REGLAMENTO DEL CANAL

INTERNO DE INFORMACIÓN DEL CRG

Índice

1. Introducción y objeto del Reglamento

El CRG tiene implementado su Sistema Interno de Información y su Canal Interno de Información como cauce preferente a disposición de todos los empleados, investigadores, técnicos, estudiantes, terceros colaboradores, proveedores, así como de cualquier otro tercero, para comunicar posibles incumplimientos o violaciones a lo dispuesto en cualquiera de las políticas internas de la organización, así como cualquier infracción u omisión de la que tenga conocimiento y que pueda suponer una infracción del derecho de la Unión Europea o sus intereses financieros o infracciones penales o administrativas en el marco jurídico español, tal como se explica en la Política del Sistema Interno de Información del CRG.

Para ello, se accede a su Canal Interno de Información a través de la dirección compliance@crg.eu existiendo también la posibilidad de remitir las comunicaciones o denuncias mediante correo postal a la Fundació Centre de Regulació Genòmica, Calle Doctor Aiguader, número 88, Edifici Parc de Recerca Biomédica de Barcelona (PRBB), 08003, a la atención del Comité de Compliance, quien ha sido designado como **Responsable** de este Sistema. Adicionalmente los informantes podrán comunicar alertas verbalmente al Coordinador/a del Comité de Compliance, por vía telefónica a su número directo, o mediante reunión presencial, dirigiendo la petición mediante alguna de las vías de comunicación anteriormente citadas, existiendo también la posibilidad de remitir las comunicaciones o denuncias de forma anónima.

A través de este Reglamento se desarrolla el **procedimiento de gestión de comunicaciones**, el cual establece las previsiones necesarias para que, el Sistema Interno de Información cumpla con los requisitos establecidos en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (en adelante, “Ley 2/2023, de 20 de febrero”).

Si bien el Sistema Interno de Información es el medio preferente, alternativamente toda persona física puede informar ante la Autoridad Independiente de Protección del Informante (en adelante, "A. A. I.") o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualquier acción u omisión, ya sea directamente o previa comunicación a través del referido Canal Interno de Información y de acuerdo con los términos establecidos en la precitada Ley 2/2023, de 20 de febrero.

2. Fases del procedimiento de gestión de las comunicaciones

2.1. Fase de Recepción de comunicaciones

En el CRG, la recepción de toda comunicación que se haga a través del Sistema Interno de Información será gestionada por el Responsable del Sistema Interno de Información, el cual garantizará en todo momento el respeto a la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones. Al tratarse de un órgano colegiado, el Responsable del Sistema delega en el/la Coordinador/a del Comité de Compliance, quien actúa como Responsable Delegado, las facultades de gestión del Sistema Interno de Información y de tramitación de expedientes de investigación.

Dicha comunicación se realizará **por escrito**, pudiendo ser de forma anónima o nominal, siendo en cualquier caso confidencial e incluyendo la descripción de los hechos, la identificación de las personas involucradas y, en caso de ser posible, aportando pruebas que acrediten el incumplimiento comunicado y explicando las circunstancias en las que ha tenido acceso a dicha información.

La comunicación también puede realizarse de **forma verbal**, ya sea presencial o por vía telefónica. El informante podrá solicitar una reunión presencial con el Responsable Delegado del Sistema Interno de Información, que se celebrará dentro del plazo máximo de 7 (siete) días desde la petición, en la forma en que la organización considere más conveniente y preservando la confidencialidad de la información. La información que se reciba a través de esta reunión será grabada, preavisando al comunicador sobre dicha circunstancia. También se le advertirá sobre el tratamiento de sus datos personales de acuerdo con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales y en la precitada Ley 2/2023, de 20 de febrero. Alternativamente, la reunión podrá documentarse a través de una transcripción completa y exacta de la conversación. Tras esta derivación, su tratamiento y gestión se realizará siguiendo el presente Reglamento.

Si la comunicación se recibiese a través de canales internos distintos a los establecidos por el CRG o fuese dirigida a miembros del personal no responsable de su tratamiento, la organización igualmente garantizará la conservación de la confidencialidad, advirtiendo que su incumplimiento

implicaría una infracción muy grave de la Ley y que, inmediatamente, la comunicación sería remitida al Responsable del Sistema.

Una vez recibida una comunicación o información, el Responsable del Sistema es el órgano encargado de iniciar el proceso de investigación correspondiente, en su caso, para el esclarecimiento de los hechos objeto de comunicación.

En el plazo de 7 (siete) días naturales siguientes a la recepción de la comunicación se enviará un **acuse de recibo** al informante. Este acuse de recibo se incorporará al expediente incluyendo, en todo caso, información clara y accesible sobre los canales externos de información ante las autoridades competentes.

En los casos en que realizar un acuse de recibo pudiera poner en peligro la confidencialidad de la comunicación, para garantizarla, no se realizará hasta que haya transcurrido un plazo que se considere prudencial.

Tal y como se menciona en párrafos anteriores, alternativamente a este Sistema Interno de Información preferente, se puede informar ante la A. A. I. o ante las autoridades u órganos autonómicos correspondientes, de la comisión de cualquier acción u omisión que pueda ser constitutiva de alguna de las infracciones susceptibles de ser comunicadas por medio del Sistema Interno de Información[1], ya sea directamente o previa comunicación a través del referido Sistema, siguiendo lo dispuesto en el **Anexo 1** sobre los canales externos de información.

2.2. Fase de admisión de comunicaciones

Tras recibir la comunicación, el Responsable Delegado le asignará un **número de registro** que corresponderá con su expediente y una serie de códigos para anonimizar tanto los datos del informante como del investigado, los hechos, y a cualquier otro tercero que pueda verse afectado por la comunicación.

En primer lugar, el Comité de Compliance (como órgano colegiado Responsable del Sistema Interno de Información) comprobará que ni el Responsable Delegado, ni ningún otro miembro del propio Comité, ni ningún miembro de sus respectivas áreas departamentales de trabajo, se encuentran implicados en dicha comunicación. En caso contrario, se exigirá la inhibición de la persona y/o área implicada y se sustituirá a efectos de garantizar la debida imparcialidad. Esta circunstancia se dejará por escrito en el expediente. La regla sobre este conflicto de interés será:

[1] Al respecto ver lo indicado en el Apartado 3, "Del contenido de las comunicaciones", de la Política del Sistema Interno de Información.

1. Si se encuentra implicado el Responsable Delegado o una persona de su misma área de trabajo, asumirá la investigación otro miembro del Comité.
2. Si se encuentran implicados otros miembros del Comité o personas de sus respectivas áreas de trabajo, seguirá la investigación el Responsable Delegado.
3. Si se encuentran implicados todos los miembros del Comité, seguirá la investigación el Sustituto designado por el órgano de gobierno, para llevar adelante estos particulares casos.

Dichas sustituciones y nuevo nombramiento se harán constar por escrito en Acta y en la apertura del expediente.

Finalmente, tras la recepción de la comunicación, el Responsable del Sistema dejará constancia de la siguiente información, entre otras:

- Los datos objetivos de la comunicación: hechos objeto de la denuncia, nombres de los autores o participantes en los hechos objeto de denuncia, fechas, cantidades, lugares, contactos, e información asociada a los hechos denunciados, que aporte el comunicador/informante.
- Los datos subjetivos: opiniones, ideas y apreciaciones del comunicador/informante que éste considere necesarios al describir la comunicación.
- Valoración del Responsable del Sistema sobre si la comunicación acerca de si la comunicación está asociada a una conducta delictiva o si es una mera reclamación o sugerencia relativa a mejorar un área del centro, la situación laboral, etc.

Si el Responsable del Sistema advirtiese que los hechos informados pudieran ser indiciariamente constitutivos de delito, remitirá la información de forma inmediata a la Gerencia y Dirección del CRG y a su órgano de gobierno, quien deberá decidir sobre su remisión a la autoridad pública competente.

2.3. Fase de investigación

En el supuesto de que se admitiera a trámite la comunicación, la regla general es que la investigación será dirigida por el Responsable del Sistema y desarrollada por éste[2].

[2] Salvo en los casos de conflicto de intereses.

En caso de que sea posible, se podrá pedir a la persona informante que aporte información adicional necesaria para el transcurso de la investigación a la que haya dado lugar su comunicación.

En esta etapa se notificará y se **entrevistará al investigado**, comunicándole su derecho a ser informado sobre las acciones u omisiones que se le atribuyen, pudiendo igualmente ejercer su derecho a ser oído, sin que en ningún caso se le comunique la identidad del informante.

También se citará y **entrevistará a los terceros implicados** (si los hubiere) a efectos de que expliquen e indiquen las alegaciones que consideren oportunas. Se realizarán cuantas diligencias de investigación sean necesarias para las partes y se dejará constancia documental de todo lo actuado en el expediente.

En el caso de que se trate de un tema relacionado con la mala práctica científica, se estará a lo establecido en el Procedimiento en casos de sospecha de mala práctica científica del CRG.

Las diligencias que se practiquen hacia terceros u otros órganos o áreas del CRG deberán realizarse manteniendo el **anonimato del comunicador/informante y del investigado**, así como los motivos de la comunicación.

En todo momento se garantizará la **confidencialidad** de la información, así como la **presunción de inocencia y el respeto al honor** de todas las personas que se vean afectadas.

Durante esta etapa el Responsable del Sistema:

1º.- Investigará los hechos comunicados y, concretamente:

- Los elementos objetivos y subjetivos aportados por el comunicador/informante, priorizando los elementos objetivos apoyados con documentación que acredite, todo o en parte, los hechos comunicados.
- La reputación, seriedad y fiabilidad del comunicador/informante.
- Las alegaciones y pruebas de defensa aportadas por el investigado.
- La prueba practicada con terceros, o con otros órganos o áreas relacionados.

2º.- Analizará y valorará las eventuales consecuencias que los hechos comunicados puedan producir:

En primer lugar, el Responsable del Sistema comprobará si estos hechos se produjeron por una importante falta de controles internos en el CRG. En su caso, propondrá medidas paliativas y preventivas urgentes para evitar nuevos riesgos.

Si el Responsable del Sistema lo estima conveniente, podrá solicitar asistencia a la Gerencia y/o Dirección para la investigación. Sin embargo, si en el hecho denunciado estuviese involucrado un miembro de la Gerencia y/o Dirección, el Comité de Compliance se abstendrá de pedir la colaboración de ese miembro.

En segundo lugar, si la gravedad, especialidad o complejidad de los hechos lo aconseja, el Responsable del Sistema podrá nombrar a otro responsable del área de gestión o científica o a una tercera persona especializada para colaborar en la investigación. Si como consecuencia de los hechos comunicados se pudieran producir pérdidas de activos, el Responsable del Sistema adoptará las medidas tendentes a detener o mitigar dichas pérdidas o daños. Si se puede producir una fuga o destrucción de pruebas relevantes para la investigación, de forma previa al inicio de la misma, el Responsable del Sistema se encargará de asegurarse evidencias. El Responsable del Sistema también valorará la pertinencia de informar a los órganos de gobierno sobre esta comunicación. Por último, comprobará si existe la posibilidad de que se hayan causado perjuicios a terceros en cuyo caso, valorará la entidad del perjuicio y la necesidad de informar al tercero perjudicado.

El plazo para desarrollar la investigación y dar una respuesta al informante sobre las actuaciones que se hayan llevado a cabo, así como el resultado de las mismas, dependerá de la gravedad de los hechos comunicados y sus potenciales consecuencias, quedando a criterio y riesgo del Responsable del Sistema la duración de esta etapa. No obstante, de acuerdo con lo establecido por el artículo 9.2. d) de la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, este plazo no podrá ser superior a 3 (tres) meses a contar desde la recepción de la comunicación o, si no se remitió un acuse de recibo al informante, 3 (tres) meses a partir del vencimiento del plazo de 7 (siete) días después de efectuarse la comunicación[3]. Esto, salvo en los casos de especial complejidad, cuyo plazo podrá extenderse hasta un máximo de otros 3 (tres) meses adicionales.

[3] Estos plazos se cumplirán, en todo caso, sin perjuicio de lo dispuesto en la normativa laboral o convenio colectivo aplicable a cada supuesto, cuyos plazos prevalecerán en caso de contradicción o de potencial infracción normativa.

Si la comunicación contiene datos personales de terceros diferentes al investigado (por ejemplo, testigos, proveedores, etc.), el Responsable del Sistema dejará constancia por escrito de que deberá suprimirse toda aquella información personal facilitada que no sea necesaria para la investigación, y proceder a informar a los terceros cuyos datos deban ser tratados. La información cumplirá con los requisitos informativos de la normativa de protección de datos, omitiendo de esta información la identidad del informante, que deberá mantenerse confidencial.

Todas estas notificaciones se decidirán por el Responsable del Sistema y constarán por escrito en el expediente.

2.4. Fase de finalización de las actuaciones

Tras la investigación de la comunicación y con la documentación acreditativa que sirviera para esclarecer los hechos, se elaborará un **Veredicto o Resolución** con el siguiente contenido:

- Descripción de los hechos: n.º de registro de la comunicación; fecha de la comunicación; hechos informados; partes intervinientes; documentación aportada a lo largo de la investigación por ambas partes (comunicador/informante e investigado), por otros órganos, áreas o departamentos de la organización o por terceros; entrevista con el investigado y/o con terceros, etc.
- Análisis y valoración de las pruebas obtenidas.
- En caso de que, efectivamente, se compruebe la irregularidad comunicada, el Responsable del Sistema dedicará un apartado del veredicto para efectuar las recomendaciones que considere necesario implementar para mejorar los controles y protocolos internos que hayan sido deficientes en esta ocasión.
- Resolución: previa aprobación por parte de la Dirección y Gerencia del CRG, o del órgano de gobierno del CRG en caso de que la decisión deba ser aprobada por el mismo, esta resolución deberá ser fundamentada y contener los motivos por los que se proceder al ARCHIVO SIN SANCIÓN o ARCHIVO CON SANCIÓN.

I. **ARCHIVO SIN SANCIÓN**: Tras la investigación, si se concluye que la infracción comunicada es manifiestamente menor y no requiere más seguimiento, se procederá a su ARCHIVO. También corresponderá el archivo en los supuestos de comunicaciones reiteradas que no contengan información nueva y significativa sobre infracciones ya comunicadas con anterioridad y cuyo procedimiento de investigación ya haya concluido, a menos que se den nuevas circunstancias de

hecho o de derecho que justifiquen un seguimiento distinto. En estos casos, deberá comunicarse al informante la resolución y ésta deberá estar motivada. Asimismo, internamente, se adoptarán acciones para garantizar que en el futuro no se repitan los hechos denunciados. Estas acciones pueden incluir la implementación de controles adicionales, la revisión de políticas y procedimientos, y la realización de capacitaciones para mejorar la conducta y el cumplimiento normativo y ético.

II. ARCHIVO CON SANCIÓN: el Responsable del Sistema podrá proponer la aplicación de una sanción, pero la decisión recaerá en la Gerencia del CRG en coordinación con las áreas de Personas y Asesoría Jurídica, de conformidad con los procedimientos indicados para la aplicación de sanciones laborales en la organización.

III. COMUNICACIÓN A LAS AUTORIDADES: Si la comunicación recibida *a priori* pareciera tener relación con la comisión de un delito, el Responsable del Sistema la reportará de inmediato a la Gerencia del CRG a efectos de la valoración de su denuncia ante las autoridades competentes. Por otra parte, si los hechos denunciados ya están siendo investigados por autoridades judiciales o policiales, el CRG cooperará plenamente y monitorizará los resultados de dichas investigaciones. Esto permitirá evaluar cualquier impacto adicional y tomar las medidas correspondientes en consonancia con la ley.

En este sentido, la Ley de Enjuiciamiento Criminal española contempla en su art. 259 que quien presenciare la perpetración de cualquier delito público[4] está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal, o funcionario fiscal más próximo al sitio en que se hallare[5].

[4] La clasificación de un delito como público tiene relación con quien impulse su persecución (de oficio o por la parte perjudicada), siendo los **delitos públicos** perseguibles de oficio sin necesidad de la previa denuncia por el perjudicado. Además de los delitos contra la vida y la libertad, en el catálogo de delitos que generan responsabilidad penal de la persona jurídica encontramos, a título ejemplificativo los siguientes delitos públicos: la estafa, cohecho, tráfico de influencias, blanqueo de capitales, financiación del terrorismo, delitos contra la Hacienda Pública y la Seguridad Social, delitos contra el medio ambiente y los recursos naturales, delitos contra la ordenación del territorio, contra los derechos fundamentales y libertades públicas, contrabando, entre otros). Por el contrario, son **delitos privados** las calumnias e injurias entre particulares (la justicia sólo podrá actuar cuando la persona perjudicada presente una denuncia o querella) y los **delitos semipúblicos** son perseguibles de oficio una vez inicialmente el perjudicado haya hecho la denuncia (delitos de descubrimiento y revelación de secretos, delitos contra la propiedad intelectual, agresiones, acosos y abusos sexuales, cotejo), entre otros.

[5] Según redacción literal actual del art. 259 de la Ley de Enjuiciamiento Criminal española.

Por su parte, el deber de denunciar a las autoridades competentes se incrementa respecto a determinados delitos que distingue la norma penal. A este respecto, el Código Penal español, en su art. 450, contempla la "omisión de los deberes de impedir delitos o de promover su acoso", sancionando a quien no impidiera la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, y a quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan unos de estos delitos y de cuya próxima o actual comisión tenga noticia.

En cuanto al régimen sancionador, si una vez finalizada la investigación de los hechos, se confirmara la veracidad de los mismos, el CRG tomará todas las medidas necesarias para poner fin al hecho denunciado y, si procede y teniendo en cuenta las características del hecho, aplicará las acciones que considere oportunas recogidas en el régimen disciplinario y la legislación laboral vigente, de acuerdo con la legislación penal precitada.

Las medidas que puedan imponerse internamente no limitarán, en ningún momento, el ejercicio de las acciones legales que pueda llevar a cabo la organización.

En todos los casos, se notificará la Resolución tanto al comunicador/informante, como al investigado, teniendo en cuenta el plazo máximo de 3 (tres) meses desde la recepción de la comunicación. No se notificará al informante cuando éste haya renunciado a ello, no se disponga de datos de contacto o se trate de un informante anónimo.

Una vez que se haya adoptado una Resolución sobre la comunicación, el Responsable del Sistema ordenará el ARCHIVO y el BLOQUEO DE LOS REGISTROS de la misma, por el plazo que considere prudente hasta su total eliminación, respetando en todo caso, la legislación vigente en materia de protección de datos personales.

En caso de ARCHIVO CON SANCIÓN, la notificación al investigado contendrá la adopción de las medidas contractuales, disciplinarias o judiciales que deban adoptarse.

El CRG garantiza que nunca se tomarán represalias contra cualquier persona que de buena fe ponga en conocimiento de la organización la comisión de un hecho delictivo, colabore en su investigación o ayude a resolverla. Esta garantía no alcanza a quienes actúen de mala fe con ánimo de difundir información falsa o de perjudicar a las personas. Contra estas conductas ilícitas, el CRG adoptará las medidas legales o disciplinarias que proceda.

3. Registro de las comunicaciones

El Responsable del Sistema cuenta con un libro registro de las informaciones recibidas y las investigaciones internas a que hayan dado lugar, sirviéndole para almacenar y/o recuperar información clave sobre cada incidencia, incluyendo la fecha y fuente de la comunicación original, el plan de la investigación, resultados de entrevistas o cualquier otro procedimiento de investigación, tareas pendientes, resolución final, así como la cadena de custodia de cualquier evidencia o información clave.

4. Protección de Datos Personales

Tal y como se expone en la Política del Sistema Interno de Información del CRG, los tratamientos de datos personales que deriven de la aplicación de dicha Política y del presente Procedimiento de Gestión de Comunicaciones, se rigen por lo dispuesto en el Título VI de Ley 2/2023, de 20 de febrero, por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Considerando el principio de minimización de los datos del Reglamento General de Protección de Datos recogido en la Ley 2/2023, de 20 de febrero, el CRG únicamente tratará los datos personales necesarios para el conocimiento e investigación de las acciones u omisiones objeto de investigación a través del Sistema Interno. En consecuencia, en la medida en la que los datos personales recabados no se consideren de necesario conocimiento o que se acreditase que no se trata de información veraz, el CRG procederá a su supresión en los términos establecidos en el artículo 32 de la Ley 3/2018[6].

Asimismo, el CRG únicamente podrá tratar datos de categoría especial[7] en la medida en que los mismos resulten necesarios para la adopción de las correspondientes medidas correctoras o los

[6] Cuando proceda la supresión, ONECHAIN bloqueará los datos adoptando cuantas medidas resulten necesarias para impedir el tratamiento de la información bloqueado (salvo su puesta a disposición a las autoridades judiciales, Ministerio fiscal o administraciones públicas competentes para la exigencia de posibles responsabilidades) durante el tiempo necesario para guardar evidencia del funcionamiento del sistema que, considerando los plazos de prescripción indicados en la Ley 2/2023, de 20 de febrero, se fija en 3 años. Es preciso destacar que la obligación de bloqueo y conservación no procede al respecto de datos personales contenidos en comunicaciones no investigadas, únicamente pudiendo ser conservadas de forma anonimizada.

[7] Datos personales que revelen el origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, biométricos, datos relativos a la salud, a la vida sexual o las orientaciones sexuales de una persona.

procedimientos sancionadores que eventualmente deban cursarse, debiendo, en caso contrario, proceder a su inmediata supresión en los términos mencionados anteriormente.

En último lugar, el CRG deberá garantizar que los sujetos afectados por el tratamiento de datos personales llevado a cabo como consecuencia de la investigación puedan ejercer los derechos de acceso, rectificación de datos inexactos, supresión, limitación, portabilidad y oposición, teniendo en cuenta que, el derecho de acceso, no podrá incluir información sobre el informante y que el derecho de oposición de las personas investigadas podrá denegarse por motivos legítimos.

5. Seguridad de la información

El canal de comunicaciones electrónico tendrá asignado un Administrador del sistema en el departamento de TIC del CRG, encargado de establecer y personalizar la seguridad necesaria del sistema, incluyendo la restricción en el acceso y habilidad de bloquear los registros, los cuales no deberían poder ser modificados una vez hayan sido registrados. Se prevé una gestión y administración especial para la eliminación de los registros del sistema.

Adicionalmente, el buzón será capaz de auditar el acceso a registros individuales y registrar la fecha, hora y nombre de usuario, incluyendo cualquier modificación realizada sobre los registros.

Con el fin de que los datos mantenidos sean lo más exactos posibles, se procederá a la inmediata cancelación de las comunicaciones que no fueran pertinentes y de aquellas respecto de las cuales, una vez investigados los hechos, se concluyera que no son exactas o veraces.

Asimismo, el buzón de comunicaciones permitirá al Responsable del Sistema almacenar y/o recuperar información clave sobre cada incidencia, incluyendo la fecha y fuente de la comunicación original, el plan de la investigación, resultados de entrevistas o cualquier otro procedimiento de investigación, tareas pendientes, resolución final, así como la cadena de custodia de cualquier evidencia o información clave.

Finalmente, se recuerda que en todo momento se mantendrá la confidencialidad del denunciante y denunciado, cuyas identidades no serán reveladas fuera del ámbito del Comité de Compliance com a Responsable del Sistema.

6. Seguimiento y Control del Reglamento

La implementación, cumplimiento y actualización de este Reglamento será supervisada por el Comité de Compliance de CRG.

El presente Reglamento se revisará y/o modificará por parte del Comité de Compliance, quien podrá externalizar el servicio a profesionales especialistas, siempre que se produzcan cambios relevantes en la organización, en la estructura de control o en la actividad desarrollada por la organización que así lo aconsejen, que haya modificaciones legales o que se pongan de manifiesto la necesidad de actualizar sus disposiciones.

Este Reglamento se revisará, aun cuando no se produzca ninguna de las circunstancias anteriormente descritas, al menos de forma bienal.

7. Documentación relacionada

1. Código de Conducta y Buen Gobierno de CRG.
2. Plan de Medidas Antifraude.
3. Manual de Compliance Penal.
4. Política de Compliance Penal de CRG
5. Política del Sistema Interno de Información del CRG

8. Aprobación del presente Reglamento

El presente Reglamento del Canal Interno de Información del CRG ha sido aprobado conforme se indica en historial de versiones que sigue a continuación y podrá ser modificado con la finalidad de mantener en todo momento la cultura de cumplimiento dentro de la organización, materializada en los principios de transparencia, responsabilidad y prudencia hacia terceros y hacia sus propios miembros y socios de negocio.

9. Historial de versiones

Versión	Fecha	Aprobado por	Motivo del cambio
V.1	28/11/2022	Coordinador del Comité de Compliance y Gerente del CRG	
	15/12/2022	Patronato del CRG	
V.2	29/11/2024	Coordinador del Comité de Compliance y Gerente del CRG	Adaptación a la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (en cuanto al contenido de las fases del procedimiento de gestión de las comunicaciones, las funciones del Responsable del Sistema, el registro de comunicaciones y los aspectos de protección de datos personales).
	19/12/2024	Patronato del CRG	

10.Anexos

FORMULARIO DE DENUNCIA

DATOS IDENTIFICATIVOS DEL DENUNCIANTE

Nombre y apellidos del denunciante	
Dirección de correo electrónico	
Dirección de correo postal (opcional)	
Teléfono (opcional)	
Área o departamento de CRG en el que presta sus servicios	

DENUNCIA

Descripción de la denuncia (si es posible, adjuntar evidencias o documentos justificativos de la denuncia)	Por favor, identifique a las personas (físicas y/o jurídicas) que han participado en los hechos, en qué concepto, el tipo de relación existente con el denunciado y si existen más personas conocedoras de los hechos (indicar quiénes)
	Por favor, indique el motivo de la denuncia (hechos e indicios), marco temporal en el que han tenido lugar, área/s de CRG afectadas y todos aquellos hechos que considere.

¿Existe algún conflicto de interés con alguno de los miembros del Comité de Compliance de CRG?

☐ Sí Señale con quién: _____

☐ No

Canal externo de información-Autoridad Independiente de Protección del Denunciante, A.A.I.

Todas las personas físicas pueden informar **ante la A.A.I. estatal o ante las autoridades u órganos autonómicos correspondientes** a través de los Canales externos debidamente habilitados al respecto, de la comisión de cualesquiera acciones u omisiones a las que se refiere el Sistema Interno de Información del CRG, ya sea directamente o bien previa comunicación a través del Canal de Información Interno del CRG.