

**MODELO DE
PREVENCIÓN
DE DELITOS
(LEY N°20.393)**

ÍNDICE

| | | |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. | INTRODUCCIÓN..... | 4 |
| 2. | ALCANCE..... | 4 |
| 3. | OBJETIVO..... | 5 |
| 4. | MARCO LEGAL..... | 5 |
| 5. | DEFINICIONES..... | 6 |
| 6. | DELITOS..... | 8 |
| 7. | MODELO DE PREVENCIÓN DE DELITOS..... | 10 |
| 7.1. | POLÍTICAS..... | 10 |
| 7.1.1. | Designación de Encargado de Prevención..... | 11 |
| 7.1.2. | Medios y facultades del Encargado de Prevención..... | 11 |
| 7.2. | ATRIBUCIONES Y RESPONSABILIDADES..... | 12 |
| 7.2.1. | Directorio..... | 12 |
| 7.2.2. | Gerente General..... | 12 |
| 7.2.3. | Encargado de Prevención de Delitos..... | 13 |
| 7.2.4. | Head Regional de Legal & Cumplimiento..... | 15 |
| 7.2.5. | Country Head de Compass Group Chile..... | 16 |
| 7.2.6. | Gerente de Gestión de Talentos,..... | 16 |
| 7.2.7. | Trabajadores y empleados (“Colaboradores”), asesores y contratistas..... | 17 |
| 7.3. | SISTEMA DE PREVENCIÓN DE DELITOS..... | 17 |
| 7.3.1. | Identificación de actividades o procesos, sean habituales o esporádicos, en cuyo contexto se generen o que incrementan el riesgo de comisión de Delitos..... | 17 |
| 7.3.2. | Establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la Matriz de Riesgos, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de Delitos..... | 18 |
| 7.3.2.1. | Matriz de Riesgo..... | 18 |
| 7.3.2.2. | Evaluación de cumplimiento de controles..... | 19 |
| 7.3.3. | La identificación de los procedimientos de administración y auditoría de los recursos financieros que permitan a la entidad prevenir su utilización en los delitos señalados..... | 19 |
| 7.3.3.1. | Proceso de Prevención de Delitos..... | 19 |
| 7.3.3.2. | Actividades de prevención..... | 20 |
| 7.3.3.3. | Actividades de detección..... | 28 |

| | |
|------------------------------------------------------------------|----|
| 7.3.3.4. Actividades de respuesta | 28 |
| 7.3.3.5. Actividades de supervisión y monitoreo | 33 |
| 7.3.3.6. Áreas de apoyo directo | 34 |
| 7.3.3.6.1. Gerencia de Compliance..... | 34 |
| 7.3.3.6.2. Gerencia Legal | 34 |
| 7.3.3.6.3. Gerencia de Gestión de Talento..... | 34 |
| 7.3.3.7. Capacitaciones | 35 |
| 7.3.3.8. Reportes | 36 |
| 7.3.3.9. Certificación del Modelo de Prevención de Delitos | 36 |
| 8. VIGENCIA..... | 36 |
| 9. APROBACIONES Y/O ACTUALIZACIONES..... | 37 |
| 10. ANEXOS | 38 |

1. INTRODUCCIÓN

En diciembre de 2009 se promulgó en Chile la Ley N°20.393, que establece la responsabilidad penal de las personas jurídicas (la “Ley N°20.393”) respecto de ciertos delitos cometidos en beneficio o interés de ella (los “Delitos”), por sus dueños, controladores, responsables, ejecutivos principales representantes o quienes realicen actividades de administración y supervisión, y siempre que la comisión de tales delitos sea consecuencia del incumplimiento de la persona jurídica de sus deberes de dirección y supervisión.

El objetivo del presente Modelo de Prevención de Delitos (el “Modelo” o el “Modelo de Prevención”) es establecer los lineamientos sobre los cuales se sustenta la adopción, implementación y operación de procedimientos adecuados para la prevención de los Delitos, de acuerdo con las disposiciones establecidas en la referida Ley N°20.393.

Las directrices contenidas en este Modelo se complementan con los siguientes manuales, políticas y protocolos de autorregulación internos:

- > Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo
- > Código Regional de Ética y Conducta
- > Política de Conocimiento y Monitoreo de Terceras Partes (Know your provider)
- > Política Regional Reporte de Actividades Contrarias a la Ética o Ilegales
- > Política Regional Prevención de Fraude y Corrupción
- > Protocolos, Reglas y Procedimientos específicos que se dicten o se establezcan en relación a cada actividad específica y que permitan a las personas que intervengan en las actividades que se definan como de riesgo de comisión de los delitos contemplados en la Ley N°20.393, programar y ejecutar sus funciones de manera de prevenir la comisión de delitos.

2. ALCANCE

El alcance del presente Modelo radica en Compass Group Chile S.A. Administradora General de Fondos (la “*Administradora*”), y sociedades del grupo Compass en Chile, (en adelante “Compass Group Chile”) e incluye a los controladores personas jurídicas y naturales, directores, ejecutivos principales, representantes, alta administración, trabajadores, contratistas, subcontratistas, proveedores y asesores que presten servicios a Compass Group Chile.

3. OBJETIVO

El Modelo de Prevención que por este medio se implementa, tiene como objetivo establecer los lineamientos y procedimientos necesarios para dar cumplimiento a los requerimientos establecidos en la Ley N°20.393, adoptando e implementado un modelo consistente en la prevención de la comisión de Delitos que opera a través de diversas actividades de control, enfocado particularmente en las actividades, operaciones o negocios de la Administradora que potencialmente presenten riesgos de comisión de Delitos.

Adicionalmente, el Modelo busca que los Delitos sean prevenidos y/o detectados tempranamente, buscando evitar su materialización, minimizando en consecuencia los riesgos señalados en la Ley N°20.393.

4. MARCO LEGAL

De acuerdo con lo dispuesto en la Ley N°20.393, las disposiciones establecidas en el presente Modelo tienen por objeto dar cumplimiento y complementar lo dispuesto en la legislación nacional sobre las materias aquí tratadas.

En consecuencia, lo dispuesto en este Modelo de Prevención se establece sin perjuicio de las demás normas que la Administradora y sus empleados deberán observar en relación con dichas materias.

De esta forma, entre las normas a considerar por la Administradora , se destacan las siguientes:

- > Ley N°20.393 y sus modificaciones posteriores, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo, cohecho a funcionario público, receptación, apropiación indebida, corrupción entre particulares y administración desleal, entre otros delitos.
- > Ley 21.121: Modifica la Ley N°20.393 y la Ley N°19.913 que creó la Unidad de Análisis Financiero (“UAF”), ampliando el catálogo de delitos base de lavado de activos, particularmente, incorporando dentro de éstos a los delitos de apropiación indebida y administración desleal.
- > Ley N°19.913, que crea la UAF, y sus modificaciones posteriores;
- > Ley 20.119: Modifica la Ley N°19.913, incorporando más categorías de sujetos obligados que tienen la obligación de informar a la UAF, entre otras materias.
- > Ley N°20.000, que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas;
- > Ley N°20.818 que perfecciona los mecanismos de prevención, detección, control, investigación y juzgamiento del delito de lavado de activos.

-
- > Ley N°17.798, sobre control de armas;
 - > Ley N°18.045, sobre mercado de valores, y sus leyes complementarias;
 - > Ley N°18.314 que determina las conductas terroristas y fija su responsabilidad;
 - > Ley N°20.712, sobre administración de fondos de terceros y carteras individuales;
 - > Circular N°1.809 dictada por la Comisión para el Mercado Financiero con fecha 10 de agosto de 2006 y sus modificaciones posteriores;
 - > Normas y Circulares impartidas por la UAF (www.uaf.cl); y
 - > Ley N°21.459 que establece normas sobre delitos informáticos.

5. DEFINICIONES

- > **Alta Administración:** conformada por el Gerente General y la plana ejecutiva de Compass Chile.
- > **Código Regional de Ética y Conducta:** es el documento que informa sobre la ética de negocios a todos los Colaboradores y personas que se relacionan con Compass Chile, que se enmarca en los altos estándares valóricos que son esenciales para lograr el éxito de sus clientes, los cuales han depositado su confianza en los servicios y fondos administrados.
- > **Country Head de Compass Chile:** lidera la gestión de la oficina de Compass en Chile, ejecutando las definiciones estratégicas y objetivos anuales de la oficina, y coordinando a las diferentes áreas internas, de manera de cumplir con la misión y visión de la firma, el presupuesto anual y los proyectos estratégicos definidos. La nominación del cargo la realiza el Chief Executive Officer (CEO) regional de Compass Group.
- > **Directorio:** es la instancia responsable de aprobar las políticas, los procedimientos incluidos en el presente Modelo y sus actualizaciones con la frecuencia que sea necesaria, en caso de que se produzcan cambios significativos en las políticas y los procedimientos establecidos en el presente Modelo de Prevención, dejando evidencia de ello, en el acta que se levante de la sesión respectiva.
- > **Encargado de Prevención de Delitos (“Encargado de Prevención”):** es el colaborador designado por el Directorio de la Administradora, quien reporta directamente a éste, cuya función principal es ser el primer responsable de la aplicación, monitoreo y fiscalización de las normas de este Modelo de Prevención, sin perjuicio de otras funciones y facultades que le sean encargadas en otras materias u otros Manuales y que no se encuentren

reguladas en este Modelo. En las respectivas políticas complementarias puede ser denominado “Oficial de Cumplimiento” u “OC”.

- > **Head Regional de Legal y Cumplimiento:** lidera el equipo de Legal & Compliance de Compass, y se encarga de mantener las políticas y procedimientos destinados a dar plena ejecución y seguimiento de las normativas legales y regulatorias aplicables a las operaciones de Compass en las diversas jurisdicciones en las que opera a nivel global. Sus responsabilidades incluyen también la implementación y supervisión de *best practices* destinadas a mantener los altos estándares de calidad y cumplimiento en protección de los intereses de los clientes y de la Firma.
- > **Política Regional de Prevención de Fraudes, Soborno y Corrupción:** El objetivo de este documento es comunicar a todos los colaboradores de Compass Chile, así como también a clientes, proveedores y/o prestadores de servicios, que ésta se opone rotundamente a la realización de cualquier acto ilegal, y que dispone de controles y procedimientos tendientes cuya finalidad es prevenir, detectar y dar respuesta a situaciones de fraude, soborno o corrupción implementando las medidas que de conformidad a la ley sean procedentes para prevenir o detener dichos delitos.
- > **Política Regional de Reporte de Actividades Contrarias a la Ética o Ilegales:** El objetivo de este documento es describir en forma simple la forma de iniciar, evaluar y resolver una denuncia sobre cualquier incidente o violación al Modelo de Prevención de Delitos, Código Regional de Conducta y Ética, Política Regional de Prevención de Fraudes y Corrupción, normativas legales locales y en general de algún procedimiento contable o de auditoría, incluyendo cualquier supuesta irregularidad de naturaleza general, operativa o financiera dentro de la Administradora en el desarrollo de sus negocios.
- > **Reglamento Interno de Orden, Higiene y Seguridad:** El objetivo de este documento es regular las condiciones, requisitos, derechos, beneficios, obligaciones, prohibiciones y, en general, las formas y condiciones de trabajo, orden, higiene y seguridad de todos los colaboradores que laboran en Compass Chile.
- > **Responsabilidad Penal:** La responsabilidad penal es la consecuencia jurídica derivada de la comisión de un hecho u omisión tipificado como delito en una ley penal.

La Responsabilidad Penal se concreta en la imposición de una pena, por parte de los tribunales penales correspondientes, a quien comete el delito, que puede ser privativa de libertad (como la pena de prisión o la relegación), privativa de otros derechos (como el derecho a conducir vehículos motorizados, o la inhabilitación para cargos públicos), o consistir en una multa.

De acuerdo con el ordenamiento jurídico chileno, la Responsabilidad Penal es por regla general, de la o las personas naturales que cometen el delito. Sin embargo, en determinadas circunstancias y para determinados delitos, la Ley N°20.393 establece que también se puede considerar penalmente responsable a la persona jurídica.

Los delitos para los cuales es aplicable el concepto de Responsabilidad Penal de las personas jurídicas son exclusivamente los indicados en la Ley N°20.393.

6. DELITOS

- > **Administración desleal:** el delito de administración desleal es aquel establecido en artículo 470 N°11 del Código Penal y sanciona a aquel que teniendo a su cargo el patrimonio de otra persona, sea esta una persona natural o jurídica, le provoque un perjuicio ejerciendo de forma abusiva cualquier acción u omisión de modo manifiestamente contrario al interés del titular.
- > **Apropiación indebida:** El delito de apropiación indebida es aquel establecido en el artículo 470 N°1 del Código Penal y consiste en apropiarse o distraer en perjuicio de otro, dinero, efectos o cualquiera otra cosa mueble que hubieren recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarla o devolverla. Este delito tiene como finalidad proteger la propiedad y sanciona a la persona que no restituya lo que se le entregó, causándole un perjuicio a otra persona.
- > **Corrupción entre particulares:** El delito de corrupción entre particulares es aquel establecido en el artículo 287 bis y ter del Código Penal y sanciona al empleado o mandatario que solicita o acepta un beneficio económico, regalía, ventaja, donativo o privilegio a cambio por favorecer o por haber favorecido, en el ejercicio de sus labores, la contratación de un oferente en perjuicio de otro oferente. También penaliza, a quien da, ofrece o consiente en dar a aquel empleado o mandatario dicho beneficio con ese mismo objetivo.
- > **Cohecho a un funcionario público nacional o extranjero:** En lo relevante para la Empresa, consiste en ofrecer o entregar cualquier tipo de regalo, premio, donativo, ventaja, privilegio de otra naturaleza o, en general, cualquier beneficio económico, a un funcionario público, sea este último nacional o extranjero, en provecho de este o de un tercero.

El cohecho, en todo caso, no excluye la oferta o entrega de regalos protocolares o autorizados por la costumbre, los cuales, en todo caso, son admisibles en los términos expuestos en la **Política Regional de Prevención de Fraudes, Soborno y Corrupción y al Código Regional de Ética y Conducta**. Tampoco constituye cohecho el pago de derechos, tasas u otros beneficios económicos de cualquier naturaleza, que un funcionario público, nacional o extranjero, tenga derecho a percibir legalmente por el ejercicio de sus funciones.

- > **Financiamiento del terrorismo:** Solicitar, recaudar o proveer fondos con la finalidad de que se utilicen en la comisión de cualquier delito terrorista (apoderarse o atentar contra

un medio de transporte público en servicio, atentado contra el jefe de Estado y otras autoridades, asociación ilícita con el objeto de cometer delitos terroristas, entre otros).

- > **Lavado de activos:** cualquier acto tendiente a ocultar o disimular el origen ilícito de determinados bienes, a sabiendas de que provienen directa o indirectamente de la perpetración de hechos constitutivos de delitos tales como tráfico ilícito de estupefacientes y sustancias sicotrópicas, conductas terroristas, tráfico de armas y organizaciones para la delincuencia (promoción de prostitución infantil, secuestro, etc.). También comete este delito quien realice cualquier acto en que se adquiera, posea, tenga o use los referidos bienes, con ánimo de lucro, cuando al momento de recibirlos ha conocido su origen ilícito.

El lavado de activos es un intento de ocultar o disimular la naturaleza, ubicación, origen, propiedad o control de dinero u otros bienes obtenidos en forma ilegal.

Es un proceso complejo y dinámico mediante el cual dichos activos, de procedencia ilícita, se introducen en una empresa y por ende en la economía de un país, intentando darle apariencia de legalidad.

- > **Negociación incompatible:** El delito de negociación incompatible es aquel establecido en el artículo 240 del Código Penal y penaliza a cualquier empleado público, árbitro, liquidador, director o gerente de sociedades anónimas que tome interés personal o familiar directa o indirectamente, en cualquier negociación, actuación, contrato, operación o gestión en la cual debiere intervenir en razón de su cargo.

En el contexto de la Administradora, lo anterior aplica a directores y gerentes que, sin cumplir las formalidades y requisitos previstos por la Ley, se benefician personalmente o benefician a un tercero asociado a ellos o a un pariente directo o indirecto con ocasión de un negocio de Compass Group Chile.

- > **Receptación:** La compra o adquisición de bienes que han sido hurtados, robados o que estaban bajo la custodia de un tercero, y su posterior venta, comercialización o transporte, sabiendo su origen ilícito.

Se deja constancia que, sin perjuicio de los delitos recién referidos, los cuales resultan relevantes para el presente Modelo teniendo en consideración el giro ordinario de la Administradora, la Ley N°20.393 también contempla otros Delitos los cuales se encuentran definidos en el Anexo N°2 y Anexo N°3.

Asimismo, la Ley 21.549 incorpora los siguientes delitos informáticos al modelo de prevención:

- > **Ataque a la integridad de un sistema informático:** El que obstaculice o impida 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 contenidos en el sistema informático.

-
- > **Acceso ilícito:** El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático y/o divulgue datos informáticos accedidos de manera ilícita.
 - > **Intercepción ilícita:** El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más.
 - > **Ataque a la integridad de los datos informáticos:** El que indebidamente altere, dañe o suprima datos informáticos, siempre que con ello se cause un daño grave al titular de estos mismos.
 - > **Falsificación informática:** El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.
 - > **Receptación de los datos informáticos:** El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos.
 - > **Fraude informático:** El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule 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.
 - > **Abuso de los dispositivos:** El que, para la perpetración de los delitos previstos en esta ley, entregare u obtuviere para su utilización, importare, difundiera o realizare 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 dichos delitos.

7. MODELO DE PREVENCIÓN DE DELITOS

7.1. POLÍTICAS

La Administradora velará permanentemente por mantener un modelo de organización, administración y supervisión adecuado para la prevención de los delitos contemplados en la Ley N°20.393, denominado Modelo de Prevención, a través del cual promoverá la prevención de los Delitos, así como también para la prevención de otro tipo de conductas impropias tipificadas en leyes, normas y reglamentos de organismos fiscalizadores, así como otras normas establecidas por la Administradora. .

7.1.1. Designación de Encargado de Prevención

El Encargado de Prevención durará hasta tres años en sus funciones y podrá ser prorrogado en su cargo por períodos de igual duración.

El Encargado de Prevención, en conjunto con la Alta Administración, deberá establecer métodos para la aplicación efectiva del presente Modelo y su supervisión. En todo caso el Encargado de Prevención será el primer responsable de la aplicación y fiscalización de las normas que este establece. Para tales efectos, contará con autonomía respecto de la Alta Administración y de los controladores de la Administradora .

El Directorio, la Alta Administración y el Encargado de Prevención serán en conjunto responsables de la adopción, implementación, administración, actualización y supervisión del Modelo de Prevención.

El Encargado de Prevención debe contar con la debida autonomía respecto de la Administradora, de sus accionistas y de sus controladores para ejercer sus funciones como Encargado de Prevención de acuerdo con los parámetros establecidos por la Ley N°20.393.

En caso de renuncia, remoción, o impedimento para ejercer el cargo, el Gerente General en consulta con el Head Regional de Legal y Cumplimiento de Compass deberá nombrar un Encargado de Prevención provisorio en tanto el Directorio nombra un reemplazante definitivo.

7.1.2. Medios y facultades del Encargado de Prevención

El Directorio proveerá los medios y facultades al Encargado de Prevención para el desarrollo de sus funciones y actividades, lo que incluye los recursos y medios materiales para realizar adecuadamente sus labores.

El Encargado de Prevención tendrá acceso a información relacionada con su ámbito de acción; tendrá acceso directo a la administración y tendrá el deber de informar al Directorio la gestión del Modelo de Prevención, al menos semestralmente y/o cuando las circunstancias de la entidad así lo ameriten.

El Encargado de Prevención en conjunto con la Alta Administración difundirá y comunicará a toda la organización el Modelo de Prevención, los roles y responsabilidades que de éste emanan y las sanciones por incumplimientos al mismo.

El Modelo de Prevención será actualizado cuando ocurran cambios relevantes en las condiciones del negocio o nuevas disposiciones legales lo hagan necesario, actividad de la cual será responsable el Encargado de Prevención en conjunto con la Alta Administración.

7.2. ATRIBUCIONES Y RESPONSABILIDADES

7.2.1. Directorio

En el contexto de la prevención de delitos, el Directorio tendrá las siguientes atribuciones y responsabilidades:

- > Aprobar el Modelo de Prevención de Delitos.
- > Designar y/o revocar de su cargo al Encargado de Prevención, de acuerdo con lo establecido por la Ley N°20.393. El Directorio podrá ratificar y prorrogar dicho nombramiento cada tres años.
- > Proveer los medios y recursos necesarios y razonables para que el Encargado de Prevención cumpla con sus atribuciones y responsabilidades.
- > Velar por la correcta implementación y efectiva operación del Modelo de Prevención de Delitos.
- > Evaluar los informes de gestión y funcionamiento del Modelo de Prevención generados por el Encargado de Prevención.
- > Analizar en forma semestral el reporte denominado “Reporte de Gestión Administrativa preparado por el Encargado de Prevención, dejando constancia en el acta respectiva.
- > Aprobar la planificación para el desarrollo y ejecución del Modelo para el siguiente período.
- > Determinar las sanciones aplicables frente a un eventual incumplimiento del presente Modelo, de acuerdo con la propuesta que realicen el Country Head de Compass Chile, el Head Regional de Legal y Cumplimiento, el Gerente de Gestión de Talento y el Encargado de Prevención y según lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad de la Administradora.
- > Requerir la certificación del Modelo de acuerdo con lo establecido en la Ley N°20.393.

7.2.2. Gerente General

- > Apoyar al Encargado de Prevención, asegurando su acceso irrestricto a la información y a las personas, así como también en la coordinación de las actividades propias del Modelo de Prevención en las áreas que se requiera.

-
- > Contribuir a la divulgación del Modelo de Prevención, en toda la organización, generando las instancias necesarias de difusión y compromiso, con el objeto de lograr una comunicación efectiva, de las políticas y procedimientos.
 - > Informar al Encargado de Prevención cualquier situación observada que tenga relación con el incumplimiento de la Ley N°20.393 y las gestiones relacionadas al Modelo de Prevención.
 - > Nombrar, junto al Head Regional Legal & Compliance un Encargado de Prevención Provisorio, en caso de que éste renuncie, sea removido o presente cualquier impedimento para ejercer el cargo, en tanto el Directorio nombra un reemplazante definitivo.
 - > Velar por que todas las áreas de Compass Chile cumplan con la entrega de información requerida por el Encargado de Prevención.

7.2.3. Encargado de Prevención de Delitos

El Encargado de Prevención tiene por misión fundamental establecer, en conjunto con el Directorio y la Alta Administración, el Modelo de Prevención al que se refiere la Ley N°20.393.

De conformidad a ello, le corresponderán las siguientes atribuciones:

- > Efectuar todas las funciones que, en su calidad de Encargado de Prevención, le competen de conformidad a la Ley N°20.393 y que el Directorio de la Administradora le asigne.
- > Velar en conjunto con la Alta Administración, por el correcto establecimiento y operación del Modelo de Prevención.
- > Procurar que los procesos y actividades internas de la Administradora, cumplan con los controles efectivos de prevención de riesgos de delitos de acuerdo con el Modelo de Prevención y la Matriz de Riesgos (Anexo N°1).
- > Mantener el registro de evidencia del cumplimiento y ejecución de los controles realizados conforme al presente Modelo y a lo regulado en la Matriz de Riesgo.
- > Determinar, en conjunto con la Alta Administración de la Administradora, los medios y recursos necesarios para lograr cumplir con su rol y responsabilidades.

-
- > Capacitar a los trabajadores de la Administradora en materias bajo el alcance de la Ley N°20.393, en conjunto con la Alta Administración o por separado, pero coordinado con ésta.
 - > Presentar al Directorio, a lo menos semestralmente y/o cada vez que las circunstancias lo ameritan, un reporte respecto de la gestión, medidas y procedimientos del Modelo, así como de cualquier hecho u omisión observado en el período respectivo y que constituya una desviación del Modelo o revista las características de uno o más Delitos.
 - > Establecer y dar cumplimiento, en conjunto con la Alta Administración, al Modelo de Prevención de Delitos, sugerir y solicitar el desarrollo e implementación de cualquier otra política y/o procedimiento que estime necesario para complementar el Sistema de Prevención existente.
 - > Evaluar permanentemente la eficacia y vigencia del Modelo de Prevención adoptado y su conformidad con las leyes y demás regulaciones, informando al Directorio respecto de la necesidad y conveniencia de su modificación.
 - > Tomar conocimiento y efectuar un análisis de toda operación inusual o sospechosa y, de considerarlo necesario, elevar el caso al Directorio cuando corresponda. A efectos del análisis, el Encargado de Prevención deberá recabar toda la documentación relacionada con esa operación, generando para tales efectos un archivo de antecedentes.
 - > Solicitar, en los casos que estime necesario para el ejercicio de sus funciones, todos los antecedentes y contratos que la Administradora celebre, especialmente con las empresas del Estado y, en general todos los servicios públicos creados por ley; empresas, sociedades públicas o privadas en que el Estado o sus empresas, sociedades o instituciones centralizadas o descentralizadas tengan aportes de capital mayoritario o en igual proporción, o, en las mismas condiciones, representación o participación, para los efectos de cautelar el cumplimiento de la Ley N°20.393, la regularidad de estas operaciones y, eventualmente, hacer efectivas las responsabilidades cuando constate una infracción a esta ley o comisión de alguno de los delitos que trata de prevenir.
 - > Analizar las denuncias recibidas, a través del canal de denuncias dispuesto en el presente Modelo de Prevención, en conjunto con el Head Regional de Legal y Cumplimiento y el Gerente de Gestión de Talentos.
 - > Determinar y coordinar, o el Head Regional de Legal y Cumplimiento, en el caso que corresponda de acuerdo a la Política Regional de Reporte de Actividades Contrarias a la Ética o Ilegales, las investigaciones derivadas de las denuncias recibidas, pudiendo requerir incluso asesoría legal externa en caso de considerarlo pertinente.

-
- > Proponer al Directorio, junto con el Head Regional de Legal & Cumplimiento y el Country Head de Compass Chile, las sanciones aplicables frente a un eventual incumplimiento del Modelo de Prevención, de acuerdo con lo establecido en el Reglamento Interno de Orden, Higiene y Seguridad de la Administradora y en el Código Regional de Ética y Conducta.
 - > Recomendar al Directorio la aplicación de sanciones disciplinarias, cuando corresponda.
 - > Ante la detección de un hecho que pueda tipificarse como Delito de aquéllos incluidos en la Ley N°20.393, el Encargado de Prevención deberá efectuar una presentación al Directorio, para que éste defina si efectuar las denuncias o querrelas respectivas.
 - > Documentar y custodiar la evidencia relativa a las actividades de prevención de delitos.
 - > Prestar amplia colaboración en el proceso de certificación del Modelo de Prevención, en caso de que así lo requiera voluntariamente Compass Group Chile o por obligación legal o normativa que sea dictada por los organismos reguladores pertinentes.
 - > Efectuar el seguimiento de las recomendaciones o instrucciones que emanen del proceso de certificación.
 - > Velar, en conjunto con la Alta Administración, por la actualización del presente Manual, de acuerdo con los cambios normativos y el entorno de negocios de Compass Chile.
 - > Velar y coordinar en conjunto con la Alta Administración, la realización de programas de capacitación a los colaboradores, en materias bajo el alcance de la Ley N°20.393.
 - > Realizar trabajos especiales que el Directorio de la Administradora le encomiende en relación con las materias de su competencia.

7.2.4. Head Regional de Legal & Cumplimiento

- > Nombrar un Encargado de Prevención provisorio en conjunto con el Gerente General, en caso de que éste renuncie, sea removido o presente cualquier impedimento para ejercer el cargo, en tanto el Directorio nombra un reemplazante definitivo.

-
- > Conocer las denuncias que se realicen por los Colaboradores, las cuales se mantendrá en estricta confidencialidad y, por lo mismo, ella sólo será conocida por el Encargado de Prevención, Head Regional de Legal y Cumplimiento, Country Head Compass Group Chile y por las personas que, por decisión de éstos, deban intervenir en el proceso de investigación
 - > Proponer al Directorio sanciones frente a un eventual incumplimiento del Modelo en conjunto con el Country Head de Compass Chile, Gerente de Gestión de Talento y el Encargado de Prevención.
 - > Proponer al Directorio, en conjunto con el Encargado de Prevención, las investigaciones derivadas de las denuncias recibidas por incumplimiento al Modelo de Prevención.
 - > Llevar a cabo la investigación, en conjunto con el Country Head de Compass Chile, ante un eventual incumplimiento al Modelo de Prevención, en caso de que el denunciado sea el Encargado de Prevención.

7.2.5. Country Head de Compass Chile

- > Conocer las denuncias que se realicen por los Colaboradores, las cuales se mantendrá en estricta confidencialidad y, por lo mismo, en conjunto con el Encargado de Prevención, el Head Regional de Legal y Cumplimiento y por las personas que, por decisión de éstos, deban intervenir en el proceso de investigación.
- > Proponer al Directorio sanciones frente a un eventual incumplimiento del Modelo en conjunto con el Head Regional de Legal y Cumplimiento, el Gerente de Gestión de Talento y el Encargado de Prevención.
- > Llevar a cabo la investigación, en conjunto con el Head Regional de Legal y Cumplimiento, ante un eventual incumplimiento al Modelo de Prevención, en caso de que el denunciado sea el Encargado de Prevención.

7.2.6. Gerente de Gestión de Talentos

- > Asistir al Encargado de Prevención en la determinación de las sanciones a proponer frente a un eventual incumplimiento del presente Modelo.
- > Velar y coordinar en conjunto con el Encargado de Prevención, la realización de programas de capacitación a los colaboradores, en materias bajo el alcance de la Ley N°20.393.

7.2.7. Trabajadores y empleados (“Colaboradores”), asesores y contratistas

- > Cumplir con lo dispuesto en el presente Modelo de Prevención.
- > Entregar la información que requiera el Encargado de Prevención para el desempeño de sus funciones en relación con la implementación, operatividad y efectividad del presente Modelo.
- > Ejecutar los controles de carácter preventivo que se establecen en la Matriz de Riesgos.
- > Informar, por los canales definidos, respecto de situaciones que pudieran ir en contra de lo establecido en el presente Manual.

7.3. SISTEMA DE PREVENCIÓN DE DELITOS

El Sistema de Prevención de Delitos, se compone de una serie de actividades y procedimientos orientados a apoyar el funcionamiento y ejecución del Modelo de Prevención, y que se detallan a continuación:

7.3.1. Identificación de actividades o procesos, sean habituales o esporádicos, en cuyo contexto se generen o que incrementan el riesgo de comisión de Delitos.

El Encargado de Prevención es el responsable del proceso de identificación de riesgos en cada una de las áreas de Compass Chile. Este proceso de identificación se deberá realizar anualmente o cuando surjan cambios relevantes e importantes en cualquier área de negocio, lo cual deberá contar con un debido respaldo.

Todos los Colaboradores de Compass Chile, deberán colaborar con la identificación de riesgos realizada por el Encargado de Prevención. Para ello, dicho Encargado de Prevención revisará los procedimientos y políticas en conjunto con sus realizadores, y recibirá cualquier información que los Colaboradores puedan aportar de acuerdo con su experiencia y funciones.

Para efectos de lo anterior, el Encargado de Prevención elaborará y mantendrá actualizada una Matriz de Riesgos, la cual, anexa al presente documento. Esta reflejará la identificación de las actividades o procesos de la Administradora que generan o incrementan el riesgo de ocurrencia de los Delitos, como asimismo establecerá sus respectivos controles de mitigación o eliminación de los riesgos.

7.3.2. Establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados en la Matriz de Riesgos, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de Delitos

7.3.2.1. Matriz de Riesgo

Las actividades de identificación, medición, control y monitoreo de los riesgos vinculados al cohecho, lavado de activos y/o financiamiento al terrorismo, se encontrarán contenidas en una Matriz de Riesgos que expresará el nivel de riesgo al que se encuentra expuesta la Administradora.

Para cada uno de los controles que se identifiquen en la Matriz de Riesgos, se deberá establecer la evidencia o respaldo de su ejecución. Por ello, para cada control se debe identificar:

- > Identificación del Procedimiento - Mapa de Procesos
 - ✓ Proceso
 - ✓ Actividad
 - ✓ Tipo de Delito

- > Identificación del Riesgo
 - ✓ Título del riesgo
 - ✓ Descripción del riesgo
 - ✓ Probabilidad de ocurrencia del riesgo
 - ✓ Impacto
 - ✓ Nivel de riesgo inherente
 - ✓ Riesgo asociado

- > Identificación de control
 - ✓ Descripción
 - ✓ Evaluación de suficiencia
 - Responsable
 - Periodicidad
 - ✓ Evaluación del control
 - Tipo de control
 - Diseño del control
 - Documentación del control
 - Importancia del control
 - Mitigación del riesgo

- > Riesgo residual
 - ✓ Probabilidad
 - ✓ Impacto

- ✓ Nivel de riesgo residual

7.3.2.2. Evaluación de cumplimiento de controles

El objetivo de la evaluación de cumplimiento de controles es identificar aquellas deficiencias que pudieran afectar de manera significativa la operación del Modelo o aumenten la probabilidad de comisión de los delitos señalados en la Ley N°20.393.

7.3.3. La identificación de los procedimientos de administración y auditoría de los recursos financieros que permitan a la entidad prevenir su utilización en los delitos señalados.

El Encargado de Prevención deberá verificar anualmente que los controles establecidos a través de la implementación del Modelo de Prevención se encuentran operando conforme a su diseño, a objeto de identificar posibles deficiencias de control que pudieran afectar de manera significativa a la Administradora o que pudieran aumentar la probabilidad de comisión de Delitos definidos en la Ley N°20.393.

Una vez recepcionados los resultados de la evaluación de cumplimiento de los controles, el Encargado de Prevención, procederán a corregir las deficiencias detectadas mediante la implementación de acciones y planes correctivos, los que serán evaluados en el siguiente proceso de revisión.

7.3.3.1. Proceso de Prevención de Delitos

Con el fin de cumplir con las políticas antes indicadas y reguladas por la Ley N°20.393, la Administradora implementará un Proceso de Prevención de Delitos que se desarrollará a través actividades de prevención, detección, respuesta y supervisión y monitoreo. Estas actividades están orientadas a apoyar el funcionamiento y ejecución del Modelo de Prevención, siendo el Encargado de Prevención el principal responsable de la ejecución y supervisión de dichas actividades.

A continuación, se presenta una vista gráfica de las actividades del Procedimiento de Prevención de Delitos.



7.3.3.2. Actividades de prevención

Una eficaz prevención de la comisión de los Delitos ayuda a evitar conductas u omisiones impropias desde su origen. En dicho sentido, el fin último de las actividades de prevención es evitar incumplimientos o violaciones al Modelo de Prevención y prevenir la comisión de los Delitos señalados en la Ley N°20.393.

Es por ello que, esta actividad incluye los siguientes procedimientos de prevención:

- > Procedimiento efectivo de difusión del Modelo de Prevención. La Administradora, a través de su Encargado de Prevención en conjunto con la Gerencia de Gestión de Talento, desarrollarán programas de capacitación, con el fin de instaurar y mantener una cultura de prevención de los Delitos contemplados en la Ley N°20.393.

Estas actividades permitirán transmitir a todos los Colaboradores de la Administradora la importancia de dar un correcto cumplimiento al presente Modelo de Prevención y la responsabilidad que estos asumen ante la comisión de los Delitos contemplados en la Ley N°20.393 y en el presente Modelo de Prevención.

Dicho procedimiento de difusión se hará de forma diferenciada en cada una de las áreas de Compass Group Chile, en cuanto al contenido, profundidad y periodicidad. Esto, de acuerdo con el nivel de exposición al riesgo de comisión de los Delitos especificados en la Ley N°20.393.

Del mismo modo y con el objeto de que todos los Colaboradores de la Administradora tengan conocimiento y acceso al presente documento, una copia del presente Modelo será publicada en el website www.cgcompass.com.

Adicionalmente, el Modelo de Prevención se considerará como parte integrante de los respectivos contratos de trabajo de los Colaboradores de la Administradora y los contratos de prestación de servicio que Compass Chile celebre con asesores,

contratistas y/o sub- contratistas y serán entregados por correo electrónico a la casilla entregada por el empleado o terceras partes.

- > Procedimientos de identificación y evaluación de los riesgos y controles. El Encargado de Prevención es responsable de la correcta y oportuna identificación y evaluación de riesgos de Delitos para la Administradora y de sus respectivos controles.

Este proceso debe ser realizado periódicamente o cuando sucedan cambios relevantes en las condiciones de la Administradora.

Para desarrollar este procedimiento, el Encargado de Prevención debe efectuar las siguientes actividades:

- ✓ Identificación del riesgo: La identificación de riesgos de comisión de Delitos se realizará por medio de reuniones entre Encargado de Prevención y los gerentes de las principales áreas que participen en actividades que pudieran implicar una responsabilidad penal de la persona jurídica.

Dicho procedimiento permite conocer y entender de mejor manera los procesos de la Administradora e identificar los principales escenarios de riesgos de comisión de los Delitos que pudieren ser cometidos en interés o provecho directo e inmediato de Compass Chile, y que pudiesen ser efectuados por los accionistas, principales ejecutivos o quienes realicen actividades de administración y supervisión, así como por las personas naturales que estén bajo la dirección o supervisión directa de alguno de los sujetos anteriormente mencionados.

Luego, y como se indicó anteriormente, los riesgos de delitos identificados se establecerán en la Matriz de Riesgos de la Administradora.

Conforme al procedimiento señalado, los riesgos identificados se clasificarán de acuerdo al nivel jerárquico y al tipo de riesgo que se presenta.

Respecto del nivel jerárquico, estos se diferenciarán en:

- Riesgos estratégicos: los cuales son definidos por la estructura estratégica de la Administradora en el ámbito de la administración de riesgos, conformado por el Directorio, Gerente General, Comités de Riesgo, Comité de Auditoría y Comités Ad-hoc.
- Riesgos operacionales: se refieren a eventos potenciales que pueden generar un daño a la organización en las actividades diarias de la Administradora.

Estos riesgos, a su vez, han sido clasificados en base a sus características propias y en base a la unidad responsable de monitorearlos de forma independiente. Los tipos de riesgos se diferenciarán en:

- Riesgo operativo.
 - Riesgo de fraude.
 - Riesgo de información.
 - Riesgos por incumplimiento normativo.
- ✓ **Evaluación de riesgos:** Los riesgos identificados deben ser evaluados para su priorización, con el objetivo de determinar las áreas o procesos de mayor exposición, lo que permitirá enfocar los recursos y esfuerzos.

Para la evaluación de los riesgos identificados debe participar el Encargado de Prevención junto a los gerentes de área que participaron en el proceso de identificación de los riesgos de Delitos. Sin embargo, también se podrá invitar a otros Colaboradores que tengan conocimiento de los riesgos y posean la autoridad necesaria para tomar decisiones relacionadas a las estrategias de control y otras formas de administración de los riesgos.

En consecuencia, todos aquellos riesgos que hayan sido identificados serán evaluados de acuerdo con su percepción de impacto y probabilidad de ocurrencia.

Para lo anterior, se evalúa la probabilidad y el impacto de acuerdo con los siguientes criterios:

- **Niveles de Probabilidad:** la probabilidad de ocurrencia corresponde a qué tan probable es que el riesgo se materialice en el periodo base de evaluación. Si consideramos base anual, se establece este elemento como la probabilidad de que el riesgo se materialice durante el próximo año.

La valorización de la probabilidad es cualitativa, asignando un valor de 1 a 5 siendo cinco el valor para la más alta probabilidad de ocurrencia. Se establecen criterios para la aplicación de este valor, considerando el evento que genera el daño en la definición del riesgo y su ubicación.

| PROBABILIDAD | DEFINICIÓN | DESCRIPCIÓN |
|--------------|------------|-------------------------------------------------------------------------------------------------------|
| Muy Alta | 5 | Se espera que el riesgo se materializa en la mayoría de las situaciones en que se encuentra presente. |

| | | |
|----------|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alta | 4 | Dada la naturaleza del riesgo es razonable esperar su materialización en el corto plazo (3 meses) y existe evidencia de su materialización |
| Media | 3 | Dada la naturaleza del riesgo es razonable esperar su materialización en el mediano plazo (6 meses) y existe evidencia de su materialización |
| Baja | 2 | El evento sólo ocurrirá en circunstancias excepcionales, o como el resultado de una combinación de eventos inusuales, existe evidencia de su materialización en la industria y se espera que se materializa en el largo plazo (mayor a 12 meses) |
| Muy Baja | 1 | No existe conocimiento acerca de la materialización del Riesgo en el pasado |

- Niveles de Impacto: es el potencial daño al patrimonio de la Administradora. Este se mide de forma cualitativa de 1 a 5, siendo el nivel 5 el más alto. Se establecen criterios para la aplicación de este valor.

| PROBABILIDAD | DEFINICIÓN | DESCRIPCIÓN |
|--------------|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Muy Alta | 5 | El error puede generar la suspensión de la licencia de funcionamiento de la AGF y el pago de multas pecuniarias que comprometen el patrimonio de esta |
| Alta | 4 | El error puede generar solicitudes de reenvío de información a las partes relacionadas ocasionando visitas del regulador para efectuar la revisión de los procesos o retiros de aportes de clientes. |

| | | |
|----------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Media | 3 | El error puede generar corrección y solicitudes de reenvío de información a las partes relacionadas, ocasionando llamados de atención escritos por parte del regulador. |
| Baja | 2 | El error ocasiona impacto en la información presentada, pero se identifica antes del envío de la información al regulador o a las demás partes interesadas |
| Muy Baja | 1 | El error no genera impactos significativos, se corrige sin mayores problemas |

Al asignar niveles cualitativos de impacto y probabilidad, simultáneamente a cada riesgo se le está asignando una calificación numérica, la cual gráficamente a través de la multiplicación de ambas cantidades permite identificar la severidad inherente de riesgo¹ para cada evento documentado:

| | | | | | | |
|--------------|---|---------|-------|----------|----------|----------|
| PROBABILIDAD | 5 | Medio | Alto | Muy Alto | Muy Alto | Muy Alto |
| | 4 | Medio | Alto | Alto | Muy Alto | Muy Alto |
| | 3 | Bajo | Medio | Alto | Alto | Muy Alto |
| | 2 | Bajo | Medio | Medio | Alto | Alto |
| | 1 | Bajo | Bajo | Bajo | Medio | Medio |
| | | 1 | 2 | 3 | 4 | 5 |
| | | IMPACTO | | | | |

- ✓ Identificación de controles: Para los riesgos detectados e identificados por el Encargado de Prevención, en conjunto con y los gerentes de las principales áreas que participen en actividades que pudieran implicar una responsabilidad penal de la persona jurídicas, se deberán identificar los controles necesarios para su mitigación.

Para efectos del presente Modelo de Prevención, se entiende por control, toda medida dispuesta a fin de mitigar o reducir la probabilidad de ocurrencia y/o la magnitud de impacto en caso de materializarse el riesgo

¹ El término “inherente” hace relación al riesgo que aún no ha sido administrado y que es susceptible a reducirse o a mitigarse a través del uso de controles o planes de acción: en la administración de riesgo es importante saber que la implementación de controles no eliminará el riesgo, pero podrá reducir a niveles tolerables la probabilidad y el impacto en caso de que se materialice.

identificado. Los controles son incorporados en los procesos con el fin de garantizar que se cumplan los requerimientos del flujo de trabajo y los objetivos generales de la Administradora.

- ✓ Evaluación de controles: Los controles identificados por cada riesgo serán evaluados en forma individual, en relación a la mitigación del riesgo de delito al que aplica. Dicha evaluación será efectuada por el Encargado de Prevención de Delitos.

La Administradora, con el fin de evaluar sus controles oportunamente, adopta un procedimiento implementado en la validación de funcionalidad de controles a partir de pruebas de diseño y eficacia operativa el cual se detalla a continuación:

- **Diseño**: consiste en la configuración de un control respecto del riesgo que pretende ser mitigado.

Esta variable se evalúa respondiendo la siguiente interrogante: *¿Las características o condiciones del control permiten mitigar el riesgo al cual está asociado?* para contestar esta pregunta se han especificado los siguientes criterios:

- ¿El control tiene asignado un responsable de su ejecución?
 - ¿El control está documentado / tiene evidencia física de su existencia?
 - ¿Qué naturaleza² tiene el control?
 - ¿De qué tipo³ es el control?
 - ¿Con qué frecuencia se implementa?
- **Eficacia**: una vez que validamos que el diseño es el apropiado para mitigar los riesgos existentes en un determinado proceso de negocio y que la forma como el control ha sido diseñado y direccionado de forma apropiada, tenemos que posteriormente validar si este control se encuentra en funcionamiento de forma consistente a lo largo del período abarcado. Para probar que el control funcione de forma consistente a lo largo del tiempo es necesario establecer pruebas "Testing" con el fin de establecer que el control se haya realizado.

² Naturaleza de los controles: **preventivos** (evitan que se produzcan errores e irregularidades), **detectivos** (Tratan de descubrir a posteriori errores o fraudes que no ha sido posible evitar con controles preventivos), **correctivos** (Tratan de asegurar que los errores identificados y materializados subsanen las consecuencias generadas).

³ Tipo de controles: manual, automático, manual con componente automático.

¿Cómo debemos testear el control? Una estrategia de testeo debe incluir:

- Indagación al personal apropiado
- Observaciones de las Operaciones de la Compañía
- Inspección de documentación relevante
- Re-ejecución de la aplicación de controles

La primera estrategia “indagación” es útil para tener un entendimiento del proceso de control, de la forma en que se realiza y nos brinda un primer y muy importante entendimiento de la forma en que el control es ejecutado. Es importante aclarar que por sí solo la indagación no es un método de prueba “sólido” dado que en el mismo no se requiere evidencia documental.

El segundo método mencionado “observación” nos permite evaluar controles mucho de los cuales a veces no tienen una evidencia documental en la cual respaldarnos.

El tercer método es Inspección, en el mismo se solicita evidencia documental a los fines de verificar que el control efectivamente se cumple. El soporte de análisis y aprobación de una conciliación bancaria es un ejemplo de este tipo de estrategia.

Finalmente, la última estrategia es re-ejecución que consiste en, bajo los parámetros / instrucciones informados por la gerencia respectiva, volver a realizar el control a los fines de llegar a las mismas conclusiones y resultados que quien lo realizó.

Para cada uno de los anteriores criterios, ha sido asignado un valor por medio del cual será posible determinar si el control está bien diseñado, la siguiente tabla muestra la ponderación para tener en cuenta:

| EVALUACIÓN DISEÑO CONTROL | | | |
|----------------------------------|-----|-----------------------|-----|
| Tipo de control | P/A | Preventivo Automático | 75% |
| | P/M | Preventivo Manual | 50% |
| | D/A | Detectivo Automático | 50% |

| | | | |
|---------------------------|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----|
| | D/M | Detectivo | |
| | Sin control | Manual | 25% |
| | | | 0% |
| Evaluación de suficiencia | Oportunidad | El control se ejecuta en el momento adecuado | |
| | Pertinencia | El control es conducente a mitigar el riesgo asociado | |
| | Frecuencia | El control se ejecuta la cantidad de veces correspondiente | |
| Documentación del control | Documentado | El control se encuentra documentado e identificado en manuales de procedimiento | |
| | Parcialmente Documentado | El control, si bien esta en conocimiento del responsable, este no se encuentra documentado y aprobado por el dueño del proceso. | |
| | No Documentado | El control no está documentado y menos está en conocimiento de los responsables. | |

De la gestión y monitoreo de los riesgos al evaluar el diseño de control, este resulta ser igual a 75%, el diseño del control resulta ser adecuado. Si, por el contrario, el riesgo no está identificado el resultado obtenido será de 1%, lo cual será necesario verificar la manera en la cual se está realizando el diseño y prepararlo nuevamente.

- ✓ Severidad Residual del Riesgo: esta corresponde a la etapa de final de la evaluación del diseño de control, tomando como criterios la solidez de los controles, los niveles inherentes de probabilidad e impacto y la naturaleza del mismo, para lo anterior, se determina la probabilidad e impacto del riesgo residual.

Para lo anterior, se debe determinar los siguientes pasos:

- El tipo del diseño de control (suficiencia).
- Si existe documentación de la actividad y control. el porcentaje de mitigación del riesgo.

La combinación de los puntos anteriores determinará el porcentaje de mitigación del riesgo, el cual aumentará o disminuirá el nivel de riesgo residual de la actividad o proceso.

| RIESGO INHERENTE | | | Evaluación del Control | | | | Mitigación Riesgo | Probabilidad | Impacto | Nivel de Riesgo Residual |
|------------------|---------|---------------------------|------------------------|--------------------|---------------------------|-------------------------|-------------------|--------------|---------|--------------------------|
| Probabilidad | Impacto | Nivel de Riesgo Inherente | Tipo de Control | Diseño del Control | Documentación del Control | Importancia del Control | | | | |
| 1 | 3 | Bajo | Preventivo/manual | No efectivo | Parcialmente Documentado | Necesario | 20% | 3 | 4 | Alto |
| 2 | 3 | Medio | Detectivo/manual | Efectivo | Parcialmente Documentado | Necesario | 20% | 2 | 2 | Medio |

7.3.3.3. Actividades de detección

El objetivo de estas actividades es desarrollar procedimientos que detecten incumplimientos al Modelo de Prevención o posibles escenarios de comisión de los Delitos señalados en la Ley N°20.393.

La actividad de detección incluye lo siguiente:

- > Procedimientos de auditorías de cumplimiento. El Encargado de Prevención junto al Área de Auditoría de la Administradora, deberán verificar periódicamente que los controles incluidos en la Matriz de Riesgos estén operando correctamente y si estos se ajustan a la realidad actual de la Administradora.

Ante deficiencias detectadas en los procesos de control, las áreas involucradas con el apoyo del Encargado de Prevención deberán corregir dichas deficiencias, mediante la implementación de planes de acción, los que deben ser evaluados en el siguiente proceso de evaluación de cumplimiento de controles.

- > Procedimiento de revisión de litigios. El Encargado de Prevención revisará y elaborará cuando corresponda un reporte que detalle entre otros; (i) demandas, juicios o cualquier acción legal que involucre a la Administradora, en algún escenario de Delito; (ii) multas y/o infracciones cursadas o en proceso de revisión, por parte de entes reguladores, asociadas a escenarios de Delito de la Ley.
- > Procedimiento de revisión de denuncias. El Encargado de Prevención deberá realizar un análisis de las denuncias recibidas, a través de los canales dispuestos por la Administradora en el siguiente numeral, para identificar aquellas que estén bajo el alcance del presente Modelo de Prevención o se encuentren asociadas a escenarios de Delitos de la Ley N°20.393.
- > Procedimiento de coordinación de investigaciones. El Encargado de Prevención deberá coordinar las investigaciones derivadas de las denuncias que tienen implicancia en el Modelo de Prevención o se encuentren asociadas a escenarios de Delitos de la Ley N°20.393.

La coordinación de la investigación de las denuncias se realizará según lo dispuesto el presente Modelo de Prevención y, en subsidio, por lo señalado en el procedimiento de denuncias establecido en **Política Regional de Reporte de Actividades Contrarias a la Ética o Ilegales**.

7.3.3.4. Actividades de respuesta

El fin de las actividades de respuesta es definir las posibles resoluciones, sanciones disciplinarias y/o sanciones aplicables a quienes incumplan el Modelo de Prevención.

Adicionalmente, dichas actividades buscan que la Administradora responda efectivamente ante la posible comisión de los Delitos de la Ley N°20.393, incluyendo, de corresponder, la revisión de las actividades de control vulneradas, a fin de fortalecerlas o reemplazarlas por nuevas actividades de control.

Las actividades de respuesta incluyen lo siguiente:

> Procedimiento de denuncia.

En caso de que algún Colaborador de Compass Chile posea sospechas fundadas de la ocurrencia de un Delito de los referidos el presente Modelo de Prevención, deberá comunicar tal hecho al Encargado de Prevención tan pronto haya observado o tomado conocimiento del hecho sospechoso a través del canal de denuncias dispuesto para ello.

El Colaborador podrá presentar su denuncia ante quien ejerza como Head Regional de Legal y Cumplimiento en caso de que el Encargado de Prevención respectivo sea objeto de la denuncia o el Colaborador no esté satisfecho con el proceso o resultado de la investigación que el Encargado de Prevención haya realizado.

En dicho sentido, el canal de denuncias corresponde a la vía por la cual el Colaborador puede enviar sus denuncias de manera anónima sobre situaciones de incumplimiento, ya sea, de las políticas regionales, políticas internas de Compass Chile o de la posible comisión de los delitos señalados en la Ley N°20.393.

Todos los Colaboradores tendrán fácil acceso al Encargado de Prevención y podrán realizar una denuncia mediante alguna de las siguientes vías:

- a. A través del sitio web del proveedor Lighthouse <https://www.lighthouse-services.com/StandardCustomURL/LHILandingPage.asp>
- b. Por teléfono al número gratuito 800-603-2869, previo ingreso del código de acceso para el país y/o sistema telefónico desde el que está llamando. Para mayor información siga las instrucciones que se detallan en el Anexo N°4.
- c. También se podrá hacer personalmente la Denuncia mediante entrevista con el Encargado de Prevención de manera confidencial. Si es necesario, se podrá considerar la posibilidad de sostener la entrevista en un lugar fuera de las instalaciones de la Administradora que salvaguarde la seguridad del Encargado de Prevención como del Denunciante.

El Encargado de Prevención es el responsable de las denuncias o reportes recibidos y que digan relación con los delitos estipulados en la Ley 20.393, y se asegurará que se tomen las medidas necesarias para dar un adecuado tratamiento a tales denuncias o reportes.

En el supuesto que el denunciado sea el Encargado de Prevención, asumirá la responsabilidad de investigar el Head Regional de Legal y Cumplimiento junto con el Country Head de Compass Chile.

Las denuncias serán revisadas por el Encargado de Prevención y tratadas con la debida prudencia y absoluta confidencialidad. La Política Regional de Reporte de Actividades Contrarias a la Ética o Ilegales se encuentra disponible en la Intranet de la Administradora y en el website www.cgcompass.com. En dicho sentido, el Encargado de Prevención evaluará primeramente el mérito de los antecedentes recibidos y dependiendo de ello deberá realizar en forma expedita una investigación preliminar inmediatamente después de haber recibido la Denuncia, sin perjuicio de lo que se indica a continuación.

El Encargado de Prevención podrá discutir la denuncia con la Alta Administración de la Administradora, en la medida que ello no frustre o perjudique la investigación.

El Encargado de Prevención deberá recomendar a la Alta Administración dar por terminado el proceso de la denuncia en caso de que la investigación no demuestre justificación para continuar con ella. Por el contrario, si la investigación preliminar muestra suficientes y serios indicios de una posible violación al presente Modelo de Prevención deberán reportar la situación al Directorio.

La investigación de cualquier incidente relacionado deberá ser manejada de manera reservada y en caso de constituir un potencial delito deberá ser inmediatamente y tan pronto como existan antecedentes del mismo, ponerlos en conocimiento de las autoridades policiales y/o investigativas locales pertinentes de conformidad a la ley.

El Denunciante recibirá información general acerca del progreso de la investigación y del resultado de la misma o si esta ha sido establecida o cerrada, a menos que: (a) exprese su deseo de no recibir ninguna información, (b) informársele pueda resultar perjudicial para el Denunciante o para la investigación, o (c) existan razones legales para no dar información.

Las denuncias realizadas sobre incumplimiento del Modelo de Prevención de Delitos deben contemplar los siguientes aspectos:

- a) El Denunciante debe describir en la forma más detallada posible la situación en la cual fue conocida la transacción u operación que motivó la denuncia. Incluir los fundamentos sobre los cuales están basados los indicios de esta posible operación o situación inusual o sospechosa;
- b) La comunicación debe contener la mayor cantidad posible de información del sospechoso o involucrados;

- c) El Encargado de Prevención mantendrá un archivo confidencial con toda la información recibida y a éste sólo podrán acceder aquellas personas que, por su posición, deban intervenir de alguna manera en la investigación de la denuncia y sólo respecto de la información indispensable para dicha intervención.
- d) Ante la detección de un hecho que pueda tipificarse legalmente como delito, el Encargado de Prevención deberá evaluar y presentar, en conjunto con el Head Regional de Legal y Cumplimiento, al Directorio los antecedentes que demuestren la conveniencia de presentar o no una eventual querrela ante los Tribunales de Justicia correspondientes o denuncias al Ministerio Público o la Policía de Investigaciones. El Directorio determinará si se procede o no con las mencionadas acciones .
- e) Toda denuncia se mantendrá en estricta confidencialidad y, por lo mismo, ella sólo será conocida por el Encargado de Prevención, el Head Regional de Legal y Cumplimiento, Country Head Compass Chile y por las personas que, por decisión de éstos, deban intervenir en el proceso de investigación.

Los Colaboradores de Compass Chile deberán ser conscientes de que podrían ser objeto de investigaciones internas, si es que existe algún indicio o se recibió alguna denuncia que diga relación con el incumplimiento de alguna ley o normativa interna de la empresa dentro del marco del Modelo de Prevención.

Los Colaboradores deberán prestar toda su colaboración en los procedimientos internos de investigación que se lleven a cabo dentro del marco del Modelo de Prevención.

Procedimiento de determinación de sanciones administrativas. La Administradora, con la asesoría legal que considere pertinente, determinará a su discreción las sanciones al o los Colaboradores que corresponda ante el incumplimiento del Modelo. Dichas medidas deberán considerar los siguientes aspectos:

- (a) Deben ser proporcionales a la gravedad de la falta cometida.
- (b) Deben ser consistentes con las políticas y procedimientos disciplinarios de la Administradora.
- (c) Deben ser aplicables a todas las personas involucradas.

Las sanciones que podrán ser aplicadas por la Administradora podrá ser alguna de las siguientes: (i) una amonestación y/o censura verbal o escrita; (ii) la devolución de cualquier ingreso o provecho que haya obtenido o el valor de los regalos recibidos por sobre los límites establecidos en este Modelo; (iii) la suspensión sin goce de sueldo por días, semanas o hasta por un mes, (iv) terminación del empleo; y (v) la interposición de acciones civiles o penales.

Para definir la gravedad de la infracción, el Encargado de Prevención en conjunto con el Head Regional de Legal y Cumplimiento y posteriormente el Directorio evaluarán:

- 1) El grado de ejecución de la infracción;
- 2) La reiteración de la conducta;
- 3) La gravedad del daño causado o potencial;
- 4) El perjuicio a Compass Chile, a sus clientes o al mercado;
- 5) Los antecedentes del infractor;
- 6) Las circunstancias de la comisión de la infracción;
- 7) El beneficio ilegalmente obtenido;
- 8) La existencia o no intencionalidad en la conducta del infractor;
- 9) La existencia de confabulación o acuerdo para la comisión de la infracción y la extensión de ésta;

Las políticas y procedimientos indicados en este Modelo y sus políticas complementarias son de obligatorio cumplimiento y se incorporan a las funciones y responsabilidades asignadas a cada empleado.

La Administradora deberá asegurarse que toda sanción estará sustentada en una investigación del hecho que la justifique fehacientemente.

- > Procedimiento de registro y seguimiento de denuncias y sanciones. El Encargado de Prevención debe mantener un registro de todas las denuncias, investigaciones (en curso y cerradas) y sanciones aplicadas en relación con incumplimiento del Modelo de Prevención.
- > Procedimiento de comunicación de sanciones. El Encargado de Prevención deberá, luego de adoptar sanciones por incumplimientos al Modelo de Prevención, comunicar las sanciones disciplinarias con el fin de transmitir a los Colaboradores y a los terceros involucrados, el firme compromiso de la Administradora de resguardar los principios y valores éticos declarados por ésta.
- > Procedimiento de mejora de controles. El Encargado de Prevención deberá, luego de lo anterior, evaluar los riesgos y actividades de control vulnerados en cada uno de los casos en los cuales se impuso algún tipo de sanción. Esto con el fin de:
 - ✓ Mejorar y actualizar las actividades de control que no operaron efectivamente en determinado caso o cuyo diseño no fue el adecuado y
 - ✓ Disponer nuevas actividades de control y mitigación de los riesgos que fueron vulnerados.
- > Procedimiento de denuncias a la justicia. Finalmente, y ante la detección de un hecho que pueda tipificarse como Delito de acuerdo a la Ley N°20.393, el Directorio, habiendo revisado los antecedentes del caso específico, podrá:
 - ✓ Instruir se realice la respectiva denuncia ante el Ministerio Público o la Policía de Investigaciones o querrellarse en los Tribunales Penales correspondientes o;

- ✓ Seguir investigando para formarse una convicción en cuanto a la existencia del Delito, de lo cual deberá dejarse constancia en actas.
- ✓ En caso de que se determine que no existió la comisión de un Delito, no se realizará acción alguna, debiendo archivar los antecedentes del caso en la Administradora.

Si bien la Administradora no se encuentra obligada por la Ley a denunciar, es una circunstancia atenuante de la responsabilidad penal de la persona jurídica. El Artículo 6° de la Ley N°20.393, establece: *“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 aportando antecedentes para establecer los hechos investigados.”*

7.3.3.5. Actividades de supervisión y monitoreo

Con el objeto de facilitar y verificar una aplicación efectiva del Modelo de Prevención, de las actividades de prevención, detección, respuestas definidas y de evaluar la necesidad de efectuar mejoras en el Modelo de Prevención, el Encargado de Prevención y el Auditor Interno de la Administradora deberán implementar las siguientes actividades de supervisión y monitoreo:

- > Procedimiento de monitoreo del Modelo de Prevención. El Encargado de Prevención deberá verificar la efectividad de los controles establecidos en la Matriz de Riesgos y en el presente Modelo de Prevención, y si producto de dicha verificación se identifican puntos relevantes tendientes a una posible ocurrencia de Delitos, deberá velar por el establecimiento e implementación de los planes de acción que correspondan. Lo anterior, sin perjuicio de las auditorías que puedan ser encargadas o bien planificadas en el programa anual de auditoría interna.
- > Procedimiento de actualización del Modelo de Prevención. La Administradora, a través del Encargado de Prevención, actualizará su Modelo de Prevención, la Matriz de Riesgos y sus controles mediante la realización del proceso de evaluación periódica del diseño y efectividad operativa de los mismos.

Para llevar a cabo el procedimiento señalado, el Encargado de Prevención, deberá:

- (i) conocer la normativa aplicable y sus posibles actualizaciones o complementaciones;
- (ii) manejar los cambios relevantes en la organización y/o industria en la que se encuentra inserta la Administradora y
- (iii) hacer seguimiento de las mejoras implementadas a las actividades de control.

7.3.3.6. Áreas de apoyo directo

A continuación, se detallan las principales áreas de apoyo y su responsabilidad en el Modelo:

7.3.3.6.1. Gerencia de Compliance

El Gerente de Compliance es el Encargado de Prevención, y junto al equipo que lidera apoyarán y asistirán a las áreas o unidades responsables, en la confección de planes de mejora para las deficiencias o vulnerabilidades detectadas en las diferentes actividades de monitoreo.

7.3.3.6.2. Gerencia Legal

Esta Gerencia participará en el proceso de inclusión de cláusulas que correspondan (Ley N°20.393) en los diversos contratos que celebre la Administradora con los Colaboradores u otros terceros. Adicionalmente, apoyará al Encargado de Prevención en la calificación legal de hechos que revistan las características de delitos.

7.3.3.6.3. Gerencia de Gestión de Talento

Esta Gerencia apoyará en la coordinación de las actividades de capacitación que deberán efectuarse para comunicar las políticas y procedimientos de control relacionados con el Modelo. Adicionalmente, deberá asegurar la inclusión de cláusulas de cumplimiento (Ley N°20.393) en los contratos de trabajo de los Colaboradores.

Sin perjuicio de lo anterior, la Administradora espera que, en el desempeño de sus labores, sus Colaboradores, cualquiera que sea su función, actúen en todo momento apegados al principio de la Buena Fe y honestidad, lo que exige, entre otros aspectos, mantener constantemente una actitud colaborativa hacia la organización. Para facilitar lo anterior, la Administradora ha diseñado e implementado un canal de comunicación para que sus Colaboradores puedan manifestar o comunicar los reportes de irregularidades que ellos detecten en el desempeño de sus labores.

Del mismo modo, la Administradora espera que sus Colaboradores tomen medidas responsables para prevenir un incumplimiento del Modelo, de modo de buscar orientación y plantear situaciones a tiempo con el fin de evitar que se conviertan en problemas. Para aquello, se debe considerar, y como principio general, que, frente a dudas o sospechas respecto a una posible violación de leyes, de esta política u otras que posee la empresa, todo empleado o colaborador podrá comunicar esta situación al Encargado o mediante el canal formal de denuncias.

7.3.3.7. Capacitaciones

La Administradora pondrá en conocimiento de todos sus Colaboradores , la existencia, contenido y el alcance del Modelo de Prevención y de la Ley N°20.393.

Además, y para que esta política sea integrada a las labores cotidianas de cada integrante de la Administradora , se efectuarán capacitaciones de forma periódica a los empleados a objeto de transmitir los conocimientos mínimos necesarios sobre la materia y la aplicación de sus procedimientos. La capacitación de los Colaboradores en materia de prevención deberá ser coordinada por la Gerencia de Gestión de Talentos en conjunto con cada departamento o gerencia y el Encargado de Prevención.

La capacitación deberá contemplar, como mínimo, los siguientes contenidos:

- > Definición de los Delitos;
- > Políticas de la Empresa sobre el Modelo de Prevención;
- > Exposición del contenido del Modelo de Prevención;
- > Herramientas y mecanismos utilizados para la ejecución del Modelo;
- > Ejemplos de situaciones de riesgo de comisión de estos delitos;
- > Reglamentación interna y normativa;
- > Políticas internas que complementan el presente Modelo de Prevención
- > Obligación de denunciar;
- > Consecuencias disciplinarias, así como legales (civiles, penales, administrativas) del incumplimiento de la normativa interna y externa en relación a los Delitos señalados en el presente Modelo de Prevención y en la Ley N°20.393;
- > Responsabilidad de cada empleado respecto de esta materia.
- > Posibles sanciones que podrán ser interpuestas por la Administradora y eventuales responsabilidades penales que podrán ser aplicadas por los Tribunales de Justicia.

Dicho procedimiento de difusión se hará de forma diferenciada en cada una de las áreas de la Administradora, en cuanto al contenido, profundidad y periodicidad. Esto, de acuerdo con el nivel de exposición al riesgo de comisión de los Delitos especificados en la Ley N°20.393.

Todo Colaborador de la Administradora deberá recibir capacitaciones, las cuales se realizarán de forma, en cuanto al contenido, profundidad y periodicidad. Esto, de acuerdo con el nivel de exposición al riesgo de comisión de los Delitos especificados en la Ley N°20.393.

Dicha capacitación podrá ser presencial o virtual, previa información a los Colaboradores.

7.3.3.8. Reportes

Semestralmente, el Encargado de Prevención informará al Directorio el estado de cumplimiento del Modelo de Prevención y las medidas y/o planes implementados, dando cuenta de su gestión.

El informe por reportar al Directorio abarcará al menos los siguientes tópicos:

- i. Deficiencias en la operatividad y diseño de los controles
- ii. Definición de planes de acción
- iii. Denuncias recibidas
- iv. Estado/resultado de investigaciones
- v. Proposición de sanciones
- vi. Otros temas relacionados con la operatividad del MPD y cumplimiento de la Ley N°20.393.

7.3.3.9. Certificación del Modelo de Prevención de Delitos

El Directorio, la Alta Administración y el Encargado de Prevención, serán en conjunto responsables de la adopción, implementación, administración, actualización y supervisión del Modelo de Prevención.

El Modelo de Prevención podrá ser certificado cuando la Administradora y su Directorio lo estime conveniente, de acuerdo a lo establecido en el Artículo 4º número 4 letra b de la Ley N°20.393.

El Encargado de Prevención deberá informar el grado de cumplimiento de las observaciones levantadas.

8. VIGENCIA

El presente Modelo de Prevención comenzó a regir con fecha 19 de diciembre de 2013, instancia en la cual el Directorio de la Administradora le otorgó su aprobación, y deberá ser actualizado en cuanto la Ley N°20.393 sea modificada o cuando así corresponda producto de las evaluaciones y reportes que se efectuarán de conformidad con lo antes establecido.

9. APROBACIONES Y/O ACTUALIZACIONES

| Versión | Fecha | Elaborado por | Aprobado por |
|----------------|--------------|-------------------------|---------------------|
| 001 | 19/12/2013 | Encargado de Prevención | Directorio |
| 002 | 26/04/2018 | Encargado de Prevención | Directorio |
| 003 | 26/12/2019 | Encargado de Prevención | Directorio |
| 004 | 25/07/2023 | Encargado de Prevención | Directorio |

10. ANEXOS

ANEXO 1
MATRIZ DE RIESGOS

Riesgos y Controles asociados a la Ley 21.459

| ATAQUE A LA INTEGRIDAD DE UN SISTEMA INFORMÁTICO | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Uso de Sistema TI de Compass Group para generar ataques a sistemas de terceros. • Dañar o intervenir sistemas informáticos de terceros para que Compass Group obtenga una ventaja competitiva. | <ul style="list-style-type: none"> • Norma de Uso Aceptable de Recursos (2.1.3) – Uso de Sistemas. • Art. 44 Reglamento Interno de OHS. • Capacitación dirigida a usuarios finales, administradores de plataforma y soporte. • “Darktrace Antigena”, una herramienta que trabaja con Inteligencia Artificial que monitorea el comportamiento del usuario. • PAM (Privileged Access Management). • Norma de Gestión de Infraestructura TI y Comunicaciones (2.8) – LOGS. • Norma de Adquisición, Desarrollo y Mantenimiento de Sistemas (2.4) – Control de acceso a Código Fuente. • Revisión periódica de las cuentas y derechos de accesos. • Acceso restringido en ciertas áreas. • Separación de ambientes, el equipo de TI encargado de compartir funciones funciona en turnos y es reducido en tamaño. |
| ACCESO ILÍCITO | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Uso de Sistema TI de Compass Group para acceder a sistemas de terceros u obtener datos sin autorización. • Acceso indebido a sistemas o datos de terceros para que Compass Group obtenga una ventaja competitiva. | <ul style="list-style-type: none"> • Norma de Control de Acceso. • Norma de Contraseñas. • Art. 44 Reglamento Interno de OHS. • Revisión periódica de las cuentas y derechos de accesos. |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Controles físicos de entrada en la organización (control biométrico, código de acceso, tarjeta de acceso, registro de entrada y salida). • Acceso restringido en ciertas áreas. • “Darktrace Antigena”, una herramienta que trabaja con Inteligencia Artificial que monitorea el comportamiento del usuario. • WAF (Web Application Firewall). • PAM (Privileged Access Management). |
| INTERCEPTACIÓN ILÍCITA | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Interceptar comunicaciones de terceros de forma no autorizada para que Compass Group obtenga una ventaja competitiva. • Uso de software malicioso para interceptar o captar comunicaciones privadas en beneficio de Compass Group. | <ul style="list-style-type: none"> • Norma de Uso Aceptable de Recursos (2.1.3, 2.1.8) – Uso de Sistemas – Uso de Herramientas que comprometan la seguridad. • Norma de Gestión de Infraestructura TI y Comunicaciones (2.8) – Monitoreo y Protección de Eventos (LOGS). • Art. 44 Reglamento Interno de OHS. • Procedimiento de Habilitación y Bloqueo de Puertos USB. • Norma de Gestión de Infraestructura TI y Comunicaciones (2.6) – Protección Código Malicioso. • WAF (Web Application Firewall). • PAM (Privileged Access Management). |
| ATAQUE A LA INTEGRIDAD DE LOS DATOS INFORMÁTICOS | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Uso de Sistema TI de Compass Group para generar ataques a datos de terceros. • Dañar datos de terceros para que Compass Group obtenga una ventaja competitiva. | <ul style="list-style-type: none"> • Norma de Uso Aceptable de Recursos (2.1.3) – Uso de Sistemas • Art. 44 Reglamento Interno de OHS. • Capacitación dirigida a usuarios finales, administradores de plataforma y soporte. • Pruebas de Phishing y Ransomware. |

| | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • “Darktrace Antigena”, una herramienta que trabaja con Inteligencia Artificial que monitorea el comportamiento del usuario. • PAM (Privileged Access Management). • Norma de Gestión de Infraestructura TI y Comunicaciones (2.8) – LOGS • Norma de Adquisición, Desarrollo y Mantenimiento de Sistemas (2.1.3, 2.4) – Gestión de la Adquisición y/o Desarrollo - Control de acceso a Código Fuente. • Revisión periódica de las cuentas y derechos de accesos. • Acceso restringido en ciertas áreas. • Hay separación de ambientes, pero el equipo de TI comparte funciones de producción, desarrollo y prueba. |
| FALSIFICACIÓN INFORMÁTICA | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Falsificar documentos electrónicos para que Compass Group cumpla con regulación y/o fiscalizaciones. • Falsificar documentos electrónicos para que Compass Group evite perjuicios legales, financieros o reputacionales. • Falsificar documentos electrónicos para obtener una ventaja de negocio. | <ul style="list-style-type: none"> • Norma de Adquisición, Desarrollo y Mantenimiento de Sistemas (2.1.2) – Separación y Seguridad de Ambientes. • Norma de Gestión de Infraestructura TI y Comunicaciones (2.8) – Monitoreo y Protección de Eventos (LOGS). • Documentos electrónicos que se producen internamente cuentan controles previos a su utilización. • Art. 44 Reglamento Interno de OHS. • Control del acceso a sistema de archivos. • Capacitaciones dirigidas a usuarios finales, administradores de plataforma y soporte. |

| RECEPTACIÓN DE DATOS INFORMÁTICOS | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Almacenar en sistemas o dispositivos de Compass Group datos de origen ilícito. • Transferir o comercializar en beneficio de Compass Group datos de origen ilícito. | <ul style="list-style-type: none"> • Cláusula sexta, N°5 y 6 de Contrato de Trabajo. • Cláusula Décima de Contrato de Trabajo. • Norma de uso aceptable de Recursos (2.1.2) – Uso de email corporativo. • Norma de Seguridad para Proveedores (2.6) – Uso aceptable de los recursos. • Art. 29, N°5 Registro Interno de OHS. • Art. 44 Reglamento Interno de OHS. • Capacitaciones dirigidas a usuarios finales, administradores de plataforma y soporte. • Procedimiento de Habilitación y Bloqueo de Puertos USB. • Implementación de DLP Office 365. |
| FRAUDE INFORMÁTICO | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Uso de Sistema TI de Compass Group para acceder a sistemas de terceros u obtener datos sin autorización. • Acceso indebido a sistemas o datos de terceros. | <ul style="list-style-type: none"> • Norma de Uso Aceptable de Recursos (2.1.3) – Uso de Sistemas • Art. 44 Reglamento Interno de OHS. • Capacitación dirigida a usuarios finales, administradores de plataforma y soporte. • Pruebas de Phishing y Ransomware. • “Darktrace Antigena”, una herramienta que trabaja con Inteligencia Artificial que monitorea el comportamiento del usuario. • PAM (Privileged Access Management). • Norma de Gestión de Infraestructura TI y Comunicaciones (2.8) – LOGS • Norma de Adquisición, Desarrollo y Mantenimiento de Sistemas (2.1.3, 2.4) – Gestión de la Adquisición y/o Desarrollo - Control de acceso a Código Fuente. • Revisión periódica de las cuentas y derechos de accesos. |

| | |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none"> • Acceso restringido en ciertas áreas. • Hay separación de ambientes, pero el equipo de TI comparte funciones de producción, desarrollo y prueba. |
| ABUSO DE LOS DISPOSITIVOS | |
| Riesgos | Controles |
| <ul style="list-style-type: none"> • Entregar a terceros dispositivos intervenidos para cometer delitos en beneficio de Compass Group. • Modificar programas o dispositivos con el fin de cometer delitos informáticos. | <ul style="list-style-type: none"> • Norma de Uso Aceptable de Recursos (2.1.3) – Uso de Sistemas. • Norma de Adquisición, Desarrollo y Mantenimiento de Sistemas (2.1.2) – Separación y Seguridad de Ambientes. • Procedimiento de Habilitación y Bloqueo de Puertos USB. • Art. 44 Reglamento Interno de OHS. • Control del acceso a sistema de archivos. • Capacitaciones dirigidas a usuarios finales, administradores de plataforma y soporte. |
| Los controles implementados son adecuados y efectivos para reducir los riesgos de que la organización incurra en responsabilidad penal por la comisión de estos delitos. | |

ANEXO 2

OTROS DELITOS CONTEMPLADOS POR LA LEY N°20.393

Contaminación de aguas: El delito de contaminación de aguas es aquel establecido en artículo 136 de la Ley de Pesca, esto es el 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.

Delitos asociados con la veda de productos: El procesamiento, el apozamiento, la transformación, el transporte, la comercialización y el almacenamiento de recursos hidrobiológicos vedados, y la elaboración, comercialización y el almacenamiento de productos derivados de éstos.

Pesca ilegal: El que realice actividades extractivas en áreas de manejo y explotación de recursos bentónicos, sin ser titular de los derechos.

Procesamiento y almacenamiento de productos escasos: El que procese, elabore o almacene recursos hidrobiológicos o productos derivados de ellos, respecto de los cuales no acredite su origen legal, y que correspondan a recursos en estado de colapsado o sobreexplotado.

Inobservancia del aislamiento u otra medida preventiva dispuesta por la autoridad sanitaria, en caso de epidemia o pandemia: Este delito sanciona el incumplimiento de cuarentenas o aislamiento sanitario obligatorio decretado por la autoridad sanitaria. Específicamente la responsabilidad penal para la persona jurídica aplica para el delito incorporado en el Código Penal en el Artículo 318 ter, a través de la Ley N°21.240, el cual establece que comete este delito “el que, a sabiendas y teniendo autoridad para disponer el trabajo de un subordinado, le ordene concurrir al lugar de desempeño de sus labores cuando éste sea distinto de su domicilio o residencia, y el trabajador se encuentre en cuarentena o aislamiento sanitario obligatorio decretado por la autoridad sanitaria”.

ANEXO 3 DELITO TRANSITORIO CODIV 19

Se deja constancia que sin perjuicio de los Delitos antes indicados en el numeral 4, en el marco de la emergencia sanitaria por coronavirus (COVID-19), se ha publicado la Ley N°21.227, sobre Suspensión Laboral y Acceso a Prestaciones del Seguro de Desempleo. Esta Ley dispone en su artículo 14 la creación del delito de obtención fraudulenta de complementos, prestaciones y/o beneficios, el que tendrá una vigencia transitoria, esto es mientras perdure la emergencia. Obtención fraudulenta de prestaciones de desempleo, mientras perdure dicha emergencia sanitaria producida por el Covid-19.

Este delito sanciona a los empleadores que sean personas jurídicas que obtengan de forma fraudulenta o mediante simulación o engaño complementos, prestaciones y/o beneficios por la pandemia ocasionada por el Covid-19.

Así, se establece que los empleadores que sean personas jurídicas serán responsables penalmente del delito señalado anteriormente cuando se cumplan los siguientes requisitos copulativos:

- > Que sea cometido directa e inmediatamente en su interés o para el provecho de la persona jurídica. Es decir, que el delito de obtención fraudulenta de complementos, prestaciones y/o beneficios se realice en beneficio o interés (pecuniario o de otro orden) directo e inmediato de la persona jurídica.
- > Que sea cometido por sus accionistas, controladores, responsables, ejecutivos principales, representantes o quienes realicen actividades de administración y supervisión de la persona jurídica y por personas naturales que estén bajo la dirección o supervisión directa de alguno de los sujetos mencionados anteriormente.
- > Que la comisión del delito fuere consecuencia del incumplimiento, por parte de la persona jurídica, de los deberes de dirección y supervisión.

El presente anexo dejará de ser aplicable tan pronto pierda vigencia el delito transitorio antes señalado.

ANEXO N°4
INSTRUCCIONES PARA LLAMAR A LA LINEA DE DENUNCIAS

1. Asegúrese de tener una línea con salida al exterior.
2. Ingrese el Código de acceso (ver abajo) para el país y/o el sistema telefónico desde el que está llamando. Entonces oírás un 'bong'.
3. Un mensaje de voz en inglés le pedirá el número al que está llamando.
4. Ingrese nuestro número gratuito: 800-603-2869. No es necesario marcar "1" antes del número gratuito.
5. Ahora está conectado a la línea directa.
6. Un saludo de Lighthouse se reproducirá en varios idiomas. Elija Idioma español presionando el número 2. Un intérprete se unirá a la llamada
7. El operador de Lighthouse lo entrevistará.
8. Luego se envía un informe a los destinatarios designados de su empresa.

CÓDIGOS DE ACCESO

Chile

Telmex 800-225-288

ENTEL 800-360-311

ENTEL {Spanish} 800-360-312

Telefonica 800-800-288

Telmex 171-00-311

Telmex {Spanish} 171-00-312

Easter Island 800-800-311

Easter Island {Spanish} 800-800-312