



Col·legi Oficial de
Psicologia de Catalunya

Política de seguretat de la informació

Nom del document			
Control de versions	Versió No.	Data	Responsable revisió
Esborrany	0.1	03/11/24	Sergi Gómez
Primera versió	1.0	03/03/25	Sergi Gómez
Autor	Sergi Gómez Figueroba - Responsable Departament Tecnologies de la Informació (TIC) i Responsable de Seguretat		
Responsable del document	Sergi Gómez Figueroba - Responsable Departament Tecnologies de la Informació (TIC)		
Distribució	Difusió pública		
Data d' aprovació de l'última versió per part de la Junta de Govern del COPC	19 de març de 2025		
Signatura de la Secretaria de la Junta de Govern del COPC	Teresa Moratalla		
Data de la propera revisió	18 de març de 2027		

Índex

1. Introducció.....	4
2. Abast.....	5
3. Rols i responsabilitats de la seguretat de la informació	5
3.1 Comitè de Seguretat de la Informació	6
3.2. Responsable de Seguretat.....	7
3.3. Responsables dels Serveis i Responsables de la Informació	8
3.4. Responsable del Sistema.....	8
3.5. Delegat de Protecció de Dades.....	9
3.6. Departament de les Tecnologies i la Informació	10
4. Missió del COPC.....	10
5. Principis bàsics	11
6. Objectius de la seguretat de la informació	12
7. Marc legislatiu i regulatori	12
8. Dades de caràcter personal	13
9. Obligacions i conscienciació del personal	13
10. Gestió de riscos.....	13
11. Notificació d'incidents	14
12. Organització de la documentació de seguretat.....	14
13. Terceres parts	15
14. Millora contínua.....	15
15. Compliment de les polítiques	16
16. Vigència, revisió i comunicació	16

1. Introducció

El Col·legi Oficial de Psicologia de Catalunya (en endavant, COPC) necessita dels sistemes TIC (Tecnologies de la Informació i les Telecomunicacions) per assolir els seus objectius. Aquests sistemes han de ser administrats amb diligència, prenent les mesures adequades per protegir-los davant de danys accidentals o deliberats que puguin afectar la confidencialitat, integritat, disponibilitat, traçabilitat i autenticitat de la informació tractada i els serveis prestats.

Per fer front a aquestes amenaces, es requereix una estratègia que s'adapti als canvis en les condicions de l'entorn per garantir la prestació contínua dels serveis. Això implica que els departaments han d'aplicar les mesures mínimes de seguretat exigides per l'Esquema Nacional de Seguretat (ENS), així com realitzar un seguiment continu dels nivells de prestació dels serveis, monitoritzar i analitzar les vulnerabilitats reportades, i preparar una resposta efectiva als incidents per garantir la continuïtat dels serveis prestats.

És per això que la Junta de Govern del COPC elabora i aprova aquesta Política d'alt nivell, amb un enfoc estratègic, per definir les bases i marcar les directrius per protegir la informació que gestiona el COPC i la continuïtat dels serveis oferts, creant una cultura de seguretat de la informació i garantint la implicació i responsabilitat de tothom en la protecció de la informació que es gestiona.

Totes les àrees i el personal del COPC tenen present que la seguretat de la informació és una part integral de cada etapa del cicle de vida del sistema, des de la seva concepció fins a la seva retirada de servei, passant per les decisions de desenvolupament o adquisició, les activitats d'explotació, la planificació d'ofertes i la gestió de projectes.

Prevenició

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

Per a garantir el compliment de la política, el COPC:

- Autoritza els sistemes abans d'entrar en operació
- Avalua regularment la seguretat, incloent-hi l'anàlisi dels canvis de configuració realitzats de manera rutinària
- Sol·licita la revisió periòdica per part de tercers, amb la finalitat d'obtenir una avaluació independent

Detecció

El COPC estableix controls d'operació dels seus sistemes d'informació amb l'objectiu de detectar anomalies en la prestació dels serveis i actuar en conseqüència segons el que es disposa en

l'article 10 de l'ENS (vigilància contínua i reavaluació periòdica). Quan es produeix una desviació significativa dels paràmetres que s'hagin preestablert com a normals (conforme a l'indicat en l'article 9 de l'ENS, Existència de línies de defensa), s'establiran els mecanismes de detecció, anàlisi i report necessaris perquè arribin als responsables regularment.

Resposta

El COPC ha establert les següents mesures:

- Mecanismes per a respondre eficaçment als incidents de seguretat
- Designar un punt de contacte per a les comunicacions respecte a incidents detectats en altres departaments o en altres organismes
- Establir protocols per a l'intercanvi d'informació relacionada amb l'incident. Això inclou comunicacions, en tots dos sentits, amb els organismes necessaris i les parts interessades interns i externs, com ara autoritats competents, afectats pels incidents, proveïdors de serveis i altres entitats que puguin ser rellevants per a la resolució o mitigació dels impactes.

Recuperació

Per a garantir la disponibilitat dels serveis, el COPC disposa dels mitjans i tècniques necessàries que permeten garantir la recuperació dels serveis més crítics.

2. Abast

L'abast d'aquesta Política inclou tots els components, actius i serveis dels sistemes que siguin propietat, llogats, operats, administrats, mantinguts i controlats per o per un tercer en nom del COPC. També s'aplica a qualsevol component, tant intern com extern, que interactui amb aquests sistemes.

Aquesta Política i els procediments associats són d'obligat compliment per a tots els integrants de COPC: membres d'òrgans de govern, directius, empleats, col·laboradors, becaris, voluntaris, treballadors d'ETT, i, en resum, qualsevol persona vinculada per relació laboral o acords i contractes, així com als seus socis de negoci en totes aquelles activitats que poden comportar riscos relacionats amb la present Política de Seguretat.

3. Rols i responsabilitats de la seguretat de la informació

El COPC, en el marc de l'ENS, ha designat diferents rols i òrgans de la Seguretat de la Informació, associant diferents responsabilitats.

La creació del Comitè de Seguretat de la Informació, el nomenament dels seus integrants i la designació dels Responsables identificats en aquest apartat, és realitzat per la Junta de Govern. El nomenament es revisarà cada dos anys o quan el lloc quedi vacant.

3.1 Comitè de Seguretat de la Informació

El Comitè de Seguretat està format pels següents rols:

- Membres permanents:
 - Secretari/ària del Comitè de Seguretat:
 - Responsable de Sistema
 - Responsable de Seguretat
 - Representants d'Informació i Serveis
 - Assessors que es considerin oportuns per als temes en qüestió
 - El Delegat de Protecció de dades
 - Gerència
 - Direcció
- Membres no permanents:
 - El Comitè de Seguretat podrà invocar la presència en les seves reunions tant d'altres representants del COPC com d'especialistes externs, per raó de la seva experiència o vinculació amb els assumptes tractats, sigui necessària o aconsellable.

Els Representants de la Informació i els Serveis seran convocats per la presidència en funció dels temes a tractar, en representació dels distints àmbits o àrees de seguretat TIC del COPC. Cada àrea estarà representada per un vocal amb vot, sense perjudici que acudeixin diversos representants d'aquesta.

El Delegat de Protecció de Dades participarà amb veu, però sense vot en les reunions del Comitè de Seguretat quan en el mateix vagin a abordar-se qüestions relacionades amb el tractament de dades de caràcter personal, així com sempre que se'n requereixi la seva participació. En tot cas, si un assumpte es sotmetés a votació, es farà constar sempre en acta l'opinió del Delegat de Protecció de Dades.

El Secretari/ària del Comitè realitzarà les convocatòries i aixecarà actes de les reunions del Comitè de Seguretat. A les sessions del Comitè de Seguretat podran assistir en qualitat d'assessors les persones que en cada cas estimi pertinents la Presidència.

Atribucions del Comitè

Les funcions del Comitè són:

- Estar permanentment informat de la normativa que regula la Certificació de Conformitat amb l'ENS, incloent-hi les seves normes d'acreditació, certificació, guies, manuals, procediments i instruccions tècniques.
- Estar permanentment informat de la relació d'Entitats de Certificació acreditades i organitzacions, públiques i privades, certificades.
- Proposar directrius i recomanacions, que seran recollides en les corresponents actes de les reunions del Comitè, a les quals el seu president, haurà de donar resposta.
- Coordinar els esforços de les diferents àrees en matèria de seguretat de la informació, per a assegurar que aquests siguin consistents, alineats amb l'estratègia decidida en la matèria, i evitar duplicitats.



- Atendre les inquietuds, en matèria de Seguretat de la Informació, de les diferents àrees, informant regularment de l'estat de la seguretat de la informació a la Direcció.
- Resoldre els conflictes de responsabilitat que puguin aparèixer entre els diferents responsables i/o entre diferents Departaments, elevant aquells casos en els quals no tingui suficient autoritat per a decidir.
- Assessorar en matèria de seguretat de la informació, sempre que li sigui requerit.
- Revisar la Política de Seguretat de la Informació pel Comitè de Seguretat prèvia aprovació per la Junta de Govern.
- Aprovar la Norma interna de bon ús dels sistemes per a tot el personal.
- Aprovar el marc normatiu amb la llista de Normativa i Procediments de seguretat

Periodicitat de les reunions i adopció d'acords

El Comitè de Seguretat es reunirà, almenys, dues vegades a l'any amb caràcter semestral, sense perjudici que, en atenció a les necessitats derivades del compliment dels seus fins i atribucions, requereixi una major freqüència en les reunions.

En qualsevol cas, les reunions es convocaran a través del Secretari, a la seva iniciativa o per majoria dels seus membres permanents.

Les decisions s'adoptaran per consens dels membres permanents.

3.2. Responsable de Seguretat

Les seves funcions són:

- Mantenir i verificar el nivell adequat de seguretat de la Informació tractada manejada i dels Serveis electrònics prestats pels sistemes d'informació.
- Elaborar programes de formació destinats a formar i sensibilitzar al personal en matèria de seguretat de la informació i protecció de dades.
- Promoure la formació i conscienciació en matèria de seguretat de la informació.
- Designar responsables de l'execució de l'anàlisi de riscos, de la Declaració d'Aplicabilitat, identificar mesures de seguretat, determinar configuracions necessàries, elaborar documentació del sistema.
- Realitzar un seguiment dels principals riscos residuals assumits i recomanar possibles actuacions respecte d'ells.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable del Sistema i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i, arribat el cas, en els plans de continuïtat, procedint a la seva validació.
- Gestionar les revisions externes o internes del sistema.
- Gestionar els processos de certificació.
- Elevar al Comitè de Seguretat l'aprovació de canvis i altres requisits del sistema.

- Elaborar (i revisar regularment) la Política de Seguretat de la Informació per al seu trasllat al Comitè de Seguretat per a la seva revisió i posterior aprovació de la Junta de Govern.
- Participar en elaboració i aprovar la normativa i procediments de Seguretat de la Informació, amb coneixement del Comitè.
- Promoure la millora contínua del sistema de gestió de la Seguretat de la Informació.

3.3. Responsables dels Serveis i Responsables de la Informació

Les seves funcions són:

- Establir i elevar per a la seva aprovació al Comitè de Seguretat de la Informació els requisits de seguretat aplicables a la Informació (nivells de seguretat de la Informació) i als Serveis (nivells de seguretat dels serveis), dins del marc establert al Real Decret de l'ENS, podent recaptar una proposta al Responsable de Seguretat i tenint en compte l'opinió del Responsable del Sistema.
- Dictaminar respecte als drets d'accés a la informació i els serveis.
- Acceptar els nivells de risc residual que afecten la informació i els serveis.
- Posar en comunicació del Responsable de Seguretat qualsevol variació respecte a la Informació i els Serveis dels quals és responsable, especialment la incorporació de nous Serveis o Informació a càrrec seu, el qual donarà trasllat d'aquests canvis al Comitè de Seguretat de la Informació, en la seva pròxima reunió.

3.4. Responsable del Sistema

Les seves funcions són:

- Desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle de vida, elaborant els procediments operatius necessaris.
- Definir la topologia i la gestió del Sistema d'Informació establint els criteris d'ús i els serveis disponibles en aquest.
- Detenir l'accés a informació o prestació de servei si té el coneixement que aquests presenten deficiències greus de seguretat.
- Cerciorar-se que les mesures específiques de seguretat s'integrin adequadament dins del marc general de seguretat.
- Proporcionar assessorament per a la determinació de la Categoria del Sistema, en col·laboració amb el Responsable de Seguretat i/o Comitè de Seguretat de la Informació.
- Participar en l'elaboració i implantació dels plans de millora de la seguretat i arribat el cas en els plans de continuïtat.
- Dur a terme, si és el cas, les funcions de l'administrador de la seguretat del sistema:
 - La gestió, configuració i actualització, si és el cas, del maquinari i programari en els quals 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 l'autoritzat.
- Aprovar els canvis en la configuració vigent del Sistema d'Informació.
- Assegurar que els controls de seguretat establerts es compleixen estrictament.
- Assegurar que són aplicats els procediments aprovats per a gestionar el Sistema d'Informació.
- Supervisar les instal·lacions de maquinari i programari, les seves modificacions i millores per a assegurar que la seguretat no està compromesa i que en tot moment s'ajusten a les autoritzacions pertinents.
- Monitorar l'estat de seguretat proporcionat per les eines de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica.
- Informar el Responsable de Seguretat de qualsevol anomalia, compromís o vulnerabilitat relacionada amb la seguretat.
- Col·laborar en la recerca i resolució d'incidents de seguretat, des de la seva detecció fins a la seva resolució.

Quan la complexitat del sistema ho justifiqui, el Responsable del Sistema podrà designar els responsables de sistema delegats que consideri necessaris, que tindran dependència funcional directa d'aquell i seran responsables en el seu àmbit de totes aquelles accions que els delegui el mateix. Així mateix, també podrà delegar en altres persones funcions concretes de les responsabilitats que se li atribueixen.

3.5. Delegat de Protecció de Dades

Les seves funcions són:

- Informar i assessorar el COPC i als usuaris que s'ocupin del tractament, de les obligacions que els incumbeixen en virtut de la normativa vigent en matèria de Protecció de Dades.
- Supervisar el compliment del que es disposa en normativa de seguretat i de les polítiques internes del COPC en matèria de protecció de dades, inclosa l'assignació de responsabilitats, la conscienciació i formació del personal que participa en les operacions de tractament, i les auditories corresponents.
- Oferir l'assessorament que se li sol·liciti sobre l'avaluació d'impacte relativa a la protecció de dades i supervisarà la seva aplicació.
- Cooperar amb l'Agència Espanyola de Protecció de Dades quan aquesta ho requereixi, actuant com a punt de contacte amb aquesta per a qüestions relatives al tractament de dades.
- El Delegat de Protecció de dades exercirà les seves funcions parant esment als riscos associats a les operacions de tractament. Per a això ha de ser capaç de:
 - Recaptar informació per a determinar les activitats de tractament.
 - Analitzar i comprovar la conformitat de les activitats de tractament.
 - Informar, assessorar i emetre recomanacions al responsable o l'encarregat del tractament.



- Recaptar informació per a supervisar el registre de les operacions de tractament.
- Assessorar en el principi de la protecció de dades per disseny i per defecte.
- Assessorar sobre si es duu a terme o no les avaluacions d'impacte, metodologia, salvaguardes a aplicar, etc.
- Prioritzar activitats sobre la base dels riscos.
- Assessorar el Responsable de Tractament sobre àrees on realitzar auditories, activitats de formació a realitzar i operacions de tractament a dedicar més temps i recursos.

3.6. Departament de les Tecnologies i la Informació

El Departament de Tecnologies i Informació presta serveis de ciberseguretat, desenvolupant la capacitat de vigilància i detecció d'amenaques en l'operació diària dels sistemes TIC, alhora que millora la capacitat de resposta del sistema davant qualsevol atac.

Les seves funcions són:

- Aplicació de les mesures de seguretat definides per protegir els sistemes i infraestructures.
- Vigilar i monitorar la seguretat dels sistemes, i dels dispositius de defensa, mitjançant interfícies o aplicacions.
- Anàlisi i correlació d'esdeveniments de seguretat i registres d'activitat dels sistemes.
- Operacions de seguretat sobre els dispositius de defensa.
- Realitzar un seguiment de la gestió dels incidents de seguretat i recomanar possibles actuacions respecte d'ells.
- Servei d'Alerta Primerenca d>alertes de seguretat en les xarxes corporatives i en les connexions a Internet dels sistemes.
- Gestió de vulnerabilitats (anàlisi i determinació de les accions de remediació/instal·lació de pegats) d'aplicacions i serveis.
- Anàlisi forense digital i de seguretat.
- Servei de cibervigilància que possibiliti la prospectiva sobre la ciberamença.

4. Missió del COPC

Vetllar pel prestigi, la qualitat i la defensa de les intervencions professionals, preservar la praxi de cada actuació i donar suport en el procés d'exercir-la, garantir a la ciutadania l'ordenació de la professió i la qualitat òptima de l'atenció i del servei. El COPC innova, desenvolupa i implementa serveis professionals competitiu en consonància amb exercici de la professió i fomenta els avantatges derivats de ser un col·lectiu. El Col·legi Oficial de Psicologia de Catalunya es regeix pels valors legals i ètics en vigor, per les pautes que les institucions determinen i per les que la deontologia mateixa dictamina.

5. Principis bàsics

Els principis bàsics són directrius fonamentals de seguretat que han de tenir-se sempre presents en qualsevol activitat relacionada amb l'ús dels actius d'informació.

S'estableixen els següents principis bàsics de seguretat:

- Visió estratègica: la seguretat de la informació compta amb el compromís i suport de tots els nivells directius del COPC, de manera que estigui coordinada i integrada amb la resta de l'estratègia de l'entitat per conformar un tot coherent i eficaç.
- Responsabilitat determinada: en els sistemes TIC s'identificarà el Responsable de la Informació, que determina els requisits de seguretat de la informació tractada; el Responsable del Servei, que determina els requisits de seguretat dels serveis prestats; el Responsable del Sistema, que té la responsabilitat sobre la prestació dels serveis i el Responsable de la Seguretat, que determina les decisions per satisfer els requisits de seguretat.
- Seguretat integral: la seguretat de la informació s'entén com un procés integral constituït per tots els elements tècnics, humans, materials i organitzatius, relacionats amb els sistemes TIC, procurant evitar qualsevol actuació puntual i sent part de l'operativa habitual.
- Línies de defensa: es disposa d'una estratègia de protecció constituïda per diferents mesures de tipus organitzatiu, físic i lògic per estar previnguts davant d'un possible incident i minimitzar el seu impacte.
- Gestió de riscos: l'anàlisi i gestió de riscos és part essencial del procés de seguretat i permet el manteniment d'un entorn controlat, minimitzant els riscos fins a nivells acceptables. La reducció d'aquests nivells es realitza mitjançant el desplegament de mesures de seguretat, que estableixen un equilibri entre la naturalesa de les dades i els tractaments, l'impacte i la probabilitat dels riscos als quals estiguin exposats i l'eficàcia i el cost de les mesures.
- Proporcionalitat: l'establiment de mesures de protecció, detecció i recuperació és proporcional als potencials riscos i a la criticitat i valor de la informació i dels serveis afectats.
- Millora contínua: les mesures de seguretat s'avaluen i actualitzen periòdicament per adequar la seva eficàcia a la constant evolució dels riscos i sistemes de protecció. La seguretat de la informació serà atesa, revisada i auditada per personal qualificat, instruït i dedicat.
- Seguretat per defecte: els sistemes han de dissenyar-se i configurar-se de forma que garanteixin un grau suficient de seguretat per defecte.
- Protecció dels actius: els actius, com a elements de gestió i tractament d'informació, han de ser protegits amb les mesures adients per evitar els riscos identificats.

6. Objectius de la seguretat de la informació

El COPC estableix aquests objectius de la seguretat de la informació:

- Garantir la qualitat i protecció de la informació gestionada per l'entitat.
- Aconseguir la plena conscienciació dels usuaris respecte a la seguretat de la informació
- Gestionar adequadament els actius d'informació, que es trobaran inventariats i categoritzats i estaran associats a un responsable
- Implementar els mecanismes necessaris per garantir que qualsevol persona que accedeixi als actius d'informació conegui les seves responsabilitats i es redueixi el risc derivat d'un ús indegut.
- Garantir la seguretat física dels actius, que seran emplaçats en àrees segures, protegides per controls d'accés físics adequats al seu nivell de criticitat i amb les mesures de protecció davant amenaces físiques o ambientals.
- Garantir la protecció de la informació que es transmeti a través de xarxes de comunicacions, tenint en compte el seu nivell de sensibilitat i de criticitat, mitjançant mecanismes que garanteixin la seva seguretat.
- Garantir una adequada gestió de la seguretat, operació i actualització dels sistemes TIC.
- Controlant l'accés a la informació, limitant l'accés als actius d'informació per part d'usuaris, processos i altres sistemes d'informació mitjançant la implantació dels mecanismes d'identificació, autenticació i autorització adequats a la criticitat de cada actiu.
- Contemplar els aspectes de seguretat de la informació en totes les fases del cicle de vida dels sistemes d'informació, garantint la seva seguretat per defecte.
- Gestionar adequadament els incidents de seguretat, implementant els mecanismes apropiats per a la seva correcta identificació, registre i resolució.
- Garantir la prestació continuada dels serveis, implementant els mecanismes apropiats per assegurar la disponibilitat dels sistemes d'informació i mantenir la continuïtat dels processos de negoci.
- Garantir el compliment legislatiu i normatiu, adoptant les mesures tècniques, organitzatives i procedimentals necessàries per al compliment de la normativa legal vigent en matèria de seguretat de la informació i privadesa.

7. Marc legislatiu i regulatori

El marc en què es desenvolupen les activitats del COPC està integrat per un conjunt de normatives reguladores i legislacions, que es troben identificades en un document específic, el qual és revisat i actualitzat periòdicament.

El COPC està compromès amb el compliment de la legislació vigent aplicable i disposa de les eines i controls per a assegurar el seu adequat compliment.

8. Dades de caràcter personal

El COPC tracta dades de caràcter personal i només les recull i tracta quan són adequades, pertinents i no excessives i aquestes es troben en relació amb l'àmbit i les finalitats per les quals s'hagin obtingut. De la mateixa manera, adopta les mesures tècniques i organitzatives necessàries per al compliment de la normativa de protecció de dades.

El COPC disposa d'una Política de Privacitat, la qual és pública, i que regula la gestió de les dades personals recollides.

9. Obligacions i conscienciació del personal

Tot el personal del COPC està obligat a conèixer i complir aquesta Política de Seguretat de la Informació i la normativa de seguretat, sent el Comitè de Seguretat el responsable de facilitar els mitjans necessaris.

El COPC ha establert un programa de sensibilització contínua per atendre a tot el personal, en particular al de nova incorporació, basat en les directrius definides internament. Apart d'altres accions que es duren a terme, tot el personal assistirà o rebrà, com a mínim, una sessió de sensibilització en matèria de seguretat i protecció de dades.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes d'informació rebran formació per la gestió segura dels sistemes en la mesura en què la necessitin per fer la seva feina. La formació serà obligatòria abans d'assumir una responsabilitat, tant si és la seva primera assignació com si es tracta d'un canvi de lloc de treball o de responsabilitats en el mateix.

10. Gestió de riscos

Tots els sistemes afectats per la present Política estan subjectes a una anàlisi de riscos amb l'objectiu d'avaluar les amenaces i els riscos als quals estan exposats.

Aquesta anàlisi es repetirà:

- Almenys un cop l'any.
- Quan es produeixin canvis en la informació i/o serveis gestionats de manera significativa.
- Quan ocorri un incident greu de seguretat o es detectin vulnerabilitats greus.

El Responsable de la Seguretat serà l'encarregat de què es dugui a terme l'anàlisi de riscos, així com d'identificar mancances i debilitats i posar-les en coneixement del Comitè de Seguretat de la Informació.

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

El procés de gestió de riscos es du a terme seguint uns procediments definits específics i fent servir una metodologia reconeguda per l'anàlisi i gestió de riscos

11. Notificació d'incidents

Segons el que disposa l'article 33 del Reial decret 311/2022, de 3 de gener, el COPC notificarà al Centre Criptològic Nacional aquells incidents que tinguin un impacte significatiu en la seguretat de la informació gestionada i dels serveis prestats, en relació amb la classificació de sistemes recollida a l'annex I de la normativa.

El COPC disposa d'una Política de gestió d'incidents, així com procediments específics, eines i mesures tècniques i organitzatives per la seva detecció, tractament i resposta.

12. Organització de la documentació de seguretat

La present Política de Seguretat de la Informació és complementada amb diversa normativa de seguretat que tracta aspectes específics.

El cos normatiu sobre seguretat de la informació es desenvoluparà en tres nivells per àmbit d'aplicació, nivell de detall tècnic i obligatorietat de compliment, de manera que cada norma d'un determinat nivell de desenvolupament es fonamenti en les normes de nivell superior.

Els nivells de desenvolupament normatiu són els següents:

- Primer nivell normatiu: constituït per la present Política de Seguretat de la Informació, la Norma interna de bon ús dels sistemes i les directrius generals de seguretat aplicables a les diferents àrees del COPC.
- Segon nivell normatiu: constituït per les normes de seguretat derivades de les anteriors.
- Tercer nivell normatiu: constituït per procediments, guies i instruccions tècniques. Són documents que, complint amb el que s'exposa en la Política de Seguretat de la Informació, determinen les accions o tasques a realitzar en el desenvolupament d'un procés.

Correspon a la Junta de Govern l'aprovació de la Política de Seguretat de la Informació. La resta de polítiques seran aprovades pel Comitè de Seguretat. Els documents de segon i tercer nivell normatiu seran aprovats pel Responsable de Seguretat i, si es considera necessari, podrà consultar-ho amb el Comitè de Seguretat abans de la seva aprovació.

El cos normatiu de seguretat i, molt especialment, la Política de Seguretat de la Informació i la Norma interna de bon ús dels sistemes, serà conegut i estarà a disposició de totes les persones treballadores i, en particular, per les que utilitzin, operen o administrin els sistemes d'informació i comunicacions.

13. Terceres parts

Quan el COPC presti serveis a altres organismes o manipuli informació d'altres organismes, se'ls farà partícip d'aquesta Política de Seguretat de la Informació. S'establiran canals per al report i la coordinació dels respectius òrgans de la Seguretat de la Informació i s'establiran procediments d'actuació per a la reacció davant incidents de seguretat.

Quan el COPC faci ús de serveis de tercers o cessi informació a tercers, se'ls farà partícip d'aquesta Política de Seguretat i de la normativa de seguretat que atenyi a aquests serveis o informació. Aquesta tercera part quedarà subjecta a les obligacions establertes en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics de report i resolució d'incidències. Es garantirà que el personal de tercers està adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establert en aquesta Política de Seguretat.

Quan algun aspecte d'aquesta Política de Seguretat de la Informació no pugui ser satisfet per una tercera part segons es requereix en els paràgrafs anteriors, es requerirà un informe del Responsable de Seguretat que precisi els riscos en què s'incorre i la forma de tractar-los. Es requerirà l'aprovació d'aquest informe pels responsables de la informació i els serveis afectats abans de continuar endavant.

14. Millora contínua

La gestió de la seguretat de la informació és un procés subjecte a una actualització permanent. Els canvis en l'organització, les amenaces, les tecnologies i/o la legislació són un exemple de casos en què és necessària una millora contínua dels sistemes.

Per això, és necessari implantar un procés permanent que comportarà, entre altres accions:

- Revisió de la Política de Seguretat de la Informació
- Revisió dels serveis i informació i la seva categorització
- Execució amb periodicitat anual de l'anàlisi de riscos
- Realització d'auditories internes o, quan procedeixin, externes.
- Revisió de les mesures de seguretat
- Revisió i actualització de les normes i procediments

Aquestes accions permetran garantir que els sistemes d'informació estan protegits davant de les amenaces actuals i futures.

És important que aquest procés sigui implementat i mantingut per un equip de professionals qualificats en seguretat de la informació.

15. Compliment de les polítiques

El Comitè de Seguretat verificarà el compliment d'aquesta política a través de diversos mètodes, incloent però no limitat a, informes d'eines de negoci, auditories internes i externes, i retroalimentació al propietari de la política.

Qualsevol excepció a la política haurà de ser aprovada prèviament pel Comitè de Seguretat.

L'incompliment d'aquesta política, a més de les sancions penals que pot comportar per a l'empresa i els seus directius i empleats, està subjecta a les sancions administratives i/o laborals corresponents que siguin d'aplicació per la normativa laboral o conveni col·lectiu vigent, així com a l'aplicació de les clàusules penals previstes en els contractes subscrits amb clients, proveïdors i altres socis de negoci.

16. Vigència, revisió i comunicació

Aquesta política i els seus documents relacionats han d'estar a disposició i accessibles pel personal i col·laboradors del COPC.

Aquesta Política de Seguretat de la Informació és efectiva des de la data indicada com a aprovació per part de Junta de Govern i serà vigent fins que sigui reemplaçada per una nova Política.

La Política serà revisada i, si escau, actualitzada, periòdicament o quan es produeixin canvis en el context intern o extern que així ho aconsellin, així com en el cas de modificacions legals que incideixin en aquesta.

Text aprovat el dia 19 de març de 2025 per la Junta de Govern del COPC