

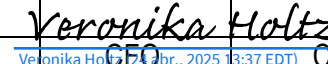
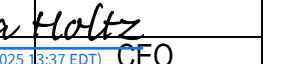


## POLITICA

|                |   |            |   |
|----------------|---|------------|---|
| N°             | : | CMP-007/03 | Referencia: <b>MANUAL SISTEMA DE PREVENCIÓN DE DELITOS</b>          |
| Página         | : | 52         |   |
| F. de Emisión  | : | 23/03/2016 |   |
| F. de Revisión | : | 31/03/2025 | <b>LEY N°20.393 RESPONSABILIDAD PENAL DE LAS PERSONAS JURIDICAS</b> |

| Rige Desde: | Emitido Por | Autorizado por   | Autorizado Por       | Autorizado Por  | Autorizado Por  |
|-------------|-------------|--|----------------------|---|---|
| 01/04/2016  | Compliance  | <br><u>Lorena Venegas (24 abr.. 2025 11:23 EDT)</u> |                      | <br><u>Darko Louit (29 abr.. 2025 10:37 EDT)</u>               |   |
|             | KHSA        | Compliance Officer   | General Counsel KHSA | <br><u>Veronika Holtz (22 abr.. 2025 13:37 EDT)</u><br>CEO KHSA | <br><u>Darko Louit (29 abr.. 2025 10:37 EDT)</u><br>CEO KCC & KHSA |

## APLICACION DE LA POLITICA

| Grupo | Total | No Aplica a:                   |
|-------|-------|--------------------------------|
| KCC   | X     |                                |
| KHSA  | X     | KCO – KMP – KMEX – KIMX - KFMX |
| KMC   | X     | KMMP – KMC México              |

**MANUAL**

**SISTEMA DE PREVENCIÓN DE DELITOS**

**GRUPO DE EMPRESAS KOMATSU CUMMINS**

|            |            |  |                           |             |                   |
|------------|------------|--|---------------------------|-------------|-------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 2 de<br>51 |
|------------|------------|--|---------------------------|-------------|-------------------|

## INDICE

|   |           |
|---|-----------|
| <b>1. MENSAJE DEL SENIOR MANAGEMENT TEAM .....</b>  | <b>6</b>  |
| <b>2. INTRODUCCIÓN LEY N°20.393 .....</b>   | <b>6</b>  |
| 2.1 Ámbito de Aplicación de la Ley .....  | 7         |
| 2.2 Presupuestos de la Responsabilidad Penal .....  | 7         |
| 2.3 Penas Previstas en la Ley.....  | 8         |
| 2.4 Cumplimiento del Deber de Dirección y Supervisión .....   | 9         |
| 2.5 Encargado de Prevención de Delitos .....  | 9         |
| <b>3. DESIGNACIÓN DE RESPONSABILIDADES .....</b>  | <b>10</b> |
| 3.1 Encargado de Prevención de Delitos (Compliance Officer) .....   | 10        |
| 3.1.1 Designación.....  | 10        |
| 3.1.2 Deberes y Responsabilidades .....   | 11        |
| 3.1.3 Medios y Recursos Necesarios para su Desempeño.....   | 12        |
| 3.2 Senior Management Team .....  | 12        |
| 3.3 Comité de Ética .....   | 13        |
| 3.4 Gerencias Generales .....   | 13        |
| 3.5 Ejecutivos y Trabajadores.....  | 13        |
| 3.6 Prestadores de Servicios, Proveedores y Distribuidores.....   | 14        |
| <b>4. GESTION DE RIESGOS.....</b>   | <b>15</b> |
| 4.1 Identificación, Análisis y Evaluación.....  | 15        |
| 4.2 Actividades de Control .....  | 15        |
| 4.3 Difusión, Comunicación e Información.....   | 15        |
| 4.4 Seguimiento y Actualización .....   | 16        |
| <b>5. POLÍTICAS Y PROCEDIMIENTOS ESPECÍFICOS DE CONDUCTA ÉTICA, DE CONTROL INTERNO Y GESTIÓN DE RIESGOS .....</b> | <b>16</b> |
| 5.1 Código de Conducta Empresarial .....  | 16        |
| 5.2 Mecanismos de Control Financiero-Contable .....   | 17        |
| <b>6. POLÍTICAS, PROCEDIMIENTOS PARA PREVENIR DELITOS EN PARTICULAR</b>   | <b>18</b> |
| 6.1 Prevención del Cohecho a Funcionario Público Nacional o Extranjero .....                                      | 18        |
| 6.1.1 Política y Procedimiento de Contacto con Funcionarios Públicos.....   | 22        |

|            |  |           |
|------------|--|-----------|
| 6.1.2      | Política y Procedimiento General de Donaciones Regulares, Política y Procedimiento de Donaciones de Emergencia o Disaster Relief ..... | 22        |
| 6.1.3      | Política de Auspicios y/o Patrocinios .....  | 23        |
| 6.1.4      | Política de Regalos, Invitaciones a Eventos y Viajes .....   | 23        |
| 6.1.5      | Política de Conflictos de Interés .....  | 24        |
| 6.1.6      | Declaración Jurada de Persona Expuesta Políticamente .....   | 24        |
| 6.2        | Prevención de la Corrupción Entre Particulares.....  | 25        |
| 6.2.1      | Política General de Compras de Insumos, Servicios y Activos Fijos .....  | 27        |
| 6.2.2      | Política General de Regalos, Invitaciones a Eventos y Viajes .....   | 27        |
| 6.2.3      | Política de Conflicto de Interés y Declaración de Conflictos de Interés .....  | 28        |
| 6.2.4      | Medidas Adicionales.....   | 28        |
| 6.3        | Prevención del Lavado de Activos, Financiamiento del Terrorismo y Receptación<br>29  |           |
| 6.3.1      | Medidas Para el Conocimiento de Clientes, Proveedores, Prestadores de Servicios y Distribuidores .....                                 | 35        |
| 6.3.2      | Procedimiento Ventas Contado Mesón .....   | 36        |
| 6.3.3      | Incorporación de Cláusula Ley N°20.393 en Contratos .....  | 37        |
| 6.3.4      | Difusión de Señales de Alertas.....  | 37        |
| 6.3.5      | Medidas sobre Aceptación, Mantención o Prohibición de Clientes, Proveedores, Prestadores de Servicios y Distribuidores .....           | 37        |
| 6.3.6      | Actualización de la Información de Clientes, Proveedores, Prestadores de Servicios y Distribuidores. ....                              | 37        |
| 6.4        | Prevención de Delitos Informáticos .....   | 38        |
| 6.5        | Prevención de Ilícitos Medioambientales .....  | 39        |
| 6.5.1      | Programa de Auditoría de Cumplimiento Legal Ambiental .....  | 40        |
| 6.5.2      | Medidas Adicionales.....   | 42        |
| 6.6        | Prevención de la Apropiación Indebida.....   | 42        |
| 6.7        | Prevención del Ilícito Contenido en el Artículo 318 ter del Código Penal.....  | 43        |
| <b>7.</b>  | <b>REGISTROS.....</b>  | <b>44</b> |
| <b>8.</b>  | <b>CONSERVACIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN.....</b>   | <b>45</b> |
| <b>9.</b>  | <b>SUPERVISIÓN Y MONITOREO .....</b>   | <b>45</b> |
| <b>10.</b> | <b>CAPACITACIÓN.....</b>   | <b>45</b> |

|   |    |
|---|----|
| 11. PLATAFORMA DE GESTIÓN ÉTICA .....   | 46 |
| 12. PROCEDIMIENTO DE INVESTIGACIONES INTERNAS .....   | 48 |
| 13. COMUNICACIÓN DE RESULTADOS A LA AUTORIDAD .....   | 49 |
| 14. MEDIDAS DISCIPLINARIAS POR INCUMPLIMIENTO DEL SISTEMA DE<br>PREVENCIÓN DE DELITOS ..... | 50 |
| 15. AUDITORÍAS ANUALES DEL MODELO DE PREVENCIÓN DE DELITOS.....                             | 50 |
| 16. CONTROL DE VERSIONES .....  | 51 |
| 17. VIGENCIA .....  | 51 |

## 1. MENSAJE DEL SENIOR MANAGEMENT TEAM

Desde sus inicios el Grupo de Empresas Komatsu Cummins<sup>1</sup> (en adelante “la Compañía”) se ha regido por estrictos principios éticos que nos han dado la fortaleza necesaria para transformarnos en una empresa exitosa. Parte de estos principios son aquellos relacionados con el estricto cumplimiento de las normas legales y éticas.

En un área tan delicada como es la responsabilidad penal de las empresas, es indispensable adoptar los procedimientos preventivos que sean necesarios para aminorar las posibilidades de incurrir en ilícitos.

El Sistema de Prevención de Delitos contenido en este Manual está al servicio de cualquier trabajador, cliente, proveedor, distribuidor o tercero relacionado con nuestro negocio y busca constituirse en una guía operativa de las diversas actividades de prevención y/o mitigación de riesgos de comisión de delitos que se han identificado como probables en las distintas empresas de la Compañía.

En la Compañía la función del Encargado de Prevención de Delitos es desempeñada por el Regional Compliance Officer de Komatsu Holding South America Ltda., razón por la que en el presente Manual se le denomina bajo ese nombre.

Adicionalmente, el Sistema de Prevención de Delitos es complementario de los siguientes instrumentos internos:

- a) Código Mundial de Conducta Empresarial de Komatsu.
- b) Reglamento Interno de Orden, Higiene y Seguridad.
- c) Cláusulas Ley N°20.393 en contratos de trabajo de colaboradores.
- d) Cláusulas Ley N°20.393 en los contratos con clientes, proveedores, prestadores de servicios y otros terceros.
- e) Komatsu Way.
- f) Plataforma de Gestión Ética (Canal de Denuncias).

## 2. INTRODUCCIÓN LEY N°20.393

El 2 de diciembre de 2009 entró en vigencia la Ley N°20.393 que estableció la Responsabilidad Penal de las Personas Jurídicas por los delitos de cohecho a funcionario público nacional y extranjero, lavado de activos y financiamiento del terrorismo.

Posteriormente, el artículo 16 de la Ley N° 20.931 de 5 de julio de 2016, -conocida como la “Ley de Agenda Corta Antidelincuencia”-, modificó el artículo 1° y 15 de la Ley N° 20.393, incorporando el delito de receptación al catálogo de delitos base de esta última.

<sup>1</sup> Para efectos de este Manual de Prevención de Delitos, se entenderá por el Grupo de Empresas Komatsu Cummins a (i) la sociedad Komatsu Cummins Chile Ltda. y sus sociedades filiales en Chile, y (ii) la sociedad Komatsu Holding South.America Ltda. y sus sociedades filiales en Chile.

|            |            |  |                           |              |                   |
|------------|------------|--|---------------------------|--------------|-------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHS A | Página 6 de<br>51 |
|------------|------------|--|---------------------------|--------------|-------------------|

En noviembre de 2018 la Ley N°20.393 sufrió una nueva modificación con la entrada en vigencia de la Ley N°21.121 que incorporó cuatro nuevos delitos económicos al catálogo, a saber; Corrupción entre particulares, Administración Desleal, Negociación incompatible y Apropiación indebida.

Dos meses después, con fecha de 31 de enero de 2019, se publicó la Ley N°21.132 que moderniza el Servicio Nacional de Pesca (SERNAPESCA), añadiendo otros cuatro delitos al catálogo existente de la Ley N°20.393, a saber, delito de contaminación de aguas, comercialización de productos vedados, pesca ilegal de recursos del fondo marino y procesamiento, elaboración y almacenamiento de productos colapsados o sobreexplotados sin acreditar origen legal.

Enseguida, en abril de 2021 se publicó la Ley N°21.235 donde se incorpora el delito de tráfico ilícito de migrantes y trata de personas.

En enero de 2022 se publicó la Ley N°21.412 que tiene como objetivo fortalecer la regulación existente relativa al control y tenencias de armas.

Ahora, con la entrada de vigencia de la Ley N°21.595 sobre Delitos Económicos y Ambientales, que, además de introducir 291 delitos al catálogo de la Ley N°20.393, establece responsabilidad penal para la persona jurídica cuando el delito fuere perpetrado en el marco de su actividad por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, siempre que la perpetración del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica.

De esta forma se instaura en Chile un sistema de responsabilidad penal aplicable a las personas jurídicas, con la identificación de sus presupuestos específicos, de las circunstancias que la modifican, estableciendo las penas asociadas y las reglas de determinación de las mismas. Es por esta razón, que la Ley N°20.393 requiere que las empresas adopten un “**Modelo de Prevención de Delitos**” efectivamente implementado.

## 2.1 Ámbito de Aplicación de la Ley

La Ley N°20.393 se aplica a todas las personas jurídicas de derecho privado (incluyendo las empresas individuales de responsabilidad limitada) y comprende asimismo a las empresas del Estado. Con la introducción de la Ley N°21.595, las disposiciones de la ley atribuyen responsabilidad penal a los delitos cometidos directa e indirectamente por sus dueños, controladores, ejecutivos, representantes o quienes realicen actividades de administración y supervisión y sus subalternos. Además, se incluye como responsable de los delitos cometidos por personas naturales estando sometidas a la autoridad de los anteriores.

## 2.2 Presupuestos de la Responsabilidad Penal

La Ley establece un sistema de atribución de responsabilidad penal para las empresas que es independiente de la responsabilidad individual de las personas naturales que intervienen en el hecho punible. Por lo anterior, la Ley N°20.393 no establece un sistema de responsabilidad objetiva, es

|            |            |  |                           |              |                   |
|------------|------------|--|---------------------------|--------------|-------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHS A | Página 7 de<br>51 |
|------------|------------|--|---------------------------|--------------|-------------------|

decir, la empresa no responde en forma “automática” cada vez que uno de sus integrantes comete uno de los delitos por los cuales se permite sancionar a la empresa.

Por el contrario, la Ley -en cuanto sistema de imputación a las empresas- permite que aquellas empresas que se organizan de manera adecuada (se autorregulan correcta y eficientemente), no sean sancionadas en aquellos casos en que sean utilizadas para la comisión de un delito por un miembro que actúa como externo a la misma, es decir, fuera del marco de sus atribuciones y en provecho exclusivamente propio o de un tercero. Dicho de otro modo, el sistema de responsabilidad penal adoptado en Chile para las personas jurídicas hace depender la responsabilidad de las empresas en el comportamiento que haya adoptado la empresa. En lo medular, se sostiene que la organización empresarial responde por haber incumplido sus deberes de “*dirección y supervisión*”, a través de la omisión de sus deberes de prevención de ciertas conductas delictivas o contribución al hecho por la vía de haberse organizado de un modo que favorece o no impide, ni dificulta la realización de ese tipo de hechos.

De acuerdo al artículo 3° de la Ley N°20.393, los requisitos de la responsabilidad penal para las personas jurídicas son los siguientes:

- a) Que el delito haya sido perpetrado en el marco de su actividad por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, siempre que la perpetración del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica.
- b) Que habiendo concurrido los requisitos del numeral anterior, una persona jurídica también será responsable por el hecho perpetrado por o con la intervención de una persona natural relacionada en los términos previstos por dicho inciso con una persona jurídica distinta, siempre que ésta le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación.
- c) Por último, lo anterior no tendrá aplicación cuando el hecho punible se perpetre exclusivamente en contra de la propia persona jurídica.

## **2.3 Penas Previstas en la Ley**

Las sanciones penales que contempla la Ley en su título segundo, para las personas jurídicas por haber incurrido en alguno de los delitos en ella establecidos, son los siguientes (asumiendo que concurren los demás presupuestos de imputación):

- Extinción de la personalidad jurídica.
- Inhabilitación para contratar con el Estado.
- La pérdida de beneficios fiscales y la prohibición de recibirlos.
- La supervisión de la persona jurídica.

|            |            |  |                           |              |                   |
|------------|------------|--|---------------------------|--------------|-------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHS A | Página 8 de<br>51 |
|------------|------------|--|---------------------------|--------------|-------------------|



- Multas.
- El comiso a que se refiere el inciso tercero del artículo 14 de la Ley.
- La publicación de un extracto de la sentencia condenatoria.

## **2.4 Cumplimiento del Deber de Dirección y Supervisión**

Conforme a la Ley N°20.393 que establece la responsabilidad penal de las personas jurídicas, la Empresa podrá ser responsable penalmente de los delitos que el artículo N° 1 de la mencionada Ley señala, siempre que estos sean cometidos en el marco de su actividad por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, siempre que la perpetración del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica.

Además, la empresa también será responsable por el hecho perpetrado por o con la intervención de una persona natural relacionada en los términos previstos por el inciso primero del artículo N° 3 de la Ley N° 20.393 con una persona jurídica distinta, siempre que ésta le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación.

El Modelo de Prevención de Delitos se refiere a un conjunto de medidas y procedimientos que una persona jurídica implementa para prevenir, detectar y responder a los delitos señalados en el artículo N° 1 de la Ley 20.393. En ese sentido, el artículo N° 4 de dicha Ley hace mención del Modelo de Prevención de Delitos y establece que se entenderá que un Modelo de Prevención de Delitos efectivamente implementado por la persona jurídica es adecuado para los efectos de eximirla de responsabilidad penal cuando, en la medida exigible a su objeto social, giro, tamaño, complejidad, recursos y a las actividades que desarrolle, considere seria y razonablemente los siguientes aspectos:

- Identificación de las actividades o procesos de la persona jurídica que impliquen riesgo de conducta delictiva según el artículo N° 1 de la Ley N°20.393.
- Establecimiento de protocolos y procedimientos para prevenir y detectar conductas delictivas en el contexto de las actividades a que se refiere el número anterior, los que deben considerar necesariamente canales seguros de denuncia y sanciones internas para el caso de incumplimiento.
- Asignación de uno o más sujetos responsables de dichos protocolos.
- Previsión de evaluaciones periódicas por terceros independientes y mecanismos de perfeccionamiento o actualización a partir de tales evaluaciones.

## **2.5 Encargado de Prevención de Delitos**

En miras a implementar un Modelo de Prevención de Delitos, la Compañía designó al Gerente de Cumplimiento (Compliance Officer) como Encargado de Prevención de Delitos que cuenta con los

|            |            |  |                           |             |                   |
|------------|------------|--|---------------------------|-------------|-------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 9 de<br>51 |
|------------|------------|--|---------------------------|-------------|-------------------|

siguientes atributos:

- Acceso directo y autonomía respecto de la administración de la Empresa para reportar respecto a su gestión.
- Autoridad efectiva de dirección y supervisión, para informar de manera oportuna respecto a las medidas y planes implementados en el cumplimiento de su gestión.
- Facultades para rendir cuenta de su gestión y solicitar la adopción de las medidas necesarias para su cometido que pudieran exceder su competencia.
- Supervisión del Sistema de Prevención de los Delitos: el Encargado de Prevención de Delitos (Compliance Officer), en conjunto con la administración de la Compañía, deberá establecer métodos para la aplicación efectiva del Sistema de Prevención de Delitos y su supervisión a fin de detectar y corregir sus fallas, así como actualizarlo de acuerdo al cambio de circunstancias de la respectiva entidad.

### **3. DESIGNACIÓN DE RESPONSABILIDADES**

Con el propósito de asegurar la eficacia de la adopción e implementación del presente Sistema de Prevención de Delitos, y su posterior monitoreo, la Compañía ha incorporado nuevas funciones y responsabilidades en su organización, las que se encuentran descritas en una “Matriz de Responsabilidades” (Anexo N°1).

#### **3.1 Encargado de Prevención de Delitos (Compliance Officer)**

El Encargado de Prevención de Delitos (Compliance Officer) será designado por el Senior Management Team (“SMT”) y estará encargado de velar por la adopción e implementación efectiva del Sistema de Prevención de Delitos. En la Compañía, la función de Encargado de Prevención de Delitos será desempeñadas por el Compliance Officer de la Compañía.

El Encargado de Prevención de Delitos (Compliance Officer) será responsable de la adecuación y actualización permanente del Sistema de Prevención de Delitos a objeto que los directores, ejecutivos, trabajadores, clientes, proveedores y otros que se relacionen con la Compañía estén capacitados respecto a las obligaciones legales relacionadas con la prevención de delitos.

##### **3.1.1 Designación**

- a) El Compliance Officer deberá contar con autonomía respecto de la administración de la Compañía, de sus dueños, socios, accionistas o controladores. No obstante, lo anterior, podrá ejercer labores de contraloría o auditoría interna.
- b) El Compliance Officer durará en su cargo un plazo de tres años, plazo que podrá ser prorrogado por períodos consecutivos de tres años.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 10 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- c) El Compliance Officer ejercerá sus funciones para todas las empresas del Grupo de Empresas Komatsu y Cummins que están constituidas en Chile.
- d) En caso que el Compliance Officer se encuentre temporal o definitivamente impedido de ejercer sus funciones, sus funciones serán cumplidas por el Director Legal o General Counsel hasta que el SMT designe un nuevo titular.
- e) La revocación de la designación del Compliance Officer sólo procederá en casos graves y calificados, circunstancia que deberá ser evaluada por el SMT.

### 3.1.2 Deberes y Responsabilidades

- a) Velar porque el Sistema de Prevención de Delitos efectivamente prevenga y detecte las infracciones a la Ley y otras regulaciones, a las políticas corporativas y al Código de Conducta Empresarial.
- b) Asegurar la obtención de recursos para garantizar la efectividad del Sistema de Prevención de Delitos y gestionar los mismos.
- c) Recibir las denuncias que se realicen través de la Plataforma de Gestión Ética, coordinar su investigación y corregir o aclarar la situación que las originó.
- d) Desarrollar, actualizar y ejecutar programas de capacitación sobre el Sistema de Prevención de Delitos para los gerentes, directores, ejecutivos y trabajadores de la Compañía, y mantenerlos informados sobre cambios en materia de los delitos individualizados en la Ley N°20.393.
- e) Asegurar que los integrantes de la Compañía tengan el conocimiento necesario sobre asuntos regulatorios y las exigencias propias de sus cargos, de forma que puedan desarrollar sus funciones con apego a las normas.
- f) Asegurar que los controles internos sean adecuados para prevenir y detectar circunstancias propicias contrarias al Sistema de Prevención de Delitos.
- g) Presentar informes semestrales al SMT (E&C Committee) sobre el funcionamiento del Sistema de Prevención de Delitos.
- h) Desarrollar e implementar mecanismos de revisión y actualización del Sistema de Prevención de Delitos.
- i) Velar para que todos los contratos de la Compañía contengan las cláusulas requeridas para la prevención de delitos de la Ley N°20.393.
- j) Elaborar anualmente una "Nómina de Personas y/o Cargos" que pueden relacionarse

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 11 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

con “Funcionarios Públicos”.

- k) Difundir entre los integrantes de la Compañía las “Señales de Alerta” señaladas por la Unidad de Análisis Financiero, relacionadas con los delitos de lavado de activos y financiamiento del terrorismo.
- l) Supervisar que las políticas y procedimientos relativos a la administración de Recursos Humanos estén alineados a los requerimientos del Sistema de Prevención de Delitos.

### **3.1.3 Medios y Recursos Necesarios para su Desempeño**

- a) El SMT deberá proveer al Compliance Officer, de forma íntegra y oportuna, todos los materiales y recursos que sean necesarios para desempeñar adecuadamente sus funciones.
- b) Los materiales y recursos deberán ser definidos anualmente por el SMT, sin perjuicio de casos excepcionales que requieran de un presupuesto adicional. Los recursos quedarán establecidos en las partidas presupuestarias correspondientes.
- c) El Compliance Officer podrá acceder directamente al SMT para informar sobre las medidas y planes implementados en el cumplimiento de su cometido y los incumplimientos al Sistema de Prevención de Delitos detectados.

## **3.2 Senior Management Team**

El SMT tendrá las siguientes funciones;

- a) Aprobar el Sistema de Prevención de Delitos de la Compañía y velar por su cumplimiento.
- b) Designar al Compliance Officer Titular y Subrogante.
- c) Garantizar la plena e idónea autonomía del Compliance Officer, de acuerdo a lo establecido en la Ley N°20.393.
- d) Conferir al Compliance Officer los medios y facultades suficientes para el correcto desempeño de sus funciones, contando con acceso directo y expedito al SMT, tanto para informar de su cometido como para solicitar su colaboración.
- e) Informar al Compliance Officer sobre cualquier situación de incumplimiento de la Ley N°20.393.
- f) Decidir, en conjunto con el Comité de Ética, si poner un hecho que puede ser constitutivo de delito en conocimiento del Ministerio Público, los Tribunales de Justicia u otras autoridades correspondientes.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 12 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

### 3.3 Comité de Ética

El Comité de Ética tendrá las siguientes funciones:

- a) Definir las acciones correctivas y/o las medidas disciplinarias que deben aplicarse a las infracciones del Sistema de Prevención de Delitos en el marco del Procedimiento de Investigaciones Internas.
- b) Decidir la aceptación o rechazo de Clientes, Proveedores, Prestadores de Servicios y Distribuidores que presenten ciertas circunstancias descritas en los procedimientos de evaluación de los mismos.
- c) Decidir, en conjunto con el SMT, si poner un hecho que puede ser constitutivo de delito en conocimiento del Ministerio Público, los Tribunales de Justicia u otras autoridades correspondientes.
- d) Requerir la opinión o asesoría de un tercero experto respecto de cualquiera de las decisiones que le han sido encomendadas.

### 3.4 Gerencias Generales

Las Gerencias Generales tendrán las siguientes funciones:

- a) Facilitar al Compliance Officer el acceso directo a información y personas relacionadas con infracciones al Sistema de Prevención de Delitos, y apoyarlo en la coordinación de las actividades que requiera su implementación.
- b) Aprobar, previa autorización del SMT, los medios y recursos necesarios para que el Compliance Officer ejerza sus funciones.
- c) Informar al Compliance Officer sobre cualquier situación de incumplimiento de la Ley N°20.393.
- d) Velar por el cumplimiento del Sistema de Prevención de Delitos.
- e) Resguardar la plena e idónea autonomía del Compliance Officer, de acuerdo a lo prevenido en la Ley N°20.393.

### 3.5 Ejecutivos y Trabajadores

Los ejecutivos y trabajadores tendrán las siguientes funciones;

- a) Proporcionar la información que requiera el Compliance Officer para el desempeño de sus funciones.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 13 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- b) Colaborar con el Compliance Officer en la ejecución de actividades relacionadas con el Sistema de Prevención de Delitos.
- c) Informar al Compliance Officer sobre cualquier situación de incumplimiento de la Ley N°20.393.
- d) Cumplir las políticas y procedimientos del Sistema de Prevención de Delitos.
- e) Mantener en reserva toda la información a la que tengan acceso, vinculada al Sistema de Prevención de Delitos.
- f) Ser diligentes en el conocimiento efectivo de clientes, proveedores y distribuidores de las operaciones que realizan, con el fin de identificar operaciones que podrían estar vinculadas al Sistema de Prevención de Delitos.
- g) Comunicar al Compliance Officer las Señales de Alerta identificadas y/o las operaciones inusuales detectadas, en el desarrollo de sus funciones y/o actividades.
- h) Registrar las operaciones en los correspondientes registros que la Compañía dispone para estos efectos.
- i) No incurrir en conductas sancionadas por la Ley N°20.393.

### **3.6 Prestadores de Servicios, Proveedores y Distribuidores**

La Compañía es consciente que la implementación de medidas de cuidado o de control interno en la organización necesariamente involucra a los Proveedores, Prestadores de Servicios y Distribuidores que se relacionan con ella. Es por ello por lo que los invita a:

- a) Desplegar sus mejores esfuerzos en la adopción e implementación de sus propios Sistemas o Modelos de Prevención de Delitos, de acuerdo a las exigencias contempladas en la Ley N°20.393.
- b) Colaborar con el Compliance Officer en la realización de actividades relacionadas con el Sistema de Prevención de Delitos.
- c) No incurrir en conductas sancionadas por la Ley N°20.393.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 14 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

#### **4. GESTION DE RIESGOS**

En atención a los requerimientos de la Ley N°20.393, la Compañía analizó las actividades y procesos -habituales o esporádicos- en cuyo contexto se pueden presentar riesgos de comisión de los delitos descritos en la normativa, se evaluaron dichos riesgos, y se definieron las medidas necesarias para contrarrestarlos, apoyándose en las técnicas, pautas y conceptos fundamentales proporcionados por el Committee of Sponsoring Organizations of the Treadway Commission (COSO).

De esta forma, la Compañía adoptó un Sistema de Prevención de Delitos basado en los requerimientos de la Ley N°20.393 y en pautas recogidas de la experiencia internacional, y estableció los mecanismos para su aplicación, supervisión y actualización efectiva, con el propósito de prevenir los delitos y de detectar y corregir las deficiencias de los controles implementados permanente y oportunamente.

##### **4.1 Identificación, Análisis y Evaluación**

Para identificar, analizar y evaluar los principales riesgos de comisión de los delitos de la Ley, la Compañía se sometió a un riguroso levantamiento de riesgos focalizado en los delitos de la Ley, considerando la actividad que desarrolla, el modelo de negocio, sus características, tamaño y organización.

El análisis de los procesos, operaciones, distribución de responsabilidades y descripción de cargos y funciones permitió identificar las brechas, evaluar el grado de exposición y frecuencia de los riesgos, y definir los controles para enfrentarlos, en consideración a su probabilidad e impacto.

##### **4.2 Actividades de Control**

Una vez identificados, analizados y evaluados los riesgos, se diseñaron los mecanismos de control y neutralización de los mismos, a través del establecimiento de políticas, procedimientos y marcos de actuación aplicables a las operaciones y actividades propias de la Compañía.

Para las actividades de control se segregaron los riesgos, distinguiendo aquellos de mayor probabilidad e impacto de aquellos de menor probabilidad e impacto, y aquellos que se presentan en procesos y cargos determinados de aquellos que no se presentan en procesos y cargos determinados.

De esta segregación surgen controles aplicables a toda la Compañía, como por ejemplo aquellos derivados de los Conflictos de Interés, del relacionamiento con Funcionarios Públicos o de la recepción o entrega de Regalos, o controles aplicables sólo a integrantes de la Compañía que por su cargo intervienen en operaciones específicas, como por ejemplo los relacionados a la entrega de donaciones o con el relacionamiento con Clientes, Proveedores, Prestadores de Servicios y Distribuidores.

##### **4.3 Difusión, Comunicación e Información**

Desde su entrada en vigencia, la Compañía ha difundido interna y externamente los controles contemplados en el Sistema de Prevención de Delitos adoptado, a través de diversos canales de

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 15 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

comunicación, tales como su página web corporativa, newsletters, afiches, comunicados internos, videos corporativos, entre otros medios.

Por su parte, el Compliance Officer vela permanentemente y por distintas vías por la adecuada difusión, comprensión y aplicación de las medidas que forman parte del Sistema, a través de actividades de capacitación, campañas de información y otros medios.

Adicionalmente, el propio Sistema contempla programas de inducción y de capacitación para todos los integrantes de la Compañía con el fin de que se interioricen y posean los conocimientos mínimos necesarios sobre la materia y sobre los controles adoptados.

Por último, la Compañía ha dado cumplimiento a lo establecido en la Ley en cuanto a la incorporación de una cláusula específica de la Ley N°20.393 en todos los contratos de trabajo, en los contratos con Proveedores y Prestadores de Servicios, y la ha extendido también a los contratos con Clientes, Distribuidores y otros terceros con los que interactúa, y ha incorporado información sobre la materia en el Reglamento de Orden, Higiene y Seguridad y en el Código de Conducta Empresarial.

#### **4.4 Seguimiento y Actualización**

La Compañía realiza un monitoreo permanente de los riesgos y de los controles adoptados a través del Compliance Officer, quien vela por la correcta aplicación de las políticas y procedimientos que forman parte del Sistema y porque éstas se encuentren debidamente difundidas.

Adicionalmente el Sistema de Prevención de Delitos contempla mecanismos de revisión y actualización que permiten identificar nuevas contingencias, ya sean derivadas del propio negocio o de eventualidades externas como sería un cambio de la actividad económica o giro, un aumento significativo de las operaciones, la creación, adquisición o fusión de nuevas compañías, o modificaciones legislativas relevantes, entre otras.

Por último, periódicamente la Compañía someterá a un proceso de revisión por un tercero independiente la adopción e implementación de su Sistema de Prevención de Delitos, conforme al N° 4, del artículo 4° de la Ley N°20.393.

### **5. POLÍTICAS Y PROCEDIMIENTOS ESPECÍFICOS DE CONDUCTA ÉTICA, DE CONTROL INTERNO Y GESTIÓN DE RIESGOS**

#### **5.1 Código de Conducta Empresarial**

La Compañía cuenta con un Código de Conducta Empresarial que establece pautas de comportamiento ético para asegurar que la conducta de todos sus integrantes se ajuste a prácticas responsables y correctas.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 16 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|



## 5.2 Mecanismos de Control Financiero-Contable

La Compañía cuenta con mecanismos de control interno y de gestión de riesgos que le permiten asegurar la eficacia y eficiencia de sus operaciones, la fiabilidad de su información financiera y el cumplimiento de leyes y normas aplicables.

Entre las exigencias de la Ley está la de establecer un sistema de contabilidad y auditoría de los recursos financieros que permita a la Compañía prevenir que sus recursos sean utilizados en los delitos descritos en la normativa.

Para dar cumplimiento a dicha exigencia la Compañía se rige por la normativa vigente en la materia y cuenta con políticas, procedimientos, protocolos y marcos de actuación.

### a) Normativa aplicable:

Para dar estricta observancia a la normativa internacional vigente sobre control interno y transparencia de la información, la Compañía adoptó las normas IFRS (International Financial Reporting Standard). Estas normas contables proporcionan información clara y fidedigna de los estados financieros, los que son auditados anualmente por auditores externos.

### b) Políticas, procedimientos, protocolos y marcos de actuación de control contable y financiero, complementarios al Sistema de Prevención de Delitos:

- Procedimiento de Rendición de Gastos y Fondos por Rendir: Busca dar cumplimiento a la normativa contable vigente y salvaguardar razonablemente la propiedad de los activos de la Compañía, asignando plazos y responsabilidades en cada una de las etapas.
- Política General de Compra de Insumos, Servicios y Activos Fijos: Busca definir las directrices necesarias para regular los procesos de compra de bienes y servicios de la Compañía, optimizando precio, calidad y oportunidad, y asegurando la satisfacción de los usuarios a través de procesos transparentes y alineados con la estrategia del negocio.
- Procedimiento para la Evaluación de Clientes Nuevos para Apertura de Líneas de Crédito: Busca conocer a los clientes y establecer autorizaciones para la creación de los mismos en el sistema SAP que la Compañía dispone para estos efectos (en donde se registra monto de crédito, fechas de pago y otros antecedentes relevantes).
- Procedimiento para la Creación, Ampliación, Modificación y Baja de Proveedores: Busca establecer controles, normas y procedimientos para la creación y modificación de proveedores nacionales e internacionales en el “sistema SAP”, estableciendo autorizaciones para este procedimiento.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 17 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- Política y/o Procedimiento de Control de Inversión: Busca definir parámetros de inversión, autorizaciones, montos y regulaciones, así como controles permanentes para evitar excesos de riesgos financieros.
- Política y/o Procedimiento de Viajes y Gastos: Busca la definición de autorizaciones, montos, declaraciones y atribuciones para el uso de viajes y gastos.

La información sobre estos instrumentos está disponible en *intranet corporativa* [http://normativa.kcl.cl/auditoria\\_usuario.php?area=2](http://normativa.kcl.cl/auditoria_usuario.php?area=2) accesible para todo el personal de la Compañía.

## **6. POLÍTICAS, PROCEDIMIENTOS PARA PREVENIR DELITOS EN PARTICULAR**

De acuerdo con lo dispuesto por el art. 4°, número 2 de la Ley N°20.393, se han establecido políticas y procedimientos específicos con el propósito que los integrantes de la Compañía que intervengan en actividades riesgosas programen y ejecuten sus tareas o labores de forma tal que puedan prevenir y detectar la comisión de alguno de los delitos por los cuales puede ser sancionada.

Estas políticas y procedimientos específicos se presentan a continuación, atendiendo al tipo de actividad delictiva que se pretende prevenir, teniendo en consideración los principales conceptos que deben manejar los destinatarios del Sistema de Prevención de Delitos, las actividades consideradas riesgosas, y las políticas y procedimientos adoptados para su control.

Se hace presente que, conforme a los resultados del proceso de levantamiento de riesgos realizado por la Compañía, en consideración de su giro, ésta no enfrenta mayores riesgos de incurrir en los delitos de Administración Desleal y Negociaciones Incompatibles descritos en los artículos 470 número 11° y 240 del Código Penal respectivamente, razón por la que en este Manual no se contemplan medidas específicas para prevenirlos.

Asimismo, luego de haberse revisado los procesos y subprocesos que pudieran ser riesgosos desde el punto de vista de los delitos contemplados en el Título II de la Ley N°17.798 sobre Control de Armas, la Compañía no estableció medidas de control específicas en este ámbito por cuanto no se identificaron riesgos de su comisión.

### **6.1 Prevención del Cohecho a Funcionario Público Nacional o Extranjero**

#### **a) Conceptos Generales**

Delito de Cohecho: de acuerdo a lo establecido por el artículo 1° de la Ley N°20.393, la persona jurídica responde de los delitos contenidos en los artículos 250 y 251 del Código Penal chileno en el caso que se cumplan con los presupuestos para la imposición de responsabilidad penal contenidos en la misma ley. La persona jurídica efectivamente podría responder en aquellos supuestos en que el delito se cometa con el propósito de generar una posición de ventaja o privilegio potencial para con un funcionario que pueda incidir en el desarrollo de su actividad económica.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 18 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

Del Código Penal chileno se desprende que comete el delito de cohecho el que soborna a un funcionario público, ya sea en razón de su cargo o para que éste lleve a cabo una conducta que es propia de su cargo, así como para que omita una obligación. Además, se agrava la pena si el objeto del soborno consiste en solicitarle que actúe con infracción de sus obligaciones. En relación al primer supuesto, si bien no resulta evidente la comprensión del vocablo “beneficio en razón del cargo”, podemos entenderlo como todo aquel regalo, donación u otros -como, por ejemplo, actividades honoríficas-, que puedan ser entendidas por un tercero como idóneas para quedar en una situación de ventaja o de favorecimiento – incluso potencial- frente a un funcionario con poder decisorio. Es importante considerar que el soborno no solo puede consistir en el ofrecimiento o entrega de un beneficio económico, ya que este puede ser de cualquier naturaleza. Lo importante es que desde un punto de vista objetivo se comprenda como una “ventaja” o una forma de mejorar la posición del sobornado y que, además, pueda entenderse como un “incentivo” para que, al menos potencialmente, esté dispuesto a actuar de determinada forma.

Pero también nos enfrentamos a este delito cuando es el funcionario público quien solicita el beneficio y el integrante de la Compañía consiente en tal prestación. A su vez, es importante tener en cuenta que también se comete este delito cuando se ofrece un beneficio económico (o si se consiente en otorgar) o de otra naturaleza, a un funcionario público nacional o extranjero, en provecho de éste o de un tercero, para que realice una acción o incurra en una omisión con miras a la obtención o mantención, para sí u otro, de cualquier negocio o ventaja indebidos en el ámbito de cualesquiera transacciones nacionales o internacionales.

Es importante considerar que el propio ordenamiento jurídico penal chileno entiende que no cualquier donación o regalo debe ser comprendido como delictivo. Es más, el propio artículo 251 sexies del Código penal chileno, sostiene que:

*“No será constitutivo de los delitos contemplados en los artículos 248, 250, incisos segundo y tercero, y 251 bis aceptar, dar u ofrecer donativos oficiales o protocolares, o aquellos de escaso valor económico que autoriza la costumbre como manifestaciones de cortesía y buena educación.*

*Lo dispuesto en el inciso anterior no se aplicará respecto del delito contemplado en el artículo 251 bis cuando se ofreciere, prometiére, diere o consintiere en dar a un funcionario público extranjero un beneficio, para que omita o ejecute, o por haber omitido o ejecutado un acto con infracción a los deberes de su cargo”.*

Funcionario Público: se entiende por funcionario público, para los efectos de este delito, a todas las personas que participen legítimamente en el ejercicio de este género de funciones, sea cuales fueren en especie, categoría o grado de permanencia. Es decir, sin importar el tipo de vinculación jurídica que exista entre la Administración del Estado y la persona que ejerce dicha función, sobre el que pesa la permanente obligación de velar por los intereses del Estado. En el caso de Chile el art. 260<sup>2</sup> considera tanto a quienes se desempeñan en los órganos del Estado, descritos y regulados por la

<sup>2</sup> El art. 260 CP dicta: (...) Se reputa empleado (público) todo el que desempeñe un cargo o función pública, sea en la administración central o en instituciones o empresas semifiscales, municipalidades, autónomas u organismos creados por el Estado o dependientes de él, aunque no sean del nombramiento del Jefe de la República ni reciban sueldo del Estado. No obstará a esta calificación el que el cargo sea de elección popular.

Constitución Política de la República, como a aquellos a que se refiere el inc. 2° del art. 1° de la Ley N°18.575 (LOC Bases Generales de la Administración del Estado), y también a quienes se encuentren regulados por estatutos especiales, incluyendo a quienes se desempeñen como gerentes, directores, administradores y funcionarios de empresas públicas creadas por ley (estén dotadas o no de un estatuto jurídico propio y rigiéndose por la ley común aplicable a los particulares) y en las corporaciones municipales dedicadas al cumplimiento de funciones municipales de educación y salud, siempre que no exista una norma expresa que los excluya de esta denominación o existan normas especiales de responsabilidad, ello independiente de que se encuentren vinculados por contrato de trabajo o contrato de honorarios. Tratándose de otros países, se estará a la legislación respectiva para determinar quiénes son funcionarios públicos.

Función Pública: según lo dispone nuestra Corte Suprema la expresión “función pública” significa “función del Estado”, enfoque desde el cual cabe hablar de una función pública legislativa, administrativa y judicial, siendo bastante, para ser titular de ella, con disponer de investidura suficiente, emanada de autoridad competente. En el fondo, se entiende que cumple una función pública quien actúa, en cualquier sentido “representando los intereses del Estado” sin importar que efectivamente esté revestido del cargo de “funcionario público”.

Donación: el Código Civil la define como “un acto por el cual una persona transfiere gratuita e irrevocablemente una parte de sus bienes a otra persona que lo acepta”. En Chile existen incentivos tributarios para donaciones en beneficio de instituciones sin fines de lucro, con la característica de permitir la devolución total de la mitad del monto donado y la rebaja de la otra mitad aproximadamente como gasto deducible de la renta imponible, dependiendo del tipo de donación que se realice.

#### **b) Actividades Riesgosas o Ilícitas**

- Trato con funcionarios públicos por un integrante de la Compañía no autorizado.
- Adquisición de activos o contratación de servicios por parte de empresas públicas.
- Adquisición de activos o contratación de servicios a nivel nacional o en el extranjero (Ej.: equipos, maquinarias especializadas, otros), a proveedores o prestadores de servicios, cuyos dueños sean funcionarios públicos.
- Negociación de condiciones especiales respecto de productos y/o servicios de la Compañía con funcionarios y/o entidades públicas.
- Asignación de fondos de la Compañía (fondos a rendir, tarjetas corporativas, otros) para realizar pagos a servicios o entidades públicas;
- Realización de donaciones, auspicios u otros aportes a proyectos o instituciones en donde participen funcionarios públicos o donde haya posibilidades que un funcionario público pueda verse beneficiado, o casos en que resulte complejo detectar el beneficiario final.

- Negociación con un funcionario público de cualquier repartición sin estar antes informado acerca de los eventuales derechos que pueda cobrar el funcionario público en razón del trámite, permiso, o negocio en particular.
- Trato con funcionarios públicos en el marco de fiscalizaciones o inspecciones de las que puedan constatar infracciones a la normativa vigente por parte de la Compañía.
- Solicitud por parte de un funcionario público de cualquier cobro o comisión con el objeto de obtener una tramitación favorable a los intereses de la Compañía.
- Cobros extraordinarios con el propósito de evitar que se cursen multas por infracciones reales o presuntas.
- Gastos excesivos o innecesarios – de hospitalidad o representación- en el marco de la obtención, mantención o ejecución de negocios con el Estado o empresas del Estado.
- Solicitud de reembolsos para gastos extraordinarios, sin documentación que avale la misma o que se presente en forma deficiente, así como la solicitud de dineros por gastos de último minuto.
- Solicitud de pagos con el objeto de modificar la información recogida por el funcionario a propósito de una inspección propia de su cargo.
- Solicitud de contribuciones financieras con fines políticos (especialmente financiamiento fuera del marco permitido por la ley).
- Pretensión por parte del funcionario público de prescindir de otorgar recibo o constancia por actuación que haya supuesto el pago de dineros por la labor efectuada.
- Relaciones comerciales internacionales con cualquier entidad cuyo propietarios, directores o ejecutivos sean funcionarios de gobierno.
- Solicitudes insistentes por parte de funcionarios públicos cuyo propósito sea el favorecer a un cliente, proveedor, intermediario o agente por sobre otros, sea que se transparente o no por parte del funcionario la intención de favorecer a la Compañía en caso de acceder a tal petición.
- Relación con cualquier funcionario del cual ya haya noticia acerca de su mala reputación o antecedentes de peticiones irregulares.
- Actividades honoríficas u otras similares donde estén involucrados funcionarios públicos con competencias relevantes para el negocio de la Compañía, que puedan malinterpretarse como un intento de incidir en las decisiones que podría adoptar la autoridad.

### **6.1.1 Política y Procedimiento de Contacto con Funcionarios Públicos.**

Para prevenir el delito de Cohecho la Compañía cuenta con una Política y Procedimiento de Contacto con Funcionarios Públicos (CMP\_002) que establece las pautas generales de conducta que deben seguir todos los integrantes de la compañía a la hora de reunirse con funcionarios públicos, y la obligación de registrar y transparentar dichos contactos y los gastos que se realicen en el marco de los mismos.

Entre las medidas contempladas en dicha Política y Procedimiento están las de la elaboración anual de una “Nómina Autorizada de Personas y/o Cargos” que habilita a ciertas personas, -en consideración de sus cargos o posiciones-, a reunirse con funcionarios públicos sin previa autorización del Compliance Officer, y la obligación de registrar toda reunión o interacción con funcionario público ya sea en una Planilla Excel o en un Formulario electrónico (dependiendo si se está o no en la Nómina), ambos de “Registro de Contacto con Funcionario Público”, que deben ser remitidos mensualmente al Compliance Officer para su conocimiento y archivo.

Por su parte, el Código Mundial de Conducta Empresarial refuerza esta medida al establecer que toda relación con funcionarios y/o organismos públicos, nacionales o extranjeros, debe ser transparente, correcta e íntegra a fin de evitar por todos los medios, actos corruptos e ilegales.

La Política y Procedimiento de Contacto con Funcionario Público acoge las directrices contempladas en la Foreign Corrupt Practices Act (FCPA) y en otras normas anticorrupción, las que se entienden como complementarias a la misma.

### **6.1.2 Política y Procedimiento General de Donaciones Regulares, Política y Procedimiento de Donaciones de Emergencia o Disaster Relief**

La Compañía realiza, apoya y promueve el desarrollo de proyectos sociales en beneficio de la comunidad en el marco de la sustentabilidad, a través de Donaciones Regulares a iniciativas sociales y/o comunitarias. Asimismo, realiza Donaciones de Emergencia en beneficio de víctimas de desastres naturales o provocados por el hombre.

Para regular ambos tipos de donaciones, la Compañía cuenta con una Política y Procedimiento General de Donaciones Regulares (SUS\_002) y con una Política y Procedimiento de Donaciones de Emergencia o Disaster Relief (SUS\_007).

Entre las medidas establecidas para el control de las donaciones regulares está la exigencia de un conocimiento acabado de la entidad que recibirá la donación, de las personas que la componen y del proyecto para que cual se están entregando los recursos, a través del llenado y firma por parte del solicitante de un Cuestionario Organización Donataria, a la que se le pide además la entrega de antecedentes legales que acrediten su vigencia como persona jurídica.

Asimismo, tanto para las donaciones regulares como para las de emergencia se ha establecido la exigencia para el área de Sustentabilidad de llenar un Formulario de Solicitud de Donaciones en donde se deja constancia de la revisión y aprobación del Compliance Officer y de los demás aprobadores de

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 22 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

acuerdo a lo señalado en el Procedimiento que las regula y, una vez entregada la donación, del registro gráfico a través del cual se acredita que ésta fue efectivamente invertida en el proyecto para el cual se entregó. Además, señala que la Gerencia de Sustentabilidad debe informar trimestralmente al Compliance Officer las donaciones que se realicen.

Respecto a los destinatarios de las donaciones, la Política General de Donaciones Regulares establece que no podrán realizarse donaciones regulares a entidades públicas, salvo que los beneficiarios sean colegios, hospitales u otras entidades públicas que por su naturaleza presten servicios a la comunidad y que sean actores relevantes del plan de relacionamiento comunitario de la Compañía. En este caso, dichas donaciones regulares no podrán realizarse en momentos en que la Compañía esté solicitando permisos, o esté participando en negociaciones, licitaciones o tratos directos con la entidad pública de la cual dependen, o bien en período de elecciones.

Por último, ambas Políticas y Procedimientos están alineados con la política interna de control de gastos o egresos, y con el comportamiento ético que se espera de todos los integrantes de la Compañía, quedando expresamente prohibido todo acto de soborno o cohecho a funcionarios públicos nacionales o extranjeros, a través de donaciones.

#### **6.1.3 Política de Auspicios y/o Patrocinios**

La Compañía cuenta con una Política de Auspicios y/o Patrocinios (CMP\_004) que establece los requisitos y el procedimiento de aprobación y entrega de aportes que ésta hace con fines de marketing y posicionamiento de imagen en la que, entre otros controles, se señala que la Gerencia de Marketing debe informar trimestralmente al Compliance Officer de los Auspicios y Patrocinios que se realicen.

#### **6.1.4 Política de Regalos, Invitaciones a Eventos y Viajes**

La Compañía cuenta con una Política de Regalos, Invitaciones a Eventos y Viajes (CMP\_003) que regula la entrega y/o recepción de regalos e invitaciones a eventos y viajes entre colaboradores y terceros, entre los que se encuentran los funcionarios públicos.

Al respecto, la Política establece lo siguiente;

- a) Está prohibido ofrecer o entregar regalos a un funcionario público y recibir regalos de un funcionario público.
  - Excepcionalmente la Compañía podrá entregar regalos de carácter “simbólico” a autoridades, con la autorización expresa y por escrito del Gerente General, con conocimiento del Compliance Officer.
  - Para los efectos de esta Política no se considerarán dentro de esta categoría los gastos de hospitalidad que eventualmente puedan surgir en la relación con un funcionario público, los que están regulados por la Política y Procedimiento de Contacto con Funcionario Público.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 23 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|



- b) Está prohibido realizar Invitaciones a Eventos a un funcionario público o aceptar Invitaciones a Eventos de un funcionario público.
- Para los efectos de esta Política no se consideran dentro de esta categoría las invitaciones que se realizan a funcionarios públicos ni que se reciben de funcionarios públicos a inauguraciones, aperturas, seminarios, charlas u otras actividades similares, las que están reguladas por la Política y Procedimiento de Contacto con Funcionario Público.
- c) Está prohibido realizar Invitaciones a Viajes a un funcionario público y aceptar Invitaciones a Viaje de un funcionario público.

### 6.1.5 Política de Conflictos de Interés

La Compañía, en su compromiso con la transparencia y probidad en los negocios, cuenta con una Política de Conflicto de Interés (CMP\_001) cuyo objetivo es regular aquellas situaciones en las que un colaborador -en razón de su cargo, función o posición- participe en negocios u operaciones de la Compañía en los que tenga un interés personal comprometido.

En virtud de la misma, todos los colaboradores de la Compañía deben declarar sus Conflictos de Interés a través del Formulario Declaración de Conflicto de Interés, en las siguientes oportunidades;

- Al momento de ser contratado
- Anualmente (sólo los ejecutivos)
- Cuando se asume un cargo nuevo que así lo requiera
- Si en el marco de una operación en particular se presenta

En términos generales esta Política establece que los Conflictos de Interés pueden surgir a causa de una relación de amistad o de parentesco ya sea con otro colaborador o con terceros ajenos a la Compañía, y señala que, si bien no impiden la participación de un colaborador en una operación, es necesario identificarlos, transparentarlos y manejarlos adecuada y oportunamente.

### 6.1.6 Declaración Jurada de Persona Expuesta Políticamente

La Declaración Jurada de Persona Expuesta Políticamente mencionada en el punto 6.3.1 como medida para conocer a Clientes, Proveedores, Prestadores de Servicios y Distribuidores con los que la Compañía realiza operaciones, también se entiende parte de los controles para prevenir este delito.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 24 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|



## 6.2 Prevención de la Corrupción Entre Particulares

### a) Conceptos Generales

Delito de corrupción entre particulares: El artículo 287 bis sanciona al director, administrador, mandatario o empleado de una empresa que solicita o acepta un beneficio económico o de otra naturaleza, para sí o un tercero, para efectos de favorecer o por haber favorecido en el ejercicio de sus labores la contratación de un oferente por sobre otro.

Como se puede observar a primera vista, este delito puede ser cometido por cualquiera de los colaboradores de la Compañía principalmente en el marco de los procesos de obtención de bienes o servicios de proveedores, en la medida que se termine privilegiando a algún proveedor debido al soborno solicitado o prometido. Es muy importante, además, que se comprenda que con este delito lo que se pretende es proteger la libre competencia, por lo que incluso se puede verificar en casos en que no exista competencia efectiva para la elección de un proveedor, pero si exista competencia potencial.

De acuerdo con el artículo 3° de la Ley N°20.393, la Compañía solo puede ser penalmente responsable por cualquiera de los delitos señalados en el artículo 1 de la referida ley, perpetrado en el marco de su actividad por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, siempre que la perpetración del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica. Con todo, esta hipótesis no se puede descartar, por ejemplo, para aquellos supuestos en que el beneficio solicitado u obtenido sea directamente en beneficio de la persona jurídica. Por lo mismo, conviene introducir medidas de refuerzo al control en la relación con proveedores que estén encaminadas a potenciar la elección de estos por su mérito económico.

Por su parte, el artículo 287 ter prohíbe dar, ofrecer o consentir en dar a un a un director, administrador, mandatario o empleado de una empresa un beneficio económico o de otra naturaleza, para sí o un tercero, para que favorezca o por haber favorecido la contratación con un oferente por sobre otro. Este delito podría ser cometido, entonces, dentro de los procesos vinculados con la obtención de cliente. Es importante que se comprenda el alcance de este delito, ya que a través de este se sanciona aquellos supuestos en que se termina obteniendo un negocio o se logra mantenerlo a través de un soborno. En este sentido, la conducta descrita debe comprenderse como un supuesto de competencia desleal especialmente grave. Es evidente que la persona jurídica puede responder por este delito, en la medida que, por lo general, se lleva a cabo justamente en interés de ésta.

Empleado o mandatario: Es muy importante partir de la base que este delito solo puede ser cometido por determinados sujetos, esto es, empleados y mandatarios. Sin embargo, para comprender quiénes pueden ser catalogados como tales no se recurre necesariamente, en el derecho penal, a las definiciones que provengan del Derecho laboral o del Derecho civil. Si bien es cierto el concepto de empleado está asociado a la relación de subordinación y dependencia con el empleador y el de mandatario en el de quien se encarga de la gestión de negocios ajenos en nombre del mandante, en ambos supuestos lo medular es la representación de intereses de un titular, por lo que se incluyen

dentro de esta categoría, por ejemplo, los intermediarios.

Oferentes: Es importante considerar que en Chile no existe acuerdo respecto a si este delito solo puede cometerse en el marco de negocios con competencia efectiva -esto es, donde efectivamente se presente más de una oferta- o si incluso puede cometerse en casos de competencia potencial -esto es, respecto de negocios en donde hay más oferentes que podrían adjudicarse el negocio-, por lo mismo, conviene entender tal concepto en un sentido amplio y no como un sinónimo de competencia real en un negocio en particular.

## **b) Actividades Riesgosas**

### **i) Riesgos en la Obtención de Clientes:**

- Pagos de beneficios económicos o de otra naturaleza, que no se encuentran expresamente contemplados en los términos y condiciones de los contratos.
- Participar de procedimientos de adquisiciones poco objetivos, competitivos o transparentes.
- Procesos de obtención de negocios que supongan gastos de representación, gastos de promoción u hospitalidad excesivos o efectuados de forma poco transparente.
- Participación en procesos de licitación de empresas que los efectúen sin la adopción de resguardos adecuados para la prevención de la corrupción.
- Participación o intervención en el diseño de las bases de licitación por parte de un tercero, agente o intermediario.
- Pagos excesivos realizados a agentes, consultores y asesores utilizados en el proceso de licitación.
- Empleado o mandatario que actúa sin supervisión en un proceso de licitación.
- Relaciones cercanas o de amistad de empleados o mandatarios de la Compañía con la licitante.
- Desarrollo de negocios en áreas que presenten prácticas de competencia agresiva sin un adecuado proceso de capacitación y supervisión.
- Procesos de negociación con eventuales clientes efectuados en forma poco transparente o con contraparte que no haya adoptado mecanismos de compliance para la prevención de la corrupción privada.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 26 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- Utilización de intermediarios para la obtención de negocios sin la adecuada adopción de medidas de resguardo.

## **ii) Riesgos Asociados a la Relación con Proveedores**

- Contratación, sea licitada o directa, con un mismo proveedor en reiteradas licitaciones y/o que haya durado un tiempo excepcionalmente largo.
- Supuestos de selección de proveedor único, sin verificación o supervisión de tal operación.
- Contratación de proveedores con los que se presente conflicto de interés o relaciones de cercanía o amistad.
- Selección de proveedores en base a razones diversas al mérito económico sin la debida autorización.
- Contratación de proveedores a través de trato directo sin justificación económica aparente.
- Falta de supervisión del encargado o área involucrada de las adjudicaciones en procesos de licitación.

### **6.2.1 Política General de Compras de Insumos, Servicios y Activos Fijos**

Para la prevención de la recepción de sobornos por los colaboradores de la Compañía se han adoptado una serie de medidas como, por ejemplo, un sistema centralizado de control financiero y contable a través de Komatsu Cummins Chile Ltda.

Además, se ha adoptado la Política General de Compras de Insumos, Servicios y Activos Fijos, la que se entiende como parte integrante del Sistema de Prevención de Delitos de la Compañía. Este instrumento define, entre otros aspectos relevantes, mecanismos y procedimientos para el llamado a licitación para la elección de proveedores, donde intervienen diversos controles y áreas, y que resguarda que las decisiones se tomen en atención a razones de eficiencia, minimizando así los riesgos asociados a la recepción de sobornos en este ámbito.

### **6.2.2 Política General de Regalos, Invitaciones a Eventos y Viajes**

La Política General de Regalos, Invitaciones a Eventos y Viajes, que se entiende integrada al Sistema de Prevención, regula, entre otros aspectos, la entrega y recepción de regalos, invitaciones a eventos y viajes con el fin de evitar posibles situaciones, prácticas o comportamientos cuestionables que no cumplan con lo establecido en el Código Mundial de Conducta Empresarial de Komatsu y en otras normas internas y externas aplicables a la Compañía. Esta se enmarca en una política global de tolerancia cero a cualquier acto de corrupción, inclusive en el ámbito estrictamente privado.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 27 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

Dentro de las principales medidas contenidas en esta política para prevenir el delito de corrupción entre particulares resultan especialmente relevantes las siguientes medidas:

- a) Requisitos para la entrega o recepción de regalos de terceros.
- b) Prohibiciones relativas a la entrega y recepción de regalos a terceros, que rigen especialmente para los casos en que colaboradores participen en procesos de compras o licitaciones.
- c) Procedimiento para la autorización de entrega o recepción excepcional de regalos de aquellos que no se encuentren expresamente prohibidos.
- d) Reglas y prohibiciones relativas a aceptación o invitación a eventos, así como procedimientos para la autorización extraordinaria de tales actividades.
- e) Reglas y prohibiciones relativas a invitaciones a viajes nacionales o internacionales. Será responsabilidad del Compliance Officer mantener actualizadas tales políticas de acuerdo a la evolución de la práctica judicial chilena o a buenas prácticas asentadas en el área del compliance penal. A su vez, será su responsabilidad capacitar permanentemente a los colaboradores respecto a aquellas prácticas permitidas, prohibidas e incluso aquellas no recomendables en lo que respecta a la entrega o aceptación de regalos, invitaciones o viajes en el contexto de la obtención de un negocio o en el contexto de la decisión respecto a la elección de un oferente.

### **6.2.3 Política de Conflicto de Interés y Declaración de Conflictos de Interés**

La Política de Conflicto de Interés mencionada en el punto 6.1.5 se entiende parte de las medidas para la prevención de la Corrupción Entre Particulares, así como también la Declaración de Conflictos de Interés mencionada en el punto 6.3.1 como medida para conocer a Clientes, Proveedores, Prestadores de Servicios y Distribuidores con los que la Compañía realiza operaciones.

### **6.2.4 Medidas Adicionales**

- a) Exigencia de identificación de proveedores que hayan sido ex colaboradores de la Compañía, y de proveedores vinculados a Programas de Sustentabilidad o de Responsabilidad Social Empresarial de la Compañía, a través del Formulario Solicitud de Creación, Ampliación, Modificación y Baja de Proveedor Nacional y del Formulario Solicitud de Creación, Ampliación, Modificación y Baja de Proveedor Extranjero.
- b) Cláusulas Contractuales Específicas o “Anexos de Contratos” de Proveedores, Prestadores de Servicios y Distribuidores que impliquen la representación de la Compañía frente a terceros, que establecen;
  - Que están en conocimiento de las medidas de prevención de delitos establecidas

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 28 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

en este Manual y, en especial, de las medidas de prevención de la corrupción.

- Que someterán su actuación de acuerdo a estas medidas.
  - Que han adoptado internamente medidas de prevención de delitos.
  - Que les está prohibido cualquier intento de soborno u otra práctica indebida para la obtención o mantenimiento de un negocio.
  - Medidas disuasivas para aquellos supuestos en que se incurra en tal falta.
- c) Existencia de una Plataforma de Gestión Ética (canal de denuncias), debidamente difundido interna y externamente, disponible para recibir información sobre cualquier conducta inapropiada de Clientes, Proveedores, Prestadores de Servicios, Distribuidores o Colaboradores de la Compañía, que busque incidir ilícitamente en las decisiones en el marco de una relación comercial.

La información recabada por esta vía será aprovechada por el Compliance Officer para la formulación de directrices que deberán ser incorporadas a los procesos de capacitación permanente de los colaboradores, así como en los procesos de debida diligencia relativo a proveedores o distribuidores.

### **6.3 Prevención del Lavado de Activos, Financiamiento del Terrorismo y Receptación**

Respecto a las medidas adoptadas por la Compañía para prevenir el lavado de activos y el financiamiento del terrorismo se hace presente que, respecto de la empresa Komatsu Finance Chile S.A., filial de la Compañía, además de los controles contenidos en el presente Manual, se han establecido controles adicionales en consideración de su calidad de Sujeto Obligado ante la Unidad de Análisis Financiero (UAF). Dichos controles adicionales están contemplados en el “Manual de Sistema de Prevención Contra el Lavado de Activos y el Financiamiento del Terrorismo de la Ley N°19.913” aplicable a dicha Compañía.

#### **a) Conceptos Generales**

Beneficiario final: es toda persona natural o jurídica que, sin tener la condición de cliente, es la propietaria o destinataria de los recursos o bienes objeto del contrato o se encuentra autorizada o facultada para disponer de los mismos.<sup>3</sup>

Cliente: persona natural o jurídica, de carácter público o privado, que utiliza los servicios de un profesional o una empresa o que habitualmente compra en un establecimiento o requiere sus servicios.

Debida diligencia: es el cumplimiento responsable y suficiente de la ejecución de los procedimientos y controles para el conocimiento del cliente, proveedores y organizaciones donatarias.

<sup>3</sup> <http://www.sarlaft.com/html/diccionario.html>

Delitos base o precedentes: según la UAF son aquellos cuyo producto -dinero o bienes- se busca ocultar o disimular, dado su origen ilícito. El narcotráfico es uno de estos delitos y a él se suman el cohecho, la malversación de caudales públicos, el uso de información privilegiada, la promoción de la prostitución infantil y el terrorismo, entre muchos otros. Todos ellos producen recursos obtenidos en forma ilegítima, condición que los delincuentes buscan limpiar, introduciéndolos en la economía a través de actividades lícitas (Ver “Catálogo de Delitos Base o Precedentes de Lavado de Activos” Anexo N°2).<sup>4</sup>

Financiamiento del terrorismo: según la UAF es cualquier forma de acción económica, ayuda o mediación que proporcione apoyo financiero a las actividades de elementos o grupos terroristas. Aunque el objetivo principal de los grupos terroristas no es financiero, requieren fondos para llevar a cabo sus actividades, cuyo origen puede provenir de fuentes legítimas, actividades delictivas, o ambas.<sup>5</sup>

Grupo de Acción Financiera Internacional (GAFI): es un organismo intergubernamental creado en 1989. Los objetivos del GAFI son establecer normas y promover la aplicación efectiva de las medidas legales, reglamentarias y operativas para la lucha contra el lavado de dinero, financiamiento del terrorismo y otras amenazas relacionadas con la integridad del sistema financiero internacional. Es un “órgano normativo” que trabaja para generar la voluntad política necesaria para llevar a cabo reformas legislativas y reglamentarias nacionales en estas áreas. El GAFI se compone actualmente de 34 estados miembros y 2 organizaciones regionales, que representan a la mayoría de los principales centros financieros de todo el mundo.

Grupo de Acción Financiera de Sudamérica (GAFISUD): Desde diciembre de 2000 Chile es miembro de esta organización intergubernamental de base regional para promover la implementación y mejora constante de políticas para combatir el lavado de activos y el financiamiento del terrorismo. GAFISUD fue creado bajo el modelo del Grupo de Acción Financiera Internacional (GAFI/FATF), organismo constituido por el G-7 en 1989 y al que actualmente pertenecen las 34 mayores economías del mundo.

Lavado de activos: de acuerdo a la UAF es el proceso delictivo que busca ocultar o disimular la naturaleza, origen, ubicación, propiedad o control de dinero y/o bienes obtenidos ilegalmente. Implica introducir en la economía activos de procedencia ilícita, dándoles apariencia de legalidad al valerse de actividades lícitas, lo que permite a delincuentes y organizaciones criminales *disfrazar* el origen ilegal de su producto, sin poner en peligro su fuente.

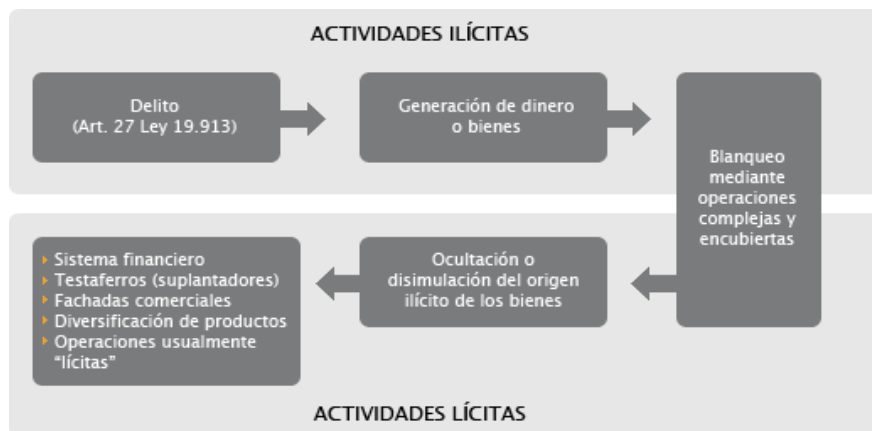
---

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 30 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

<sup>4</sup> [http://www.uaf.cl/legislacion/nuestra\\_delitos.aspx](http://www.uaf.cl/legislacion/nuestra_delitos.aspx)

<sup>5</sup> <http://www.uaf.cl/lavado/terrorismo.aspx>

**Etapas del lavado de activos:** este delito comprende las siguientes fases de realización: (i) Colocación: el lavador introduce sus ganancias ilícitas en el sistema financiero (por ejemplo: mediante depósito en cuenta bancaria); (ii) Estratificación: transacciones múltiples que separan los fondos de su fuente ilegal, dificultando con ello su rastreo (por ejemplo: transferencias bancarias); (iii) Integración: reinserción de los fondos ilegales en el sistema financiero. Los fondos aparecen como legítimos y pueden ser reutilizados (por ejemplo: red de empresas de fachada, compra de bienes raíces o de bienes de lujo).<sup>6</sup> Esta realidad, la UAF la describe en virtud del siguiente esquema:<sup>7</sup>



**Ley N°19.913:** publicada en el Diario Oficial el 18 de diciembre de 2003, creó la Unidad de Análisis Financiero, estableciendo entre sus principales funciones recibir y resguardar la información sobre actos, transacciones y operaciones sospechosas de lavado de activos que deben remitirle personas naturales y jurídicas de 34 sectores económicos; analizar dichos informes; y remitirlos al Ministerio Público en los casos en que detecte indicios del delito. Asimismo, la Unidad de Análisis Financiero puede recomendar a los sectores público y privado medidas para prevenir el lavado de activos e impartir instrucciones de aplicación general para los sujetos obligados a informar. Esta ley contiene, además, el listado de delitos base que pueden dar origen al lavado de activos; prevé la tipificación culpable del delito de lavado y las normas especiales que rigen su investigación y eventual sanción criminal.

**Patrón transaccional:** es el conjunto de características de las operaciones realizadas por el cliente o proveedor en el ejercicio de su profesión, oficio, actividad o giro de negocio, antes o durante la relación comercial con la entidad, considerando información sobre el tipo de operaciones, montos, monedas, lugares de realización, periodicidad u otra que se considere relevante.



<sup>6</sup>. <http://www.uaf.cl/lavado/configura.aspx>

<sup>7</sup>. Contenido en: <http://www.uaf.cl/lavado/>

Perfil de actividad: es el conjunto de características del cliente o proveedor, definidas a partir de su naturaleza jurídica (persona natural o persona jurídica), actividad comercial, edad o tiempo en la actividad, cuantía y frecuencia de las operaciones realizadas con la entidad, condición de PEP o no residente y nacionalidad, entre otras, en tanto resulten pertinentes dependiendo del tipo de cliente o proveedor de que se trate.

Perfil de riesgo de lavado de activos y financiamiento del terrorismo: es el nivel de exposición del cliente o proveedor al riesgo de lavado de activos o del financiamiento del terrorismo que se determina a partir de la aplicación de la metodología para la determinación del riesgo de dichos ilícitos, la cual comprende el perfil de actividad.

Personas Expuestas Políticamente (PEP): La Circular N° 49 de la UAF, del 3 de diciembre de 2012, define como Personas Expuestas Políticamente (PEP) a “los chilenos o extranjeros que desempeñan o hayan desempeñado funciones públicas destacadas en un país, hasta a lo menos un año de finalizado el ejercicio de las mismas”. Las entidades supervisadas por la UAF deben implementar y ejecutar, respecto de estas personas, medidas reforzadas de debida diligencia y conocimiento de los clientes.

Se incluyen en la categoría de PEP a Jefes de Estado o de Gobierno, políticos de alta jerarquía (entre ellos, a los miembros de mesas directivas de partidos políticos), funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, así como sus cónyuges, sus parientes hasta el segundo grado de consanguinidad y las personas naturales con las que hayan celebrado un pacto de actuación conjunta mediante el cual tengan poder de voto suficiente para influir en sociedades constituidas en Chile.

Se entiende que en Chile a lo menos deberán estar calificados como PEP los siguientes, sin que este enunciado sea taxativo:

1. Presidente de la República
2. Senadores, Diputados y Alcaldes
3. Ministros de la Corte Suprema y Ministros de las Cortes de Apelaciones
4. Ministros de Estado, Subsecretarios, Intendentes, Gobernadores, Embajadores, Jefes Superiores de Servicio, Secretarios Regionales Ministeriales
5. Comandante en Jefe del Ejército, Comandante en Jefe de la Fuerza Aérea, Comandante en Jefe de la Armada, Director General Carabineros, Director General de Investigaciones
6. Fiscal Nacional del Ministerio Público y Fiscales Regionales
7. Contralor General de la República



8. Consejeros del Banco Central de Chile
9. Consejeros del Consejo de Defensa del Estado
10. Ministros del Tribunal Constitucional
11. Ministros del Tribunal de la Libre Competencia
12. Integrantes titulares y suplentes del Tribunal de Contratación Pública
13. Consejeros del Consejo de Alta Dirección Pública
14. Directores y ejecutivos principales de empresas públicas
15. Directores de sociedades anónimas nombrados por el Estado o sus organismos
16. Miembros de las directivas de los partidos políticos

Proveedor: persona natural o jurídica, de carácter público o privado, que realice actividades de producción, fabricación, importación, distribución o comercialización de bienes o de prestación de servicios.

Receptación: este delito sanciona a quien conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, transporte, compre, venda, transforme o comercialice especies que provengan de hurto, robo, receptación, apropiación indebida y/o hurto de animales. Asimismo, el delito de receptación sanciona las conductas negligentes de quienes adquieren o poseen dichos bienes.

Riesgos que involucra el lavado de activos: según la UAF los riesgos son los siguientes: (i) Sociales: al favorecer indirectamente la criminalidad, permitiendo al delincuente *legitimar* el producto del delito; (ii) Económicos: al producir distorsiones en los movimientos financieros e *inflar* industrias o sectores más vulnerables; (iii) Financieros: al introducir desequilibrios macroeconómicos y dañar la integridad del sistema financiero y; (iv) Reputacionales: por la pérdida de prestigio, crédito y/o reputación tanto de entidades financieras como no financieras y de sus profesionales.

Señales de alerta: de acuerdo a la UAF son aquellas situaciones que especialmente deben considerarse como indiciarias de operaciones o transacciones sospechosas de lavado o blanqueo de activos, a fin de que los sujetos obligados adopten las medidas preventivas necesarias para evitar su materialización y/o sean reportadas a la Unidad de Análisis Financiero (Anexo N°3).<sup>8</sup>

Sujetos obligados: de acuerdo al artículo 3° de la Ley N°19.913, son sujetos obligados, esto es, personas naturales y jurídicas que estarán obligadas a informar a la Unidad de Análisis Financiero sobre los actos, transacciones u operaciones sospechosas que adviertan en el ejercicio de sus actividades, las siguientes: los bancos e instituciones financieras; empresas de factoraje; empresas de arrendamiento financiero; las empresas de securitización; las administradoras generales de fondos y las administradoras de fondos de inversión; el Comité de Inversiones Extranjeras; las casas de

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 33 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

cambio y otras entidades que estén facultadas para recibir moneda extranjera; las emisoras y operadoras de tarjetas de crédito; las empresas de transferencia y transporte de valores y dinero; las bolsas de comercio; los corredores de bolsa; los agentes de valores; las compañías de seguros; los administradores de fondos mutuos; los operadores de mercados de futuro y de opciones; los representantes legales de zonas francas; los casinos, salas de juegos e hipódromos; los agentes generales de aduana; las casas de remate y martillo; los corredores de propiedades y las empresas dedicadas a la gestión inmobiliaria; los notarios y los conservadores.

Transferencia: es la transacción efectuada por una persona natural o jurídica denominada ordenante, a través de una entidad autorizada en la respectiva jurisdicción para realizar transferencias internacionales, mediante movimientos electrónicos o contables, con el fin de que una suma de dinero se ponga a disposición de una persona natural o jurídica denominada beneficiaria, en otra entidad autorizada para realizar este tipo de operaciones. El ordenante y el beneficiario pueden ser la misma persona.<sup>9</sup>

#### **b) Actividades Riesgosas**

- Adquisición, venta y arrendamiento de inmuebles (Ej. propiedades, terrenos), por parte de la Compañía a una persona natural o empresa cuya actividad no se haya comprobado previamente;
- Adquisición de activos o contratación de servicios a nivel nacional o en el extranjero (Ej. equipos computacionales, software, otros), a proveedores o prestadores de servicios, cuya procedencia no esté plenamente verificada;
- Realizar negocios o mantener operaciones en países considerados paraísos fiscales, de acuerdo a la OCDE, con personas involucradas en actividades terroristas (Resolución N° 1267 de las Naciones Unidas), incluidas en listas OFAC y Países y Territorios No Cooperantes;
- Realizar negocios con personas (naturales o jurídicas) que, de acuerdo al presente Sistema de Prevención de Delitos, requieran de medidas adicionales de conocimiento.
- Realizar negocios o mantener operaciones con Personas Expuestas Políticamente (PEP).
- Realizar operaciones con clientes y proveedores sin que las mismas se encuentren registradas física o electrónicamente.
- Realizar donaciones, auspicios u otros aportes a proyectos o instituciones en donde no se pueda identificar o determinar el beneficiario final;

<sup>9</sup> <http://www.sarlaft.com/html/diccionario.html>

- Contratar trabajadores sin que se realicen o se apliquen eficientemente las políticas de reclutamiento y selección de personal.
- Actividades comerciales o de reparación de bienes nuevos o usados.

### **6.3.1 Medidas Para el Conocimiento de Clientes, Proveedores, Prestadores de Servicios y Distribuidores**

En su compromiso con la prevención de los delitos contemplados en este Manual, la Compañía ha adoptado medidas de control y registro de todas las operaciones realizadas con Clientes, Proveedores, Prestadores de Servicios y Distribuidores.

El objetivo de estas medidas es determinar la identidad de los mismos, y la finalidad y la naturaleza de la relación comercial que inician con la Compañía, para facilitar la detección de operaciones inusuales o sospechosas que podrían estar vinculadas a los delitos de lavado de activos, financiamiento del terrorismo y receptación.

Por esta razón, el conocimiento de Clientes, Proveedores, Prestadores de Servicios y Distribuidores se realiza al inicio de la relación comercial y se logra a partir de la obtención, verificación y actualización de la información que ellos mismos proporcionan, la que se contiene en Declaraciones Juradas y en las Carpetas de Clientes, Proveedores, Prestadores de Servicios y Distribuidores dispuestos para estos efectos.

Entre estas medidas adoptadas están las de conocer y evaluar a los Clientes, Proveedores, Prestadores de Servicios y Distribuidores con los que la Compañía realiza operaciones, mediante el llenado y firma de las siguientes Declaraciones Juradas (Anexo N°4);

- Declaración Jurada de Conflicto de Interés
- Declaración Jurada de la Ley N°20.393
- Declaración Jurada de Persona Expuesta Políticamente
- Declaración Jurada Trabajo Forzado

Asimismo, se establecieron procedimientos o se adecuaron procedimientos ya existentes para la regulación de la aceptación y/o rechazo de los terceros con los que la Compañía realiza operaciones, se asignaron funciones y responsabilidades a las Unidades de Negocios involucradas en dichas operaciones, y se realizaron las capacitaciones pertinentes. Entre estos Procedimientos están;

- Procedimiento Creación, Ampliación, Modificación y Baja de Proveedores (ABA-P-01)

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 35 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- Procedimiento de Creación/Actualización de Clientes Línea de Crédito (para compras superiores a US\$6.000) (CRE\_001)
- Procedimiento de Financiamiento Leasing KFCH (FNC\_001)
- Procedimiento de Otorgamiento de Crédito Off Shore (FNC\_002)

En términos generales, el procedimiento que la Compañía aplica para conocer y evaluar a un nuevo Cliente, Proveedor, Prestadores de Servicios o Distribuidor comienza con el envío de una carta a través de la cual se les informa del compromiso de la Compañía con el cumplimiento de la Ley N°20.393, y se les solicita la firma de las Declaraciones Juradas antes mencionadas.

Una vez firmadas las Declaraciones por parte de Clientes, Proveedores, Prestadores de Servicios y Distribuidores, la Unidad de Negocio involucrada debe revisar la firma de las mismas y, en especial, verificar si se da una o más de las siguientes circunstancias;

- Existencia de un PEP en la administración o directorio
- Existencia de un Conflicto de Interés
- Existencia de una Señal de Alerta

En caso de existir alguna de las situaciones de riesgos antes mencionadas, la Unidad de Negocio debe informarla al Compliance Officer para que éste revise por distintos medios la existencia o no de alguna causal por la cual la Compañía no debiera iniciar la relación comercial con el Cliente, Proveedor, Prestador de Servicios o Distribuidor.

Si el Compliance Officer concluye que puede iniciarse la relación comercial con el Cliente, Proveedor, Prestador de Servicios o Distribuidor, comunicará su decisión a la Unidad de Negocio para que siga adelante con su proceso de incorporación.

Si el Compliance Officer concluye que no debiera iniciarse la relación comercial con el Cliente, Proveedor, Prestador de Servicios o Distribuidor, convocará al Comité de Ética para que se pronuncie sobre su aceptación o rechazo del mismo, debiendo dejar por escrito esta decisión.

### **6.3.2 Procedimiento Ventas Contado Mesón**

En consideración de la naturaleza, periodicidad y monto de las ventas que se realizan en el Mesón, la Compañía estableció en el Procedimiento Ventas Contado Mesón (FIN\_001) medidas preventivas como la Prohibición de Recibir Pagos en Dinero en Efectivo por sumas superiores a USD 10.000 o su equivalente en pesos chilenos, y la obligación de firmar una “Declaración Jurada Simple de Origen de Fondos” (Anexo N°5) a Clientes que realicen pagos en efectivo por sumas entre USD 6.000 y USD 10.000.

Ambas medidas están efectivamente comunicadas al personal de la Compañía que atiende en el

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 36 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

Mesón, y a los Clientes a través de un “Afiche Ley N°20.393” (Anexo N°6) que se mantiene en las cajas.

### **6.3.3 Incorporación de Cláusula Ley N°20.393 en Contratos**

La Compañía incorpora en todos los contratos que firma con Clientes, Proveedores, Prestadores de Servicios y Distribuidores cláusulas que dan cuenta de las obligaciones y compromisos asumidos respecto de la prevención de los delitos de la Ley N°20.393, les impone exigencias y establece medidas disuasivas para evitar la comisión de ilícitos.

### **6.3.4 Difusión de Señales de Alertas**

Para la prevención de los delitos de Lavado de Activos y Financiamiento del Terrorismo la Compañía tiene en consideración las Señales de Alerta señaladas por la Unidad de Análisis Financiero (UAF), las que se difunden internamente.

### **6.3.5 Medidas sobre Aceptación, Mantención o Prohibición de Clientes, Proveedores, Prestadores de Servicios y Distribuidores**

La Compañía no aceptará ni mantendrá a Clientes, Proveedores, Prestadores de Servicios o Distribuidores respecto de los que se observe alguna de las siguientes situaciones:

- Condenados por el delito de lavado de activos, delitos precedentes, delito de receptación o el delito de financiamiento del terrorismo.
- No cuenta con domicilio real o tributario ubicable o tenga paradero desconocido.
- No se pueda establecer u obtener información sobre el propósito y naturaleza de la relación comercial.
- Identidad o información no verificada u omisiones o discrepancias que impidan comprobar la información proporcionada.
- Repercute negativamente en la reputación de la Compañía.

La Unidad de Negocio que identifique a un Cliente, Proveedor, Prestador de Servicios o Distribuidor respecto del que concurra alguna de las prohibiciones anteriores, deberá informar inmediatamente y por cualquier vía al Compliance Officer sobre esta circunstancia, señalando la causal que prohíbe la mantención de su relación comercial con la Compañía.

El Compliance Officer evaluará la efectividad de la causal y solicitará al Comité de Ética su pronunciamiento, de acuerdo a los criterios establecidos para el adecuado conocimiento de Clientes, Proveedores, Prestadores de Servicios y Distribuidores.

### **6.3.6 Actualización de la Información de Clientes, Proveedores, Prestadores de Servicios y Distribuidores.**

|            |            |   |                        |              |                 |
|------------|------------|---|------------------------|--------------|-----------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos Ley N°20.393 | Gerencia de Compliance | KCC<br>KHS A | Página 37 de 51 |
|------------|------------|---|------------------------|--------------|-----------------|

Las Unidades de Negocio son las responsables de mantener actualizada la información de sus Clientes, Proveedores, Prestadores de Servicios y Distribuidores con el fin de determinar la necesidad de aplicar medidas adicionales de conocimiento o la existencia de causales sobrevinientes que podrían incidir en la mantención o rechazo de los mismos.

Estas deberán prestar especial atención a los eventos que puedan representar Señales de Alerta respecto de operaciones que se estén realizando, e informar de cualquier situación que le parezca inusual o sospechosa al Compliance Officer.

Por su parte, los Clientes, Proveedores, Prestadores de Servicios y Distribuidores deberán informar a la Unidad de Negocio con la que mantienen la relación comercial, cualquier modificación de los datos contenidos en las Declaraciones Juradas o sus Carpetas correspondientes, en la medida que éstas ocurran.

#### **6.4 Prevención de Delitos Informáticos**

La Compañía asigna a sus colaboradores, para el desempeño de sus labores, recursos materiales y tecnológicos. Estos, son de propiedad de la Compañía y su uso debe regirse por el presente Reglamento y posteriores directrices que puedan dictarse según sea necesario dado el contexto normativo o el propio avance de la tecnología.

En virtud de lo anterior y, en lo señalado en la Ley N°21.459 sobre Delitos Informáticos es que, la Compañía ha de prevenir el uso inadecuado tanto de los sistemas como de los dispositivos tecnológicos que sean usados por los colaboradores, proveedores o terceros que mantengan relaciones con la Compañía.

En miras cumplir con los requerimientos que la ley establece, es que la Compañía ha de implementar los controles adecuados y pertinentes para evitar que, tanto los sistemas como los datos que estén o puedan estar almacenados en ellos, no sean objeto de afectación por medio de sustracción, interceptación, modificación o destrucción no autorizada de los mismos.

a) En este sentido, se consideran como conductas ilícitas:

- **Ataque a la integridad de un sistema informático:** Obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.
- **Acceso Ilícito:** Acceder a un sistema informático sin autorización o excediendo la autorización que posee superando las barreras técnicas o medidas tecnológicas de seguridad.
- **Interceptación Ilícita:** Indebidamente interceptar, interrumpir o interferir, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos. De igual forma es ilícito captar por medios electrónicos, sin la autorización requerida, datos contenidos en sistemas informáticos a través de las

emisiones electromagnéticas provenientes de éstos.

- Ataque a la integridad de datos informáticos: Alterar, dañar o suprimir indebidamente datos informáticos.
- Falsificación de datos informáticos: Introducir, alterar, dañar o suprimir datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.
- Receptación de datos informáticos: Comercializar, transferir o almacenar con fines ilícitos datos informáticos conociendo su origen o no pudiendo menos que conocerlo.
- Fraude informático: Manipular un sistema informático mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, causando perjuicio a otro con la finalidad de obtener un beneficio económico para sí o un tercero.
- Abuso de dispositivos: Entregar u obtener para la utilización propia, importar, difundir o realizar otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de los delitos señalados en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N°20.009.

## **6.5 Prevención de Ilícitos Medioambientales**

### **a) Conceptos Generales**

De acuerdo con lo establecido por el artículo 136 de la Ley General de Pesca, se sanciona al que, sin autorización o contraviniendo sus condiciones o infringiendo la normativa aplicable, introdujere o mandare introducir en el mar, ríos, lagos o cualquier otro cuerpo de agua, agentes contaminantes químicos, biológicos o físicos que causen daño a los recursos hidrobiológicos.

Recursos hidrobiológicos: De acuerdo con lo establecido por el artículo 2° de la Ley General de Pesca y Acuicultura las especies hidrobiológicas se definen como “*especie de organismo en cualquier fase de su desarrollo, que tenga en el agua su medio normal o más frecuente de vida. También se las denomina con el nombre de especie o especies*”.

Agentes contaminantes: El artículo 2° letra d) de la Ley sobre Bases Generales del Medioambiente señala que “contaminante” es “todo elemento, compuesto, sustancia, derivado químico o biológico, energía, radiación, vibración, ruido, luminosidad artificial o una combinación de ellos, cuya presencia en el ambiente, en ciertos niveles, concentraciones o periodos de tiempo, pueda constituir un riesgo a la salud de las personas, a la calidad de vida de la población, a la preservación de la naturaleza o a la conservación del patrimonio ambiental”.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 39 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

**b) Actividades Riesgosas**

- Manejo de residuos contaminantes, específicamente aceite usado.
- Procesos de cromado.
- Procesos de emisión industriales de líquidos a sistemas de alcantarillado.
- Manejo de residuos contaminantes resultantes del lavado de componentes.
- Utilización de proveedores para el tratamiento de residuos (desechos sólidos). Sin embargo, se debe advertir que en estos procesos se han instaurado fuertes controles para verificar el cumplimiento de la norma vigente.
- Manejo de residuos físicos (maquinaria descartable), que podría ser eventualmente entendida como contaminante.

**6.5.1 Programa de Auditoría de Cumplimiento Legal Ambiental**

Como parte de los lineamientos corporativos y directrices globales su casa matriz, Komatsu Limited, la Compañía debe dar cabal cumplimiento a la normativa legal ambiental aplicable a sus operaciones.

Este compromiso forma parte de la Carta Komatsu sobre el medio ambiente en el planeta (alcance global), como también del Código Mundial de Conducta Empresarial, política de sustentabilidad y política SSOMA integrada de la Compañía.

Para cumplir con dichos lineamientos y directrices, la Compañía cuenta con un Programa de Auditoría de Cumplimiento Legal Ambiental, aplicable a la totalidad de las sucursales a nivel nacional de las empresas que lo conforman. El Programa cuenta con una metodología estandarizada constituida por 6 etapas, las cuales se describen a continuación de manera general:

**a) Identificación de la Normativa Legal Ambiental Aplicable a la Compañía**

Listado de cuerpos legales aplicables a las operaciones de la Compañía, los cuales se van actualizando a medida que entran en vigencia nuevas regulaciones, o en su defecto, que algunas sean modificadas o derogadas. Para esto se cuenta de forma permanente con un servicio externo que reporta dichas actualizaciones. Dentro de los cuerpos legales se encuentran los asociados al manejo de residuos peligrosos, no peligrosos e industriales líquidos, los cuales contemplan los requisitos legales para su almacenamiento, transporte y disposición final.

**b) Solicitud de Requerimientos Solicitados a las Sucursales para la Auditoría**

Listado de requerimientos legales enviado a las sucursales, quienes deben recopilar la evidencia

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 40 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|



solicitada para acreditar el cumplimiento de la normativa ambiental asociada a permisos, autorizaciones sanitarias, infraestructura, equipamiento, proveedores, entre otros.

### **c) Verificación del Nivel de Cumplimiento Legal Ambiental**

A partir del nivel de satisfacción de la evidencia entregada por la sucursal, se procede a categorizar cada requisito legal ambiental en:

- **Cumplimiento Total:** Nivel satisfactorio de cumplimiento del requerimiento normativo ambiental. Implica que todas las acciones contempladas en el requerimiento fueron ejecutadas correctamente por las sucursales respectivas, existiendo información que respalda dicho desempeño.
- **No Cumple:** Nivel de cumplimiento insatisfactorio del requerimiento normativo ambiental. Implica que no existe información que respalde el cumplimiento de las acciones comprometidas o bien, que dichas acciones no fueron ejecutadas por la sucursal.
- **En Tramitación:** El requerimiento normativo ambiental se encuentra en proceso de tramitación en la autoridad correspondiente, donde ya fue ingresada la solicitud junto a la carpeta con los documentos requeridos. Se encuentra a la espera de ser categorizado en cumplimiento total y existe evidencia de respaldo.

### **d) Análisis de Riesgo Ambiental**

A través de la metodología de Análisis de Riesgo Ambiental (probabilidad de ocurrencia v/s impacto), la Compañía categoriza los riesgos ambientales en:

- **Riesgo Alto:** El riesgo por el incumplimiento normativo ambiental tiene una alta probabilidad de ocurrencia y su impacto puede ser significativo sobre los grupos de interés. En un escenario negativo puede poner en riesgo la continuidad operacional de la sucursal, además de una sanción económica.
- **Riesgo Medio:** El incumplimiento está asociado a una sanción económica o amonestación escrita, no está en riesgo la continuidad operacional de la sucursal.
- **Riesgo Bajo:** La materialización del riesgo genera un impacto bajo en la sucursal. En caso de fiscalización no debería superar una amonestación escrita y/o una oportunidad de mejora.

### **e) Plan de Acción Para el Cierre de Brechas**

Elaboración, ejecución y actualización de los planes de acción establecidos para el cierre de brechas legales ambientales, los cuales deben indicar al menos:

- Actividad a realizar para cerrar la brecha levantada.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 41 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- Establecer responsable del cierre de brecha.
- Indicar plazo para el cierre de brecha.

Los plazos establecidos en los Planes de Acción deben estar en concordancia al esfuerzo requerido y nivel de urgencia demandado por el cierre de brecha.

#### **f) Reportabilidad**

Cada mes se elabora un Reporte con la estadística de cumplimiento y riesgo ambiental, además del estatus del proceso cierre de brechas, hasta llegar al 100% de cumplimiento.

#### **6.5.2 Medidas Adicionales**

Las Unidades de Negocios encargadas de las Auditorías Medioambientales deberán Informar trimestralmente al Compliance Officer, de acuerdo a lo señalado en el “Instructivo de Cumplimiento Medioambiental” (Anexo N°7), lo siguiente;

- a) Los resultados de las Auditorías Medioambientales que identifiquen situaciones relativas a los delitos por los cuales puede responder penalmente la Compañía, inmediatamente después de obtenidos.
- b) Los incumplimientos a la normativa medioambiental detectados por la autoridad en inspecciones, y las medidas que se adoptarán para remediarlos, inmediatamente cuando éstos ocurran.
- c) Los incumplimientos por parte de proveedores respecto al manejo de residuos de la Compañía, inmediatamente cuando éstos ocurran.
- d) Los cambios en el marco regulatorio que sean relevantes para la adopción de medidas de actualización del Sistema de Prevención de Delitos, inmediatamente cuando éstos ocurran.
- e) La adopción de nuevas medidas preventivas, en caso de modificación de la normativa aplicable, inmediatamente después de adoptadas.

La información recabada en estos Reportes deberá ser considerada por el Compliance Officer en los procesos de capacitación sobre cumplimiento de la normativa medioambiental.

#### **6.6 Prevención de la Apropiación Indevida**

##### **a) Conceptos Generales**

De acuerdo a lo dispuesto en el artículo 470 número 1° el delito de Apropiación Indevida puede cometerse, ya sea a través de la no devolución o entrega de determinados bienes o de la distracción de dinero o bienes fungibles. En este último supuesto, el delito se asemeja bastante al de

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 42 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

Administración Desleal, aunque se remite más bien a supuestos donde no existen amplios poderes de administración o disposición sobre el patrimonio ajeno, sino cuando se reciben determinadas sumas en administración para fines particulares y se termina defraudando a quien se representa.

Considerando el giro del negocio la Compañía, ésta ha optado por centrar sus esfuerzos en la prevención de eventuales casos de Apropiación Indevida de bienes muebles no fungibles, como se desprende de la descripción de las actividades riesgosas.

#### **b) Actividades Riesgosas**

- Devolución o manejo de especies no recuperadas.
- Procesos de devolución de componentes posterior a la reparación, especialmente cuando el componente queda en condición de descartado.
- Procesos de disposición de tales componentes como chatarra.

#### **c) Medidas de Mitigación de Riesgos**

De acuerdo a lo señalado en el “Instructivo de Disposición de Componentes” (Anexo N°8), las Unidades de Negocio que realicen procesos de disposición de componentes deberán;

- Solicitar a los clientes, al momento de dejar un componente para su revisión y/o reparación, la firma de la “Declaración de Autorización de Disposición” (Anexo N°9), en donde autoriza a la Compañía a disponer de ellos transcurrido un tiempo sin haber sido retirados.
- Llevar un Registro por escrito de los procesos de disposición que realicen, con indicación de fecha, lugar, responsable y descripción del proceso que se llevará a cabo.
- Informar al Compliance Officer cualquier incidente relativo a disposición de componentes con un cliente, inmediatamente cuando éste ocurra.
- Enviar al Compliance Officer, trimestralmente, un Reporte con los procesos de disposición registrados conforme a lo señalado en el N°1 del “Instructivo de Disposición de Componentes” (Anexo N°8).

### **6.7 Prevención del Ilícito Contenido en el Artículo 318 ter del Código Penal**

#### **a) Conceptos Generales**

De acuerdo a lo consignado por el artículo 318 ter del Código Penal, se sanciona al que en el ejercicio de sus facultades de mando ordene a un trabajador a concurrir al lugar de desempeño de sus labores a sabiendas de que este se encuentra en cuarentena o aislamiento sanitario decretado por la autoridad sanitaria. Lo primero que se debe considerar es que este delito busca proteger la salud pública de

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 43 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

conductas que resultan peligrosas por las posibilidades de contagio vinculadas a la reunión de un número elevado de personas sin que la autoridad lo permita. Por lo mismo, este delito, solo puede ser cometido en aquellas unidades de negocio que no tengan permiso para operar por no tratarse, por ejemplo, de actividades esenciales.

#### **b) Actividades Riesgosas**

Como se señaló con anterioridad, los riesgos de comisión de este delito están asociados, principalmente a los procesos efectuados en unidades que efectúan actividades no declaradas esenciales en el marco del retorno al desarrollo de actividades presenciales como, por ejemplo, el plan de “retorno seguro”, en la medida que se podría terminar ordenando a un colaborador que vive en alguna comuna todavía en cuarentena, o que se encuentra en aislamiento por otras circunstancias, que se presente a su lugar de trabajo.

#### **c) Medidas de Mitigación de Riesgos**

- Conformación de un Comité Táctico Central integrado, entre otras personas, por el Compliance Officer.
- Prohibición de operar con trabajadores en aislamiento en rubros no esenciales.
- Plan de Reporte liderado por Comité Táctico Central, relativo a desarrollo de retorno de colaboradores.
- Directrices y capacitación relativas al 318 ter del Código Penal, especialmente a jefatura, Recursos Humanos, líderes operacionales y generalistas.
- Solicitud de salvoconductos y permisos para operar en rubros declarados esenciales.

### **7. REGISTROS**

Los Procedimientos, Declaraciones Juradas y Formularios implementados en el marco del Sistema de Prevención de Delitos dan origen a una serie de Registros que permiten a la Compañía revisar, comparar y evaluar permanentemente el comportamiento de las personas naturales y jurídicas a las que se les aplican las medidas contenidas en el presente Manual, y mantener archivada la información proporcionada por los mismos.

Entre estos Registros están;

- Registro de Conflictos de Interés
- Registro de Donaciones Regulares / de Emergencia
- Registro de Patrocinios y Auspicios
- Registro de Contactos con Funcionarios Públicos
- Registro de Proveedores
- Registro de Clientes (Leasing y Crédito)

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 44 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

- Registro de Operaciones en Efectivo
- Registro de Declaraciones Juradas de Origen de Fondos
- Registro de Transferencias Electrónicas de Fondos

## **8. CONSERVACIÓN DE LA INFORMACIÓN Y DOCUMENTACIÓN**

Los Registros obtenidos a partir de la implementación de los procedimientos del Sistema de Prevención de Delitos serán conservados en carpetas físicas y/o electrónicas por el plazo de 5 años, y quedarán a disposición del Compliance Officer y de cualquier autoridad competente, para el caso que sea requerida.

Si se trata de carpetas físicas, la Unidad de Negocio correspondiente deberá mantener resguardada la información de que disponga en sus respectivas dependencias. En el caso de carpetas electrónicas, la seguridad y mantenimiento estará a cargo del respectivo usuario.

## **9. SUPERVISIÓN Y MONITOREO**

La supervisión y monitoreo del Sistema de Prevención de Delitos está a cargo del Encargado de Prevención de Delitos (Compliance Officer), quien velará por su cumplimiento, realizará seguimiento, identificará oportunidades de mejora y revisará regularmente la información y documentación de respaldo.

Para el debido cumplimiento de las actividades anteriores, el Compliance Officer elabora anualmente un Programa de Trabajo que es puesto en conocimiento y aprobado por el SMT, en el que se señala la metodología empleada para las revisiones del nivel de cumplimiento del Sistema de Prevención de Delitos, y las actividades, plazos y fechas para la ejecución de las labores antes señaladas.

Asimismo, con el fin de revisar y actualizar la operatividad del Sistema de Prevención de Delitos y de definir e implementar mejoras, el Compliance Officer solicita periódicamente a Auditoría Interna la verificación del cumplimiento de los procedimientos que éste contempla.

## **10. CAPACITACIÓN**

### **Programa Anual de Capacitación**

La Compañía desarrolla, con cargo a sus recursos económicos, programas de capacitación con el propósito de instruir a sus directores, ejecutivos, trabajadores, prestadores de servicios y otros que se relacionen con ella sobre los conceptos, normas, políticas y procedimientos establecidos para la prevención de delitos, sus sanciones tanto administrativas como penales, las Señales de Alerta y los procedimientos a ejecutar frente a una operación de carácter sospechosa.

El Compliance Officer es el responsable de confeccionar el Programa Anual de Capacitación en consideración a los niveles de capacitación establecidos en el punto siguiente, para lo cual establece las fechas de las sesiones de capacitación y lleva el registro detallado de los integrantes que hayan recibido las capacitaciones pertinentes.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 45 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

## Niveles de Capacitación

Las sesiones de capacitaciones que formen parte del programa anual de capacitación se realizan mediante cualquier medio físico o electrónico, y de ellas se deja constancia en el expediente personal de cada integrante que haya participado en la capacitación respectiva.

### Capacitación Inductiva

Dentro de los 60 días siguientes a la fecha de la incorporación de un integrante a la Compañía, se le instruye sobre los alcances del Sistema de Prevención de Delitos, de acuerdo con las funciones que le corresponda a dicho trabajador.

### Capacitación General

Cada año el Compliance Officer preparará planes de capacitación dirigidas a los integrantes de la Compañía que estén en situaciones de riesgo, a fin de instruirlos sobre las normas vigentes en materia de prevención de delitos, las modificaciones que pudieran haberse incorporado en el presente Manual y en la normativa que sea aplicable, Señales de Alerta para detectar operaciones inusuales y sospechosas, y otros aspectos que considera relevantes el Compliance Officer.

### Capacitación Especializada

Una vez al año se desarrolla una sesión de capacitación adicional a la capacitación general, dirigida a los integrantes de la Compañía que manejen fondos o recursos de la misma, con el propósito de instruirlos en la ejecución de las políticas relativas a la prevención del cohecho a funcionario público nacional o extranjero, procedimientos de conocimiento de Clientes, Proveedores, Prestadores de Servicios y Distribuidores, identificación de operaciones inusuales y sospechosas, y otros aspectos que considera relevantes el Compliance Officer.

### Capacitación del Compliance Officer

El Compliance Officer cuenta a lo menos con una capacitación especializada al año, distinta a las que se realizan a los demás integrantes de la Compañía, a fin de ser instruido detalladamente sobre las materias vigentes para la prevención de delitos, Señales de Alerta para identificar operaciones inusuales y sospechosas, y otros aspectos relacionados, tales como cursos de inteligencia aplicables a la prevención del lavado de activos y del financiamiento del terrorismo, entre otros temas que se ameriten.

## 11. PLATAFORMA DE GESTIÓN ÉTICA

La Compañía cuenta con una Plataforma de Gestión Ética para canalizar las denuncias de manera confiable, anónimo y seguro, que complementa los conductos regulares de comunicación de la Compañía.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 46 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

La Plataforma de Gestión Ética está disponible las 24 horas del día todos los días del año, es confidencial y seguro, y su anonimato está resguardado por un sistema externalizado que cuenta con servidores localizados en el extranjero, a los que ningún integrante de la Compañía tiene acceso.

La Plataforma de Gestión Ética está a disposición de ejecutivos, trabajadores, proveedores, clientes y otros terceros que se relacionen con la Compañía en <https://etica.resguarda.com/komatsucummins/main.html>.

Las Denuncias pueden ser relativas a conductas o situaciones reñidas con la ética y el cumplimiento normativo, tales como acoso laboral, acoso sexual, violencia en el trabajo, conflicto de interés, discriminación, mal uso de información confidencial o privilegiada, mal uso de recursos de la compañía, medioambiente, robo, hurto, fraude o estafa, adulteración de estados financieros, incumplimiento de las normas de seguridad y salud ocupacional, incumplimientos al Sistema de Prevención de Delitos, entre otras.

Para realizar una Denuncia se debe ingresar a la página web <https://etica.resguarda.com/komatsucummins/main.html>, o al número telefónico 800835133 o al WhatsApp +56 2 27121737 o al email [lineaetica.komatsucummins@resguarda.com](mailto:lineaetica.komatsucummins@resguarda.com), seleccionar la opción adecuada “Reporte Línea Ética”, “Reporte Temáticas Ley Karin” o “Seguimiento de una denuncia” y seguir los siguientes pasos:

- Seleccionar la Compañía, unidad de negocio, región y sucursal o faena correspondiente.
- Aceptar la “Política de Privacidad Resguarda”.
- Identificarse (nombre, e-mail y teléfono) o seleccionar la opción “anónima”.
- Si se trata de “Reporte Temáticas Ley Karin” se debe identificar al denunciado y denunciante.
- Seleccionar el tipo de irregularidad que se desea denunciar proporcionando todos los detalles de la situación (fecha, lugar, testigos, etc.) y adjuntar evidencias como documentos, mensajes, correos, videos, audios, fotos y otros que respalden lo denunciado.
- Completar la denuncia ingresando un correo de contacto (opcional)
- El sistema enviará un Código Único y Clave para hacer seguimiento del caso. Los cuales deben ser guardados por el denunciante, ya que no son recuperables.
- Dentro de 3 días hábiles, el denunciante recibirá un Mensaje acusando recibo de la denuncia y/o solicitando más información.
- Para revisar el estado de avance se debe ingresar a <https://etica.resguarda.com/komatsucummins/main.html>, seleccionar “Seguimiento de una

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 47 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

denuncia” e ingresa el Código Único y la Clave.

## 12. PROCEDIMIENTO DE INVESTIGACIONES INTERNAS

La Compañía cuenta con un Procedimiento de Investigaciones Internas (CMP\_003) que establece las etapas, responsables, plazos, formalidades y principios rectores de las investigaciones que se llevan adelante en virtud de denuncias recibidas a través de la Plataforma de Gestión Ética.

Este Procedimiento se aplica a denuncias relativas a transgresiones a las reglas establecidas en el Código Mundial de Conducta Empresarial, en el Sistema de Prevención de Delitos, en el Reglamento Interno de Orden, Higiene y Seguridad y en otras Políticas y Procedimientos de la Compañía.

En términos generales, este Procedimiento establece que;

- Las investigaciones internas las lidera el Compliance Officer con el apoyo de un Investigador o una Comisión Investigadora Interna o Externa designada para el caso.
- El Investigador o Comisión Investigadora tienen 60 días, prorrogables, para recopilar antecedentes, hacer entrevistas a involucrados, testigos, jefaturas y realizar otras actividades conducentes a aclarar los hechos, excepto en el caso de las denuncias que se rigen por la Ley N°21.643, conocida también como “Ley Karin”, en cuyo caso el referido plazo será de 30 días hábiles.
- Transcurrido ese plazo, el Investigador o Comisión Investigadora emite un Informe de Investigaciones Internas que contiene las declaraciones, compromisos de confidencialidad, evidencia, conclusiones y recomendaciones.
- Dicho Informe es revisado por el Compliance Officer, el área legal y por el Comité de Ética cuando el caso es confirmado, para decidir las acciones correctivas y/o las medidas disciplinarias que se adoptarán.
- El Comité de Ética podrá requerir la opinión de un tercero experto para que lo oriente en la toma de decisiones.
- El afectado/a por alguna medida disciplinaria podrá utilizar el procedimiento de apelación general cuando la sanción sea una multa, es decir, podrá reclamar de su apelación ante la Inspección del Trabajo.

### Principios del Procedimiento de Investigaciones Internas

El Procedimiento de Investigación Internas debe respetar los siguientes principios:

- Se promoverá una investigación justa, racional, oportuna y transparente con garantías de imparcialidad, objetividad, diligente y con perspectiva de género para el denunciante

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSA | Página 48 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|



y el denunciado.

- Se procurará que durante el proceso de investigación las partes involucradas conozcan de su existencia y de su derecho a ser escuchadas.
- Se resguardará el anonimato de la denuncia.
- Se mantendrá en reserva toda la información obtenida en la investigación, quedando estrictamente prohibida su difusión por cualquier medio.
- Se realizará la investigación en forma rápida, oportuna y efectiva.
- Se resguardará el principio de inocencia durante todo el proceso, por lo que se considerarán inocentes a las personas hasta que se pruebe lo contrario.
- Se reconocerá y valorará la ayuda que trabajadores, proveedores, clientes y otras personas proporcionen en una denuncia, y en la identificación de problemas que se requiera abordar.
- No se tolerará ni aceptará ningún tipo de represalia o acciones en contra de un trabajador, proveedor o cliente que presente una denuncia, o participe en el proceso de investigación, que lo perjudique en el empleo, la prestación de servicios o su relación comercial con la Compañía. En el caso de trabajadores, cualquier acto de separación de su cargo, descenso de categoría, suspensión temporal, pérdida de beneficios, amenazas, acoso o discriminación serán considerados actos que infringen el Código Mundial de Conducta Empresarial.
- En el caso de proveedores, cualquier acto que afecte el nivel de servicio entregado, disminución de precios acordados, eliminación de licitaciones futuras sin fundamentos técnicos, serán considerados actos que infringen el Código Mundial de Conducta Empresarial.

### **13. COMUNICACIÓN DE RESULTADOS A LA AUTORIDAD**

Ante la detección de un hecho que puede ser constitutivo de delito, el Comité de Ética debe evaluar, en conjunto con el SMT, la decisión de ponerlo en conocimiento del Ministerio Público (o sus órganos auxiliares) u otras entidades regulatorias o tribunales de justicia, de acuerdo con el Procedimiento de Investigaciones Internas. En dicho caso, debe además ponerlo en conocimiento del Departamento de Compliance de KLTD.

Si el hecho involucra a alguno de los integrantes del SMT, el Comité de Ética podrá requerir la opinión de un tercero experto respecto de la formulación de denuncias a las entidades mencionadas anteriormente.

Debe tenerse en consideración que dicha comunicación de resultados o el reporte de antecedentes

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 49 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

relativos a las investigaciones que hubieren determinado la existencia de un hecho constitutivo de delito, de acuerdo al artículo 6° N°2 de la Ley N°20.393 se contempla como circunstancia atenuante de responsabilidad penal de la empresa, en el siguiente sentido: “Se entenderá especialmente que la persona jurídica colabora sustancialmente cuando, en cualquier estado de la investigación o del procedimiento judicial, sus representantes legales hayan puesto, antes de conocer que el procedimiento judicial se dirige contra ella, el hecho punible en conocimiento de las autoridades o aportado antecedentes para establecer los hechos investigados”.

#### **14. MEDIDAS DISCIPLINARIAS POR INCUMPLIMIENTO DEL SISTEMA DE PREVENCIÓN DE DELITOS**

El incumplimiento de las disposiciones establecidas en el Sistema de Prevención de Delitos se considerará siempre como faltas y serán objeto de medidas disciplinarias, las que dependerán de la gravedad de la conducta.

Se entiende que la falta es “culposa” cuando por imprudencia se contraviene cualquiera de las previsiones del Manual, sin que exista una real voluntad de infringirlo. En este caso, se aplicará al trabajador una amonestación verbal o escrita, sin descuentos en las remuneraciones, conforme a lo dispuesto en la Ley y en el Reglamento Interno de Orden, Higiene y Seguridad vigente de la Compañía.

Se entiende que la falta es “dolosa” cuando se infringe alguna de las disposiciones del Manual, con conciencia y voluntad. En este caso, se aplicará al trabajador una amonestación verbal o escrita, con el descuento máximo del 25% de sus remuneraciones, conforme a lo dispuesto en la ley y en el Reglamento Interno de Orden, Higiene y Seguridad vigente de la Compañía. Lo anterior es sin perjuicio de que la Compañía pueda, atendida la gravedad de los hechos, aplicar lo establecido en el artículo 160 del Código del Trabajo.

#### **15. AUDITORÍAS ANUALES DEL MODELO DE PREVENCIÓN DE DELITOS**

Las auditorías al Modelo de Prevención de Delitos (MPD) son una herramienta clave para asegurar su efectividad y fomentar la mejora continua. A través de este proceso, es posible identificar deficiencias, evaluar el cumplimiento de las normativas aplicables y verificar que las políticas y procedimientos establecidos estén siendo implementados de forma adecuada. Asimismo, permiten detectar áreas de riesgo no contempladas previamente y proponer recomendaciones que fortalezcan tanto el modelo como la cultura organizacional de cumplimiento.

Estas auditorías se realizarán de forma anual y permitirán evaluar la adecuación del modelo frente a nuevos riesgos, revisar la eficacia de los controles implementados, y asegurar que el MPD se mantenga actualizado frente a los cambios en el entorno regulatorio y operativo. Sus resultados serán clave para orientar acciones de mejora y reforzar el compromiso institucional con una cultura de cumplimiento.

|            |            |  |                           |             |                    |
|------------|------------|--|---------------------------|-------------|--------------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos<br>Ley N°20.393 | Gerencia de<br>Compliance | KCC<br>KHSa | Página 50 de<br>51 |
|------------|------------|--|---------------------------|-------------|--------------------|

## 16. CONTROL DE VERSIONES

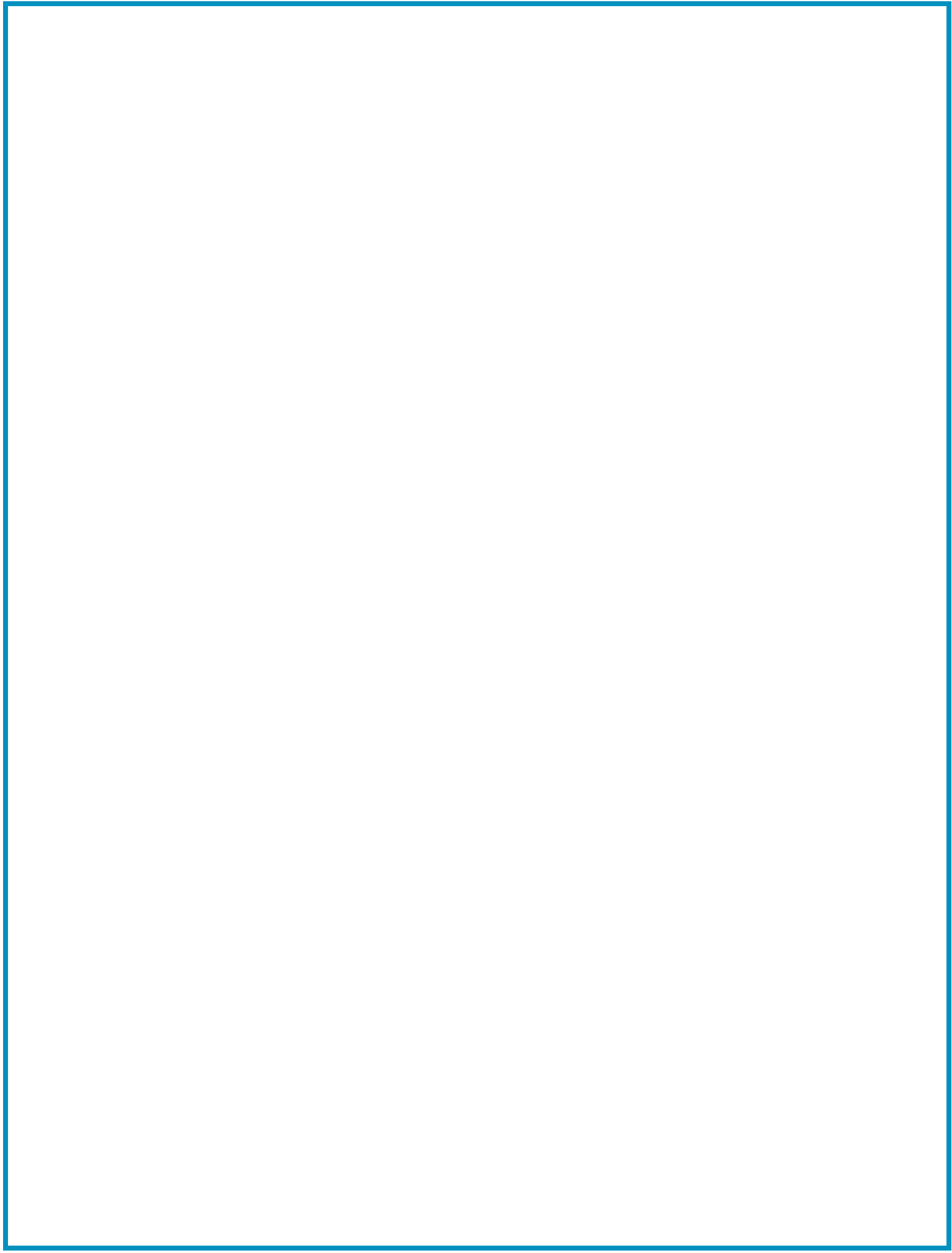
| Versión | Fecha      | Descripción   |
|---------|------------|---|
| 1.0     | 23-03-2016 | Creación del Manual Sistema de Prevención de Delitos.   |
| 2.0     | 03-03-2022 | <ul style="list-style-type: none"> <li>Incorporación de los nuevos delitos como: corrupción entre privados, administración desleal, apropiación indebida, contaminación de aguas, ordenar a un trabajador infringir el aislamiento en Pandemia y delitos contemplados en la Ley de control de armas y sustancias químicas que permitan la fabricación de explosivos.</li> <li>Incorporación formal de KMC Chile al Sistema de Prevención de Delitos.</li> </ul>   |
| 3.0     | 31-03-2025 | <ul style="list-style-type: none"> <li>Actualización respecto a la Ley N°21.595 sobre Delitos Económicos y Ambientales, que introdujo 291 delitos al catálogo de la Ley N°20.393.</li> <li>Actualización de los requisitos penales para las personas jurídicas.</li> <li>Eliminación del catálogo de delitos.</li> <li>Actualización de las penas previstas en la ley.</li> <li>Actualización del cumplimiento del deber de dirección y supervisión.</li> <li>Incorporación de la prevención de delitos informáticos.</li> <li>Actualización del Canal de Denuncias.</li> <li>Actualización del Procedimiento de Investigaciones Internas.</li> <li>Actualización de la Matriz de Riesgos y mapa de calor</li> <li>Actualización de anexos.</li> <li>Incorporación de versiones y vigencia del Manual.</li> </ul> |

## 17. VIGENCIA

La presente política entrará en vigor en la fecha de publicación. Su contenido será objeto de revisión y actualización cada 2 años o con anticipación, si se presentan cambios relevantes en la normativa o en su aplicación.

---

|            |            |   |                        |             |                 |
|------------|------------|---|------------------------|-------------|-----------------|
| CMP-007/03 | 31/03/2025 | Política Manual Sistema de Prevención de Delitos Ley N°20.393 | Gerencia de Compliance | KCC<br>KHSA | Página 51 de 51 |
|------------|------------|---|------------------------|-------------|-----------------|













# Manual Sistema de Prevención de Delitos Komatsu (KAREN H)

Informe de auditoría final

2025-04-29


|                    |   |
|--------------------|---|
| Fecha de creación: | 2025-04-24  |
| Por:               | Maria Pilar Troncoso Guzman (pilar.troncoso@global.komatsu) |
| Estado:            | Firmado   |
| ID de transacción: | CBJCHBCAABAAMaDaMkhCDYsnyLOkP6BxxkmVL9S-BmPE                |

## Historial de “Manual Sistema de Prevención de Delitos Komatsu (KAREN H)”

-  Maria Pilar Troncoso Guzman (pilar.troncoso@global.komatsu) ha creado el documento.  
2025-04-24 - 13:55:49 GMT- Dirección IP: 190.22.85.65.
-  El documento se ha enviado por correo electrónico a lorena.venegas@global.komatsu para su firma.  
2025-04-24 - 13:55:58 GMT
-  El documento se ha enviado por correo electrónico a francisco.vial@global.komatsu para su firma.  
2025-04-24 - 13:55:58 GMT
-  El documento se ha enviado por correo electrónico a veronika.holtz@global.komatsu para su firma.  
2025-04-24 - 13:55:58 GMT
-  El documento se ha enviado por correo electrónico a darko.louit@global.komatsu para su firma.  
2025-04-24 - 13:55:58 GMT
-  lorena.venegas@global.komatsu ha visualizado el correo electrónico.  
2025-04-24 - 15:23:22 GMT- Dirección IP: 52.102.13.85.
-  El firmante lorena.venegas@global.komatsu firmó con el nombre de Lorena Venegas  
2025-04-24 - 15:23:56 GMT- Dirección IP: 152.230.186.6.
-  Lorena Venegas (lorena.venegas@global.komatsu) ha firmado electrónicamente el documento.  
Fecha de firma: 2025-04-24 - 15:23:58 GMT. Origen de hora: servidor.- Dirección IP: 152.230.186.6.
-  francisco.vial@global.komatsu ha visualizado el correo electrónico.  
2025-04-24 - 15:42:58 GMT- Dirección IP: 104.47.23.190.
-  El firmante francisco.vial@global.komatsu firmó con el nombre de Francisco Vial  
2025-04-24 - 15:43:56 GMT- Dirección IP: 186.67.71.67.

 Francisco Vial (francisco.vial@global.komatsu) ha firmado electrónicamente el documento.

Fecha de firma: 2025-04-24 - 15:43:58 GMT. Origen de hora: servidor.- Dirección IP: 186.67.71.67.

 veronika.holtz@global.komatsu ha visualizado el correo electrónico.


2025-04-24 - 17:36:18 GMT- Dirección IP: 52.102.13.5.

 El firmante veronika.holtz@global.komatsu firmó con el nombre de Veronika Holtz

2025-04-24 - 17:37:23 GMT- Dirección IP: 190.116.19.114.

 Veronika Holtz (veronika.holtz@global.komatsu) ha firmado electrónicamente el documento.


Fecha de firma: 2025-04-24 - 17:37:25 GMT. Origen de hora: servidor.- Dirección IP: 190.116.19.114.

 darko.louit@global.komatsu ha visualizado el correo electrónico.

2025-04-29 - 14:36:57 GMT- Dirección IP: 104.47.23.126.

 El firmante darko.louit@global.komatsu firmó con el nombre de Darko Louit

2025-04-29 - 14:37:16 GMT- Dirección IP: 186.67.71.67.

 Darko Louit (darko.louit@global.komatsu) ha firmado electrónicamente el documento.

Fecha de firma: 2025-04-29 - 14:37:18 GMT. Origen de hora: servidor.- Dirección IP: 186.67.71.67.

 Documento completado.

2025-04-29 - 14:37:18 GMT