Contingut

1.- INTRODUCCIÓ

1.1.- JUSTIFICACIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

El Col·legi Oficial d'Ambientòlegs de Catalunya (en endavant COAMB) depèn dels sistemes TIC (Tecnologies d'Informació i Comunicacions) per assolir els 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 prestesa als incidents.

Els sistemes TIC han d'estar protegits contra amenaces de ràpida evolució amb potencial per incidir en la confidencialitat, la integritat, la disponibilitat, l'ús previst i el valor de la informació i els serveis. Per defensar-se d'aquestes amenaces, cal una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació continuada dels serveis. És per això que l'Esquema Nacional de Seguretat (Reial Decret 311/2022, de 3 de maig, ENS en endavant), a l'article 2 estableix que "..... s'obliga a disposar amb la polític de seguretat a que es refereix l'article 12, quan, d'acord amb la normativa aplicable i en virtut d'una relació contractual, prestin serveis o proveeixin solucions a les entitats del sector públic per l'exercici per aquestes de les seves competències i potestats administratives..... La política de seguretat a que es fa referència a l'article 12 serà aprovada en el cas d'aquestes entitats per l'òrgan que ostenti les màximes competències executives...".

Això implica que les diferents àrees i/o departaments del Col·legi han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat, així com fer un seguiment continu dels nivells de prestació de serveis, seguir i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per 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. Els departaments han d'estar preparats per prevenir, detectar, reaccionar i recuperar-se d'incidents, segons l'article 8 de l'ENS.

1.2.- MISSIÓ I SERVEIS PRESTATS

El COAMB, per a la gestió dels seus interessos, i en l'àmbit de les competències, serveix amb objectivitat els interessos generals i actua d'acord amb els principis d'eficàcia, jerarquia, descentralització i coordinació, promou tota classe d'activitats i presta els serveis públics que contribueixen a satisfer les necessitats i les aspiracions dels habitants de la comunitat.

Aquesta Política de Seguretat aplica a les diferents activitats en què participa l'Entitat a través de mitjans electrònics, en concret:

1. Les relacions de caràcter juridicoeconòmic entre els ciutadans i l'Entitat.
2. La consulta per part dels ciutadans de la informació pública administrativa i de les dades administratives que estiguin a poder de l'Entitat.
3. La realització dels tràmits i procediments administratius incorporats per a la seva tramitació a la Seu Electrònica de l'Entitat, de conformitat amb el que preveu la normativa reguladora sobre l'ús de l'Administració Electrònica.
4. El tractament de la informació obtinguda per l'Entitat en l'exercici de les seves potestats.

2.- 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 Pública pel que fa a administració electrònica, i que implica la implantació de forma explícita de mesures de seguretat sistemes d'informació. El marc legal en matèria de seguretat de la informació ve establert per la següent legislació:

1. 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 la integritat, autenticitat, confidencialitat, qualitat, protecció i conservació dels documents emmagatzemats; i, estableix també, a l'art. 27.3 que les administracions públiques han de complir 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, mitjançant la Disposició Derogatòria Única, deroga la Llei 11/2007, del 22 de juny, d'accés electrònic dels ciutadans als serveis públics.

2. El Reial Decret 311/2022, de 3 de maig, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, fixa els principis bàsics i els requisits mínims, així com les mesures de protecció a implantar en els sistemes de les entitats del seu àmbit d'aplicació.

3. 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 l'adequat nivell d'interoperabilitat tècnica, semàntica i organitzativa dels sistemes i les 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.

4. Reglament (UE) 2016/679, del Parlament Europeu i del Consell, de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades (d'ara endavant RGPD).

5. Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals.

3.- ORGANITZACIÓ DE LA SEGURETAT

3.1 DEFINICIÓ DE ROLS

Tal com indica l'article 13 de l'ENS, La seguretat haurà d'implicar tots els membres de l'organització. La Política de Seguretat, tal i com indica l'article 13.2 i com detalla l'Annex II de l'ENS a la secció 3.1, ha d'identificar uns clars responsables per vetllar pel seu compliment i ser coneguda per tots els membres de l'organització administrativa.

S'estableixen els rols següents a l'organització relacionats amb la Seguretat de la Informació:

A. RESPONSABLE DE LA INFORMACIÓ

S'ha designat responsable de la Informació a la persona **Gerent o Junta de Govern** del COAMB, a qui corresponen les funcions següents:

1. 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.
2. Té la responsabilitat última de l'ús que es faci duna certa informació i, per tant, de la seva protecció.
3. El Responsable de la Informació és el responsable últim de qualsevol error o negligència que porti a un incident de confidencialitat o integritat.
4. 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.
5. Determinarà els nivells de seguretat en cada dimensió dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.
6. 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 (executor directe del servei).

B. RESPONSABLE DEL SERVEI

S'ha designat responsables del Servei a **cadascun dels responsables d'unitats funcionals**, als quals corresponen les funcions següents:

1. Pel que fa al RGPD, per delegació del Responsable del tractament s'encomana al Responsable del Servei el desenvolupament de les tasques relacionades amb la gestió dels tractaments de dades personals que es realitzen a la seva àrea en concret.
2. 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.
3. Té la responsabilitat última de l'ús que es faci de determinats serveis i, per tant, de la protecció.
4. El Responsable del Servei és el responsable últim de qualsevol error o negligència que porti a un incident de disponibilitat dels serveis.
5. Determinarà els nivells de seguretat en cada dimensió del servei dins del marc establert a l'Annex I de l'Esquema Nacional de Seguretat.
6. 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.
7. La prestació d'un servei sempre ha d'atendre els requisits de seguretat de la informació que maneja, de manera que es poden heretar els requisits de seguretat d'aquesta, afegint-hi requisits de disponibilitat, així com altres com accessibilitat, interoperabilitat, etc.

Responsables dels serveis:

1. **Secretaria: Secretari del Col·legi Oficial.**
2. **Col·legiacions: Secretari del Col·legi Oficial.**
3. **Cultura i Formació: Vocal de cultura del Col·legi Oficial.**
4. **Delegacions: Vocal de les Delegacions del Col·legi Oficial.**
5. **Comissió Deontològica i Defensa de la professió: President Comitè Ètic del Col·legi Oficial.**
6. **Concursos: Vocal de cultura del Col·legi Oficial.**
7. **Comptabilitat: Tresorer del Col·legi Oficial.**

8. **Visats: Secretari del Col·legi Oficial.**

C.- RESPONSABLE DE SEGURETAT DE LA INFORMACIÓ

S'ha designat com a Responsable de Seguretat de la Informació al DPO, a qui correspondran les funcions següents:

1. 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.
2. Reportarà directament el Comitè de Seguretat de la Informació.
3. Actuarà com a secretari del Comitè de Seguretat de la Informació.
4. Convocarà el Comitè de Seguretat de la Informació, recopilant la informació pertinent.
5. Mantindrà la seguretat de la informació manejada 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.
6. Promourà la formació i conscienciació en matèria de seguretat de la informació dins del seu àmbit de responsabilitat.
7. Recopila els requisits de seguretat dels Responsables d'Informació i Servei i determina la categoria del Sistema.
8. Realitzarà l'Anàlisi de Riscos.
9. 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.
10. 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.
11. Coordinarà l'elaboració de la documentació de seguretat del sistema.
12. 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.

13. Participarà en l'elaboració i l'aprovació, en el marc del Comitè de Seguretat de la Informació, de la normativa de Seguretat de la Informació.
14. Elaborarà i aprovarà els procediments operatius de seguretat de la informació.
15. Facilita 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).
16. 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.
17. 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.
18. 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.
19. 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 secretari/ària del Comitè de Seguretat de la Informació li correspon:

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

3.2.- COMITÈ DE SEGURETAT DE LA INFORMACIÓ

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

PRESIDENT: Presidència.

SECRETARI: Responsable de Seguretat de la Informació.

VOCALS:

- Vocal 1. Secretari del Col·legi Oficial

- Vocal 2. Vocal de Cultura del Col·legi Oficial

- Vocal 3. Vocal de Territorials del Col·legi Oficial

- Vocal 4. Tresorer del Col·legi Oficial

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

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

1. Atendre les inquietuds de l'alta Direcció i dels diferents departaments.
2. Informar regularment de l'estat de seguretat de la informació a l'Alta Direcció.
3. Promoure la millora contínua del sistema de gestió de la seguretat de la informació.
4. Elaborar l'estratègia d'evolució de l'entitat pel que fa a la seguretat de la informació.
5. 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.
6. Elaborar (i revisar regularment) la Política de Seguretat de la informació perquè sigui aprovada per la Direcció.
7. Aprovar la normativa de seguretat 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 principals riscos residuals assumits per l'Entitat i recomanar-ne possibles actuacions.
10. Monitoritzar l'exercici dels processos de gestió d'incidents de seguretat i recomanar-ne possibles actuacions. En particular, vetllar per la coordinació de

les diferents àrees de seguretat en la gestió d'incidents de seguretat de la informació.

11. Promoure la realització de les auditories, i/o controls, periòdiques que permetin verificar el compliment de les obligacions de l'organisme en matèria de seguretat.
12. Aprovar plans de millora de la seguretat de la informació de l'entitat. En particular, vetllarà per la coordinació de diferents plans que es puguin fer en diferents àrees.
13. 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.
14. 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.
15. Demanar regularment del personal tècnic propi o extern, la informació pertinent per prendre decisions.
16. 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 altre tipus d'entorns formatius o d'intercanvi d'experiències.

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

1. Aprovarà el Pla de millora de la seguretat, amb la dotació pressupostària corresponent.
2. Assignarà els rols i funcions que corresponguin segons l'esmentat Pla.

3.3.- 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: el Comitè de Seguretat de la Informació dóna instruccions al Responsable de la Seguretat de la Informació que s'encarrega d'executar, supervisant que administradors i operadors implementen les mesures de seguretat segons el que estableix la política de seguretat aprovada per a l'Organització.

- El **Responsable de la Seguretat** del Sistema:

a) reporta al Responsable del Sistema corresponent:

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

b) 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.

c) informa el 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.

d) reporta al Comitè de Seguretat de la Informació, com a secretari:

   1. Resum consolidat d'actuacions en matèria de seguretat.
   2. Resum consolidat d'incidents relatius a la seguretat de la informació.
   3. Estat de la seguretat del sistema, en particular del risc residual a què el sistema està exposat.
   4. Quan, circumstancialment, no s'hagi constituït el Comitè de Seguretat de la Informació, el Responsable de la Seguretat reporta directament a la Direcció de l'Organització.

e) informa la Direcció de l'Organització, segons allò acordat al Comitè de Seguretat de la Informació.

- El **Responsable del Sistema** informa de les incidències funcionals relatives a la informació que li competeix:

a) al Responsable de la Informació
b) al Responsable del Servei
c) reporta al Responsable de la Seguretat:

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

3.4.- PROCEDIMENTS DE DESIGNACIÓ DE PERSONES

La Direcció de l'Entitat nomenarà formalment en plenari, decret o acord de la Junta de Govern:

1. Al Responsable de la Informació; pot ser un càrrec unipersonal o un òrgan col·legiat.
2. Als Responsables del Servei; pot ser el mateix que el Responsable de la Informació; pot ser un càrrec unipersonal.
3. 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.
4. Als membres que formaran part del Comitè de Seguretat de la Informació, que serà un òrgan col·legiat que prendrà les decisions per majoria simple –amb vot qualificat de la Presidència del Comitè en cas d'empat- i que haurà de reunir-se com a mínim sempre que hi hagi una greu crisi de seguretat a l'Entitat i, com a mínim, un cop semestralment.

En el cas del **COAMB, s'ometen les figures de Responsable del Sistema i d'Administrador del Sistema, degut a la mida de l'organització**. Per això, aquestes figures queden **reemplaçades pel Responsable de Seguretat**, i les seves funcions, assumides pel mateix.

4.- 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 les Avaluacions d'Impacte i/o Anàlisis de Riscos, realitzades sobre els tractaments. 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.

4.1.- FIGURES VINCULADES A PROTECCIÓ DE DADES DE CARÀCTER PERSONAL

4.1.1 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 aquests efectes s'ha atribuït la condició de responsable de tractament a la persona jurídico-pública, és a dir, al mateix COAMB. De manera que, s'ha entès que el Col·legi és Responsable del Tractament de les dades de caràcter personal, que es troben als 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 Col·legi, en qualitat del càrrec o lloc (com per exemple, la persona Gerent, Presidenta o Secretària).

Les funcions del Responsable del tractament són:

1. Adoptar les mesures d'índole tècnica i organitzatives necessàries que garanteixin la seguretat de les dades de caràcter personal i evitin la seva alteració, pèrdua, tractament o accés no autoritzat.
2. Haurà d'informar als titulars de les dades els drets que els assisteixen i en els termes en que els poden exercir.

3. Haurà d'excloure del tractament les dades relatives a l'afectat que s'oposi al tractament, sempre i quan no hi hagi cap altra base de legitimació que obligui a la seva conservació i/o tractament.
4. Haurà de cessar en la utilització o cessió il·lícita de les dades quan així ho requereixi l'interessat.
5. Obligació de fer efectiu el dret de rectificació o supressió de l'interessat en el termini màxim d'un mes des de que hagi acreditat tal circumstància.
6. Notificar les rectificacions o supressió 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 supressió.

4.1.2 FUNCIONS I OBLIGACIONS DEL DELEGAT DE PROTECCIÓ DE DADES

El DPO pot ser una persona física o un òrgan col·legiat, intern o extern, 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 en on desenvolupa les seves funcions.

El COAMB ha nomenat com a Delegat de Protecció de Dades extern al professional **IVAN DE SAN NICOLÀS I CASTEJÓN** (rgpd@coamb.cat).

El delegat de protecció de dades tindrà com a mínim les funcions següents:

1. 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 de la normativa vigent en protecció de dades de la Unió Europea o dels Estats membres;
2. supervisar el compliment del que disposa la normativa en protecció de dades de la Unió Europea o dels Estats membres i de les polítiques del responsable o de l'encarregat del tractament en matèria de protecció de dades personals, inclosa l'assignació de responsabilitats , la conscienciació i formació del personal que participa en les operacions de tractament, i col·laborar a les auditories corresponents;
3. 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;

4. cooperar amb l'autoritat de control;
5. 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 realitzar consultes, si escau, sobre qualsevol altre assumpte.

El delegat de protecció de dades exerceix 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 els fins del tractament.

Per això haurà de ser capaç de:

1. Recollir informació per determinar les activitats de tractament,
2. analitzar i comprovar la conformitat de les activitats de tractament, i
3. informar, assessorar i emetre recomanacions al responsable o encarregat del tractament.
4. Recollir informació per supervisar el registre de les operacions de tractament.
5. Assessorar en l'aplicació del principi de la protecció de dades per disseny i per defecte.
6. Assessorar sobre:
    - Si heu de dur a terme o no una avaluació d'impacte de la protecció de dades
    - Quina metodologia s'ha de seguir en fer una avaluació d'impacte de la protecció de dades.
    - Si heu de dur a terme l'avaluació d'impacte de la protecció de dades amb recursos propis o amb contractació externa.
    - Quines salvaguardes (incloses mesures tècniques i organitzatives) aplicar per mitigar qualsevol risc per als drets d'interessos dels afectats.
    - Si heu dut a terme correctament o no l'avaluació d'impacte de la protecció de dades i
    - Si les vostres conclusions (si seguir endavant o no amb el tractament i quines salvaguardes aplicar) són conformes al Reglament.
7. Prioritzar les seves activitats i centrar els seus esforços en aquelles qüestions que presentin més riscos relacionats amb la protecció de dades.

8. Assessorar el responsable del tractament sobre:
    - Quina metodologia emprar 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 DPO 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 DPO es poden concretar en tasques d'assessorament i supervisió, entre d'altres, a les àrees següents:

1. Compliment de principis relatius al tractament, com ara els de limitació de finalitat, minimització o exactitud de les dades.
2. Identificació de les bases jurídiques dels tractaments.
3. Valoració de compatibilitat de finalitats diferents de les que van originar la recollida inicial de les dades.
4. 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.
5. Disseny i implantació de mesures d'informació als afectats pels tractaments de dades.
6. Establiment de mecanismes de recepció i gestió de les sol·licituds d'exercici de drets per part dels interessats.
7. Valoració de les sol·licituds d'exercici de drets per part dels interessats.
8. Contractació d'encarregats de tractament, inclòs el contingut dels contractes o actes jurídics que regulin la relació responsable-encarregat.

9. 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.
10. Disseny i implantació de polítiques de protecció de dades.
11. Auditoria de protecció de dades.
12. Establiment i gestió dels registres d'activitats de tractament.
13. Anàlisi de riscos dels tractaments realitzats.
14. Implantació de les mesures de protecció de dades des del disseny i protecció de dades per defecte adequades als riscos i naturalesa dels tractaments.
15. Implantació de les mesures de seguretat adequades als riscos i naturalesa dels tractaments.
16. 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.
17. Determinació de la necessitat de fer avaluacions d'impacte sobre la protecció de dades.
18. Realització d'avaluacions d'impacte sobre la protecció de dades
19. Relacions amb les autoritats de supervisió
20. Implantació de programes de formació i sensibilització del personal en matèria de protecció de dades.

4.1.3 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:

1. No es permet la difusió de dades de caràcter personal ni confidencial pertanyent a l'entitat. Estan obligats a guardar secret de la informació fins i tot acabada la relació laboral.

2. 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.
3. L'usuari es responsabilitzarà de tots els accessos que es facin sota el seu identificador i contrasenya, per tant, no haurà de revelar la contrasenya.
4. L'usuari es responsabilitzarà sempre que abandoni el lloc de treball de tancar la seva sessió o bloquejar l'equip amb contrasenya.
5. No es podran instal·lar aplicacions als sistemes de l'entitat sense el consentiment del delegat de protecció de dades.
6. No es permet la còpia de dades de caràcter personal, en suports, sense l'autorització expressa del delegat de protecció de dades.
7. A l'usuari se li responsabilitzarà del desament de còpies de qualsevol correu que inclogui annexos amb dades personals vinculades a l'entitat.

4.1.4 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 haurà 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:

1. Tractar les dades del tractament.
2. Realitzar el control de tractament, qualitat i seguretat de les dades.

3. Controlar la forma i els requisits per procedir a les addicions i cancel·lacions.
4. Controlar els suports de seguretat.
5. Control i accés de contrasenyes.
6. Manteniment del registre d'incidències.
7. Crear una llista per a les situacions en què un afectat no vulgui que les dades personals s'emmagatzemin en el tractament.
8. Traslladar al responsable del tractament d'aquelles sol·licituds d'exercici de dret que rebin els interessats.

En conseqüència, **el Col·legi haurà de dur a terme un document actualitzat on s'identificaran els encarregats de tractament que estan prestant serveis a l'Entitat, així com la indicació de la formalització del contracte pertinent amb aquests prestadors de serveis amb accés a dades**.

5.- GESTIÓ DE RISCOS

5.1.- 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.

5.2.- CRITERIS D'AVALUACIÓ I 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 manejats 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 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.

5.3.- 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.

5.4.- 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 (incloent-hi la implantació de les **mesures de seguretat previstes a l'annex II de l'ENS**) hauran de ser acceptats prèviament pel seu responsable d'aquesta informació.

Els nivells de Risc residuals esperats sobre **cada servei** 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 seu 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 sigui procedent, si escau, a avaluar, aprovar o rectificar les opcions de tractament proposades.

5.5.- NECESSITAT DE REALITZAR 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 10 de l'ENS. Aquesta anàlisi es repetirà:

1. Regularment almenys **una vegada a l'any**.

2. Quan es produeixin canvis significatius a la informació manejada.
3. Quan es produeixin canvis significatius als serveis prestats.
4. Quan es produeixin canvis significatius en els sistemes que tracten la informació i intervenen en la prestació dels serveis.
5. Quan es produeixi un incident greu de seguretat.
6. Quan es reportin vulnerabilitats greus.

6.- GESTIÓ D'INCIDENTS DE SEGURETAT

6.1.- 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. L'ENS a través del seu article 20 estableix que els sistemes s'han de dissenyar i configurar de manera que atorguin el **mínim privilegi necessari**. De la mateixa manera, l'article 18 de l'ENS esmentat defineix que els **sistemes s'instal·laran en àrees separades**, dotades d'un procediment de control d'accés.

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:

1. Establir àrees segures per als sistemes d'informació crítica o confidencial.
2. Autoritzar els sistemes abans d'entrar en operació.
3. Avaluar regularment la seguretat, incloent-hi avaluacions dels canvis de configuració realitzats de forma rutinària.
4. Sol·licitar la revisió periòdica per part de tercers per obtenir una avaluació independent.

6.2.- MONITORITZACIÓ I DETECCIÓ D'INCIDENTS

Atès que els serveis es poden degradar ràpidament a causa d'incidents, que van des d'una simple desacceleració 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 els articles 9 i 10 de l'ENS. S'establiran **mecanismes de detecció, anàlisi i report** 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.

6.3.- RESPOSTA DAVANT INCIDENTS

Els departaments han de:

1. Establir mecanismes per respondre eficaçment als incidents de seguretat.
2. Designar punt de contacte per a les comunicacions pel que fa a incidents detectats en altres departaments o altres organismes.
3. 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).

6.4.- RECUPERACIÓ DAVANT 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.

7.- 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 rebran 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 primera assignació o si es tracta d'un canvi de lloc de treball o de responsabilitats en aquest.

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.

8.- 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 a que es pugui 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. Aquest tercer queda subjecte a les obligacions establertes en aquesta normativa, i pot desenvolupar els seus propis procediments operatius per satisfer-la.

S'establiran procediments específics per reportar i resoldre 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 un tercer segons es requereix als paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que

determini 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.

9.- REVISIÓ I APROVACIÓ DE LA POLÍTICA 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, essent vàlid la seva publicació a l'entorn digital.

10.- DOCUMENTACIÓ COMPLEMENTÀRIA

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

1. Normes de seguretat (*security standards*).
2. Guies de seguretat (*security guides*).
3. 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. 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. GLOSSARI DE TERMES

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

Ciutadà/-ana: Qualssevol persones físiques, persones jurídiques i ens sense personalitat que es relacionin, o siguin susceptibles de relacionar-se, amb les administracions i/o entitats del sector públic.

Dades de caràcter personal: Qualsevol informació que es refereix a 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 d'acompliment 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 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 d'una 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, és a dir, la persona sobre la que recau la prestació/execució directa del servei.

Servei: Funció o prestació exercida per alguna entitat oficial, pública o semipública 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.