'incompliment una infracció als efectes de possibles procediments sancionadors, la qual serà qualificada en funció del grau d'incompliment i l'impacte que aquest hagi generat sobre els serveis corporatius.

Així mateix, i sense perjudici del procediment sancionador, l'Organització denunciarà davant de les autoritats competents les accions que puguin ser constitutives de qualsevol tipus de presumpte delictes.

## 13.2 Caracterització del lloc de treball.

El CAT inclourà en la descripció de llocs de treball els perfils, titulacions, acreditacions i experiència requerits per a aquells llocs dedicats a tasques relacionades amb la Seguretat de la Informació. Els processos de selecció tindran en compte aquesta caracterització.

El CAT inclourà en la descripció de llocs de treball les funcions i les responsabilitats en matèria de seguretat de cadascun d'aquests llocs.

## 13.3 Formació.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes d'informació rebran formació per al maneig segur dels sistemes en la mesura que la necessitin per realitzar la seva tasca. L'assistència a les sessions de formació és obligatòria i el seu aprofitament podrà ser avaluat.

El CAT elaborarà anualment un Pla de Formació, sobre el qual es farà un seguiment detallat, registrant totes les persones assistents als cicles formatius.

### 13.4 Conscienciació.

El CAT realitzarà activitats periòdiques de conscienciació cap al personal, implementant mecanismes de comunicació de regles de seguretat, canvis normatius, incidents, resolucions d'Autoritats i, en general, tota informació rellevant per millorar la consciència del personal quant a seguretat de la informació i el compliment dels marcs normatius aplicables.

## 14 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 respectius Comitès de Seguretat de la Informació o òrgans equivalents, i s'establiran procediments de actuació per a la reacció davant d'incidents de seguretat.

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

La contractació de serveis de tercers parts inclourà, en la mesura del possible, l'establiment d'acords de nivell de servei, els quals hauran de ser controlats per part de les persones responsables dels serveis esmentats i, si escau, entaular les reclamacions pertinents a cas d'incompliment, esdeveniments que hauran de ser comunicats al Responsable de Seguretat en cas d'afectar la disponibilitat, confidencialitat, integritat, autenticitat o traçabilitat dels serveis i/o informacions del CAT, i el Delegat de Protecció de Dades quan es veiessin afectades dades de caràcter personal.

Les entitats tercers s'han de seleccionar atenent els principis d'idoneïtat i compliment dels marcs normatius exigibles, a més de la resta de criteris aplicables a la seva contractació.

S'establiran procediments específics de reporti 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.

En cas que algun aspecte de la Política no pugui ser satisfet per una tercera part, segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que necessiti els riscos en què s'incorre i la manera de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables departamentals afectats abans de seguir endavant amb la contractació.

En cas que els tractaments desenvolupats per tercers parts involucrin dades de caràcter personal, es realitzaran totes les actuacions requerides pel RGPD i LOPDGDD. En aquest darrer cas, s'avaluarà la idoneïtat dels proveïdors, tal com requereix el RGPD, i se signaran els corresponents contractes de "encarregat de tractament" o "corresponsabilitat" amb tot proveïdor que desenvolupi les seves tasques tractant dades personals o "compromisos de confidencialitat" i seguretat de la informació" quan els tractaments de dades personals siguin incidentals.

## 15 Revisió i aprovació de la Política de Seguretat

La Política General de Seguretat de la Informació serà revisada pel Comitè de Seguretat Integral 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.

Qualsevol canvi sobre la Política de Seguretat de la Informació haurà de ser difós a totes les parts afectades i, si escau, objecte de reciclatge en la formació per al personal afectat.

## 16 Documentació complementària.

La Política de Seguretat de la Informació es completarà amb documents més detallats que ajuden a materialitzar els seus preceptes. Per això s'utilitzaran:

### 16.1 Normatives de seguretat.

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

### 16.2 Procediments de seguretat.

Els procediments de seguretat detallen tasques concretes, indicant-ne clarament la seva operativa.

### 16.3 Instruccions de seguretat.

Les instruccions de seguretat desenvolupen l'operativa descrita en els procediments, explicant-ne a nivell tècnic la implementació.