Col·legi Oficial de
Psicologia de Catalunya

Política de prevenció de riscos en privacitat, confidencialitat i ciberseguretat

Nom del document	Política prevenció riscos privacitat, confidencialitat i ciberseguretat		
Control de versions	Versió núm.	Data	Responsable revisió
Primera versió	01	Octubre 2024	Comitè d'Ètica i de *Compliance*
Autor	Comitè d'Ètica i de *Compliance*		
Responsable del document	Comitè d'Ètica i de *Compliance*		
Política aprovada per acord de Junta de Govern	14/06/2025		
Data de la propera revisió	14/06/2025 (2 anys després del dia d'aprovació JG)		

Contingut

1. Objecte

Aquest document sobre la **POLÍTICA PER LA PREVENCIÓ DE RISCOS DE PRIVACITAT, CONFIDENCIALITAT I CIBERSEGURETAT** s'ha elaborat de conformitat amb la política de *Compliance* Penal vigent del COPC i amb l'objectiu de desenvolupar els requisits establerts en l'esmentada política respecte als següents riscos:

1. Riscos de *compliance* penal en matèria de privacitat i protecció de dades personals.
2. Riscos de *compliance* penal relacionats amb el deure de guardar confidencialitat i protegir els secrets i la propietat intel·lectual o industrial, pròpia o de tercers, que gestionen els integrants del COPC en l'acompliment de les seves funcions.
3. Riscos de *compliance* penal a causa d'una possible fallida en la ciberseguretat derivada de l'ús inadequat dels mitjans tecnològics que el COPC posa a disposició de les persones integrants de l'organització, o dels mitjans propis dels integrants (*BYOwnDevices*), incloent-hi els riscos provocats pel teletreball.
4. Fomentar la consciència i la formació en seguretat: La política promou l'educació i la formació en seguretat dels empleats i altres actors rellevants dins de l'organització. Això inclou la sensibilització sobre bones pràctiques de seguretat i la formació en la identificació d'amenaces cibernètiques.
5. Mitigar riscos cibernètics: El document busca identificar i abordar els riscos cibernètics que podrien afectar l'organització, com ara atacs de programari maliciós, pesca de credencials, intrusions i robatori de dades. Estableix polítiques i procediments per prevenir, detectar i respondre a amenaces cibernètiques.

L'objecte del present document és establir un codi de conducta i bones pràctiques orientades a minimitzar, en nombre i impacte, els incidents relatius als riscos indicats que poguessin presentar-se a l'entorn de treball del COPC, així com establir les normes que hauran de ser observades i complertes en l'ús diari de la informació i dispositius tecnològics que els integrants del COPC tinguin a la seva disposició per al desenvolupament de la seva activitat professional.

2. Àmbit d'aplicació

La present política és d'obligat compliment per a totes les persones integrants del COPC.: membres de la Junta de Govern, càrrecs directius, persones empleades, persones col·laboradores, persones becàries, persones voluntàries, persones treballadores d'empreses de treball temporal i en resum, qualsevol persona vinculada al COPC. per relació laboral o anàloga, així com a les seves persones sòcies de negoci en totes aquelles activitats que poden comportar riscos en matèria de privacitat, confidencialitat i ciberseguretat.

El COPC espera dels seus membres que adeqüin les seves conductes als principis que desenvolupa, sense limitació territorial ni temporal, havent de ser coneguda i acceptada per tots els seus integrants.

Així mateix, el COPC. promourà l'acceptació de les directrius de la present política entre tots els seus clients i proveïdors, i en general els seus socis de negoci, assumint-lo com a propi o comptant amb

declaracions similars que respectin els seus principis, adequant-hi la seva conducta en el mercat i, concretament, en les seves relacions amb el COPC.

3. Vigència

Aquesta política desenvolupa la política de *compliance* penal i ha estat aprovada per la Junta de Govern, entrant en vigor l'endemà de la seva publicació per a totes les persones integrants de l'organització a través de la intranet corporativa.

Aquesta política serà degudament actualitzada per raó a canvis en el context intern o extern que així ho aconsellin, així com en el cas de modificacions legals que incideixin dins del COPC.

4. Termes i definicions

L'organització: Terme que identifica al Col·legi Oficial de Psicologia de Catalunya: a efectes del sistema de gestió de *compliance* penal s'utilitzarà indistintament aquest terme o el nom de COPC.

Junta de Govern: Òrgan de govern de l'organització, en la mesura que té assignades la responsabilitat i autoritat fonamental de les activitats, la governabilitat i les polítiques estratègiques i al qual l'alta direcció de l'organització informa i ret comptes.

Alta direcció: Òrgan que dirigeix i controla la gestió operativa de l'organització. La figura de l'alta direcció resideix actualment en gerència i en el degà o degana de tant en tant és la persona representant legal del COPC.

Òrgan de *compliance* penal: Òrgan dotat d'autonomia i independència, al qual se li confia, entre d'altres comeses, la responsabilitat de supervisar el funcionament i observança del sistema de gestió de *compliance p*enal de l'organització. L'òrgan de *compliance* penal és dirigit pel Comitè d'Ètica i de *Compliance* de l'organització.

Direcció operativa: Està integrada pels caps i coordinadores de Departament que assumeixen la direcció de les diverses àrees o departaments de l'organització; són responsables de complir i fer complir en l'àmbit de les seves responsabilitats operatives amb les polítiques i procediments establerts per l'organització.

Integrants de l'organització Identifica totes les persones que formen part de l'òrgan de govern, alta direcció, direccions operatives, personal laboral fix o temporal o personal sota conveni de col·laboració i pràctiques i la resta de les persones sota subordinació jeràrquica de qualsevol de les anteriors.

Socis de negoci: Qualsevol persona jurídica o física, llevat de les integrants de l'organització, amb qui l' organització manté o preveu establir algun tipus de relació de negocis. A mode enunciatiu, però no limitatiu, s'inclouen agents o comissionistes, assessories externes, persones proveïdors, clients i clientes, *joint-ventures* o persones físiques o jurídiques contractades per l'organització per al lliurament i/o recepció de béns i/o prestació de serveis.

Tercer: Persona física o jurídica o organisme independent de l'organització.

Parts interessades/ Grups d'interès: Les persones físiques o jurídiques que, no essent socis de negoci ni integrants de l'organització, poden veure's afectades o percebre's com a afectades per una decisió o activitat de l'organització.

Persones que ocupen posicions especialment exposades: Persones que participen en activitats que estan exposades a un risc penal major que baix, segons deriva de l'avaluació de riscos penals.

Política de *compliance p*enal (Política corporativa de prevenció de la comissió de delictes): Document que fixa com un dels objectius estratègics de l'organització no tolerar cap conducta que pugui ser constitutiva de delicte o d'un incompliment i explicita i publica el compromís de l'òrgan de govern i l'alta direcció amb aquest objectiu.

Reglament de la funció de *compliance* penal i sistema de gestió de *compliance p*enal: Conjunt de disposicions que regulen els òrgans de la funció de *compliance* penal i el sistema de gestió de *compliance p*enal de l'organització i que estan contingudes en aquest document.

Catàleg o manual de conductes prohibides i comportaments esperats: Document que reflecteix el llistat de delictes aplicables a l'organització conforme al règim de responsabilitat penal de la persona jurídica, així com una relació de conductes que s'esperen dels membres de l'organització per a la seva prevenció, detecció o gestió primerenca.

Sistema de gestió de *compliance* penal (SGCP) o "sistema": Sistema d'organització i gestió per a la prevenció de delictes, l'objectiu dels quals és la prevenció, detecció i gestió de riscos penals mitjançant la seva integració en els processos de negoci, així com el mesurament per a la seva millora contínua, i la base essencial del qual es representa en la política de *compliance* penal i en els rols, processos i procediments establerts en aquest document i la documentació que el desenvolupa.

Requisit: Exigència prevista i obligatòria. Els requisits poden provenir de les lleis penals i normativa complementària o estar fixats per l'organització a través de la política de *compliance* penal o qualsevol dels documents del sistema de gestió de *compliance* penal que li donen suport.

No conformitat: Incompliment d'un requisit.

Unitat d' avaluació: Àrea, departament, procés o procediment que és objecte de delimitació per al tractament de risc penal, que comporta la realització d'una anàlisi i mapa de riscos propi i diferenciat d' altres unitats d'actuació.

Nivells de risc inacceptables (*apetit de risc*): Per intentar assolir el risc zero, l'organització determinarà a través del seu òrgan de govern i a proposta de l'òrgan de *compliance* les condicions en què el nivell de risc penal fa inacceptable executar un procés o procediment o realitzar qualsevol activitat de l'organització.

Riscos penals: Conductes realitzades per qualsevol integrant de l'organització que, atenent les obligacions i requisits de *compliance* penal aplicables al COPC., comporten o poden comportar la materialització d'un il·lícit penal que pugui imposar una sanció penal a l'organització conforme al règim de responsabilitat penal de la persona jurídica.COPC.

5. Principis de la política per a la prevenció de riscos de privacitat, confidencialitat i ciberseguretat

5.1 Respecte per la privacitat i les dades personals

L'apartat 3.1- Privacitat i intimitat de la nostra política de *compliance* penal estableix:

> "La normativa reguladora del dret a la intimitat i a la privacitat de les persones que es relacionen amb el COPC ens exigeix un profund respecte per la privacitat i els secrets personals i professionals que gestionem.
>
> Per a això, hem d'observar els nostres protocols de protecció de dades, així com les polítiques tecnològiques i de ciberseguretat".

El COPC ha aprovat i aplicat una política de protecció de dades i de mesures de seguretat bàsiques que han de complir tots els empleats del COPC en el marc del sistema de protecció de dades personals que és responsabilitat del Comitè de Protecció de Dades i Seguretat de la Informació i compta amb un delegat de protecció de dades.

Tots els integrants del COPC han de ser conscients que la privacitat i la protecció de les dades personals tenen una protecció penal enfront de les vulneracions doloses més greus, que a vegades es poden cometre a través del sistema de gestió de dades personals i en altres ocasions poden executar-se pels integrants de l'organització mitjançant comportaments i iniciatives personals.

En aquesta política es concreten les Conductes i procediments de control, que han d'observar tots els integrants de l'organització a fi d'evitar conductes que puguin materialitzar aquests riscos de *compliance* penal.

5.2 Respecte per la informació reservada i els secrets aliens

Es considera informació confidencial qualsevol informació propietat del COPC. Gran part de la informació reservada –però no tota-, és interna o confidencial. També pot estar subjecta a copyright, patents o altres drets legals o de propietat intel·lectual.

La informació reservada inclou assumptes com: deliberacions de la Junta de Govern, plans i accions del COPC, expedients de Deontologia, borsa de treball o registre sanitari. La informació reservada del COPC és, a vegades, resultat de les idees i esforços dels seus empleats i empleades, i d'inversions en planificació, recerca i desenvolupament.

El valor de la informació reservada pot interessar altres persones del sector professional, competidors dels nostres col·legiats i usuaris i fins i tot a periodistes i consultors. L'organització es veuria perjudicada per la revelació no autoritzada de la seva informació reservada, o l'ús no autoritzat per qualsevol d'aquestes persones. Per tant, és fonamental no utilitzar o revelar aquesta informació llevat que estigui expressament autoritzat, així com mantenir en tot moment conductes i procediments que assegurin que protegim aquesta informació.

5.3 Respecte pel coneixement aliè

La constant activitat cultural, acadèmica, publicitària i formativa que es desenvolupa al COPC ens fa gestors de múltiples classes de continguts subjectes a drets de propietat intel·lectual que venen presentats al seu torn en diversos formats analògics i digitals.

Cal ser conscients que els límits del dret a la propietat intel·lectual són expansius a conseqüència de la multiplicació de canals i mitjans de creació i difusió digital.

La propietat industrial que es pot veure afectada per l'activitat del Col·legi abasta des de marques, logos, eslògans i dissenys industrials fins a programari, patents tecnològiques o models d'utilitat.

Els actius aliens que gestionem exigeixen que siguem molt respectuosos en tot moment amb la llicència o autorització d'ús que ens ha concedit el seu propietari o amb el règim legal a través del qual hem accedit a aquest coneixement.

5.4 Ciberseguretat

La implementació d'un conjunt de mesures tècniques i organitzatives bàsiques i imprescindibles per garantir la seguretat que han de reunir els fitxers automatitzats o no automatitzats, els centres de tractament, locals, equips, sistemes, programes i persones que intervinguin en el tractament de la informació és un requisit imprescindible per evitar els riscos de *compliance* penal que són objecte de la present política.

L'organització té el deure de definir aquestes mesures i tots els seus integrants tenen el deure ineludible d'aplicar-les.

En matèria de ciberseguretat, el COPC es regeix per la Política de Seguretat de la Informació que ve regulada segons les directrius que s'emmarquen en funció del que determina l'*Esquema Nacional de Seguridad* (ENS) i per la Norma d´ús dels sistemes d'informació que desenvolupa l'esmentada "Política de seguretat de la informació". Per la qual cosa, haurem d'adreçar-nos en aquesta regulació més específica.

6. Conductes i procediments de control

En el marc d'aquesta política es defineixen les conductes i procediments de control que ha d'establir, observar i complir totes les persones integrants de l'organització.

6.1 Conductes relatives a la privacitat

6.1.1.- Totes les persones integrants del COPC han d'acatar i aplicar la política de protecció de dades i mesures de seguretat bàsica aprovada per l'organització i que se'ls ha comunicat. Qualsevol conducta de l'organització relativa a la gestió de dades personals ha de respectar els principis establerts en la mateixa:

- La lleialtat i la transparència en el seu tractament.
- Limitació de la finalitat.

- Minimització de dades.
- Exactitud.
- Limitació del termini de conservació.
- Integritat i confidencialitat.
- Responsabilitat proactiva.
- Obtenció del consentiment de la persona interessada, quan sigui necessari.
- Reconeixement dels drets que poden exercir els interessats

6.1.2. Tots els integrants del COPC han d'assegurar i respectar la intimitat de les persones en els espais comuns d'ús privatiu habilitats en l'organització com són els vestuaris, serveis sanitaris, zones de menjador o descans.

6.1.3. Tots els integrants del COPC s'han d'abstenir d'accedir a espais privats aliens, com calaixos i taquilles o bosses, carteres i equips informàtics o telefònics personals, tot i que considerin que existeix una raó per fer-ho. El COPC habilitarà i comunicarà, si s'escau, els protocols pertinents en el marc de procediments de recerca interna o supòsits excepcionals i sobrevinguts.

6.1.4. La imatge personal dels integrants de l'organització no pot ser objecte d'invasió o ús no autoritzat, quedant prohibida qualsevol gravació audiovisual que no hagi estat autoritzada expressament o no se suporti un ús legítim fonamentat en la normativa de protecció de dades.

6.1.5. Qualsevol activitat del COPC que requereixi l'enregistrament o de registres audiovisuals de persones haurà d'haver estat objecte d'autorització per les persones afectades, l'alta direcció previ informe favorable emès pels òrgans responsables de privacitat i/o, si s'escau, de *compliance*.

6.1.6. Queda terminantment prohibida la creació de nous fitxers que suposin el tractament de dades personals, així com la cessió d'aquests, fora dels procediments establerts en el marc dels seus Sistemes de Protecció de Dades. En cap cas, a més, es demanaran més dades de les estrictament necessàries. Mai s'afegirà informació subjectiva o addicional.

6.2 Conductes relatives a la confidencialitat i el secret empresarial

6.2.1. No està permès utilitzar la informació de l'organització, de qualsevol índole, per a ús diferent del professional, i no se'n podrà disposar de cap altra forma o per a finalitat diferent.

6.2.2. Tota la informació a la qual es té accés i/o que es genera a conseqüència de les funcions desenvolupades per les persones integrants de COPC és considerada confidencial, sent propietat del COPC, que establirà regles per al seu ús intern. Aquesta informació confidencial no podrà ser divulgada ni directament ni indirectament per la persona treballadora ni per un tercer sense una autorització prèvia i per escrit, quedant, a més, emparada dins del secret professional.

6.2.4. S'indicarà de manera clara i inequívoca tots els documents i arxius sensibles que continguin informació restringida o secrets, fent servir marques d'aigua o mecanismes similars.

6.2.5. Queda prohibit burlar els mecanismes o dispositius de seguretat d'accés a la informació. S'ha d'evitar qualsevol intent d'accés no autoritzat a dades o recursos i informar de les possibles debilitats en els sistemes d'informació que tracten dades de caràcter personal.

6.2.6. Queda prohibit accedir o utilitzar informació confidencial o secrets d'altres organitzacions o professionals als quals hagin tingut accés, ni legítimament, qualsevol persona que s'incorpori al COPC per

prestar serveis laborals o professionals. Els processos d'incorporació hauran d'aplicar clàusules i condicions contractuals que assegurin aquest objectiu.

6.2.7. Per assegurar la confidencialitat de la documentació i informació a la qual de forma natural i a conseqüència del desenvolupament de les seves funcions accedeixen els integrants de l'organització, tots han de posar els mitjans raonables al seu abast per custodiar-la i impedir-ne un mal ús i l'accés per part de tercers no autoritzats.

6.3 Revelació inadvertida i taules netes

6.3.1. Cal posar especial atenció per evitar la revelació inadvertida de dades personals o informació reservada. Per evitar aquest tipus de revelació, no s'ha de discutir amb cap persona aliena al COPC. Tampoc s'ha de discutir informació confidencial ni tan sols amb persones autoritzades del COPC, si s'està en presència d'altres; per exemple, en una exposició comercial o en una àrea pública, com un avió, o en fer ús d'un telèfon o una base de dades o butlletí electrònic. Això s'aplica igualment a converses amb membres de la família o amb amics que poden passar la informació, innocentment o inadvertidament, a qualsevol altra persona.

6.3.2. Tots els fitxers temporals que els usuaris mantinguin en els seus equips informàtics o de comunicació hauran de ser esborrats, un cop hagi finalitzat la utilitat per a la qual van ser creats.

6.3.3. És possible que per a l'acompliment del treball es generi documentació escrita en paper, d'ús temporal, que pogués contenir informació sensible o confidencial. Aquesta documentació, una vegada deixi de ser útil, haurà de ser destruïda mitjançant un sistema de destrucció de paper, evitant en tot moment la seva destrucció manual i/o dipòsit a les papereres existents.

6.3.4. En situacions de teletreball domiciliari, l'esmentada documentació s'ha de conservar confidencialment fins que es pugui lliurar a la seu del COPC per a la seva destrucció segura.

6.3.5. **Enquestes**: Només les persones autoritzades directament per COPC, podran atendre a enquestadors i complimentar qüestionaris en els quals es demani qualsevol mena d'informació relativa al COPC.

6.4 Polítiques d'ús dels mitjans tecnològics

Tota la regulació que s'engloba dins de les polítiques d'ús dels mitjans tecnològics, polítiques d'ús responsable del correu electrònic corporatiu per a ús personal, ús i gestió de les credencials d'accés, ús i gestió de xarxes i accés a internet, llocs web inadequats en l'entorn de treball i regles per evitar la infecció i propagació de virus informàtics, s'atendrà al que regula la política de seguretat de la informació que ve regulada segons les directrius que s'emmarquen en funció del que determina l'Esquema Nacional de Seguridad (ENS), i per la norma d´ús dels sistemes d'informació que desenvolupen l'esmentada a "Política de seguretat de la informació".

7. Deures de comunicació

7.1. Els integrants del COPC tenen el deure de fer tots els esforços possibles per impedir i donar a conèixer de forma immediata al seu superior qualsevol possible risc d'incompliment de la present política, així com les possibles infraccions que directament o indirectament arribin al seu coneixement.

7.2. Tota incidència de qualsevol tipus que afecti el funcionament de l'organització haurà de ser comunicada.

7.3. En cas de conèixer o sospitar que un tercer ha entrat en qualsevol dels dispositius tecnològics sense el consentiment de la persona treballadora, aquesta haurà de notificar-ho immediatament al responsable del Departament de les Tecnologies i la Informació i dels sistemes informàtics del COPC.

7.4. Qualsevol irregularitat o problema de qualsevol mena relacionat amb els dispositius tecnològics, com ara virus, sospita d'accés no autoritzat, pèrdua d'informació confidencial en dispositius especials (com USB), s'hauran de notificar immediatament al responsable del Departament de les Tecnologies i la Informació i dels sistemes informàtics del COPC.

8. Altres obligacions i consideracions

8.1 Comunicació i difusió

De la present política es donarà una àmplia difusió entre les persones integrants del COPC, recavant la seva acceptació expressa.

8.2. Sancions per incompliment

L'incompliment d'aquesta política, a més de les sancions penals que pot comportar per a l'empresa i a les seves persones directives i empleades, 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 persones clientes, proveïdores i altres socis i sòcies de negoci.