Manual de Cumplimiento y Prevención de Delitos

Versión: 2.0

Redacción	Verificación	Aprobación
Rodolfo Köck	Yénifer Barrera	Luis Quiroz
Encargado de Prevención de Delitos	Subgerente de Administración y personas	Gerente General
Firma: 		
22-10-2024	23-10-2024	24-10-2024

ESTADO DE EDICIONES

Versión	Fecha	Incorporación de Modificaciones
1.0	1/7/2024	Original
2.0	24/10/2024	Incluye modificaciones a la ley 20.393 incluidas en la ley 21.595. Se elimina el requisito de certificar el MCPD.

INDICE

1. ASPECTOS GENERALES

1.1. INTRODUCCIÓN

La Ley N°20.393[1], que entró en vigor con fecha 2 de diciembre de 2009, sobre la Responsabilidad Penal de las Personas Jurídicas estableció, por primera vez en Chile, la posibilidad de que la empresa responda criminalmente en el caso que sus colaboradores o personas naturales vinculadas a la empresa, cometan ciertos delitos en su beneficio.

Para que sea exigible la responsabilidad penal de la empresa, era necesario que la comisión del delito haya resultado del incumplimiento, por parte de ésta, de sus deberes de dirección y/o supervisión. Además, la ley establecía que la empresa sólo será responsable criminalmente si los delitos referidos fuesen cometidos directa e inmediatamente por las personas naturales antes indicadas, en el interés de la empresa o para el beneficio de ésta.

En septiembre de 2022 esta ley fue actualizada, debido a la promulgación en junio de 2022 de la Ley 21.459[2] de delitos informáticos. A partir de esta fecha la empresa responde penalmente en forma directa en caso de que sus dueños, directores, ejecutivos principales, representantes, quienes ejecuten actividades de administración y supervisión o quienes están bajo la dirección o supervisión directa de los anteriores, cometan alguno de los siguientes delitos:

1. Lavado de activos.
2. Financiamiento del terrorismo.
3. Cohecho o soborno a funcionario público, nacional o extranjero.
4. Receptación.
5. Soborno entre privados.
6. Negociación incompatible.
7. Apropiación indebida.
8. Administración desleal.
9. Delitos informáticos.

A partir de del 1 de septiembre de 2024 entró en vigor la ley 21.459[3] sobre delitos económicos y el panorama legal se modifica drásticamente. Por una parte, se incluye una gran cantidad adicional de delitos y por otra parte se modifican severamente los criterios bajo los cuales la empresa asume responsabilidad penal.

La normativa señala que se entiende que los deberes de dirección y supervisión se han cumplido cuando, en forma anterior a la comisión del delito, la empresa hubiere adoptado e implementado modelos de organización, administración y supervisión para la prevención de los delitos por parte de sus empleados y también por parte de sus empresas prestadoras de servicio. El hecho de que alguno de esos delitos se hubiese cometido sin beneficiar a la empresa ya no constituye un elemento de mitigación.

[1] Ley 20.393 del Ministerio de Hacienda, establece la responsabilidad penal de las personas jurídicas en los delitos que indica. Última Versión: 21-12-2022

[2] Ley 21.459 del Ministerio de Justicia y Derechos Humanos. Establece normas sobre delitos informáticos, deroga la ley n°19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

[3] Ley 21.595 del Ministerio de Justicia y Derechos Humanos. Establece nuevos delitos económicos y modifica la ley 20.393. Entró en vigor el 1 de septiembre de 2024.

En consecuencia, la ley entrega a la empresa algún grado de protección ante los eventuales delitos que puedan ser cometidos en el marco de su accionar, siempre que esta haya cumplido a cabalidad con sus deberes de dirección y supervisión, implementando de manera eficaz un modelo de prevención adecuado a su objeto social, giro, tamaño, complejidad, recursos y a las actividades que desarrolle.

Por lo tanto, los requisitos impuestos a las empresas por la ley 20.393 vienen a configurar un sistema de control del cumplimiento normativo o “compliance” en su nivel más elemental.

En cumplimiento de su deber de dirección y supervisión, la Gerencia General de CADETECH autorizó la implementación de un Modelo de Cumplimiento y Prevención de Delitos, (en adelante “MCPD”).

El presente Manual de Cumplimiento y Prevención de Delitos, (en adelante el “Manual”), establece la operativa y lineamientos de las diversas actividades establecidas en CADETECH para velar por los cumplimientos normativos y para la prevención de la comisión de delitos.

El MCPD está compuesto de los siguientes elementos:

1. Código de Conducta de Negocios.
2. Reglamento Interno de Orden, Higiene y Seguridad.
3. Matriz de Riesgos de Cumplimiento y Delitos.
4. Políticas y Procedimientos definidos para apoyar las iniciativas implementadas para mitigar los riesgos identificados en la Matriz de Riesgos de Delitos.
5. Cláusulas Contractuales.
6. Monitoreo y Supervisión.
7. Plan de Entrenamiento dirigido a los colaboradores de CADETECH.
8. Canal de Denuncia.

1.2. OBJETIVO

Los principales objetivos del presente documento son:

- Exponer en forma simplificada todos los elementos considerados por el MCPD de CADETECH bajo las disposiciones de la Ley.
- Instituir mecanismos para lograr el cumplimiento y para la prevención y mitigación de los riesgos de delitos a los cuales CADETECH se encuentra expuesto.
- Disponer las actividades del MCPD a cargo del Encargado de Cumplimiento y Prevención de Delitos de acuerdo con sus funciones de supervisión del Modelo y dar cumplimiento cabal a los requerimientos establecidos al amparo de la Ley 20.393 y sus modificaciones, así como la demás normativa que sea aplicable en la materia.

1.3. CAMPO DE APLICACIÓN

El presente Manual es aplicable a todos quienes prestan servicios directos e indirectos a CADETECH.

El alcance incluye a los accionistas, directores, gerentes, subgerentes, gestores de proyectos, colaboradores permanentes, personal temporal, agentes comerciales, contratistas, subcontratistas y asesores de CADETECH, así como a todos quienes desempeñen funciones

para la empresa, sin importar la calidad, forma o modalidad laboral o contractual bajo la cual presten sus servicios.

1.4. DEFINICIONES

- **Compliance:** Es un conjunto de normas y buenas prácticas que permiten identificar los riesgos operativos (dentro de cuales se incluyen los compromisos con proveedores, políticas internas e imagen institucional) y legales a los que se enfrentan las organizaciones. Su objetivo es evitar que la empresa incurra en delitos, sanciones o situaciones que puedan repercutir en el negocio o su reputación y comprometer su viabilidad. El modelo general se apoya en el marco regulatorio global que ofrece la norma ISO 37.301[4] y puede ser focalizado en las siguientes áreas: corporativo, fiscal y tributario, medioambiental, de prevención de riesgos laborales y anticorrupción.
- **Cumplimiento normativo**: ver “Compliance”.
- **Debida diligencia:** también conocido como *Due Dilligence* (del inglés) es una investigación formal o análisis exhaustivo a la que deben someterse las empresas antes de completar una asociación o acuerdo comercial. Esta auditoría permite a las partes obtener una radiografía completa del estado en el que se encuentra la empresa para identificar posibles riesgos o desajustes que pueda haber en sus cuentas.
- **Due Dilligence:** Ver “Debida Diligencia”.
- **Cohecho:** se entiende como el ofrecer, dar o consentir en dar cualquier beneficio (económico o de otra naturaleza) a un funcionario público, nacional o extranjero, para que actúe de forma contraria a los deberes de su cargo u obstaculice injustificadamente una acción.
- **Lavado de Activos:** el lavado de activos busca ocultar o disimular la naturaleza, origen, ubicación, propiedad o control de dinero y/o bienes obtenidos ilegalmente. Implica introducir en la economía activos de procedencia ilícita, dándoles apariencia de legalidad al valerse de actividades lícitas, lo que permite a delincuentes y organizaciones criminales disfrazar el origen ilegal de su producto, sin poner en peligro su fuente.

  Generalmente se identifica al narcotráfico como el principal delito base del lavado de activos, sin embargo, no es el único. También se puede originar en la venta ilegal de armas, la trata de personas, el tráfico de órganos, la malversación de fondos públicos, el uso malicioso de información privilegiada, el cohecho, la presentación de información falsa al mercado y el terrorismo, entre otros delitos descritos en el artículo 27 de La ley 19.913[5]. Todos ellos producen beneficios y ganancias mal habidas, que crean incentivos para que se intente legitimarlas.

  Es importante tener presente que, aun cuando el colaborador no conozca el origen ilícito de los bienes, incurrirá en el delito de lavado de dinero cuando debió conocerlo y por una falta de cuidado que le era exigible no lo hizo.
- **Soborno:** este delito se presenta entre privados y puede configurarse de dos formas:

[4] La ISO 37.301 del 2021, aborda los “sistemas de gestión de compliance”. Proporciona directrices para establecer, desarrollar, implementar, evaluar, mantener y mejorar un sistema de gestión de cumplimiento eficaz y receptivo dentro de las organizaciones.

[5] La ley 19.913 del Ministerio de Hacienda, crea la unidad de análisis financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos. Última Versión: 22-11-2023

- Cuando un colaborador solicita o acepta recibir un beneficio económico o de otra naturaleza, para sí o un tercero, para favorecer o por haber favorecido en el ejercicio de sus labores la contratación con un oferente por sobre otro; o bien,
- Cuando se diere, ofreciere o consintiere en dar a un colaborador un beneficio económico o de otra naturaleza, para sí o un tercero, para que favorezca o por haber favorecido la contratación con un oferente por sobre otro.

En ambas hipótesis, el "pago indebido" o "coima" busca que se favorezca la contratación de un oferente por sobre otro.

Esto también puede aplicar al momento de la contratación de un colaborador, cuando el o los responsables de la contratación solicitan o reciben dineros para favorecer la contratación de una persona en particular.

- **Negociación incompatible:** será sancionado el que directa o indirectamente se interesare, es decir, tenga un conflicto de interés, en cualquier negociación, actuación, contrato, operación o gestión que involucre la sociedad.
- **Apropiación indebida:** la apropiación indebida se configura cuando no se restituyen ciertos bienes que se recibieron en virtud de un cargo que obligaba a devolverlos en un momento determinado (bienes recibidos en depósito, comisión o administración, comodato, arrendamiento, leasing, etc.), causándole un perjuicio a la empresa.
- **Administración desleal:** este delito busca sancionar a quien, teniendo a su cargo la salvaguarda o la gestión de un patrimonio de la empresa, le causa perjuicio, ya sea ejerciendo abusivamente sus facultades, o ejecutando actos manifiestamente contrarios al interés de la empresa.

  En definitiva, lo que se castiga es la infracción a los deberes de cuidado y lealtad de una persona que se encuentra a cargo del patrimonio de la empresa.
- **Receptación:** comete este delito toda persona que, conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies hurtadas, robadas, de receptación o de apropiación indebida, las transporte, compre, venda, transforme o comercialice en cualquier forma, aun cuando ya hubiese dispuesto de ellas.
- **Delito informático de 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.
- **Delito informático de acceso ilícito:** por acceder a un sistema informático sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas de seguridad con el ánimo de apoderarse, usar o divulgar la información contenida.
- **Delito informático de interceptación ilícita:** por interceptar, interrumpir o interferir, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos.
- **Delito informático de ataque a la integridad de los datos informáticos:** Por alterar, dañar o suprimir datos informáticos, causando un daño grave a la empresa.
- **Delito informático de falsificación informática:** por introducir, alterar, dañar o suprimir datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.

- **Delito informático de receptación de datos informáticos:** por comercializar, transferir o almacenar datos informáticos, provenientes de un acceso ilícito, interceptación ilícita o falsificación.
- **Delito informático de fraude informático:** por causar perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipulando 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. También será considerado autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita anteriormente facilite los medios con que se comete el delito.
- **Delito informático de abuso de los dispositivos:** el que para la perpetración de los delitos de ataque a la integridad de un sistema informático, acceso ilícito, interceptación ilícita, ataque a la integridad de los datos informáticos o de las conductas señaladas en el artículo 7° de la Ley 20.009[6], 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.
- **Delito informático de uso de software sin licencia:** ver acceso ilícito. Por emplear un software o sistema informático sin la debida licencia o autorización o superando barreras técnicas o medidas de seguridad con el ánimo de usar el recurso.

[6] La ley 20.009 del Ministerio de Hacienda, establece un régimen de limitación de responsabilidad para titulares o usuarios de tarjetas de pago y transacciones electrónicas en caso de extravío, hurto, robo o fraude. Última versión: 17-08-2023.

2. CUMPLIMIENTO (COMPLIANCE)

El cumplimiento se ha convertido en la estrategia necesaria para prevenir riesgos corporativos y legales, y responder así a las exigencias de las normas internacionales. Aunque el concepto de cumplimiento no es reciente, su práctica se ha convertido en una tendencia debido a la rápida evolución de la legislación internacional y a la necesidad de las empresas de emprender caminos más transparentes. Hay países que vienen incorporando estrategias de cumplimiento desde la década del 70. Chile, en el 2010, fue el primer país de América Latina en incorporar estas actividades en su normativa interna.

El Cumplimiento es un conjunto de normas y buenas prácticas que impulsan la creación de estrategias, las cuales permiten identificar los riesgos operativos y legales a los que se enfrentan las organizaciones. Este conjunto de buenas prácticas permite incorporar mecanismos internos de prevención, control y protección frente a posibles riesgos.

La clave de estas estrategias es la detección temprana para evitar las estrictas sanciones que están ejerciendo los países alrededor del mundo y así no perjudicar la competitividad de la organización. Sin embargo, es importante aclarar que no solo son cumplimientos legislativos, sino también compromisos con proveedores, políticas internas, imagen institucional, entre otros aspectos. Para la implementación se distinguen los modelos genéricos y los modelos específicos de cumplimiento:

- El modelo genérico o de superestructura de cumplimiento se apoya en el marco regulatorio global que ofrece la norma ISO 37.301, la cual fija las directrices y buenas prácticas para implantar la función de cumplimiento en cualquier empresa u organización.
- Los modelos específicos de cumplimiento son los que abordan áreas jurídicas concretas, por ejemplo:
    - Cumplimiento penal, abordado principalmente por la Ley 20.393.
    - Cumplimiento corporativo, abordado por el SGI de CADETECH.
    - Cumplimiento de prevención de riesgos, abordado por el SGI de CADETECH.
    - Cumplimiento anticorrupción, abordado principalmente por el Código Penal.
    - Cumplimiento fiscal y tributario, abordado principalmente por el Código Penal.

2.1. FACTORES DE RIESGO A EVALUAR

En el marco del análisis de contexto y evaluación de riesgos que se lleva a cabo todos los años sobre la base del “Procedimiento de análisis de contexto y gestión de riesgos”, se debe incluir los factores externos e internos relevantes para los objetivos del período y que afectan a la capacidad de gestión.

Factores externos	Factores internos
• Marco legal y regulatorio. • Contexto sociocultural y medioambiental. • Tecnología. • Situación económica.	• Estructuras, políticas, procedimientos, procesos y recursos internos. • Modelo de negocio (estrategia, naturaleza, tamaño, escala de complejidad y sostenibilidad de la actividad de la organización). • Naturaleza y alcance de las relaciones de negocio. • Cultura del cumplimiento actual.

Además de lo anterior, se debe identificar las expectativas del personal clave de la compañía en relación con el sistema de cumplimiento, en particular a nivel Gerencial y de Gestores de Proyectos.

2.2. ALCANCE DEL CUMPLIMIENTO EN CADETECH

Un programa de cumplimiento no puede ser visto como una serie de meros trámites a fin de no ser sancionados en caso de cometer algún delito, pues, de ser así, no se estará logrando el verdadero objetivo, que es concientizar a todos los miembros de la organización con respecto a los límites, pautas y objetivos que tienen cada uno en el desempeño de sus funciones para así poder lograr una empresa más eficiente y competitiva con mejores estándares de calidad y compromiso.

Para gestionar el cumplimiento normativo, la GCSMA debe integrar el Sistema de Cumplimiento (SC) con el Sistema de Gestión Integrado (SGI). Además, debe mantener una coordinación y supervisión para garantizar la eficacia del cumplimiento y que las acciones estén alineadas con las necesidades del negocio.

Figura 2-1. integración SGI con el Cumplimiento.

2.3. RESPONSABILIDAD DE LA ADMINISTRACION SUPERIOR

2.3.1. Responsabilidad Civil

Las leyes en Chile establecen la normativa general con relación a la administración de sociedades y de los deberes de todo administrador y las consecuencias de su infracción. Los administradores deben responder frente a la sociedad, frente a los socios y frente a los acreedores sociales, del daño que causen por actos u omisiones contrarios a la ley o a los estatutos o por los realizados incumpliendo los deberes inherentes al desempeño del cargo.

2.3.2. Due Dilligence y lealtad

Actualmente se entiende como una exigencia derivada de los deberes mercantiles el elaborar e implantar dentro de la empresa los adecuados códigos de buen gobierno; códigos éticos o de conducta; sistemas disciplinarios; canales de denuncia, etc.

Su implantación es un requisito exigido por ley y se asocian al cumplimiento adecuado de los deberes de lealtad y diligencia.

Su inexistencia agravará la responsabilidad penal que pudiera enfrentar la empresa.

2.3.3. Delegación de funciones

No sirve para salvar la responsabilidad del administrador que el acto cuestionable lo haya llevado a cabo una persona en la que se han delegado funciones propias del cargo de administrador si esa persona no contaba con los conocimientos y medios materiales suficientes para llevar a buen puerto esas facultades delegadas.

Tampoco podrá excusar el administrador su actuar porque la decisión fuera presentada y aprobada en junta general, o en que también fue apoyada por los otros miembros del consejo. Los administradores, de hecho, también serán responsables de cuantos hechos negativos sucedan por razón de su actuación.

Lo anterior aplica a los Gerentes y Subgerentes en los aspectos relacionados con la administración general, pero también aplica a los Gestores de Proyectos en aquellos aspectos relacionados con la administración de los proyectos.

2.3.4. Responsabilidad penal

De manera sostenida en el tiempo, los delitos contenidos en el Código Penal se incrementan, año tras año, en número y extensión. A lo anterior se suman las leyes específicas que se han promulgado con el objetivo de modernizar y hacer más eficiente la lucha contra el crimen organizado y los delitos económicos.

Autor del delito será quien lleve a cabo la acción concreta descrita como delito, pero la empresa será considerada responsable si esa actuación se realizó por un representante suyo (Gerente, Subgerente, Gestor, Responsable de área, etc.) en el ejercicio de sus funciones y donde éste buscó (no es necesario que lo haya logrado) un beneficio directo o indirecto de cualquier clase para la empresa.

También si los hechos fueron provocados por trabajadores debido a la falta de supervisión, vigilancia y control de su actividad, atendidas las concretas circunstancias del caso.

2.4. CODIGO DE CONDUCTA DE NEGOCIOS

2.4.1. Conducta con el cliente y proveedores

- Priorizaremos entablar relaciones comerciales con aquellos clientes y proveedores que dispongan de principios similares a los expuestos en este Código.
- Velaremos por establecer relaciones mutuamente provechosas de largo plazo con nuestros clientes y proveedores, basados en prácticas profesionales éticas, justas y transparentes.
- Toda la información de nuestros clientes y proveedores y de los que han dejado de serlo será tratada de forma reservada y preservamos su confidencialidad y privacidad.
- Nos preocuparemos por brindar a nuestros clientes un servicio con estándares de calidad elevados y exigidos, basándose en sus requisitos y necesidades.
- Nos comprometemos a solucionar rápida y eficientemente los problemas, dudas o reclamos que los clientes nos puedan hacer por los servicios que entregamos.
- Favoreceremos el diálogo abierto, transparente y colaborativo con nuestros clientes y proveedores.

- Nuestros proveedores, de categorías equivalentes, participarán en igualdad de condiciones en las adjudicaciones, sin dar prioridad por motivos ajenos a las características del producto/servicio requerido.
- Respetaremos los compromisos adquiridos con nuestros proveedores, pagamos por sus servicios puntualmente y seguimos los procedimientos estipulados en las políticas de pago de la empresa.
- Defenderemos el principio de la competencia leal, absteniéndonos de conductas colusorias, predatorias y del abuso de una posición dominante y/o de poder.
- No aprobaremos métodos anticompetitivos y/o contrarios a la legislación de libre competencia en nuestras transacciones en el mercado, ni mucho menos toleraremos que nuestros empleados realicen tales actividades.
- No aceptaremos obsequios de valor por parte de nuestros proveedores y/o clientes.

2.4.2. Conducta con nuestros compañeros

- Actuamos con respeto, sencillez y cooperación entre trabajadores, fortaleciendo las relaciones humanas y laborales y beneficiando el desempeño de los equipos laborales.
- Rechazamos cualquier tipo de discriminación arbitraria, ya sea de raza, color, sexo, edad, estado civil, discapacidad, sindicación, religión, opinión política, nacionalidad, ascendencia nacional u origen social.
- No toleraremos el tratamiento inhumano de empleados. Algunas prácticas prohibidas son: el trabajo forzado, los castigos físicos y la violencia verbal.
- No aceptaremos conductas impropias como el abuso de poder, el favoritismo y el acoso sexual, entre otros.

2.4.3. Conducta con la empresa

- Los colaboradores no deben anticipar sus intereses personales, económicos o familiares por sobre los de la empresa. En caso de enfrentarse a un conflicto de interés el trabajador deberá informar a su jefatura o dirección de la empresa y abstenerse de participar o decidir respecto de la situación.
- Se espera que los colaboradores sean responsables en realizar sus funciones y obligaciones contractuales con transparencia, probidad y en conformidad con los principios y valores de la empresa. Practiquen la honestidad en todos los aspectos de su relación con clientes, proveedores, socios comerciales, comunidades y autoridades de gobierno.
- Los colaboradores no deben usar en beneficio propio o para el beneficio de terceros, los recursos materiales, inmateriales y/o financieros de la empresa.
- Es deber tanto de la empresa como de su personal no hacer un mal uso en beneficio propio o de terceros de la información de la empresa correspondiente a:
    - Datos personales de los trabajadores.
    - Productos que estén protegidos por la legislación vigente sobre propiedad intelectual y secreto industrial.
    - Cualquier información que no es de público conocimiento o que sería de ayuda para la competencia en perjuicio de la empresa.
- Podrá ser entregada información de la empresa y de su personal sólo cuando se autorice su difusión o sea exigida de conformidad a la ley.
- La prohibición de hacer un mal uso de la información confidencial o privilegiada de la compañía continúa aun cuando el trabajador o miembro de la empresa haya dejado de trabajar en ella.

2.5. MODELO DE PREVENCIÓN

CADETECH ha determinado voluntariamente la implementación de un Modelo de Cumplimiento y Prevención de Delitos que considera las siguientes etapas:

1. Designación de un "Encargado de Cumplimiento y Prevención de Delitos" (en adelante "ECPD").
2. Definición de medios y facultades del ECPD.
3. Establecimiento de un Modelo de Cumplimiento y Prevención de Delitos (en adelante "MCPD").
4. Supervisión, control y mejoramiento del MCPD.

El MCPD consiste en un sistema preventivo y de supervisión que, a través de diversas actividades de control sobre los procesos o actividades de negocio, busca prevenir la comisión de los delitos señalados en la Ley 20.393, y cualquier otro delito que en el futuro pueda ser incorporado mediante una modificación legal.

A continuación, una representación gráfica del MCPD:

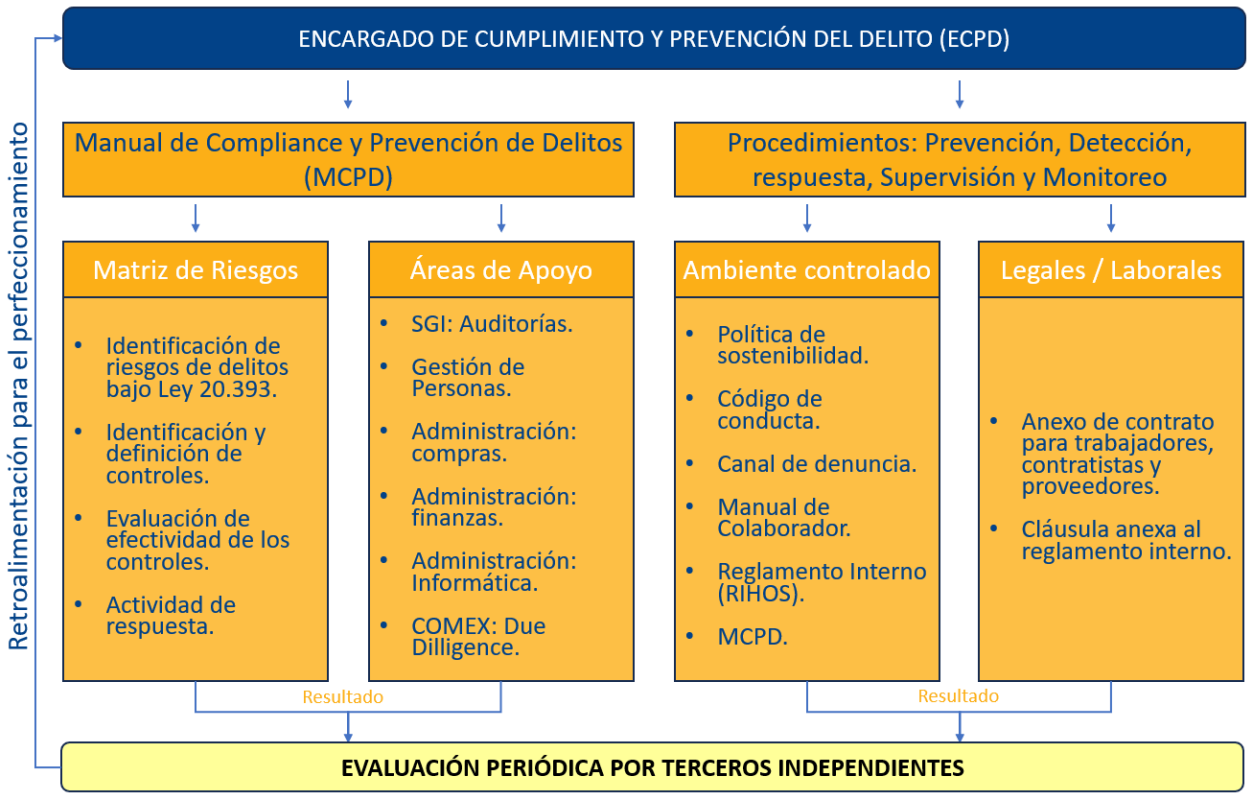

Figura 2-2. Modelo de Prevención de Delitos.

Es importante destacar que el modelo contempla evaluaciones periódicas llevadas a cabo por terceros independientes[7] y mecanismos de perfeccionamiento y/o actualización a partir de tales evaluaciones.

2.6. ENCARGADO DE CUMPLIMIENTO Y PREVENCIÓN DE DELITOS (ECPD)

En el artículo 4° de la norma se describen los elementos mínimos que debe contener un Modelo de Prevención de Delitos, siendo uno de ellos una persona facultada para asumir la responsabilidad de administrar el modelo, es decir, un Encargado de Prevención, quien es el colaborador especialmente designado por la Gerencia General para que, en conjunto con la administración de la empresa, diseñe, implemente y supervise el Modelo. Este cargo es equivalente al "Compliance Officer" identificado en otras normativas.

En CADETECH, la designación del ECPD será realizada por un período de hasta tres años y podrá renovarse por períodos de igual duración. El rol del Encargado de Cumplimiento y Prevención de Delitos recae en el Representante de la Gerencia para la Gestión de la Calidad y Seguridad.

2.6.1. Función del Encargado de Cumplimiento y Prevención de Delito

El ECPD contará con medios y facultades suficientes para la realización de sus labores:

I. Autonomía respecto de la Administración para efectos de acceder y reportar directamente a la Gerencia General y Directorio de CADETECH y a los niveles ejecutivos con el objetivo fin de informar sus hallazgos y rendir cuenta de su gestión.
II. Recurso presupuestario anual, así como personal suficiente para efectuar la implementación, operación y revisión del MCPD en concordancia con la Ley.
III. Acceso absoluto a toda la información necesaria para el adecuado desempeño de sus funciones, y a la que se pueda tener acceso conforme a la ley.
IV. Infraestructura básica y adecuada para el buen desempeño de su rol y responsabilidades, esto es, herramientas tecnológicas e infraestructura física.

2.6.2. Responsabilidades del ECPD

I. Diseñar, desarrollar e implementar el MCPD.
II. Velar por la actualización del Manual y Modelo de Cumplimiento y Prevención de Delitos, de acuerdo con los cambios normativos y el entorno de negocios de CADETECH.
III. Informar su gestión a nivel Gerencial al menos anualmente y/o cuando las circunstancias lo ameriten sobre el estado del MCPD y temas de su competencia.
IV. Proponer, desarrollar e implementar con la gerencia responsable o dueña del proceso, aquellas políticas, procedimientos y/o actividades de control necesarias para complementar el MCPD.
V. Validar el diseño y alcance de los programas de entrenamiento del Modelo de Cumplimiento y Prevención de Delitos bajo la Ley 20.393 para los colaboradores de CADETECH.
VI. Velar que la información relativa al MCPD contenido en protocolos, políticas y procedimientos sea de conocimiento en el diario actuar de los empleados y colaboradores.
VII. Solicitar a las correspondientes áreas los registros evidencias de cumplimiento y ejecución de los controles bajo su responsabilidad;

[7] Se entiende por terceros independientes no solo como "independiente a la empresa", sino también como independiente a cualquier consultora que hubiese participado en el diseño total o parcial del modelo. Tampoco podrán actuar como terceros independientes aquellos que hubiesen prestado otro servicio como revisor externo a la empresa, ya que ello les privaría de objetividad e imparcialidad al dictaminar.

VIII. Identificar brechas y determinar planes de acción para el cierre de éstas.
IX. Investigar y recopilar la información sobre las denuncias presentadas por la falta de cumplimiento del MCPD o comisión de un acto ilícito.
X. En coordinación con las personas responsables de las áreas deberá proponer las medidas que a su juicio le parezcan más oportunas, incluyendo la denuncia a la policía, fiscalía tribunal entre otras, con asistencia del área Legal.
XI. Establecer procesos de monitoreo y auditoría cuando correspondan para confirmar el cumplimiento de las actividades del MCPD.
XII. Registrar y mantener la evidencia referente a sus tareas de prevención de delitos.
XIII. Colaborar en el proceso de evaluación y perfeccionamiento del Modelo de Cumplimiento y Prevención de Delitos.

2.7. ESTABLECIMIENTO DE UN SISTEMA DE PREVENCIÓN DE DELITOS

El ECDP, en conjunto con la Administración de CADETECH, deberá disponer un Sistema de Prevención de delitos, que al menos, contemple lo siguiente:

I. Identificación de las actividades o procesos, ya sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de los delitos contemplados en la Ley.
II. Establecimiento de protocolos, reglas y procedimientos que permitan a las personas que intervengan en las actividades o procesos identificados como riesgosos, programar y ejecutar sus labores de una manera que prevengan la materialización de delitos.
III. Identificación de los procedimientos de administración y auditoría de los recursos financieros que permitan a CADETECH prevenir su utilización en delitos.
IV. Implementar sanciones administrativas internas, así como mecanismos de denuncia y/o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el Sistema de Prevención de Delitos.
V. Incorporar las obligaciones, sanciones y prohibiciones en los reglamentos y manuales internos que la compañía dicte al efecto, así como cláusulas de cumplimiento de la Ley 20.393 en los contratos de trabajo, proveedores y socios comerciales.

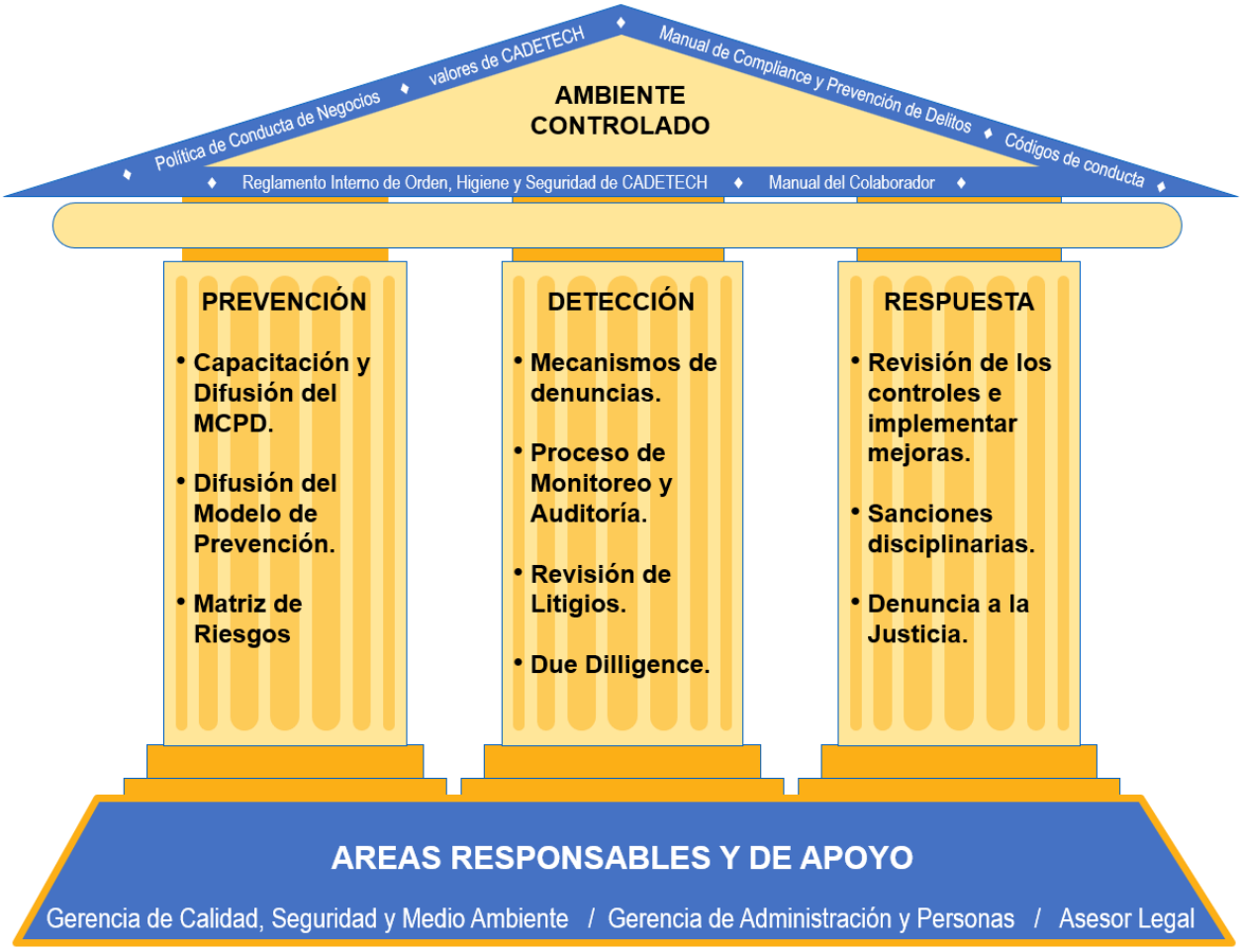

Figura 2-3. Sistema de prevención de delitos.

2.8. SUPERVISIÓN DEL MCPD

El ECPD deberá establecer métodos para la supervisión efectiva del Modelo de Cumplimiento y Prevención de Delitos, con el fin de identificar y corregir sus fallas, así como modificarlo de acuerdo con el cambio de condiciones que eventualmente CADETECH pueda enfrentar.

El ECPD, podrá requerir la realización de auditorías, sobre diversos aspectos de funcionamiento del Modelo de Cumplimiento y Prevención de Delitos, estar enterado de cualquier cambio que se produzca en el entorno interno y/o externo de la Compañía, con el fin de actualizar o modificar el modelo según requiera.

3. SISTEMA DE PREVENCIÓN DE DELITOS

El Sistema de Prevención de Delitos de CADETECH, contempla los siguientes aspectos:

3.1. AMBIENTE CONTROLADO

Es el conjunto de documentos y cultura, incluyendo los valores éticos de la organización, que conforman la base en la que se respalda el Sistema de Prevención de Delitos, puesto que facilita su estructura y funcionamiento.

En este sentido, la actuación de los Directores, Gerentes, Subgerentes, Colaboradores y Destinatarios del Manual, debe ajustarse siempre a los valores, políticas, normas y procedimientos establecidos en los siguientes documentos, pudiendo existir otros:

- Manual de Cumplimiento y Prevención de Delitos.
- Políticas y valores de CADETECH.
- Código de Conducta establecido en el Manual del Colaborador.
- Política de Conducta de Negocios.
- Reglamento Interno de Orden, Higiene y Seguridad de CADETECH.
- Matriz de identificación y control de riesgos.

Queda absolutamente prohibido a cualquier Director, Gerente, Subgerente, Colaborador o Destinatario del Manual, planear, desarrollar o practicar directa o indirectamente, individual o en forma conjunta, cualquier tipo de iniciativa o actividad, que tenga por fin obtener cualquier beneficio o ventaja personal o en favor de CADETECH que sea acreditado como un acto constitutivo de delito establecido en la Ley 20.393. Las jefaturas deberán vigilar por la continua difusión a sus colaboradores respecto de las disposiciones indicadas en este manual y su cumplimiento.

3.2. ACTIVIDADES DE PREVENCIÓN

El objetivo de las actividades de prevención es prevenir infracciones o violaciones al MCPD y evitar la comisión de los delitos. La prevención efectiva permitirá evitar conductas u omisiones impropias. Entre estas actividades encontramos:

3.2.1. Capacitación y Difusión del MCPD

El ECPD implementará programas de capacitación cuyo objeto será:

- Capacitar a los colaboradores respecto del funcionamiento del MCPD.
- Inducción de nuevos empleados y colaboradores en los contenidos y alcances del MCPD, así como la Ley 20.393.

3.2.2. Difusión del Modelo de Prevención

Con el fin de difundir los conceptos indicados en el MCPD entre todos los colaboradores, el ECPD deberá:

- Comunicar a todos los Gerentes, Subgerentes y Colaboradores sobre la puesta en vigencia del Modelo, así como las modificaciones y/o actualizaciones de este.
- Gestionar la publicación y difusión del MCPD en la web corporativa y en la intranet de la Compañía, así como mediante cualquier otro medio idóneo, según corresponda.

3.2.3. Matriz de Riesgos

La Gerencia de Calidad, Seguridad y Medio Ambiente (en adelante GCSMA) junto a las áreas de apoyo, identificará las actividades o procesos de mayor riesgo o exposición a la comisión de los delitos contenidos en la Ley 20.393, las que serán documentadas en una Matriz de Riesgos.

El propósito de la Matriz de Riesgos será evaluar los riesgos existentes en los distintos procesos, con objeto de estimar su impacto y probabilidad de ocurrencia, evaluar la eficacia de los controles existentes, y determinar los procesos que deban ser mejorados junto a eventuales remediaciones.

Una vez identificados y evaluados los controles, se procederá a estructurar en conjunto con las áreas de apoyo, la conformación, actualización o mejoramiento de políticas, protocolos y/o procedimientos específicos de manera de prevenir y/o detectar la comisión de los delitos.

3.3. ACTIVIDADES DE DETECCIÓN

Las actividades de detección permiten realizar diligencias que identifican incumplimientos al MCPD o posibles escenarios de comisión de los delitos señalados en la Ley 20.393.

Es responsabilidad de todos los colaboradores apoyar el proceso de detección, entregando toda la información relevante, y de manera oportuna, sobre irregularidades que tuvieron conocimiento o fueron presenciadas.

3.3.1. Mecanismos de denuncias

CADETECH dispone de canales de denuncia asequibles para todos sus colaboradores, clientes, proveedores y terceros que deseen efectuar denuncias sobre posibles violaciones al MCPD y la Ley 20.393, así como reportar infracciones al Código de Conducta de Negocios.

Los medios habilitados para realizar estas denuncias son:

- Comunicación verbal.
- Comunicación por escrito en papel o digital.
- Portal de denuncia en la página web de la empresa.

En cualquier caso, si el denunciante así lo desea, se podrá mantener en secreto la identidad de quién reporte el hecho.

Las investigaciones serán realizadas por la GCSMA y el ECPD tomará conocimiento de estas en la medida que sea necesaria su intervención, especialmente si se tratase de alguna de las conductas relacionadas a la Ley 20.393.

Las investigaciones cumplirán siempre con todos los requisitos legales, y siempre respetará los derechos de los involucrados. Dentro de sus principios, se encuentran la transparencia, confidencialidad, anonimato, prohibición de cualquier acto de represalia frente a quienes ejecuten denuncias de buena fe, y la objetividad en el tratamiento y análisis de los antecedentes recibidos.

3.3.2. Proceso de Monitoreo y Auditoría

El proceso de monitoreo consiste en la verificación de cumplimiento y efectividad de los controles del MCPD. Las auditorias de cumplimiento serán incluidas en los procesos de auditoría interna gestionadas por la GCSMA.

3.3.3. Revisión de Litigios

El ECPD, en conjunto con el Asesor Legal de CADETECH, revisará cada vez que ocurran, demandas, juicios, multas, infracciones y/o cualquier acción legal o actividad fiscalizadora que

involucre a CADETECH en algún escenario de delito, con objeto de detectar incumplimientos al MCPD y analizar las medidas necesarias para su tratamiento.

3.3.4. Due Dilligence

El término “due dilligence”, que en su traducción literal al español significa “diligencia debida”, es una revisión de cumplimiento efectuada sobre terceros, que se lleva a cabo para obtener una panorámica completa del estado en el que se encuentra la otra empresa. Esta operación se debe realizar cuando va a implementarse algún tipo de asociación o se desea invertir en otra empresa con el fin de analizar su situación.

Un “due dilligence” permite conocer en profundidad el estado de una empresa, su funcionamiento o modelo de negocio. Para que sean de utilidad, es imprescindible que se trabajen de manera exhaustiva y transparente, por lo que ninguna de las partes podrá ocultar o tergiversar la información.

Cuando se trata de empresas extranjeras, se deberá investigar sobre la equivalencia entre los certificados y documentos locales con los de Chile, de manera de requerir los adecuados.

A la hora de elaborar estas investigaciones, algunos de los aspectos que deben analizarse son:

Aspecto	Descripción	Documentos mínimos que requerir en Chile.
Estado financiero y contable	La auditoría debe incluir la información financiera de los últimos tres ejercicios de la empresa y su estructura de capital	• Balance Clasificado de últimos 2 períodos • Estado de resultado de últimos 2 períodos
Situación fiscal y legal	La investigación también debe reflejar cuáles son los contratos y licencias que la empresa ha firmado con terceros, su cumplimiento de la normativa y obligaciones fiscales vigentes y si existe algún litigio previo contra la empresa.	• Certificado de no deuda con la Tesorería General • Certificado de vigencia de la sociedad. • Certificado de vigencia del representante legal • Informe DICOM Empresarial
Tecnológicos	Se debe comprobar cuáles son las herramientas y dispositivos digitales que emplea la compañía y si están actualizados, revisar que se cumple con las normas de seguridad y el grado de madurez de la tecnología que utiliza la empresa.	• Evaluación seguridad de la información
Situación laboral	Se debe informar cuál es el organigrama de trabajo de la compañía, las funciones, responsabilidades e incentivos de los trabajadores. Además, se debe informar el estado de cumplimiento con los compromisos laborales asociados a salud y previsión.	• Certificado de cumplimiento de obligaciones laborales y previsionales

3.3.4.1 Ejecución del proceso

1. El proceso de “due dilligence” se inicia cuando las empresas han declarado sus intenciones de participar en un proyecto común o una oferta no vinculante.
2. CADETECH, designará a un encargado del proceso. En el caso particular de asociaciones comerciales de representación de CADETECH en el extranjero, esta función recaerá en el Director de Negocios Internacionales.
3. La primera diligencia corresponderá a un acuerdo de confidencialidad NDA por ambas partes (del inglés “Non Disclosure Agreement”). En ocasiones es posible confeccionar un único documento que incluya el MOU y el NDA.

4. El encargado del proceso solicitará los documentos necesarios a la contraparte. En el caso de empresas extranjeras deberá definir los documentos equivalentes en el país que corresponda, para lo cual podrá solicitar apoyo a Prochile. Además, reunirá los documentos equivalentes de CADETECH para ponerlos a disposición de la contraparte en caso de que esta los requiera.
5. El encargado del proceso analizará la documentación recibida y emitirá un reporte a la Gerencia donde dé cuenta de los hallazgos y de su recomendación de proseguir las negociaciones, solicitar mayores antecedentes o detener la iniciativa.

3.3.4.2 Evaluación de los antecedentes

Aspecto	Antecedentes para evaluar	Criterio de evaluación
Datos de la empresa	• Nombre comercial • Nombre legal • Tipo de empresa o sociedad • País, región o estado y dirección • N° de registro tributario • Giro • Año de fundación	• Certificado de vigencia o equivalente.
Datos del representante legal	• Nombre del representante legal • Documento de identificación • Relación con la empresa	• Certificado de personería jurídica o equivalente.
Datos del Gerente	• Nombre del Gerente • Documento de identificación	• Acta de Directorio con nombramiento y descripción de poderes.
Acuerdos	• NDA firmado • MOU firmado	• Documentos firmados por los representantes legales de ambas empresas.
Estado financiero y contable	**Contabilidad** • Balance Clasificado • Activo circulante • Inventario • Activo no circulante • Pasivo circulante • Pasivo no circulante • Patrimonio **Finanzas** • Estado de resultado • Ingresos • Margen bruto • Resultado antes de impuestos • Resultado operacional • Resultado neto • Gastos financieros	**Liquidez** • Capital de trabajo Neto ≥ 200.000 USD • Índice de solvencia > 2,0 • Test ácido > 0,8 **Endeudamiento** • Razón endeudamiento < 0,4 (40%) • Estabilidad < 0,9 • Inversión en activos NC > 0,5 • Propiedad < 0,9 • Endeudamiento < 1,0 • Cobertura financiera > 2,0 **Rentabilidad** • Margen bruto > 35% • Margen de utilidad > 5% • Retorno sobre patrimonio > 5% • Retorno sobre los activos > 5%
Contratos vigentes	Empresas • Alcance del contrato, Logros • Referencia: Contacto, teléfono, correo	• Respuesta favorable por parte de la(s) empresa(s) referida(s).

Aspecto	Antecedentes para evaluar	Criterio de evaluación
Situación fiscal y legal	• Certificado de deuda fiscal regional • Certificado de inscripción tributaria	• No existe deuda fiscal a nivel nacional o regional según corresponda. • Inscripción activa, sin observaciones.
Aspectos Tecnológicos	• Política de seguridad de la Información. • Otras certificaciones y/o auditorías. • Matriz de Riesgos de Activos de Información. • Capacitación sobre el intercambio de información. • Política de BYOD. • Sistema de autentificación o logs de acceso para los sistemas de intercambio de información. • Personal dedicado al monitoreo de la seguridad de la información. • Personal responsable ante la ocurrencia de incidentes de seguridad de la información. • Sistema de protección antimalware y virus. • Incidentes de seguridad significativos que hayan afectado sus servicios o información. • Licenciamiento para todas las herramientas de intercambio de información. • Política de Tratamiento de Información o similar. • Acuerdos formales de confidencialidad. • Procedimiento de Transferencia de información por medios extraíbles.	• Aprobación por parte del Responsable de Seguridad de la Información de CADETECH.
Situación laboral	• Certificado de no deuda previsional • Certificado de no deuda laboral	• No exista deuda laboral de ningún tipo.

El nivel de profundidad de esta investigación dependerá del tipo de relación que se desea implementar, pero al menos debe abordar el estado financiero, fiscal, tecnológico y laboral. Esta investigación es fundamental para identificar y analizar potenciales riesgos que podría registrar el tercero en un corto o largo plazo de tiempo.

3.4. ACTIVIDADES DE RESPUESTA

Las actividades de respuesta buscan establecer resoluciones, acciones correctivas, medidas disciplinarias o sanciones para quienes incumplan con el MCPD, o cuando se encuentren infracciones de los delitos señalados en la Ley 20.393.

Las actividades de respuesta se componen, pero no se limitan, a las siguientes:

3.4.1. Revisar los controles e implementar mejoras

El ECPD evaluará los riesgos y actividades de control transgredidos en cada caso sancionado, con el fin de establecer nuevas actividades de control o bien, mejoras en las actividades en donde

no opera efectivamente el control, o el diseño no es el indicado. La responsabilidad de la implementación de las acciones correctivas será del área correspondiente.

El ECPD evaluará los resultados de las auditorías internas o externas, así como de las Investigaciones con el fin de identificar cualquier observación relevante con respecto al sistema de control del MCPD.

3.4.2. Sanciones disciplinarias

La Compañía aplicará medidas disciplinarias ante el incumplimiento de las políticas y procedimientos de prevención de delitos y ante la determinación de comisión de alguno de los delitos estipulados en la Ley 20.393, considerando lo siguiente:

I. Las sanciones deberán ser consistentes con los procedimientos internos.
II. Las sanciones deberán ser aplicables a todos los individuos implicados, es decir, deben ser universales y uniformes.
III. Las sanciones deberán ser proporcionales a la falta cometida.

Estas sanciones estarán descritas en la Reglamentación Interna.

3.4.3. Denuncia a la Justicia

Ante la identificación de un hecho que pudiera caracterizarse como delito en la Ley N°20.393, el ECPD evaluará en conjunto con el Asesor Legal, la probabilidad de llevar a cabo acciones de denuncia ante la Policía o el Ministerio Público, con el fin de ejecutar las acciones legales en contra de quienes resulten responsables, con las sanciones penales y civiles que establezcan los Tribunales de Justicia en conformidad a la legislación vigente.

3.5. ÁREAS RESPONSABLES Y DE APOYO

Las áreas de apoyo son de gran importancia en el MCPD, puesto que entregan apoyo al ECPD en las diligencias de prevención, detección, respuesta, así como supervisión y monitoreo.

En función de la operación del MCPD, las actividades que realizará cada área de apoyo serán las siguientes, siendo solo una enumeración representativa y no exhaustiva.

3.5.1. Gerencia de Calidad, Seguridad y Medio Ambiente

- Realizar actividades de detección y prevención en relación con la operación efectiva del MCPD.
- Analizar y evaluar periódicamente los riesgos de comisión de los delitos de la Ley 20.393.
- Proponer controles que permitan prevenir y detectar oportunamente situaciones relacionadas a los delitos de la Ley 20.393.
- Acompañar a las unidades de negocio en la implementación de controles que permitan mitigar riesgos comisión de los delitos de la Ley 20.393.
- Recomendar en el proceso de inclusión de cláusulas de cumplimiento (Ley 20.393) en los diversos contratos que celebre con terceros.
- Informar a las Gerencias de su gestión al menos anualmente o cuando las circunstancias lo ameriten sobre el estado del MCPD y temas de su competencia.
- Recomendar en el proceso de inclusión de cláusulas de cumplimiento (Ley 20.393) en los contratos de trabajo y en el Reglamento Interno de Orden, Higiene y Seguridad de la Compañía.
- Asesorar en la toma de decisiones en relación con las sanciones y acciones correctivas a implementar producto de las investigaciones efectuadas y concluidas.
- Entrenar a los cargos con mayor exposición en materias relacionadas con los delitos nombrados en Ley 20.393.

- Facilitar la aplicación de la metodología de evaluación de riesgos para apoyar los procesos de evaluación de riesgos relacionados con los delitos contemplados en la Ley 20.393 y leyes relacionadas.
- Facilitar los talleres de riesgos con el involucramiento de APR, los responsables de las instancias de control y los responsables de las áreas.

3.5.2. Gerencia de Administración y Personas

- Asegurar la inclusión de cláusulas de cumplimiento en los contratos (Ley 20.393) que celebre CADETECH con sus trabajadores y/o terceros.
- Entregar la información que requiera el ECPD para el ejercicio de sus funciones en relación con la implementación y ejecución del MCPD.
- Apoyar la implementación de controles para las brechas identificadas producto de las investigaciones y/o auditorías realizadas en relación con el MCPD o cualquier riesgo nuevo identificado.
- Apoyar en la coordinación de las actividades de difusión del MCPD que efectúa el ECPD.

3.5.3. Asesor Legal

- Entregar la información que requiera el ECPD para el ejercicio de sus funciones en relación con la implementación y ejecución del MCPD.
- Aconsejar en el proceso de inclusión de cláusulas de cumplimiento (Ley 20.393) en los diversos contratos que celebre CADETECH con sus trabajadores y terceros.
- Aconsejar en la toma de decisiones en relación con las sanciones y acciones a seguir producto de las investigaciones efectuadas.

3.5.4. Todos los Colaboradores y Terceros

- Conocer a cabalidad el contenido del presente Modelo de Cumplimiento y Prevención de Delitos, en especial aquellas conductas que están prohibidas y podrían ser tipificadas como alguno de los delitos de la Ley.
- Denunciar inmediatamente en caso de tomar conocimiento sobre cualquier hecho o acto que podría constituir delito.
- Cumplir con lo establecido en el MCPD de CADETECH.
- Entregar la información que requiera el Encargado de Prevención de Delitos para el ejercicio de sus funciones en relación con la implementación, operatividad y efectividad del MCPD.
- Consultar con la GCSMA en caso de cualquier duda o necesidad de asesoría.

3.6. SANCIONES ADMINISTRATIVAS

Es responsabilidad de todo colaborador de CADETECH estar al tanto del contenido del Modelo y deberá regirse por sus lineamientos en todo momento. El ECPD vigilará el cumplimiento de este Manual y además pondrá en práctica estándares de verificación.

El incumplimiento a lo establecido en el presente Manual por parte de los colaboradores podrá ser considerado causa de sanciones que pueden ir desde una amonestación verbal hasta la desvinculación.

En cada carpeta personal del empleado, dicho incumplimiento formará parte de ésta. En el caso de los asesores, contratistas o proveedores, el incumplimiento de los términos de este Manual también será causal de término inmediato del contrato que se mantenga vigente.

Los empleados deberán comunicar sobre las infracciones observadas en el Modelo de Prevención de Delitos a sus supervisores o al ECPD a través del mecanismo de denuncias, establecido e informado en este Manual.

Los colaboradores de CADETECH, deberán ser conscientes de que podrían ser objeto de investigaciones internas, si es que existe algún indicio o se recibió alguna denuncia que implique el incumplimiento de alguna ley o normativa interna. Los empleados deberán prestar toda su colaboración en los procedimientos internos de investigación que sean llevados a cabo dentro del marco de MCPD. Las políticas y procedimientos indicados en este Manual, el Código de Conducta y los demás documentos en los que se respalda el MCPD son de cumplimiento mandatorio y se incorporan a las labores asignadas a cada uno. Por lo tanto, su incumplimiento comprende las sanciones previstas en el Reglamento Interno de Orden, Higiene y Seguridad, sin perjuicio de las correspondientes sanciones tanto civiles como penales.

Será exigida a los asesores, proveedores y contratistas de CADETECH la misma obligación de colaboración, constatándose aquello en los respectivos contratos o acuerdos que al respecto se puedan suscribir.

El presente Manual no reemplaza la prudencia y buen criterio que los colaboradores deben tener en cuenta en todo momento en el desarrollo de sus funciones.

Cualquier duda respecto de la interpretación y aplicación del presente Manual, o la forma en que deban ser resueltas algunas situaciones no descritas de forma específica, deberá ser sometida a conocimiento del Encargado de Cumplimiento y Prevención de Delitos.

3.7. VIGENCIA Y ACTUALIZACIÓN

Este Manual de Cumplimiento y Prevención de Delitos, tendrá vigencia inmediata desde su publicación oficial por CADETECH.

Además, el presente Manual deberá ser controlado permanentemente y revisado cada año, a partir de su entrada en vigor, por el Encargado de Cumplimiento y Prevención de Delitos, proponiendo los cambios tanto de forma como de fondo necesarios en función de las circunstancias y necesidades que enfrente la empresa o de los cambios normativos o legales.