CIRSA

# POLÍTICA DE FUNCIONAMIENTO DEL CANAL DE LÍNEA ÉTICA

2021

# 1. INTRODUCCIÓN

## 1.1. Justificación de la reforma

**La Ética, la integridad, el respeto a la legalidad, la transparencia y la honestidad son principios que se defienden desde el Grupo CIRSA, rechazando así cualquier posible actuación irregular.** Nuestra actividad está diseñada para que cada persona que forma parte de la Compañía cumpla estrictamente con la legalidad vigente, en cada momento y en cada lugar donde se sitúe dicha actividad. Asimismo y, tal y como recoge el Código de Conducta del Grupo, se defiende el estricto cumplimiento de los compromisos y obligaciones propios de la Compañía respecto a las relaciones con clientes, proveedores, socios y con el entorno en general. Esta es la base para evitar cualquier posible acto ilícito que supondría un fuerte impacto a la reputación y al propio negocio.

En el marco de la cultura de cumplimiento que impera en todo el Grupo y dentro de los planes de mejora continua que se vienen implementando sobre las políticas de Compliance, se ha introducido una nueva plataforma que acoge el Canal de Línea Ética de la Compañía. Dicho canal, permite seguir cumpliendo con las nuevas directivas de ámbito europeo, reforzar el elevado grado de cumplimiento regulatorio del Grupo y mantener un firme compromiso con la sociedad en general, ya que la plataforma permite comunicar de forma anónima -si se desea- y confidencial posibles irregularidades de potencial trascendencia que puedan producirse en el seno de la empresa o en nombre de esta.

**Este cumplimiento es uno de los factores que permite a la Compañía ser una de las empresas líderes del sector y un referente a nivel empresarial.**

### 1.2. Contexto normativo

La necesidad de la existencia de un Canal de Línea Ética aparece como elemento esencial de los Modelos de Compliance y Prevención de Riesgos Normativos. Así, y de conformidad con lo dispuesto en el apartado 4º del párrafo 5º del artículo 31 bis del Código Penal: "los modelos de organización y gestión (...) impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención". Del mismo modo, el párrafo 5º del apartado 5º del artículo 31 bis del Código Penal, establece la necesidad de un Sistema Disciplinario en materia de Compliance, al referir literalmente que "(...) los modelos de organización y gestión (...) establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo". Ambas cuestiones son afrontadas en la elaboración de esta Política para dar efectivo cumplimiento a los requisitos exigidos por parte del legislador.

Desde el punto de vista de la normativa interna del Grupo CIRSA, esta Política debe considerarse parte integrante del Sistema de Gestión Global de Compliance del Grupo. CIRSA quiere dejar claro que la Política de Funcionamiento del Canal de Línea Ética no pretende sustituir las competencias propias de Direcciones de gestión ordinaria del mismo. Por ello, las relaciones entre unos y otros han de basarse en la complementariedad, la coordinación y la colaboración para conseguir el mejor resultado.

Desde el punto de vista del contenido y estructura de esta Política, obedece a las directrices impuestas por la siguiente normativa:
En primer lugar, obedece a la Circular 1/2016 de la Fiscalía General del Estado, de 22 de enero, sobre la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, en la que se afirma que para que los empleados de las empresas puedan alertar de aquellas conductas potencialmente ilícitas, es necesaria la existencia de una adecuada regulación interna que proteja de forma específica al Alertador.
Además, cumple con la ISO 37001 en materia de Sistemas de Gestión del Soborno y la Corrupción, en donde se hace una especial referencia al proceso que deberá seguirse en la investigación de las Alertas, señalando que la necesidad de desarrollar procesos internos de Alertas en los que se garantice: (i) la efectividad de las acciones llevadas a cabo, (ii) la capacidad de las personas encargadas de la investigación, (iii) el necesario reflejo de la implicación y cooperación de otras áreas y (iv) la confidencialidad de la Alerta, la investigación y la resolución.
Por su parte, la Norma 37301 para Sistemas de Gestión de Cumplimiento, establece la necesidad de contar con canales de Alerta. Así, en el apartado relativo al planteamiento

de inquietudes, establece de forma literal: “incluso en los casos en los que no lo requiera la reglamentación local, las organizaciones deberían considerar desarrollar un mecanismo de Alertas que permita el anonimato o la confidencialidad, a través del cual los empleados y agentes de la organización puedan informar o buscar orientación en términos de no cumplimiento de Compliance sin miedo a represalias”. Además, en esta norma se hace referencia específica a los requisitos y recomendaciones incluidos en la Norma ISO 37002 para Sistemas de Gestión de Denuncias e Irregularidades - sobre los Canales de Denuncias-, y que ha servido de base, al desarrollo de esta Política.
Asimismo, es destacable la relevancia en este ámbito de la legislación en materia de protección de datos, así como en materia de protección de los Alertadores, especialmente tras la protección del Alertador -*whistleblower*- con la Directiva (UE) 1937/2019 de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Dicha Directiva asegura que los Alertadores puedan informar, internamente y a las autoridades, de cualquier posible infracción de la normativa europea que se produzca en el seno de una organización a través de canales que garanticen la seguridad del Alertador, sin temor a represalias por parte de la empresa.

Es por ello por lo que, de conformidad con los requisitos establecidos en la Directiva referida y para la efectiva implantación de los canales de Alerta internos -ordinarios y alternativos- esta Política de Funcionamiento del Canal de Línea Ética del Grupo CIRSA prevé el desarrollo del alcance y contenido de los procedimientos y tramitación de Alertas. En este sentido, se establecen los siguientes requisitos:

1. Permite la posibilidad de formular Alertas por escrito, así como por vía analógica y telemática y, también, de manera presencial si así lo quiere el Alertador;
2. Acuse de recibo de la Alerta en un plazo máximo de 7 días;
3. Permite la designación *ad hoc* por parte del Órgano de Cumplimiento de un Equipo de Investigación, vigente hasta la terminación del caso, así como la designación de un responsable del caso quien tramitará las Alertas y mantendrá la comunicación con el Alertador. En caso necesario, se encargará de solicitar información adicional y de dar respuesta;
4. Tramitación diligente de todas las Alertas (incluidas las anónimas);
5. Establecimiento de un plazo general de 3 meses para dar respuesta al Alertador sobre la tramitación de la Alerta, a contar desde el acuse de recibo.

Finalmente, en lo que respecta a la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en concreto respecto a los sistemas de información de Alertas internas, su artículo 24 prevé algunas cuestiones importantes que se destacan a continuación.
Primero, que las comunicaciones o Alertas puedan ser anónimas. Segundo, establece el deber de información a los empleados o terceros de la existencia de estos sistemas de

información (“Canal de Línea Ética”). Además, deja claro que el acceso a los datos deberá limitarse a aquellas personas que -con independencia de su pertenencia o no a la entidad- ocupen funciones de control interno y de cumplimiento, o a los encargados del tratamiento de datos. Todo ello sin perjuicio de su acceso por otras personas o a la posible comunicación de datos que haya que realizar a terceros o a las autoridades cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales. Y de manera destacable, además, señala que deberá preservarse la identidad y confidencialidad de los datos correspondientes a las personas afectadas y, en especial, los datos de la persona que hubiera informado de los hechos si no lo hubiera realizado de manera anónima.

Por último, en lo que respecta a la posibilidad de interponer Alertas anónimas, nos referimos a la Sentencia del Tribunal Supremo 272/2020 de fecha 6 de febrero, en la que destaca y valida el uso de las Alertas anónimas para la detección de posibles actos ilícitos penales que se puedan corroborar, como sucede en este procedimiento, con la posterior investigación interna y policial. Así, apunta la sala Penal que: “(...) Importancia tiene la Alerta llevada a cabo y en la que, con la inexistencia de un programa de cumplimiento normativo interno, sí que resulta notablemente interesante que en el periodo de los hechos probados se lleve a cabo una mecánica de actuación ‘ad intra’ en el seno de la empresa, recientemente regulada en el denominado “canal de Alertas interno” o, también denominado ‘*whistleblowing*’, y que ha sido incluido en la reciente Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión”.

## 2. FINALIDAD

El Grupo CIRSA, en pro de seguir avanzando con su compromiso de establecer una sólida cultura de cumplimiento, más allá de cualquier obligación de carácter legal, basándose en unos valores y principios, reconoce la importancia de adoptar un reglamento interno (en adelante la "Política"). Dicha normativa está integrada por el Código de Conducta del Grupo y el Modelo de Organización, Gestión y Control. Esta tiene como objetivo desarrollar la obligación de la utilización del Canal de Línea Ética, así como regular la forma de utilizar el aplicativo que lo alberga (en adelante: "Plataforma"), con el propósito de proporcionar consejo y certidumbre en el proceso de toma de decisión de la persona conocedora de posibles infracciones.

En este sentido, con el fin de contar con las herramientas necesarias para facilitar cualquier detección de un posible acto ilícito y para proteger a todas las personas que forman parte del Grupo y a la reputación de la misma frente a nuestros públicos de interés, **la Compañía ha reforzado el Canal de Línea Ética existente con la implementación e implantación de una Plataforma para recibir, analizar y tramitar Alertas** (en adelante: "Alertas"), que garantiza íntegramente la confidencialidad y cumple con los máximos estándares en materia de Seguridad de la Información y Protección de Datos. Y si así lo desea el usuario, esta comunicación pueda realizarse de manera completamente anónima, garantizando la no existencia de cualquier posible represalia.

Para ello, es preciso determinar los siguientes aspectos fundamentales:

1) Ámbito subjetivo de aplicación: **¿A quién se aplica esta Política?**
2) Ámbito objetivo de la Alerta: **¿Qué se puede Alertar?; ¿Cuándo debo hacerlo?**
3) Puesta en práctica del canal: **¿Cómo utilizar el Canal de Línea Ética del Grupo CIRSA?; ¿Puede hacerse una Alerta anónima?**
4) Consecuencias de la Alerta: **¿Qué ocurre cuando se hace una Alerta a través del Canal de Línea Ética?**
5) La Política de Funcionamiento del Canal de Línea Ética del Grupo CIRSA es una Política universal de aplicación para todas las sociedades pertenecientes al Grupo, a menos que exista una justificación normativa que disponga una excepción a dicha aplicación.

### 2.1. Ámbito subjetivo de aplicación: ¿A quién se aplica esta Política?

Las personas sujetas a esta Política (en adelante "Destinatarios" y/o "Alertadores") son todos los empleados y colaboradores del Grupo CIRSA, miembros de los órganos corporativos, clientes, proveedores, socios, consultores, accionistas y, en general, cualquier persona que presta servicios para el Grupo en base a un contrato, además de las partes interesadas del propio Grupo (en adelante, los "Terceros").

## 2.2. Ámbito objetivo de la Alerta: ¿Qué se puede Alertar?; ¿Cuándo debo hacerlo?

### 2.2.1. ¿Qué puedo Alertar aplicando esta Política de Funcionamiento del Canal de Línea Ética?

Esta Política fomenta la notificación de cualquier preocupación que pueda tener el Alertador en relación con posibles vulneraciones del Sistema de Gestión Global de Compliance del Grupo CIRSA, de conformidad con la amplitud con la que se define en la Directiva (UE) 1937/2019. Esto incluye información sobre infracciones en un sentido amplio: sospechas razonables, infracciones reales o potenciales, que se hayan producido o que sea probable que se produzcan, entre otras.

A tal efecto, se destacan las siguientes posibles comunicaciones:

**A. CORRUPCIÓN:** violación de la legislación, políticas, normas, directrices y/o procedimientos en materia de:
**- Soborno/Cohecho/Tráfico de influencias:** ofrecer o aceptar ventajas inapropiadas de cualquier tipo, tanto en un contexto empresarial privado como de carácter público a funcionarios, autoridades, etc.
Ejemplos: ofrecer o aceptar comisiones o regalos monetarios; invitación de socios comerciales o a través de ellos, con la apariencia de querer influir en una relación comercial.
**- Fraude/Estafa:** presentar hechos, datos o información falsos, u omitir los verdaderos, con el fin de obtener, o no necesariamente, un beneficio económico ilícito para uno mismo o para terceros.
Ejemplos: emisión de facturas excesivas para quedarse con el excedente; fraude de créditos; fraude de subvenciones; fraude a los seguros; falsificación de documentos de identidad, llaves u otros medios de identificación; manipulación de máquinas o métodos de prueba.
**- Robo:** sustracción no autorizada de sumas de dinero u objetos ajenos para uso propio o para cedérselos a un tercero.
Ejemplos: robo de mercancías del almacén; retención de fondos de la empresa o materiales de trabajo.
**- Incumplimiento de la normativa contable y de información financiera / Delitos contra la Hacienda Pública y la Seguridad Social:** representación fraudulenta deliberada de las transacciones, controles inadecuados de las operaciones de una organización.
Ejemplos: información falsa sobre los ingresos, los gastos, los activos o los bienes; representación fraudulenta de las transacciones; destrucción de justificantes; ocultación de activos.

**B. BLANQUEO DE CAPITALES**
Violación de la legislación, políticas, manuales y/o procedimientos en materia de

Prevención del Blanqueo de Capitales y Financiación del Terrorismo mediante la introducción de dinero obtenido de manera ilegal o de activos adquiridos ilegalmente, en el circuito económico y financiero legal.
Ejemplos: transferencias de fondos a través de un «paraíso fiscal»; pretensión de un socio comercial de liquidar en efectivo la totalidad de una transacción o parte de ella; indicios de proximidad del socio comercial a organizaciones criminales o terroristas; dudas sobre la identidad del cliente o sospechas de que el cliente actúa como testaferro para un tercero.

**C. PROTECCIÓN DE DATOS**
Violación de la legislación, políticas, manuales y/o procedimientos en materia de Protección de Datos y del Secreto de las Telecomunicaciones.
Ejemplos: recogida, tratamiento o divulgación no autorizada de datos personales; vigilancia técnica no autorizada de los empleados; utilización de datos con fines privados; uso de datos de clientes con fines comerciales sin su consentimiento.

**D. SEGURIDAD DE LA INFORMACIÓN**
Violación de la normativa, políticas, directrices y/o procedimientos en materia de Seguridad de la Información diseñada para proteger los datos frente a la falsificación, la destrucción y la divulgación no autorizada, contra los daños informáticos o la revelación de secretos.
Ejemplos: menoscabo de la seguridad de los sistemas y redes informáticos que comprometa gravemente la confidencialidad, la integridad o la disponibilidad de la información o de los equipos; divulgación de cuentas y contraseñas de usuario a personas no autorizadas; ciberataques.

**E. PRÁCTICAS POCO ÉTICAS**
Violación de las normas y directrices de comportamiento, de las obligaciones profesionales y requisitos legales por prácticas o acciones indebidas realizadas de forma deliberada o involuntaria contrarias a lo establecido por el Código de conducta.
Ejemplos: violaciones de la Política de Juego Responsable o de Protección del Medio Ambiente, uso de publicidad engañosa; tráfico de drogas; incidencias en el normal desarrollo de la operativa de juego.

**F. BUSCO CONSEJO**
Aquí se pueden plantear dudas o consultas sobre cuestiones en general relacionadas con su cumplimiento en la empresa y pedir consejo sobre dichas cuestiones.

### 2.2.2. ¿Cuándo se debe informar?

En el Grupo CIRSA existe la convicción de que la mejor formar de promover las Alertas parte de la generación de un entorno donde las personas se sientan cómodas para compartir cualquier posible incidencia vulneradora del Sistema de Gestión Global de

Compliance del Grupo. Y, por tanto, promueve el fomento de un entorno en el que se puedan reflejar hechos relacionados con posibles infracciones del mencionado Sistema.

Lo anterior ha de ir en consonancia con un principio que preside todas las relaciones del Grupo CIRSA con sus grupos de interés: Las Alertas deben hacerse siempre de buena fe, lo que equivale a la implantación de una "cultura de equidad", de conformidad con lo establecido por la Directiva (UE) 1937/2019. Esto significa que, en el momento de la Alerta, el Alertador ha de tener motivos razonables para creer que la información que indica es cierta y que contiene posibles infracciones.

### 2.2.3. ¿Qué ocurre en los casos de urgencia?

De manera indiscutible, la tramitación de las Alertas planteadas a través de los diferentes canales con los que cuenta el Grupo CIRSA exige, que por parte del órgano encargado de recibirlas -el Órgano de Cumplimiento-, se realice una clasificación, de uso interno, del contenido de la Alerta que permitirá adecuar la tramitación al contenido de la misma. A tal efecto, la clasificación establecida es:

- Alerta Falsa
- Recursos Humanos
- Alto
- Medio
- Bajo
- Otros

En cualquier caso, lo preceptivo es asegurarse de informar al superior jerárquico y/o a la Órgano de Cumplimiento del Grupo tan pronto como sea posible para, una vez atendidos los hechos, poder atajar la cuestión de la manera más eficiente posible, tramitando la Alerta conforme al Protocolo de Investigación ante actos de Fraude e Incumplimiento.

## 2.3. Puesta en práctica del canal: ¿Cómo se utiliza el Canal de Línea Ética del Grupo CIRSA?; ¿Puede haber una Alerta anónima?

### 2.3.1. Pasos a seguir en la presentación de una Alerta

Cualquier Alerta de las comprendidas en esta Política puede realizarse a través de uno de los canales que se detallan a continuación:

a) Canales principales:

1. En la página web corporativa de carácter público en la sección RSC – Cumplimiento – Canal de Línea Ética a través del siguiente enlace: https://www.cirsa.com/

2. En la Intranet en la sección de Accesos Rápidos – Canal de Línea Ética a través del siguiente enlace: https://cirsa.sharepoint.com/sites/es_intranet
3. O directamente a través del siguiente enlace: https://www.bkms-system.com/COMPLIANCE-CIRSA

b) Otros canales:

4. Personal:
   i. Superior directo
   ii. Miembro del Órgano de Cumplimiento (Director Corporativo Recursos Humanos, Director Corporativo Auditoría Interna y Director Corporativo Área Legal y de Compliance)
   iii. Miembro del Área de Compliance
5. Correo electrónico: compliance@cirsa.com
6. Correo postal:
   CIRSA Servicios Corporativos, S.L.
   Área de Compliance
   Carretera de Castellar, 338
   08226 – Terrassa (Barcelona) Spain

### 2.3.2. ¿Qué información debo aportar al enviar una Alerta?

El Grupo CIRSA recomienda que la información que se facilite sea lo más completa y veraz posible. Y por ello ruega que, en caso de Alertar, se comparta toda la información que el Alertador conozca en relación con las posibles infracciones. Y que lo haga de forma detallada. Además, lo preferible es que se proporcione, o que la Alerta se refiera de manera clara, a cualquier prueba o documento que la sustente. Esto permite la gestión del caso de la forma más rápida y eficaz posible.

### 2.3.3. Identificación al presentar la Alerta: el anonimato

El Canal de Línea Ética permite que las Alertas puedan llevarse a cabo de forma anónima.
No obstante, el Grupo CIRSA promueve que, en el caso de presentar una Alerta, el Alertador se identifique facilitando su nombre y datos de contacto. De este modo, el personal que se encargue de tramitarla podrá ponerse en contacto con la persona Alertadora para solicitar información adicional y aclaraciones, dar soporte y ayuda, realizar un seguimiento si es necesario, etc. Y, al mismo tiempo, CIRSA considera que es la mejor forma de acreditar los altos estándares sobre los que se fundamenta esta Política al poder así certificar el principio de no represalia ante una Alerta.
En el sentido anteriormente apuntado, ha de tenerse en cuenta que cuando se presenta una Alerta (no anónima), el Grupo CIRSA asegura que el procedimiento de Alerta interna

se llevará a cabo de una manera segura que garantice la confidencialidad de la identidad de la persona Alertadora y otra información relacionada.

**2.3.4 Consecuencias de la Alerta: ¿Qué ocurre cuando se hace una Alerta a través de los canales alternativos del Grupo CIRSA?**

Grupo CIRSA utiliza una plataforma digital para apoyar la administración de los Canales Alternativos, en línea con lo exigido en la Directiva 1937/2019.

Las Alertas a través de los canales alternativos se guardan directamente en la plataforma, que tiene implementadas medidas robustas de seguridad de la información dirigidas a preservar la integridad, disponibilidad y confidencialidad de la información.
La plataforma permite al Alertador concretar el lugar, fecha, sociedad, división, etc. afectadas, así como las personas relacionadas con la Alerta. Además, permite optar por la comunicación anónima. Y dará opción al Alertador de poder acompañar la comunicación con la documentación de soporte que justifique el contenido de la misma.

A través del Área de Compliance se acusará recibo en un plazo de siete días laborales a partir de la misma.

Una vez se haya producido el acuse de recibo, tanto si el Alertador se haya identificado como si lo ha hecho de forma anónima habilitando el acceso al buzón de comunicación, Grupo CIRSA a través de la persona designada internamente, podrá ponerse en contacto con el Alertador directamente para identificarse como instructor, y proporcionarle comentarios y actualizaciones. La tramitación de la Alerta se resolverá en un plazo razonable, no superior a tres meses desde el acuse de recibo, plazo que podrá extenderse a seis meses en supuestos de especial relevancia o complejidad. No obstante, transcurridos los primeros tres meses desde la recepción de la Alerta se procederá a eliminar del canal de Alertas cualquier información de carácter personal, referente al Alertador, a las personas mencionadas o a terceros, salvo que sea imprescindible su conservación con el fin de dejar evidencia del funcionamiento del Modelo de Prevención de Delitos.

Es importante resaltar que la plataforma traslada estas Alertas solo a personas específicas dentro de Grupo CIRSA que están expresamente autorizadas y capacitadas para gestionarlas. Asimismo, el equipo interno que maneja los documentos aportados recibe formación sobre cómo gestionarlos de forma eficaz, así como de asegurar su confidencialidad.

El principio de actuación es que, cuando la Alerta indique una posible violación del Sistema de Gestión Global de Compliance de Grupo CIRSA, se iniciará una investigación de conformidad con el Protocolo de Investigación ante actos de Fraude e Incumplimiento.

CIRSA proporcionará información al Alertador sobre la Alerta y, en la medida de lo posible, del resultado de la evaluación del asunto. Debe tenerse en cuenta que, en algunos casos, puede haber limitaciones en cuanto a las actualizaciones que se puedan proporcionar sobre la Alerta, de conformidad con lo desarrollado en el mencionado Protocolo de Investigación ante actos de Fraude e Incumplimiento del Grupo.

### 2.3.5 Tratamiento justo y responsable de las Alertas

El principio de buena fe también aplica desde el lado de la empresa. Por ello, en CIRSA se respeta los derechos de los empleados, y se asegura de proteger también los derechos de los empleados mencionados en las Alertas realizadas de acuerdo con esta Política.

### 2.3.6 Prohibición de represalias

En Grupo CIRSA no se tolera ninguna forma de represalia. Esto incluye la amenaza, o cualquier otra forma de amedrentar a una persona que alerte hechos involucrados con esta Política.

### 2.3.7 ¿Qué se debe entender por buena fe desde la empresa y desde el Alertador?

Desde el punto de vista del Alertador, la buena fe supone Alertar teniendo, como mínimo, motivos razonables para creer que la información sobre posibles infracciones comunicada era cierta en el momento de informar.
Desde el punto de vista de la empresa, en este contexto de canales de Alerta, la buena fe quiere decir que la empresa no va a adoptar ninguna represalia por el hecho de presentar una Alerta, y protegerá la confidencialidad y la identidad de la persona del Alertador en cualquier caso y solo con las excepciones siguientes:

a) Cuando la Ley, en sus diferentes modalidades, exija comunicarlo a una autoridad judicial o administrativa.
b) Cuando sea imprescindible respecto a asesores y consultores externos y otros proveedores de Grupo CIRSA para el funcionamiento del Canal de Línea Ética o la investigación de los hechos Alertados, conforme se recoge en el apartado 3.6 de la presente Política. En estos casos, CIRSA exige contractualmente la máxima confidencialidad a estos proveedores.

### 2.3.8 ¿Qué significa la prohibición de represalias?

La prohibición de represalias abarca cualquier acto u omisión, directo o indirecto, que pueda perjudicar a un Alertador debido a su Alerta de buena fe de posibles infracciones. Por ejemplo, Grupo CIRSA no tomará ninguna de las siguientes medidas contra los Alertadores por la presentación de una Alerta:

1. Suspensión, despido, destitución o medidas equivalentes;
2. Una evaluación negativa del rendimiento;
3. Denegación de la promoción;
4. Cambio injustificado de ubicación del lugar de trabajo, reducción de salario, cambio de horario de trabajo;
5. Coacción, intimidación, acoso u ostracismo;
6. Discriminación, trato desventajoso o injusto;
7. No renovación o resolución anticipada de un contrato de trabajo temporal;
8. Daño, incluso a la reputación de la persona, en particular en los medios sociales, o pérdida financiera, incluida la pérdida de negocio y la pérdida de ingresos;
9. Resolución anticipada de un contrato de bienes o servicios;
10. Cancelación de un permiso;
11. Otras medidas que pudieran considerarse como represalias.

### 2.3.9 La prohibición de represalias en caso de Alertas externas y revelaciones públicas

La protección contra las represalias se extiende también a las personas que Alertan sobre posibles infracciones a las autoridades competentes.
Se prohíben tanto las represalias directas como las indirectas.
La Política de Funcionamiento del Canal de Línea Ética extiende la prohibición de represalias a las siguientes personas:

1. Cualquier tercera persona relacionada con el Alertador (como compañeros y familiares) que pueda sufrir represalias en un contexto laboral;
2. Cualquier persona que haya ayudado al Alertador en el proceso de Alerta;
3. Cualquier entidad jurídica de la que el Alertador sea propietario, trabaje o esté vinculado de otro modo en un contexto laboral o profesional.

En caso de que cualquier miembro de Grupo CIRSA, en contra de esta Política, tome directa o indirectamente represalias, será el propio Grupo quien tomará las medidas necesarias para que cesen las represalias lo antes posible y, cuando proceda, tomará medidas disciplinarias contra los responsables de las mismas.

## 3. PROTECCIÓN, TRATAMIENTO Y CONSERVACIÓN DE DATOS

CIRSA desea poner en conocimiento de sus empleados y clientes la presente información adicional sobre protección de datos (en adelante, "Política de Protección de Datos"), en la que se proporciona de manera transparente y sencilla toda la información legalmente exigida en relación con el tratamiento de gestión del sistema de información de Alertas internas, las finalidades para las cuales se tratan sus datos y los derechos que pueden ejercer. La presente Política de Protección de Datos estará siempre disponible en la plataforma digital habilitada como Canal alternativo.

### 3.1. ¿Quiénes son los responsables de tus datos y como puedes contactar con ellos?

La gestión del sistema de información de Alertas internas conlleva necesariamente el

tratamiento de los datos de carácter personal por parte de CIRSA:

- CIRSA SERVICIOS CORPORATIVOS, S.L (en adelante "CIRSA"), constituida conforme a la legislación española, titular del CIF número B-25.421.199 con domicilio social en Carretera Castellar número 298, 08227 Terrassa (Barcelona) e inscrita en el Registro Mercantil de Barcelona en el Tomo 32.339, Folio 194, Hoja B-207.353.

- Cualquier empresa del Grupo CIRSA que corresponda en virtud de la Alerta formulada cuando resulte necesario para investigar con mayor detalle los hechos alertados, adoptar medidas disciplinarias y/o para la tramitación de los procedimientos judiciales que, en su caso, procedan. Puedes obtener más información sobre la presencia a nivel internacional de Grupo CIRSA en https://www.cirsa.com/cirsa/presencia-internacional/.

Las sociedades mencionadas actúan como corresponsables del tratamiento de tus datos de carácter personal, pues determinan y efectúan conjuntamente el tratamiento de la información personal para la gestión del sistema de información de Alertas internas.
Ante cualquier duda relacionada con los tratamientos que se realizan de tus datos personales, puedes ponerte en contacto con el Delegado de Protección de Datos a través del correo electrónico: protecciondedatos@cirsa.com.

### 3.2. ¿Qué es un dato de carácter personal y un tratamiento?

Dato de carácter personal es toda información sobre una persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como, por ejemplo, un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona. Un tratamiento de datos de carácter personal es toda operación o conjunto de operaciones que se realizan sobre tus datos personales, como, por ejemplo, la recogida, registro, conservación, utilización y comunicación de tus datos.

### 3.3. ¿Qué datos personales se recopilan y a través de qué vía?

Únicamente se podrán recopilar datos personales e identificarte en aquellos supuestos en que reveles tu identidad. En estos casos, CIRSA podrá recabar a través del sistema de información de Alertas internas la siguiente información:

- Nombre y apellidos
- Dirección de correo electrónico
- Número de teléfono
- Número de DNI, NIE o Pasaporte
- Contenido de la Alerta efectuada

En aquellos supuestos en que los interesados realicen las Alertas de forma anónima, CIRSA no podrá identificar a los mismos y, por tanto, no tratará ningún dato de carácter personal de los interesados.

### 3.4. ¿Qué derechos puedes ejercer?

**A. Derecho de acceso**
Tienes derecho a saber si CIRSA está tratando tus datos personales y, en tal caso, conocer qué datos trata.
**B. Derecho de rectificación**
Tienes derecho a modificar aquellos datos tuyos que sean inexactos o incompletos. Para ello deberás indicar qué datos deseas modificar y acreditarlos adecuadamente.
**C. Derecho de oposición**
En los supuestos legalmente previstos puedes oponerte en cualquier momento, por motivos relacionados con tu situación particular, a que se traten tus datos. Recuerda que tu oposición a la realización de dichos tratamientos conllevará la imposibilidad de que CIRSA pueda gestionar dichas peticiones.
**D. Derecho de supresión**
Tienes derecho a cancelar tus datos personales. Esto no significa que tus datos sean totalmente eliminados, sino que tus datos se conservarán bloqueados de manera que se impida su tratamiento, sin perjuicio de su puesta a disposición de las administraciones públicas, jueces y tribunales para la atención de posibles responsabilidades que hayan surgido como consecuencia del tratamiento durante el plazo de prescripción de estas últimas.
**E. Derecho a la portabilidad de datos**
Tienes derecho a recibir y/o a transferir a otro responsable del tratamiento diferente de CIRSA aquellos datos personales que te incumban y que nos hayas facilitado.
**F. Derecho a la limitación en el tratamiento**
Tienes derecho a solicitar que se suspenda el tratamiento de tus datos cuando (i) hayas impugnado la exactitud de tus datos, mientras CIRSA verifica dicha exactitud; o (ii) hayas ejercido tu derecho de oposición al tratamiento de tus datos, mientras se verifica si los motivos legítimos de CIRSA prevalecen sobre los tuyos como interesado. Igualmente, este derecho te permite solicitar a CIRSA que conserve tus datos personales cuando (i) el tratamiento de datos sea ilícito y como interesado te opongas a la supresión de tus datos, solicitando en su lugar una limitación de su uso; o (ii) CIRSA ya no necesite tus datos personales para los fines del tratamiento, pero los necesite para la formulación, ejercicio, o defensa de reclamaciones.
Podrás ejercer tus derechos mandando tu petición a través de tu perfil de usuario creado en el propio buzón de información de Alertas internas. Asimismo, se te informa de que, en el caso de que consideres que CIRSA no ha satisfecho correctamente el ejercicio de tus derechos podrás presentar una reclamación ante la Agencia Española de

Protección de Datos (AEPD), dirigiéndote a su página web http://www.aepd.es.

**3.5. ¿Qué tratamientos se realizan con tus datos?**

Para poder informarte de forma transparente y con detalle sobre las finalidades para las cuales se tratan tus datos se ha procedido a separar la información relativa a cada tratamiento en cuadros independientes. Así, podrás encontrar toda la información específica del tratamiento que se realiza de tus datos en su correspondiente cuadro de forma individualizada. El cuadro descriptivo recoge la siguiente información:

• ¿Para qué finalidades se tratan tus datos?

En esta columna se explica para qué finalidades se tratan tus datos personales.

• ¿Cuál es la base legal que legitima a Grupo CIRSA el tratamiento de tus datos?

Esta columna explica el fundamento o justificación legal que permite al Grupo tratar tus datos personales de forma lícita. La normativa de protección de datos requiere que se realice el tratamiento de tus datos sobre una base o justificación legal que legitime dicho tratamiento. Así, para tratar tu información personal nos basamos en distintas bases o justificaciones legales dependiendo del tratamiento que se lleven a cabo de tus datos. Las bases legales para el tratamiento de tus datos personales pueden ser:

- Interés legítimo
- La ejecución del contrato
- El cumplimiento de una misión realizada en interés público
- El cumplimiento por parte de CIRSA de una obligación legal
- Interés vital
- Tu consentimiento

• ¿Durante cuánto tiempo se conservan tus datos?

En esta columna se informa de manera orientativa cuánto tiempo se conservarán tus datos. El tiempo de conservación dependerá en todo caso del tratamiento que se lleve a cabo sobre tu información personal. Se debe tener en cuenta que determinada normativa puede obligar a conservar algunos datos de interesados durante un tiempo determinado.

A continuación, se encuentran descritos con mayor detalle el tratamiento que CIRSA realiza de tus datos personales:

| ¿Para qué finalidades se tratan tus datos? | ¿Sobre qué base lega se tratan tus datos? | ¿Durante cuánto tiempo se conservan tus datos personales? |
|---|---|---|
| Tener conocimiento e investigar la comisión, tanto en el seno de la corporación como en la actuación de terceros contratados por la misma, de actos o conductas contrarias a la ley o al convenio colectivo que resulte de aplicación. | El cumplimiento de una misión realizada en interés público. | Los datos personales del interesado serán tratados únicamente durante el plazo de tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos alertados.<br>En todo caso, transcurridos tres meses desde la introducción de los datos, CIRSA procederá a la supresión de la información del sistema de Alertas, salvo que la misma sea necesaria para continuar con la investigación. |

### 3.6. ¿A quién se comunican tus datos?

CIRSA podrá comunicar tus datos, previo requerimiento legal o base que legitime la comunicación a:

- Asesores legales, peritos, empresas de ciberseguridad y/o, otros terceros necesarios para llevar a cabo las investigaciones oportunas para discernir los hechos alertados por los interesados
- Juzgados y Tribunales
- Organismos de Gobierno y Administración Pública
- Fuerzas y Cuerpos de Seguridad del Estado
- Miembros del Órgano de Cumplimiento o del Área de Compliance

### 3.7. ¿Quién puede acceder a tus datos?

CIRSA te informa que se trabaja con terceros, en concreto, proveedores de servicios necesarios para el correcto desarrollo del sistema de información de Alertas interno. Estos proveedores de servicio pueden, en ejercicio de su actividad, tener acceso a tus datos. Este acceso no constituye una cesión de datos, sino un acceso en calidad de encargado de tratamiento, figura regulada y prevista en el RGPD. En todo caso, te informamos que CIRSA vela por tus datos y, por tanto, ha verificado que estos proveedores ofrecen un nivel de seguridad adecuado y velan por la protección de los derechos y libertades de los interesados.

### 3.8. ¿Están tus datos seguros?

Con el fin de asegurar un procesamiento justo y transparente de tu información personal, se adoptan los procedimientos adecuados que incluirán la implementación de medidas técnicas y organizativas que tengan en cuenta el posible riesgo y corrijan cualquier impresión identificada en los datos personales tratados, de modo que el riesgo de cualquier error de minimice, tratando tus datos de manera justa y segura.

### 3.9. Cambios en la presente política de protección de datos

La presente Política de Protección de Datos podrá variar con el tiempo debido a los posibles cambios de criterio seguidos por la autoridad de control competente en materia de protección de datos en cada momento. CIRSA se reserva por tanto el derecho a modificar la presente Política de Protección de Datos para poder adaptarla a dichos criterios, así como a novedades jurisprudenciales o legislativas.

## 4. PROCEDIMIENTOS RELACIONADOS

Como quiera que la Política descrita en este documento está directamente relacionada con otras políticas y/o procedimientos, se enumera, a continuación, las que el Grupo CIRSA considera más determinantes a la hora de poder entender la pretensión y alcance de la misma.

Así, en concreto, estos son los procedimientos vinculados y/o afectados por esta Política y que se encuentran publicados en la página web de la compañía en el apartado

"Políticas y Procedimientos de Compliance":

- Código de Conducta
- Política de Gobierno Corporativo
- Modelo de Prevención de Delitos Penales
- Política Anticorrupción
- Política de Seguridad de la Información
- Política de Prevención del Blanqueo de Capitales
- Política de Derechos Humanos
- Política de Recursos Humanos
- Política Medioambiental
- Protocolo de Investigación ante actos de Fraude e Incumplimiento

www.cirsa.com

2021

Ctra. de Castellar, 298 · 08226 Terrassa. Barcelona. Spain · T 34 93 728 33 18 · lineaetica@cirsa.com · www.cirsa.com