

POLÍTICA DEL SISTEMA INTERNO DE INFORMACIÓN
KERABEN GRUPO, SAU

| | |
|---------------------------|---|
| Título del documento | Política del Sistema Interno de Información |
| Propietario del contenido | Departamento de Cumplimiento |
| Versión | 1.0 |
| Fecha | Junio de 2023 |
| Aprobado por | Consejo de Administración |

1. Objetivo de esta Política

El 23 de octubre de 2019, el Parlamento Europeo y el Consejo de la Unión Europea aprobó la Directiva relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (la "Directiva"). Esta Directiva, que se aplicará en la legislación nacional de todos los Estados miembros de la UE, exige que todas las Organizaciones con más de 50 empleados dispongan de una política de denuncia de irregularidades.

La Directiva fue transpuesta en España por 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 el resto del mundo se aplica una legislación similar.

Las conductas indebidas solo se denuncian si las personas que las observan se sienten seguras para hacerlo; a menudo, los empleados son reacios a comunicar sus sospechas por miedo a represalias.

Sin embargo, la comunicación, por parte de los empleados, de comportamientos potencialmente incorrectos es la forma más eficaz de que las empresas descubran comportamientos poco éticos. Por lo tanto, es esencial contar con una política de comunicación de irregularidades adecuada, que garantice la confidencialidad y la protección del informante (tal y como se define más adelante).

Si observas un mal comportamiento o una mala conducta, tienes que hablar. Al hacerlo, das a Keraben Grupo, SAU (en adelante "Keraben" o la "Empresa") la oportunidad de tratar el asunto. Permanecer en silencio ante una posible mala conducta puede empeorar la situación y disminuir la confianza.

El objetivo principal de esta política de comunicación de irregularidades (en adelante, la "**Política del Sistema Interno de Información**" o, indistintamente, "**Política de Comunicación de Irregularidades**" o la "**Política**") es apoyar los valores de Keraben mediante:

- contribuir a disuadir la comisión de delitos;
- fomentar la revelación de irregularidades;
- garantizar que las personas que denuncien irregularidades puedan hacerlo de forma segura y con la confianza de que estarán protegidas frente a represalias; y
- el cumplimiento de las obligaciones legales y reglamentarias de Keraben.

2. A quién va dirigida esta Política

La Política de Comunicación de Irregularidades se aplica interna y externamente a todos (i) los empleados y ex empleados, (ii) los consultores independientes, (iii) los accionistas y personas pertenecientes al Órgano de Administración o Dirección de la Empresa, incluidos los miembros no ejecutivos, (iv) los candidatos a procesos de selección, (v) personal en prácticas, remunerados y no remunerados, (vi) los voluntarios, (vii) los facilitadores y (viii) los proveedores y contratistas, incluidos los subcontratistas y empleados de contratistas de Keraben con información relevante sobre actividades poco éticas o ilegales y/o para plantear inquietudes.

3. **Ámbito de aplicación de la política**

La comunicación de conductas ilegales, deshonestas y/o ilícitas dentro de las operaciones de Keraben, de forma confidencial o anónima, con protección frente a represalias.

La persona que comunica los hechos es el "**informante**".

La Política de Comunicación de Irregularidades no cubre todos los tipos de irregularidades que pueden ocurrir; se aplican algunas restricciones sobre qué tipo de divulgaciones pueden presentarse dentro del ámbito de esta Política. Se pueden comunicar acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, infracciones de las Políticas de Keraben y/o violaciones de leyes y reglamentos, incluidos las conductas u omisiones contrarias a los siguientes asuntos (en adelante, la "**Malas Conductas**" o la "**Mala Conducta**"):

- Prevención del fraude social, como el empleo ilegal, la evasión del pago de cotizaciones a la Seguridad Social, la percepción de prestaciones injustificadas y, en general, cualquier infracción de la legislación social;
- Prevención del fraude fiscal, como ingresos no declarados, fraude del IVA, pago de salarios con ingresos no declarados, construcciones para ocultar ingresos a las autoridades competentes, blanqueo de dinero, inexactitud de los estados financieros, irregularidades contables y de auditoría, etc;
- Contratación pública;
- Servicios, productos y mercados financieros, blanqueo de capitales y la financiación del terrorismo;
- Seguridad, conformidad y calidad de los productos;
- Seguridad en el transporte;
- Medio ambiente;
- Protección contra las radiaciones y seguridad nuclear;
- Salud pública;
- Seguridad y salud en el trabajo;
- Protección del consumidor;
- Protección de la intimidad y los datos personales, y seguridad de la red y los sistemas de información;
- Infracciones relacionadas con las leyes de competencia y antimonopolio pertinentes;
- Infracciones relacionadas con el Código de Conducta;
- Soborno, corrupción o pagos ilegales;
- Intimidación;
- Acoso sexual;

- Cuestiones éticas (por ejemplo, racismo, discriminación, conflicto de intereses, violación de los derechos humanos etc);
- Sanciones económicas;
- Inexactitud de los registros financieros: irregularidades contables y de auditoría;
- Robo;

4. Informes no cubiertos por la Política

Es importante señalar que esta Política no se aplica a las quejas personales relacionadas con el trabajo, como preocupaciones o insatisfacción con el salario, los turnos o las circunstancias del lugar de trabajo, cuestiones interpersonales o evaluaciones del rendimiento.

Este tipo de asuntos deben comunicarse a través de los canales internos habituales, por ejemplo, poniéndose en contacto directamente con su jefe o con el departamento de RRHH. En la mayoría de los casos, su jefe directo, el jefe del siguiente nivel y el responsable de RR.HH. son excelentes recursos para obtener orientación o resolver dudas relacionadas con las políticas y procesos de la Empresa y/o específicos del puesto, las responsabilidades laborales, los problemas con los compañeros de trabajo, las cuestiones disciplinarias o los problemas relacionados con el entorno laboral.

5. Cuándo y cómo comunicar una Mala Conducta

Si Usted descubre, tiene conocimiento o tiene motivos razonables para sospechar que se está produciendo una potencial Mala Conducta dentro de las operaciones de Keraben, se le anima a notificar inmediatamente a Keraben el incidente en cuestión.

Toda persona que presente una comunicación en virtud de esta Política debe actuar de buena fe.

Todas las preocupaciones se tomarán en serio. El Informante no necesita disponer de pruebas concluyentes antes de presentar una comunicación: basta con tener una sospecha razonable de conducta indebida. Aunque no tiene que probar sus alegaciones, es más probable que se consideren razonables si puede respaldarlas con alguna información objetiva de apoyo, como correos electrónicos, notas de archivo o recibos, entre otros.

5.1. Diferentes canales de información

Keraben recomienda utilizar el Sistema Interno de Información antes que el externo, ya que esto permite a Keraben investigar y resolver rápidamente la inquietud planteada.

El Informante puede elegir a su entera discreción si desea comunicar los hechos de forma anónima o si desea revelar su identidad. No obstante, debe tenerse en cuenta que es muy importante obtener la máxima información posible que ayude a investigar los hechos. Permanecer en el anonimato puede repercutir en la calidad y el nivel de la investigación del caso o puede imposibilitar la continuación de la investigación.

(i) Sistema Interno de Información (“Canal Interno de Información”).

Keraben dispone de una herramienta de comunicación interna on line.

La herramienta de comunicación de irregularidades está gestionada por una organización externa e independiente y garantiza que las revelaciones de hechos se traten en todo momento de forma confidencial.

Se puede acceder a la herramienta de comunicación a través de un portal web, pero también utilizando su teléfono móvil o tableta a través del siguiente enlace: <https://keraben.integrityline.com>

Puede seleccionar su país y su idioma. Si desea comunicar hechos, se le pedirá que incluya una descripción del incidente o de su sospecha y también se le pedirá que responda a preguntas como: ¿cuál es su relación con la empresa?, ¿en qué país se encuentra?, ¿nombre del departamento donde se produjo el incidente?, ¿quién estuvo implicado?

Todas las respuestas a estas preguntas son importantes para la investigación.

Si desea enviar un informe de audio, hay un botón en la parte superior de la página que, una vez activado, grabará su mensaje. Puede dejar un mensaje en su propio idioma. Tenga en cuenta que la herramienta distorsionará la voz del mensaje grabado para garantizar el anonimato.

Independientemente de que la comunicación se realice a través de la aplicación o del portal web, el Informante puede permanecer en el anonimato, ya que la herramienta incorpora un buzón seguro que el Informante anónimo puede utilizar al realizar la comunicación y que le permite recibir comentarios o solicitudes de información adicional. El Informante recibirá un número de identificación del expediente y se le pedirá que elija una contraseña para acceder al buzón seguro. Si el Informante opta por el anonimato, el Responsable del Sistema Interno de Información no conocerá su identidad.

(ii) Canal Externo

Aunque se anima a los empleados y partes interesadas a utilizar el Canal Interno de Información previsto por Keraben en la Sección 5.1 (i) anterior, la Autoridad Independiente de Protección del Informante (A.A.I.) también ofrece un canal externo de información (el “Canal Externo”).

La comunicación puede presentarse oralmente o por escrito a la A.A.I. o, en su caso, ante las autoridades u órganos autonómicos correspondientes.

Las normas relativas al Canal Externo pueden consultarse en el sitio web de la autoridad competente. Es importante saber que la A.A.I. puede decidir archivar una comunicación sin consecuencias. En caso de un elevado número de comunicaciones, la A.A.I. puede establecer prioridades.

6. ¿Cómo se gestionan e investigan las comunicaciones?

Todas las comunicaciones recibidas en el Sistema Interno de Información se tratarán de acuerdo con el siguiente procedimiento:

6.1. Acuse de recibo

Cuando se comuniquen unos hechos en la herramienta del Sistema Interno de Comunicación, el Informante recibirá una notificación inmediata y automática del acuse de recibo.

6.2. Primera proyección y comentarios

El Responsable del Sistema Interno de Información realizará un primer examen de la Comunicación recibida. Comprobará si la conducta indebida informada entra en el ámbito de aplicación de la Política (véase la Sección 3) y, en caso afirmativo, solicitará a un equipo de investigación (el “Equipo de Investigación”) que investigue los hechos comunicados, respetando siempre las obligaciones de confidencialidad y privacidad.

En un plazo de siete (7) días laborables a partir de la recepción de la comunicación, el Informante recibirá una comunicación inicial relativa a la investigación.

Asimismo, en caso de que los hechos comunicados se consideren fuera del ámbito de aplicación de la Política, se informará de ello al Informante (dentro de dicho plazo) y se le animará a tratar el asunto con su Superior o con RR.HH..

6.3. Investigación

Si la Mala Conducta comunicada entra en el ámbito de aplicación de la Política, los hechos se investigarán con prontitud y diligencia, de conformidad con esta Política.

En caso de ser necesario, los hechos se investigarán en estrecho diálogo con el Informante. Si el Informante reveló su identidad, la comunicación con el Equipo de Investigación puede tener lugar por vía telefónica, correo electrónico, o de manera presencial. Si el Informante comunicó la Mala Conducta de forma anónima, la comunicación tendrá lugar a través del buzón seguro de la herramienta del Sistema Interno de Información.

La identidad del Informante solo podrá revelarse con su consentimiento explícito por escrito.

Cuando sea necesario para llevar a cabo una investigación exhaustiva y confidencial, podrán participar en el proceso de investigación personas externas (por ejemplo, abogados externos, empresas de investigación, empresas de contabilidad etc), siempre respetando las obligaciones de confidencialidad y privacidad. Si se ha producido un delito penal, también pueden participar las autoridades policiales. El Equipo de Investigación puede estar compuesto por diferentes funciones, dependiendo de la naturaleza de los hechos comunicados y del departamento o unidad de negocio implicado. Los representantes de los departamentos Financiero, Jurídico, RR.HH., Calidad y Medio Ambiente etc podrían participar en la investigación en función de la naturaleza de los hechos comunicados.

6.3.1. Conflicto de intereses

Si el Responsable del Sistema Interno de Información y/o un miembro del Equipo de Investigación tienen un conflicto de intereses, serán excluidos del Equipo de Investigación.

6.3.2. Decisión

Una vez concluida la investigación, el Equipo de Investigación elaborará un informe resumido en el que se describirán las medidas de investigación llevadas a cabo. Una versión anónima del informe de conclusiones podrá compartirse fuera del Equipo de Investigación con el Consejo de Administración, únicamente en la medida en que sea necesario, con el fin de llegar a una decisión final.

El Equipo de Investigación tomará una decisión final sobre si los hechos comunicados están probados y, en consecuencia, se definirán las acciones pertinentes necesarias para poner fin a la Mala Conducta y proteger a la Empresa.

En caso de que no haya pruebas suficientes, no se tomará ninguna medida.

El Informante será informado a través de la herramienta del Sistema Interno de Información de la conclusión de la investigación, y de la decisión adoptada en el plazo de tres (3) meses desde el acuse de recibo de la comunicación de los hechos. Cuando existan razones justificadas, dicho plazo podrá prorrogarse por tres (3) meses más.

6.3.3. Mantenimiento de registros

El registro de los hechos comunicados por el Informante se conservarán en la herramienta del Sistema Interno de Información garantizando un tratamiento estrictamente confidencial del expediente.

Una vez que se haya tramitado y resuelto el expediente, todos los datos personales incluidos en el mismo se anonimizarán y, como tales, se archivarán a efectos de informes históricos sin incumplir las obligaciones de la normativa reguladora de Protección de Datos (Reglamento UE 2016/679 y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales).

7. Protección del Informante

(i) No divulgación

El procedimiento del Sistema Interno de Información garantizará que no se revele la identidad del Informante y que, debido a la investigación, no pueda establecerse ningún vínculo con él. Durante todo el proceso de investigación y posteriormente, todos los miembros del Equipo de Investigación están sujetos a una estricta confidencialidad.

Salvo mandato legal y/o judicial, no se revelará la identidad del Informante. Dependiendo del tipo de conducta indebida informada, puede ser legalmente necesario involucrar a las autoridades públicas para iniciar una investigación oficial. En tales casos, Keraben puede verse obligada a comunicar el nombre del Informante a las autoridades públicas. Keraben informará al Informante cuando se haya comunicado su identidad, excepto cuando dicha revelación pudiera poner en peligro la investigación o el proceso judicial.

Para conocer el número y las categorías de hechos informados, se puede elaborar un resumen anónimo de los expedientes para el Consejo de Administración.

ii) **No represalias**

A menos que un Informante haya realizado de manera consciente una comunicación falsa, haya facilitado información falsa o engañosa en el curso de la investigación, o haya actuado de mala fe, el Informante no podrá ser despedido, suspendido, amenazado, acosado, intimidado ni objeto de represalias por haber realizado una comunicación de buena fe o por haber colaborado en la tramitación o investigación de unos hechos en virtud de esta Política.

Las denuncias de represalias contra un Informante se toman muy en serio. Todas las denuncias de este tipo deben elevarse y revisarse con prontitud y, cuando proceda, investigarse.

Este principio de no represalia y no divulgación también aplica si la investigación demuestra finalmente que los hechos comunicados era infundados.

8. **Protección de datos**

La tramitación de un expediente conlleva inevitablemente el tratamiento de datos personales (en adelante, "**Datos Personales**") en el sentido del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de Datos Personales y a la transferencia de estos datos dentro de su territorio ("RGPD"), la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el resto de leyes de privacidad aplicables.

Sus Datos Personales son tratados por Keraben Grupo SAU, Carretera Valencia- Barcelona Km 44,3; 12520-Nules (Castellón) como Responsable del tratamiento. Para la prestación del Sistema Interno de Información (herramienta de comunicación online), utilizamos un proveedor de servicios que tiene la consideración de Encargado del tratamiento y destinatario de sus Datos Personales. Puede ponerse en contacto con nosotros con respecto a cuestiones relacionadas con el tratamiento de sus Datos Personales a través del correo electrónico lopd@victoriaceramics.com.

Los intereses legítimos del Responsable del tratamiento para recibir y tramitar la investigación de los hechos comunicados justifican claramente el tratamiento de los Datos Personales. Se asegurará de que cada tratamiento de Datos Personales a este respecto se realice de conformidad con el RGPD, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y todas las demás leyes de privacidad aplicables.

La herramienta del Sistema Interno de Información es operada y mantenida por EQS Group AG, un proveedor internacional de software en la nube sobre cumplimiento corporativo. El Grupo EQS no puede leer los expedientes, ya que están cifrados con una clave a la que el Grupo EQS no tiene acceso. El Grupo EQS mantiene las medidas técnicas adecuadas para garantizar la

protección y confidencialidad de los datos. Los datos que proporcione se almacenarán en una base de datos segura de EQS. Todos los datos almacenados en la base de datos son encriptados por EQS utilizando tecnología de última generación.

Los datos procesados también podrán ser transferidos a terceros, tales como autoridades policiales, financieras o de otro tipo, auditores o asesores externos, a los que se recurriría en el marco de la tramitación de una investigación de hechos comunicados.

Dentro de Keraben, los datos solo serán accesibles por las funciones pertinentes y solo en la medida en que dicho acceso sea necesario para la correcta aplicación de esta Política. Todo tratamiento será documentado y los datos no probados o irrelevantes serán suprimidos.

Cuando los Datos Personales se transfieran fuera de la UE, tomaremos las medidas de seguridad adecuadas para proteger sus Datos Personales.

En cualquier caso, los Datos Personales no se conservarán más allá del plazo de prescripción aplicable a los hechos examinados.

Los Informantes tendrán derecho a acceder a los Datos Personales que les conciernan y a rectificarlos. Los Datos Personales de otros interesados no son accesibles. Los Datos Personales incompletos, que ya no sean necesarios o exactos serán suprimidos. Estos derechos pueden ejercerse poniéndose en contacto con el Coordinador de Protección de Datos en lopd@victoriaceramics.com. No obstante, este derecho podrá limitarse o aplazarse en interés de una investigación.

El interesado reconoce haber sido informado de los siguientes derechos, en la medida en que sean aplicables:

- derecho a solicitar al Responsable del tratamiento que limite el tratamiento que le concierne, derecho a oponerse al tratamiento, derecho de rectificación o supresión y derecho a la transferibilidad de los Datos Personales;
- derecho a presentar una reclamación ante la autoridad de protección de datos.