# POLÍTICA GENERAL DEL SISTEMA INTERN D'INFORMACIÓ I DEFENSA DE L'INFORMANT

CORPORATE LINE
Canal de comunicaciones

FACE to FACE LINE
Canal presencial

ESCOLES CARMELITES MISSIONERES

# ÍNDEX

1 INTRODUCCIÓ

2 PRINCIPIS D'ACTUACIÓ I GARANTIES ESSENCIALS

3 RESPONSABLE DEL SISTEMA INTERN D'INFORMACIÓ

4 AUTORITAT INDEPENDENT DE PROTECCIÓ DE L'INFORMANT

5 CONFIDENCIALITAT I PROTECCIÓ DE DADES PERSONALS

6 MESURES DE PROTECCIÓ

7 RÈGIM DISCIPLINARI

8 PUBLICITAT, REVISIÓ I ACTUALITZACIÓ

9 CANALS INTERNS D'INFORMACIÓ

COPYRIGHT

# 1 INTRODUCCIÓ

La transposició de la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre de 2019 al Dret espanyol amb **la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció**, implica la incorporació d'instruments específics perquè, els qui coneixen actuacions il·legals o irregulars, puguin facilitar dades i informació útils, quedant assegurada una total protecció efectiva d'aquests informants.

En aquest sentit, la citada normativa regula els aspectes mínims que han de satisfer els diferents mitjans d'informació interns i externs, juntament amb el règim d'especial protecció dels informants que actuïn amb bona fe i consciència honesta, de manera desinteressada.

De conformitat amb l'anterior, l'ENTITAT ha implementat un **Sistema Intern d'Informació (SIIF)**, el qual es configura com un eix fonamental per a la supervisió, control i prevenció en l'àmbit del compliment normatiu. Tal sistema constitueix un mitjà preferent i una eina d'utilització obligatòria per a canalitzar la informació de manera diligent, a l'efecte d'enfortir la cultura de la informació en el si de la pròpia organització.

El SIIF ha estat dissenyat com un instrument de control i de prevenció, que contempla els canals d'informació gestionats tant internament com per una empresa externa especialitzada. Aquests canals gaudeixen dels més alts nivells de professionalitat, experiència, independència, confidencialitat, compliment de la normativa de protecció de dades i altres marcs normatius aplicables. Així mateix, el SIIF garanteix els principis bàsics d'anonimat, adequat registre, conservació i no alteració, prevenció de conflictes d'interès, protecció de l'informant i prohibició de represàlies.

En atenció a l'esmentada Llei, és un requisit indispensable que el SIIF compti amb una **Política que enunciï els principis generals del sistema i la defensa de l'informant**, degudament publicitada en el si de l'Entitat. Per tant, juntament amb el Procediment de gestió de les informacions rebudes, la present Política és un element essencial de la configuració i funcionament del SIIF.

# 2 PRINCIPIS D'ACTUACIÓ I GARANTIES ESSENCIALS

El **Sistema Intern d'Informació (SIIF)** és un dels principals eixos dels sistemes de compliment normatiu i prevenció penal. Ateses les més altes exigències de diligència en la matèria, l'Entitat ha dotat el SIIF d'una sèrie de garanties per a assegurar la seva efectivitat, amb la col·laboració i suport de l'expert extern **BONET consulting.** En concret, els principis bàsics i garanties fonamentals que regeixen el procés i l'actuació de l'Entitat en relació amb el SIIF són els següents:

- **Independència, autonomia, imparcialitat i absència de conflictes d'interès:** En la recepció i tractament de la informació sobre les infraccions s'han definit mecanismes de reacció per a gestionar i controlar possibles conflictes d'interès i/o falta d'independència, quan els responsables de la gestió, control i/o supervisió presentin una sèrie de característiques que comprometin i condicionin l'acompliment de les seves funcions. Així mateix, totes les comunicacions rebudes són objecte d'anàlisi amb els requisits necessaris d'independència, que garanteixen l'equitat i justícia en el tractament d'aquestes.

- **Professionalitat i experiència:** Professionals experts en compliment normatiu, prevenció penal i bon govern són els encarregats del tractament i gestió adequada de les comunicacions, preservant els drets dels informants i els denunciats.

- **Exhaustivitat, integritat i confidencialitat de la informació:** Els participants en les diferents fases d'investigació tenen el deure de confidencialitat respecte de qualsevol informació a la qual poguessin tenir accés o coneixement per raó de l'exercici de les seves funcions. A més, s'impedeix l'accés a ella per personal no autoritzat i es permet un emmagatzematge durador i segur d'aquesta, a través de la generació de còpies de seguretat de la informació i fitxers independents.

- **Protecció de dades i secret de les comunicacions:** El tractament de dades s'ajusta i compleix amb les més altes mesures i polítiques de protecció de dades personals, segons la normativa aplicable en matèria de Protecció de Dades de caràcter personal. De la mateixa manera, existeix el deure de guardar secret sobre qualsevol aspecte relacionat amb la informació comunicada.

- **Anonimat i Anonimització:** Es preveu la possibilitat de presentació i posterior tramitació de comunicacions anònimes, així com el deure general de preservar la identitat de l'informant que s'hagi identificat en formular la comunicació, mantenint-lo en l'anonimat i no revelant la seva identitat a terceres persones.

- **Ús assequible, simplicitat i gratuïtat:** Es garanteix la senzillesa en la realització de la comunicació, que permet l'accés universal al sistema sense cap cost associat, i l'aplicació efectiva de la legalitat i principis ètics que regeixen l'activitat de l'Entitat.

- **Registre adequat i independent:** S'elabora un llibre-registre privat de les informacions rebudes i de les recerques internes al fet que hagin donat lloc, com a garantia del seu tractament, gestió i no alteració, de manera independent i sense conflictes d'interès, durant un període de temps necessari i proporcionat de conformitat amb la legislació vigent. En cap cas les dades es conservaran per un termini superior a deu anys.

- **Pràctiques correctes de seguiment i investigació:** Amb la finalitat de comprovar la veracitat de les comunicacions, la correcta obtenció de les evidències i garantir els drets dels afectats, es regularà el cicle de vida de la comunicació en un procediment intern eficaç i transparent. Aquestes pràctiques estaran documentades en el Procediment de gestió de les informacions rebudes.

- **Protecció de l'informant i de les persones afectades:** Les persones que comuniquen o revelen infraccions tenen dret a mesures de protecció i no seran objecte de cap represàlia ni conseqüència adversa per la seva col·laboració, incloses les amenaces de represàlia i les temptatives de represàlia. D'igual forma, les persones afectades per la comunicació tindran dret a la mateixa protecció establerta per als informants, preservant-se la seva identitat i garantint-se la confidencialitat dels fets i dades del procediment.

- **Actuació diligent, responsabilitat i bona fe de l'informant:** L'ús del sistema s'assenteixi en els principis de responsabilitat, diligència i bona fe, per la qual cosa tot informant ha de tenir motius raonables per a pensar que la informació és veraç en el moment de la seva comunicació. La comunicació de fets infundats, falsos o tergiversats, així com la remissió d'informacions obtingudes de manera il·lícita, amb actitud maliciosa i moralment deshonesta, suposa una infracció del principi de bona fe i pot derivar en l'aplicació de mesures disciplinàries.

# 3 RESPONSABLE DEL SISTEMA INTERN D'INFORMACIÓ

Per a l'eficàcia del **Sistema Intern d'Informació (SIIF)** resulta indispensable la designació d'un responsable del seu correcte funcionament, organització i tramitació diligent de les informacions. Així mateix, aquest s'encarregarà d'assegurar la deguda comunicació i difusió del SIIF, així com de realitzar i actualitzar el pertinent pla de formació.

L'òrgan d'administració o òrgan de govern de l'Entitat és el competent per a la designació i comunicació a l'autoritat competent, de la persona física o òrgan col·legiat responsable de la gestió d'aquest sistema i de la seva destitució o cessament (d'ara endavant, el **Responsable del Sistema**).

El Responsable del Sistema desenvolupa les seves funcions de manera **independent i autònoma** respecte de la resta dels òrgans d'organització de l'Entitat, evitant possibles situacions de conflicte d'interès amb l'acompliment ordinari del seu càrrec. No obstant això, el Responsable del Sistema pot recórrer a uns altres tercers per a rebre suport especialitzat i/o complir amb els requisits d'independència, per a assegurar el degut compliment de les seves funcions.

Especialment, per a l'exercici de les seves funcions el Responsable del Sistema es coordinarà amb els següents subjectes:

- **A** El Responsable de recursos humans, quan pogués procedir l'adopció de mesures disciplinàries contra les persones implicades i/o coordinar l'aplicació de mesures de protecció.
- **B** Els responsables de compliment normatiu i/o dels serveis jurídics de l'Entitat, si procedís l'adopció de mesures de caràcter legal o de compliment normatiu que han de ser preses en consideració, per aquests, en relació amb les comunicacions rebudes en el SIIF.
- **C** Els encarregats del tractament que eventualment es designin.
- **D** El Delegat / Responsable de Protecció de Dades.
- **E** Altres persones i/o entitats intervinents en la gestió del SIIF.

# 4 AUTORITAT INDEPENDENT DE PROTECCIÓ DEL INFORMANT

El **Sistema Intern d'Informació (SIIF)** de l'Entitat és el mitjà prioritari i d'utilització obligatòria per a la comunicació de conductes il·lícites o infraccions de les quals es tingui coneixement, perquè permet assegurar la deguda adopció de mesures de protecció i fomentar la cultura de la informació dins de l'organització.

No obstant això, s'han determinat altres canals d'informació "externs", amb la finalitat d'oferir als ciutadans una alternativa on presentar la comunicació i/o reclamació, en els supòsits que els canals interns no compleixin amb les garanties exigides per la normativa aplicable, no s'apliquin les pertinents mesures de protecció o les persones siguin exposades a represàlies per la seva condició d'informants.

Per consegüent, tota persona física pot informar directament **l'Autoritat Independent de Protecció de l'Informant**, **A.A.I.** de la comissió de qualssevol accions o omissions constitutives d'infracció de l'ordenament jurídic, a través del canal extern d'informació d'aquesta autoritat pública especialitzada. L'accés a aquest canal d'informació extern i les dades de contacte de l'Autoritat es troben publicats en la seva pàgina web.

# 5 CONFIDENCIALITAT I PROTECCIÓ DE DADES PERSONALS

Els tractaments de dades personals que deriven del **Sistema Intern d'Informació (SIIF)** es regeixen pel que es disposa en el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, en la Llei orgànica 3/2018, de 5 de desembre i en la Llei orgànica 7/2021, de 26 de maig. Per això, en el moment de la captació, els interessats són informats del tractament de les seves dades i dels seus drets, d'acord amb la normativa vigent.

En compliment del principi de **minimització de dades**, les dades de caràcter personal recopilats són aquells necessaris i pertinents per al tractament de la comunicació. En el cas que es recopilin dades per accident, que no siguin necessaris per al coneixement i investigació de les accions o omissions, aquests seran eliminats sense dilació indeguda. Així mateix, les dades es conservaran durant el temps imprescindible per a decidir sobre la precedència d'iniciar una investigació.

D'altra banda, el disseny del SIIF garanteix la **confidencialitat** de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació, així com de les actuacions desenvolupades en la gestió i tramitació d'aquesta. En aquest sentit, l'accés a les dades personals i la resta d'informació continguda en el sistema està limitada als responsables de la gestió, dins de l'àmbit de les seves competències i funcions. Per tant, es disposa de mesures tècniques i organitzatives adequades per a preservar la identitat dels afectats i impedir l'accés de persones no autoritzades.

En el cas de qualsevol dubte o consulta sobre el tractament de dades de caràcter personal dut a terme en el si de l'Entitat en relació amb el SIIF, tot interessat pot dirigir-se al **Delegat / Responsable de Protecció de Dades** designat, a través de les dades de contacte que li han estat prèviament comunicats i que estan a la seva disposició.

# 6 MESURES DE PROTECCIÓ

Les persones que comuniquin o revelin infraccions utilitzant el Sistema Intern d'Informació (SIIF) de l'Entitat tenen dret a protecció, en les mateixes condicions que els qui informin per canals externs, sempre que tinguin motius raonables per a pensar que la informació referida és veraç en el moment de la comunicació o revelació, encara que no aportin proves concloents.

En aquest sentit, es prohibeixen expressament els actes constitutius de represàlia, inclosa l'amenaça i temptativa, contra les persones que presentin una comunicació. S'entén per represàlia:

**a** Actes o omissions prohibits per la llei.

**b** Actes o omissions que de manera directa o indirecta suposin un tracte desfavorable, situant a la persona en desavantatge respecte a una altra.

A títol enunciatiu i no limitatiu, es consideren represàlies:

- Suspensió del contracte de treball, acomiadament o extinció de la relació, terminació anticipada, anul·lació del contracte de treball i/o mercantil, mesures disciplinàries, amonestació o una altra sanció, degradació o denegació d'ascensos, modificació substancial de les condicions i no conversió del contracte temporal en indefinit o mesures equivalents.
- Danys (inclosos reputacionals), pèrdues econòmiques, coaccions, intimidacions, assetjament o ostracisme.
- Avaluació o referències negatives sobre l'acompliment laboral o professional.
- Llistes negres o difusió d'informació que dificulti o impedeixi l'accés a ocupació / contractes d'obres o serveis.
- Denegació o anul·lació de llicència o permís.
- Denegació de formació.
- Discriminació, tracte desfavorable o injust.
- Denegació d'incentius, beneficis, bons, comissions i qualsevol altre tipus de compensació.

- Terminació anticipada, suspensió, alteració o anul·lació de contractes de béns o serveis.

Aquests actes seran nuls de ple dret i donaran lloc, si és procedent, a mesures correctores disciplinàries o de responsabilitat, podent incloure la corresponent indemnització de danys i perjudicis al perjudicat.

A l'efecte de garantir el dret de protecció de l'informant i el de les persones afectades per la comunicació, l'Entitat té establertes les següents mesures tècniques i organitzatives les quals s'apliquen des del moment inicial en el qual es rep la comunicació:

1. **Configuració del SIIF:** El SIIF s'ha dissenyat amb les mesures tècniques i organitzatives adequades per a garantir la protecció de la identitat de l'informant, així com d'aquelles dades i informacions que es derivin de les comunicacions presentades. En aquest sentit, l'Entitat ha habilitat una sèrie de canals interns d'informació, els quals permeten presentar comunicacions de manera anònima. Aquests canals són:

    - **Canal en línia / digital:** Plataforma digital per a la presentació de comunicacions per escrit.

    - **Canal presencial / "face to face":** El Sistema de recepció de comunicacions mitjançant reunió presencial o per videoconferència.

    Amb independència del canal que s'utilitzi, el SIIF garanteix l'aplicació efectiva dels principis bàsics i garanties especificades en la present Política, a fi de complir amb els requisits del marc normatiu i protegir els drets dels informants i les persones afectades.

2. **Responsable del SIIF:** Per a assegurar la deguda aplicació del SIIF, l'Entitat té designat a un Responsable la funció del qual radica en la supervisió, vigilància i control del funcionament d'aquest. En aquest sentit, el Responsable, juntament amb l'expert extern, adoptaran les mesures de protecció necessàries i vetllaran pel seu degut seguiment i aplicació. La participació de l'expert extern dota a les funcions del Responsable dels elements d'autonomia i independència requerits per la normativa vigent.

Així mateix, el Responsable serà l'encarregat de realitzar una anàlisi preliminar de les comunicacions rebudes a l'efecte de determinar la idoneïtat d'adoptar mesures de protecció específiques respecte a l'informant i/o tercers afectats. A més, en funció de la naturalesa i abast de la informació, el Responsable comptarà amb el suport i assessorament dels responsables de les diferents àrees operatives l'Entitat, per al bon fi de la investigació. També podrà recórrer a uns altres tercers especialitzats en aquelles matèries que requereixin una opinió experta.

3. **Custòdia, gestió i seguretat de la informació del SIIF**: L'Entitat disposa d'un sistema de gestió documental configurat amb les mesures apropiades de seguretat i control, a l'efecte d'evidenciar la pròpia eficàcia del SIIF. Cal destacar que aquest sistema inclou processos d'anonimització, a fi de no permetre la identificació dels informants. Addicionalment, l'Entitat ha adoptat mesures tècniques raonables per a la conservació, recuperació i eliminació de manera segura de la informació, així com la implantació de controls d'accés per a impedir l'ús no autoritzat.

No obstant això, queden excloses de l'esmentada protecció les informacions remeses que siguin falses, tergiversades, manquin manifestament de tota versemblança i fonament o existeixin indicis racionals d'haver-se obtingut mitjançant la comissió d'un delicte. Això és pel fet que totes les comunicacions han de realitzar-se sota el principi de **bona fe** i, per tant, l'informant ha de tenir motius raonables per a pensar que la informació és veraç en el moment de la comunicació. En resum, el principi de bona fe requereix que en cap cas pugui desprendre's que existeix falsedat, falta a la veritat, intenció de venjança o de perjudicar un tercer.

És important recordar que les mesures de protecció no es dirigeixen només a favor dels informants. També aquelles persones a les quals es refereixin els fets relatats en la comunicació (**persones afectades**) compten amb una singular protecció davant el risc que la informació, encara amb aparent aparença de veracitat, hagi estat manipulada, sigui falsa o respongui a altres motivacions. Durant la tramitació de l'expedient, aquestes persones tenen dret a la presumpció d'innocència, a la tutela judicial i defensa, a l'accés a l'expedient, així com a la confidencialitat dels fets i dades del procediment i a la reserva de la seva identitat. En conclusió, tenen la mateixa protecció i drets que gaudeix l'informant.

# 7 RÈGIM DISCIPLINARI

L'incompliment de la normativa aplicable i les conductes contràries a les instruccions, polítiques, codis, procediments i protocols de l'Entitat és motiu d'aplicació del règim disciplinari en l'àmbit laboral i mercantil, en coordinació amb el que s'estableix en el Conveni Col·lectiu d'aplicació, l'Estatut dels Treballadors i la resta de les normes aplicables.

L'Entitat et notificarà i sancionarà les accions o omissions contràries a la present Política en les quals incorrin els empleats, col·laboradors o qualsevol membre relacionat amb l'Entitat i, en particular:

- La no comunicació de qualsevol sospita o coneixement d'infraccions i incompliments del marc normatiu i dels protocols i normes internes de l'Entitat a través del SIIF.
- Qualsevol intent o acció efectiva d'obstaculitzar la presentació de comunicacions o impedir, frustrar o alentir el seu seguiment.
- La utilització del SIIF de mala fe, per exemple, amb l'aportació d'informació o documentació sabent la seva falsedat.
- L'adopció de qualsevol represàlia derivada de la comunicació enfront dels informants o les altres persones afectades.
- La vulneració de les garanties de confidencialitat i anonimat, revelant la identitat de les persones afectades i infringint el deure de secret de les informacions.
- L'incompliment de l'obligació de col·laboració amb la investigació d'informacions.

# 8 COMUNICACIÓ, REVISIÓ I ACTUALIZACIÓ

La present Política, així com tota la informació necessària sobre l'ús del **Sistema Intern d'Informació (SIIF)** implantat, està disponible en una secció separada i ràpidament identificable, perquè tots els interessats la tinguin al seu abast de manera clara i fàcilment accessible. No obstant això, qualsevol persona pot sol·licitar informació addicional a l'Entitat a través de les dades de contacte del Responsable.

El **Responsable del Sistema** revisarà periòdicament i, si escau, proposarà a l'òrgan d'administració o òrgan de govern de l'Entitat l'actualització de la present Política, amb la finalitat d'adaptar-la a totes aquelles circumstàncies i canvis que puguin anar sorgint, així com a la normativa o jurisprudència que pugui dictar-se. Tot això, amb l'objectiu d'adequar el SIIF a les màximes exigències de compliment normatiu per al seu correcte funcionament i eficàcia.

Així mateix, l'Entitat està oberta a qualsevol **suggeriment i/o proposta** que pugui millorar la seva actuació ètica i afavorir una cultura de compliment normatiu, remarcant la necessitat que tots els empleats i membres relacionats amb l'Entitat o tercers col·laborin per a complir amb els seus valors i principis.

# 9 CANALS INTERNS D'INFORMACIÓ

A l'efecte de complir amb les disposicions recollides en la Llei 2/2023, l'Entitat té implementat un sistema configurat amb els requisits tècnics i procedimentals requerits per aquesta Llei per a la deguda atenció de les comunicacions. Tot això amb la finalitat d'oferir als informants un entorn de comunicació segur, confidencial o fins i tot anònim amb l'Entitat, i tramitar les informacions de manera eficient, professional i independent.

Per a això, l'Entitat s'ha dotat de recursos materials, tècnics i humans per a habilitar diferents canals interns que permeten la presentació de comunicacions en format escrit o verbal. Aquests canals compten amb la configuració, disseny i suport d'un expert extern a fi d'aportar els més alts nivells de professionalitat, experiència, independència, confidencialitat, protecció de dades i de l'informant, i altres àmbits aplicables per a aquesta mena de canals.

Cal destacar que, la informació proporcionada mitjançant qualsevol dels canals interns serà tractada de manera confidencial, i només tindrà accés a la mateixa el personal autoritzat per a la seva deguda gestió i tramitació.

A continuació, es detallen els canals dels quals disposa qualsevol empleat o tercer vinculat amb l'Entitat per a la presentació de les comunicacions:

## Canal On-line/Digital

CORPORATE LINE
Canal de comunicaciones

L'Entitat disposa d'una eina digital que permet presentar comunicacions per escrit mitjançant un formulari, el qual permet adjuntar arxius. Una vegada emplenat el formulari, l'eina genera automàticament un codi que permet el degut seguiment i gestió per part del responsable de la tramitació. Així mateix, s'envia una confirmació a l'informant respecte a l'entrada i registre de la comunicació en el sistema, la qual conté un resum de la informació aportada, així com el codi perquè aquest també pugui realitzar aquest seguiment.

Aquesta eina compta amb mesures de seguretat que garanteixen la protecció de la informació, la identitat de l'informant i la d'aquelles persones afectades per aquesta, així com la confidencialitat i reserva de tot el procés de gestió i tramitació de la comunicació. En aquest sentit, l'Entitat garanteix un entorn de comunicació segur i diligent per a la recepció de comunicacions.

L'eina també permet la presentació de comunicacions de manera anònima. Gràcies al sistema de comunicació i seguiment que disposa, l'informant i el Responsable del Sistema podran comunicar-se a través de l'eina, amb independència de si la comunicació s'ha presentat anònimament.

L'enllaç d'accés a aquesta eina i el seu àmbit d'ús està disponible en la pàgina web de de l'Entitat.

## Canal Presencial / "Face to face"

Una altra de les vies que l'Entitat posa a la disposició dels seus empleats i aquells tercers que es relacionen amb aquesta és el canal presencial / "face to face", la finalitat del qual és la de permetre la presentació de comunicacions verbals mitjançant una reunió presencial o per videoconferència. En aquest cas, i tenint en compte la complexitat que comporta per a l'Entitat garantir l'anonimat de l'informant en aquells casos que així se sol·liciti, l'Entitat ha encomanat aquesta funció a l'expert extern BONET consulting, el qual s'encarrega de rebre i gestionar les comunicacions amb aquestes característiques, així com aquelles altres en les quals s'identifiquin els informants i es requereixi la gestió presencial. En aquest sentit, l'expert extern garanteix la protecció de la identitat de l'informant tant en el procés de sol·licitud de cita prèvia, en la presentació d'una comunicació en format presencial, com en el lloc de realització d'aquesta.

A l'efecte de garantir la seguretat i preservar la integritat de la informació que aportació l'informant, la reunió serà gravada conforme a l'estipulat en la Llei i amb el consentiment previ de l'informant. Aquesta reunió quedarà documentada en un format segur, amb les mesures de seguretat i anonimització requerides pel marc normatiu. En aquesta línia, BONET consulting disposa i habilitarà els mecanismes tecnològics necessaris per a l'enviament de documentació complementària a la informació aportada en la reunió.

Per a poder fer ús d'aquest canal, l'Entitat ha habilitat un telèfon i un correu electrònic de contacte per a sol·licitar la presentació de comunicacions en aquest format, l'atenció i la coordinació del qual de la reunió serà realitzada exclusivament per BONET consulting. Les dades de contacte per a realitzar aquesta sol·licitud estan degudament publicats en la pàgina web de l'Entitat.

**COPYRIGHT**
El contingut d'aquesta política general sobre el sistema intern d'informació està subjecte a copyright. En conseqüència, per a procedir a la seva distribució o comunicació a altres entitats, es requereix el consentiment exprés del titular del copyright.