

REGLAMENT DEL CANAL INTERN D'INFORMACIÓ DEL CRG



Índex

1. Introducció i objecte del Reglament	3
2. Fases del procediment de gestió de les comunicacions	4
2.1. Fase de Recepció de comunicacions	4
2.2. Fase d'admissió de comunicacions.....	5
2.3. Fase d'investigació	6
2.4. Fase de finalització de les actuacions.....	8
3. Registre de les comunicacions	11
4. Protecció de dades personals.....	11
5. Seguretat de la informació	12
6. Seguiment i Control del Reglament	13
7. Documentació relacionada	13
8. Aprovació del present Reglament.....	13
9. Historial de versions	14
10. Annexos.....	15
FORMULARI DE DENÚNCIA.....	15

1. Introducció i objecte del Reglament

El CRG té implementat el seu Sistema Intern d'Informació i el seu Canal Intern d'Informació com a via preferent a disposició de tots els empleats, investigadors, tècnics, estudiants, tercers col·laboradors, proveïdors, així com de qualsevol altre tercer, per comunicar possibles incompliments o violacions al que disposa qualsevol de les polítiques internes de l'organització, així com qualsevol infracció o omisió de què tingui coneixement i que pugui suposar una infracció del dret de la Unió Europea o els seus interessos financers o infraccions penals o administratives en el marc jurídic espanyol, tal com s'explica a la Política del Sistema Intern d'Informació del CRG. A tal efecte, s'accedeix al Canal Intern d'Informació a través de l'adreça compliance@crg.eu existint també la possibilitat de remetre les comunicacions o denúncies mitjançant correu postal a la Fundació Centre de Regulació Genòmica, Carrer Doctor Aiguader, número 88, Edifici Parc de Recerca Biomèdica de Barcelona (PRBB), 08003, a l'atenció del Comitè de Compliance, que ha estat designat com a **Responsable** d'aquest sistema.

Adicionalment els informants podran comunicar alertes verbalment al Coordinador/a del Comitè de Compliance, per via telefònica al seu número directe, o mitjançant reunió presencial, dirigint la petició mitjançant alguna de les vies de comunicació anteriorment esmentades, existint també la possibilitat de remetre les comunicacions o denúncies de forma anònima.

A través d'aquest Reglament es desenvolupa el **procediment de gestió de comunicacions**, el qual estableix les previsions necessàries perquè, el Sistema Intern d'Informació compleixi els requisits establerts a 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 (d'ara endavant, "Llei 2/2023, de 20 de febrer").

Si bé el Sistema Intern d'Informació és el mitjà preferent, alternativament tota persona física pot informar davant de l'Autoritat Independent de Protecció de l'Informant (d'ara endavant, "A. A. I.") o davant de les autoritats o òrgans autonòmics corresponents, de la comissió de qualsevol acció o omisió, ja sigui directament o prèvia comunicació a través del referit Canal Intern d'Informació i d'acord amb els termes establerts a la precitada Llei 2/2023, de 20 de febrer.

2. Fases del procediment de gestió de les comunicacions

2.1. Fase de Recepció de comunicacions

Al CRG, la recepció de qualsevol comunicació que es faci a través del Sistema Intern d'Informació serà gestionada pel Responsable del Sistema Intern d'Informació, el qual garantirà en tot moment el respecte a la independència, la confidencialitat, la protecció de dades i el secret de les comunicacions. En tractar-se d'un òrgan col·legiat, el Responsable del Sistema delega al/la Coordinador/a del Comitè de Compliance, que actua com a responsable Delegat, les facultats de gestió del Sistema Intern d'Informació i de tramitació d'expedients d'investigació.

Aquesta comunicació es realitzarà **per escrit**, podent ser de forma anònima o nominal, sent en qualsevol cas confidencial i incloent-hi la descripció dels fets, la identificació de les persones involucrades i, en cas de ser possible, aportant proves que acreditin l'incompliment comunicat i explicant les circumstàncies en què ha tingut accés a aquesta informació.

La comunicació també es pot fer de **forma verbal**, ja sigui presencial o per via telefònica. L'informant podrà sol·licitar una reunió presencial amb el Responsable Delegat del Sistema Intern d'Informació, que se celebrarà dins del termini màxim de 7 (set) dies des de la petició, en la forma que l'organització consideri més convenient i preservant la confidencialitat de la informació. La informació que es rebi a través d'aquesta reunió serà enregistrada, preavisant el comunicador sobre aquesta circumstància. També se l'advertirà sobre el tractament de les seves dades personals d'acord amb el que estableix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, la Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals i en la precitada Llei 2/2023, de 20 de febrer. Alternativament, la reunió es podrà documentar a través d'una transcripció completa i exacta de la conversa. Després d'aquesta derivació, el tractament i la gestió es realitzarà seguint el present Reglament.

Si la comunicació es rebés a través de canals interns diferents dels establerts pel CRG o anés adreçada a membres del personal no responsable del seu tractament, l'organització igualment garantirà la conservació de la confidencialitat, advertint que el seu incompliment implicaria una infracció molt greu de la Llei i que, immediatament, la comunicació seria remesa al Responsable del Sistema.

Una vegada rebuda una comunicació o informació, el Responsable del Sistema és l'òrgan encarregat d'iniciar el procés d'investigació corresponent, si escau, per l'aclariment dels fets objecte de comunicació.

En el termini de 7 (set) dies naturals següents a la recepció de la comunicació s'enviarà un **justificant de recepció** a l'informant. Aquest justificant de recepció s'incorporarà a l'expedient incloent-hi, en tot cas, informació clara i accessible sobre els canals externs d'informació davant de les autoritats competents.

En els casos en què fer un justificant de recepció pogués posar en perill la confidencialitat de la comunicació, per garantir-la, no es realitzarà fins que hagi transcorregut un termini que es consideri prudencial.

Tal com s'esmenta en paràgrafs anteriors, alternativament a aquest Sistema Intern d'Informació preferent, es pot informar davant de l'A. A. I. o davant de les autoritats o òrgans autonòmics corresponents, de la comissió de qualsevol acció o omissió que pugui ser constitutiva d'alguna de les infraccions susceptibles de ser comunicades per mitjà del Sistema Intern d'Informació¹, ja sigui directament o prèvia comunicació a través del referit Sistema, seguint el que disposa l'**Annex 1** sobre els canals d'informació externs.

2.2. Fase d'admissió de comunicacions

Després de rebre la comunicació, el Responsable Delegat li assignarà un **número de registre** que correspondrà amb el seu expedient i una sèrie de codis per anonimitzar tant les dades de l'informant com de l'investigat, els fets, i a qualsevol altre tercer que es pugui veure afectat per la comunicació.

En primer lloc, el Comitè de Compliance (com a òrgan col·legiat Responsable del Sistema Intern d'Informació) comprovarà que ni el Responsable Delegat, ni cap altre membre del propi Comitè, ni cap membre de les seves respectives àrees departamentals de treball, es troben implicats en aquesta comunicació. En cas contrari, s'exigirà la inhibició de la persona i/o àrea implicada i se substituirà als efectes de garantir la deguda imparcialitat. Aquesta circumstància es deixarà per escrit a l'expedient. La regla sobre aquest conflicte serà:

1. Si hi està implicat el Responsable Delegat o una persona de la seva mateixa àrea de treball, assumirà la investigació un altre membre del Comitè.

¹ Al respecte veure allò indicat a l'Apartat 3, "Del contingut de les comunicacions", de la Política del Sistema Intern d'Informació.

2. Si s'hi troben implicats altres membres del Comitè o persones de les respectives àrees de treball, seguirà la investigació el Responsable Delegat.

3. Si hi estan implicats tots els membres del Comitè, seguirà la investigació el Substitut designat per l'òrgan de govern, per tirar endavant aquests casos particulars.

Aquestes substitucions i el nou nomenament s'han de fer constar per escrit en Acta i a l'obertura de l'expedient.

Finalment, després de la recepció de la comunicació, el Responsable del Sistema haurà de deixar constància mitjançant acta de la següent informació:

- Les dades objectives de la comunicació: fets objecte de la denúncia, noms dels autors o participants en els fets objecte de denúncia, dates, quantitats, llocs, contactes, i informació associada als fets denunciats, aportats pel comunicador/informant.
- Les dades subjectives: opinions, idees i apreciacions del comunicador/informant que aquest consideri necessaris en descriure la comunicació.
- Valoració del Responsable del Sistema sobre si la comunicació està associada a una conducta delictiva o si és una simple reclamació o suggeriment relacionat amb la millora d'una àrea del centre, la situació laboral, etc.

Si el Responsable del Sistema advertís que els fets informats poguessin ser indiciàriament constitutius de delictes, remetrà la informació de forma immediata a la Gerència i Direcció del CRG i al seu òrgan de govern, que haurà de decidir sobre la seva remissió a l'autoritat pública competent.

2.3. Fase d'investigació

En cas que s'admetés a tràmit la comunicació, la regla general és que la investigació serà dirigida pel Responsable del Sistema i desenvolupada per aquest².

En cas que sigui possible, es podrà demanar a la persona informant que porti informació addicional necessària per al transcurs de la investigació a què hagi donat lloc la seva comunicació.

En aquesta etapa es notificarà i **entrevistarà a l'investigat**, comunicant-li el seu dret a ser informat sobre les accions o omissions que se li atribueixen, i també pot igualment exercir el seu dret a ser escoltat, sense que en cap cas se li comuniqui la identitat de l'informant.

² Excepte en els casos de conflicte d'interès.

També se citarà i **entrevistarà als tercers implicats** (si n'hi hagués) a l'efecte que expliquin i indiquin les al·legacions que considerin oportunes. Es realitzaran totes les diligències d'investigació que siguin necessàries per a les parts i es deixarà constància documental de tot allò actuat a l'expedient.

En cas que es tracti d'un tema relacionat amb la mala pràctica científica, cal atènyer-se al que estableix el procediment en casos de sospita de mala pràctica científica del CRG.

Les diligències que es practiquin cap a tercers o altres òrgans o àrees del CRG s'han de fer mantenint l'**anonimat del comunicador/informant i de l'investigat**, així com els motius de la comunicació.

En tot moment es garantirà la **confidencialitat** de la informació, així com la **presumpció d'innocència i el respecte a l'honor** de totes les persones que es vegin afectades.

Durant aquesta etapa el Responsable del Sistema:

1r.- Investigarà els fets comunicats i, concretament:

- Els elements objectius i subjectius aportats pel comunicador/informant, prioritant els elements objectius recolzats amb documentació que acrediti, total o parcialment, els fets comunicats.
- La reputació, serietat i fiabilitat del comunicador/informant.
- Les al·legacions i proves de defensa aportades per l'investigat.
- La prova practicada amb tercers, o amb altres òrgans, àrees o departaments de l'organització.

2n.- Analitzarà i valorarà les possibles conseqüències que els fets comunicats puguin produir.

En primer lloc, el Responsable del Sistema haurà de comprovar si aquests fets es van produir a causa d'una manca important de controls interns al CRG. En aquest cas, proposarà mesures pal·liatives i preventives urgents per evitar nous riscos.

Si el Responsable del Sistema ho considera convenient, podrà sol·licitar assistència a la Gerència i/o Direcció per a la investigació. No obstant això, si en el fet denunciat hi estigués implicat un membre de la Gerència i/o Direcció, el Comitè de Compliance s'abstindrà de demanar la col·laboració d'aquest membre.

En segon lloc, si la gravetat, especialitat o complexitat dels fets ho aconsella, el Responsable del Sistema podrà nomenar un altre responsable de l'àrea de gestió o científica o una tercera persona especialitzada per col·laborar en la investigació. Si com a conseqüència dels fets comunicats es poguessin produir pèrdues d'actius, el Responsable del Sistema haurà d'adoptar les mesures

tendents a aturar o mitigar aquestes pèrdues o danys. Si es pogués produir la pèrdua o eliminació de proves rellevants per a la investigació, de forma prèvia a l'inici de la mateixa, el Responsable del Sistema s'encarregarà de garantir les evidències. El Responsable del Sistema també valorarà la pertinència d'informar els òrgans de govern sobre aquesta comunicació. Finalment, comprovarà si hi ha la possibilitat que s'hagin causat perjudicis a tercers en aquest cas, valorarà l'entitat del perjudici i la necessitat d'informar el tercer perjudicat.

El termini per dur a terme la investigació i donar una resposta a l'informant sobre les actuacions que s'hagin portat a terme, així com el resultat de les mateixes, dependrà de la gravetat dels fets comunicats i les seves potencials conseqüències, quedant a criteri i risc del Responsable del Sistema la durada d'aquesta etapa. No obstant això, d'acord amb el que estableix l'article 9.2.d) de 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, aquest termini no podrà ser superior a 3 (tres) mesos a comptar de la recepció de la comunicació o, si no es va remetre un justificant de recepció a l'informant, 3 (tres) mesos a partir del venciment del termini de 7 (set) dies després d'efectuar-se la comunicació³. Això, llevat dels casos d'especial complexitat, el termini del qual es pot estendre fins a un màxim de 3 (tres) mesos addicionals més.

Si la comunicació conté dades personals de tercers diferents de l'investigat (per exemple, testimonis, proveïdors, etc.), el Responsable del Sistema deixarà constància per escrit que s'haurà de suprimir tota aquella informació personal facilitada que no sigui necessària per a la investigació, i procedir a informar els tercers les dades dels quals hagin de ser tractades. La informació ha de complir els requisits informatius de la normativa de protecció de dades, i ha d'ometre d'aquesta informació la identitat de l'informant, que s'ha de mantenir confidencial.

Totes aquestes notificacions es decidiran pel Responsable del Sistema i constaran per escrit a l'expedient.

2.4. Fase de finalització de les actuacions

Després de la investigació de la comunicació i amb la documentació acreditativa que hagi servit per esclarir els fets, s'elaborarà un **Veredict** o **Resolució** amb el següent contingut:

- Descripció dels fets: número de registre de la comunicació; data de la comunicació; fets comunicats; parts intervinents; documentació aportada al llarg de la investigació per ambdues parts (comunicador/informant i investigat), per altres òrgans, àrees o

³ Aquests terminis es compliran, en tot cas, sense perjudici d'allò disposat a la normativa laboral o conveni col·lectiu aplicable a cada supòsit, els terminis dels quals prevaldran en cas de contradicció o de potencial infracció normativa.

departaments de l'organització, per tercers; entrevista amb l'investigat i/o amb tercers, etc.

- Anàlisi i valoració de les proves obtingudes.
- En cas que es comprovi efectivament la irregularitat comunicada, el Responsable del Sistema dedicarà un apartat del veredicta per efectuar les recomanacions que consideri necessàries implementar per millorar els controls i protocols interns que hagin estat deficients en aquesta ocasió.
- Resolució: prèvia aprovació per part de la Direcció i Gerència del CRG, o de l'òrgan de govern del CRG en cas que la decisió hagi de ser aprovada per aquest, aquesta resolució haurà de ser fonamentada i contenir els motius pels quals es procedeix a l'ARXIU SENSE SANCIO o ARXIU AMB SANCIO.

I. ARXIU SENSE SANCIO: Després de la investigació, es pot decidir que la infracció denunciada és manifestament menor i no requereix més seguiment, sinó que procedirà al seu ARXIU. També correspondrà l'arxiu en casos de denúncies reiterades que no continguin informació nova i significativa sobre infraccions ja comunicades amb anterioritat i respecte de les quals ja hagi conclòs el procediment, llevat que es donin noves circumstàncies de fet o de Dret que justifiquin un seguiment diferent. En aquests casos, s'haurà de comunicar a l'informant la resolució i aquesta haurà d'estar motivada.

Així mateix, internament, s'adoptaran accions per a garantir que en el futur no es repeteixin els fets denunciats. Aquestes accions poden incloure la implementació de controls addicionals, la revisió de polítiques i procediments, i la realització de capacitacions per a millorar la conducta i el compliment normatiu i ètic.

II. ARXIU AMB SANCIO: el Responsable del Sistema podrà proposar l'aplicació d'una sanció, però la decisió recaurà en la Gerència del CRG en coordinació amb les àrees de Persones i Assessoria Jurídica, d'acord amb els procediments indicats per a l'aplicació de sancions laborals a l'organització.

III. COMUNICACIO A LES AUTORITATS: Si la comunicació rebuda *a priori* sembla tenir relació amb la comissió d'un delicta, el Responsable del Sistema haurà de reportar-la immediatament a la Gerència del CRG a efectes de la valoració de la denúncia davant les autoritats competents. D'altra banda, si els fets denunciats ja són investigats per autoritats judicials o policials, el CRG cooperarà plenament

i monitoritzarà els resultats d'aquestes investigacions. Això permetrà avaluar qualsevol impacte addicional i prendre les mesures corresponents d'acord amb la llei.

En aquest sentit, la Llei d'Enjudiciament Criminal espanyola contempla al seu article 259 que qui presenciés la perpetració de qualsevol delictes públic⁴ estarà obligat a posar-ho immediatament en coneixement del Jutge d'instrucció, de pau, comarcal o municipal, o funcionari fiscal més proper al lloc on es trobés⁵.

Per la seva part, el deure de denunciar a les autoritats competents s'incrementa respecte a determinats delictes que distingeix la norma penal. A aquest respecte, el Codi Penal espanyol, en el seu art. 450, contempla "*l'omissió dels deures d'impedir delictes o de promoure la seva persecució*", sancionant a qui no impedeixi la comissió d'un delictes que afecti les persones en la seva vida, integritat o salut, llibertat o llibertat sexual, podent fer-ho amb la seva intervenció immediata i sense risc propi o aliè, i a qui, podent fer-ho, no acudeixi a l'autoritat o als seus agents perquè impedeixin un d'aquests delictes i de la qual propera o actual comissió en tingui coneixement.

En quant al **règim sancionador**, si una vegada finalitzada la investigació dels fets, se'n confirmés la veracitat, el CRG prendrà totes les mesures necessàries per posar fi al fet denunciat i, si escau i tenint en compte les característiques del fet, aplicarà les accions que consideri oportunes recollides al règim disciplinari i la legislació laboral vigent, d'acord amb la legislació penal precitada.

Les mesures que es puguin imposar internament no limitaran, en cap moment, l'exercici de les accions legals que pugui dur a terme l'organització.

En tots els casos, es **notificarà la Resolució** al comunicador/informant i a l'investigat, tenint en compte el termini màxim de 3 (tres) mesos des de la recepció de la comunicació. No es notificarà a l'informant quan aquest hi hagi renunciat, no es disposi de dades de contacte o es tracti d'un informant anònim.

⁴ La classificació d'un delictes com a públic té relació amb qui impulsi la seva persecució (d'ofici o per la part perjudicada), i els **delictes públics** són perseguibles d'ofici sense necessitat de la denúncia prèvia pel perjudicat. A més dels delictes contra la vida i la llibertat, al catàleg de delictes que generen responsabilitat penal de la persona jurídica trobem, a títol exemplificatiu els delictes públics següents: l'estafa, suborn, tràfic d'influències, blanqueig de capitals, finançament del terrorisme, delictes contra la Hisenda Pública i la Seguretat Social, delictes contra el medi ambient i els recursos naturals, delictes contra l'ordenació del territori, contra els drets fonamentals i llibertats públiques, contraban, entre d'altres). Per contra, són **delictes privats** les calúmnies i injúries entre particulars (la justícia només podrà actuar quan la persona perjudicada presenti una denúncia o querella) i els **delictes semipúblics** són perseguibles d'ofici un cop inicialment el perjudicat hagi fet la denúncia (delictes de descobriment i revelació de secrets, delictes contra la propietat intel·lectual, agressions, assetjaments i abusos sexuals, confrontació), entre d'altres.

⁵ Segons redacció literal actual de l'art. 259 de la Llei d'Enjudiciament Criminal espanyola.

Una vegada s'hagi adoptat una Resolució sobre la comunicació, el Responsable del Sistema ordenarà l'ARXIU i el BLOQUEIG DELS REGISTRES de la mateixa, pel termini que consideri prudent fins a la seva total eliminació, respectant en tot cas la legislació vigent en matèria de protecció de dades personals.

En cas d'ARXIU AMB SANCIÓ, la notificació a l'investigat contindrà l'adopció de les mesures contractuals, disciplinàries o judicials que s'hagin d'adoptar.

El CRG garanteix que mai es prendran represàlies contra qualsevol persona que de bona fe posi en coneixement de l'organització la comissió d'un fet delictiu, col·labori en la seva investigació o ajudi a resoldre'l. Aquesta garantia no arriba a aquells que actuïn de mala fe amb ànim de difondre informació falsa o de perjudicar les persones. Contra aquestes conductes il·lícites, el CRG adoptarà les mesures legals o disciplinàries que procedeixin.

3. Registre de les comunicacions

El Responsable del Sistema compta amb un llibre registre de les informacions rebudes i les investigacions internes a què hagin donat lloc, servint-li per emmagatzemar i/o recuperar informació clau sobre cada incidència, incloent la data i font de la comunicació original, el pla de la investigació, resultats d'entrevistes o qualsevol altre procediment d'investigació, tasques pendents, resolució final, així com la cadena de custòdia de qualsevol evidència o informació clau.

4. Protecció de dades personals

Tal com s'exposa a la Política del Sistema Intern d'Informació del CRG, els tractaments de dades personals que derivin de l'aplicació d'aquesta Política i del present Procediment de Gestió de Comunicacions, es regeixen pel que disposa el Títol VI de Llei 2 /2023, de 20 de febrer, pel que disposa el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 de abril de 2016, la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals, la Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a fins de prevenció, detecció, investigació i enjudiciament d'infraccions penals i d'execució de sancions penals.

Considerant el principi de minimització de les dades del Reglament General de Protecció de Dades recollit a la Llei 2/2023, de 20 de febrer, el CRG únicament tractarà les dades personals necessàries per al coneixement i investigació de les accions o omissions objecte d'investigació a

través del Sistema Intern. En conseqüència, en la mesura que les dades personals demanades no es considerin de coneixement necessari o que s'acredités que no es tracta d'informació veraç, el CRG procedirà a la seva supressió en els termes establerts a l'article 32 de la Llei 3/ 2018⁶.

Així mateix, el CRG únicament podrà tractar dades de categoria especial⁷ en la mesura que aquestes resultin necessàries per a l'adopció de les corresponents mesures correctores o els procediments sancionadors que eventualment s'hagin de cursar, i, en cas contrari, procedir a la seva immediata supressió en els termes esmentats anteriorment.

En darrer lloc, el CRG haurà de garantir que els subjectes afectats pel tractament de dades personals dut a terme com a conseqüència de la investigació puguin exercir els drets d'accés, rectificació de dades inexactes, supressió, limitació, portabilitat i oposició, tenint en compte que el dret d'accés no podrà incloure informació sobre l'informant i que el dret d'oposició de les persones investigades es podrà denegar per motius legítims.

5. Seguretat de la informació

El canal de comunicacions electrònic tindrà assignat un Administrador del sistema al departament de TIC del CRG, encarregat d'establir i personalitzar la seguretat necessària del sistema, incloent la restricció en l'accés i habilitat de bloquejar els registres, els quals no haurien de poder ser modificats un cop hagin estat registrats. Es preveu una gestió i administració especial per l'eliminació dels registres del sistema.

Adicionalment, la bústia serà capaç d'auditar l'accés a registres individuals i registrar la data, hora i nom d'usuari, incloent qualsevol modificació realitzada sobre els registres.

Amb la finalitat que les dades conservades siguin el més exactes possible, es procedirà a la immediata cancel·lació de les comunicacions que no fossin pertinents i d'aquelles respecte de les quals, una vegada investigats els fets, es concloués que no són exactes o veraces.

A més, la bústia de comunicacions permetrà al Responsable del Sistema emmagatzemar i/o recuperar informació clau sobre cada incidència, incloent la data i font de la comunicació original, el pla de la investigació, resultats d'entrevistes o qualsevol altre procediment d'investigació,

⁶ Quan sigui procedent la supressió, ONECHAIN bloquejarà les dades adoptant totes les mesures que siguin necessàries per impedir el tractament de la informació bloquejat (llevat de la posada a disposició a les autoritats judicials, el Ministeri fiscal o les administracions públiques competents per a l'exigència de possibles responsabilitats) durant el temps necessari per guardar evidència del funcionament del sistema que, considerant els terminis de prescripció indicats a la Llei 2/2023, de 20 de febrer, es fixa a 3 anys. Cal destacar que l'obligació de bloqueig i conservació no procedeix de dades personals contingudes en comunicacions no investigades, únicament podent ser conservades de forma anonimitzada.

⁷ Dades personals que revelin l'origen ètnic o racial, opinions polítiques, conviccions religioses o filosòfiques, o l'afiliació sindical, i el tractament de dades genètiques, biomètriques, dades relatives a la salut, a la vida sexual o les orientacions sexuals d'una persona.

tasques pendents, resolució final, així com la cadena de custòdia de qualsevol evidència o informació clau.

Finalment, s'ha de recordar que en tot moment es mantindrà la confidencialitat del denunciant i denunciat, les identitats dels quals no seran revelades fora de l'àmbit del Comitè de Compliance com a Responsable del Sistema.

6. Seguiment i Control del Reglament

La implementació, compliment i actualització d'aquest Reglament serà supervisat pel Comitè de Compliance del CRG.

El present Reglament es revisarà i/o modificarà per part del Comitè de Compliance, el qual en podrà externalitzar el servei a professionals especialistes, sempre que es produeixin canvis rellevants en l'organització, en l'estructura de control o en l'activitat desenvolupada per l'organització que ho aconsellin, que hi hagi modificacions legals o que es posi de manifest la necessitat d'actualitzar les seves disposicions.

Aquest Reglament es revisarà, encara que no es produeixi cap de les circumstàncies anteriorment descrites, al menys de forma biennal.

7. Documentació relacionada

1. [Codi de Conducta i Bon Govern del CRG](#)
2. [Pla de Mesures Antifrau](#)
3. [Manual de Compliance Penal](#)
4. [Política de Compliance Penal del CRG](#)
5. [Política del Sistema Intern d'Informació del CRG](#)

8. Aprovació del present Reglament

El Reglament del Canal Intern d'Informació del CRG ha estat aprovat conforme s'indica a l'historial de versions que segueix a continuació i podrà ser modificat amb la finalitat de mantenir en tot moment la cultura de compliment dins de l'organització, materialitzada en els principis de

transparència, responsabilitat i prudència envers tercers i envers els seus propis membres i socis de negoci.

9. Historial de versions

Versió	Data	Aprovat per	Motiu del canvi
V.1	28/11/2022	Coordinador del Comitè de Compliance i Gerent del CRG	
	15/12/2022	Patronat del CRG	
V.2	29/11/2024	Coordinador del Comitè de Compliance i Gerent del CRG	Adaptació a la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informen sobre infraccions normatives i de lluita contra la corrupció (en quant al contingut de les fases del procediment de gestió de les comunicacions, les funcions del Responsable del Sistema, el registre de comunicacions i els aspectes de protecció de dades personals).
	19/12/2024	Patronat del CRG	

10. Annexos

FORMULARI DE DENÚNCIA

DADES IDENTIFICATIVES DEL DENUNCIANT:

Nom i cognoms del denunciant	
Direcció de correu electrònic	
Direcció de correu postal (opcional)	
Telèfon (opcional)	
Àrea o departament del CRG en el que presta els seus serveis	

DENÚNCIA

Descripció de la denúncia (si és possible, adjuntar evidències o documents justificatius de la denúncia)	Si us plau, identifiquei les persones (físiques i/o jurídiques) que han participat en els fets, en quin concepte, el tipus de relació existent amb el denunciat i si existeixen més persones coneixedores dels fets (indicar qui).
	Si us plau, indiquei el motiu de la denúncia (fets i indicis), marc temporal en el que s'han dut a terme, àrea/es del CRG afectada/es, i tots aquells fets que consideri oportuns.

Existeix algun conflicte d'interès amb algun dels membre del Comitè de Compliance del CRG?

Sí Assenyali amb qui: _____

No

Canal extern d'informació-Autoritat Independent de Protecció del Denunciant, A.A.I.

Totes les persones físiques poden informar **davant de l'A.A.I. estatal o davant de les autoritats o òrgans autonòmics corresponents** a través dels canals externs degudament habilitats al respecte, de la comissió de qualssevol accions o omissions a què es refereix el Sistema Intern d'Informació del CRG, ja sigui directament o bé prèvia comunicació a través del Canal d'Informació Intern del CRG.