

**MANUAL DE PREVENCIÓN DE LAVADO DE
ACTIVOS Y FINANCIAMIENTO DEL
TERRORISMO,**

**LEY 20.393 Sobre responsabilidad
penal de las personas jurídicas.**

IMPORTACIONES Y EXPORTACIONES

TECNODATA S.A.

(Con anexo y actualizado al 2022)

1. OBJETIVOS

El propósito del presente Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo (en adelante, el “Manual”) consiste en establecer las directrices, normas y procedimientos que Importaciones y Exportaciones Tecnodata S.A., sus directores y sus colaboradores, deben adoptar en relación a la prevención del lavado de activos, financiamiento del terrorismo y cohecho, concerniente al cumplimiento de las obligaciones establecidas en la Ley N° 19.913 que crea la Unidad de Análisis Financiero, y en las circulares emitidas por ese organismo regulador. Además, se ha desarrollado e implementado un programa de Prevención del Lavado de Activos, Financiamiento del Terrorismo y Cohecho, que tiene por finalidad mitigar la posibilidad que dineros provenientes de actividades ilícitas sean transformados en dineros lícitos, utilizando como vehículo a Tecnodata S.A (en adelante, la “Empresa”), dicho programa está contenido en el presente Manual, que considera políticas y procedimientos obligatorios para todas los colaboradores que se desempeñan en la organización.

2. DEFINICIONES

Para los efectos del presente Manual, se entenderá por:

2.1. Cliente o Clientes

Toda persona natural o jurídica con la que la Empresa crea, establece o mantiene una relación de origen contractual, a fin de obtener el primero la prestación de un servicio o contratación de un producto, ofrecido dentro del marco propio del giro exclusivo o complementario del segundo, conforme al marco legal y/o reglamentario, ya sea que la relación sea de carácter ocasional, esporádico, único, reiterado, frecuente o permanente, hasta 1 año atrás contado desde la fecha de revisión.

2.2. Personas Expuestas Políticamente (PEP)

Chilenos y extranjeros que desempeñen o hayan desempeñado funciones públicas destacadas en un país, hasta a lo menos un año de finalizado el ejercicio de las mismas.

2.3. Lavado de Activos

De acuerdo a lo establecido en el Artículo 27 de la Ley N° 19.913, se entiende por Lavado de Activos “cualquier acto tendiente a ocultar o disimular el origen ilícito de determinados bienes, a sabiendas que provienen de la perpetración de delitos relacionados con el tráfico ilícito de drogas, terrorismo, tráfico de armas, promoción y prostitución infantil, secuestro, cohecho, y otros”.

2.4. Financiamiento al Terrorismo

Comete este delito aquella persona, que por cualquier medio, solicite, recaude o provea fondos con la finalidad que se utilicen en la comisión de cualquier de los delitos terroristas, como por ejemplo, apoderarse o atacar 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. (Definición de acuerdo a la Ley N° 18.314).

2.5. Cohecho a Funcionario Público Nacional o Internacional

El que ofreciere, diere o consintiere en dar a un empleado público (nacional o extranjero) un beneficio económico o de otra naturaleza, en provecho de éste o de un tercero, para que realice acciones o incurra en omisiones propias de su cargo, con objeto de obtener un negocio o ventaja indebida.

2.6. Receptación

El que conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies hurtadas, robadas u objeto de abigeato o de apropiación indebida, las transporte, compre, venda, transforme o comercialice en cualquier forma

2.7. Operación Sospechosa

Todo acto, operación o transacción que, de acuerdo con los usos y costumbres de la actividad de que se trate, resulte inusual o carente de justificación económica o jurídica aparente, sea que se realice en forma aislada o reiterada.

2.8. Operación en Efectivo

Toda operación en efectivo superior a diez mil dólares de los Estados Unidos de América, o su equivalente en pesos chilenos según el valor del dólar observado el día en que se realizó la operación.

2.9. Encargado de Prevención del Delito o Encargado De Prevención Del Delito (EPD).

Funcionario que ostentará un cargo de alto nivel y tendrá como función principal la coordinación de las políticas y procedimientos de prevención de Lavado de Activos y Financiamiento del Terrorismo, como asimismo, responsabilizarse por el cumplimiento de las obligaciones contenidas en la Ley N° 19.913 que crea la Unidad de Análisis Financiero y en circulares emitidas ese organismo.

2.9.10. Señal o Señales de Alerta

Son aquellos comportamientos de Clientes, o las características de ciertas operaciones financieras, que podrían conducir a detectar una Operación Sospechosa, ayudando a

distinguir hechos, situaciones, transacciones, eventos, cuantías o indicadores financieros que la experiencia identifica como elementos de juicio a partir de los cuales se puede inferir la posible existencia de un hecho o situación que escapa a lo que la Empresa, en el giro ordinario de sus operaciones, ha determinado como normal.

3. NORMATIVA APLICABLE

El presente Manual ha sido elaborado en consideración a las instrucciones contenidas en la Circular N° 1.809 de la Superintendencia de Valores y Seguros, con sus respectivas modificaciones; a las normas contenidas en la Ley N° 19.913, a la Circular N° 049/2012 de la Unidad de Análisis Financiero, y a las demás instrucciones impartidas por ese organismo regulador (todas estas normas, en adelante, denominadas como el “Marco Normativo”).

4. ÁMBITO DE APLICACIÓN

El alcance de esta política es de carácter corporativo, es decir, incluye a los Dueños, Controladores, Directores, Ejecutivos Principales, Representantes, Alta Administración, Empleados y Terceros de la Empresa. En este sentido, la Empresa compromete a sus Colaboradores y Ejecutivos a mantener un comportamiento correcto, estricto y diligente en el cumplimiento del Modelo de Prevención de Delitos (MPD).

De acuerdo con lo anterior, es obligación de todo el personal que trabaje o preste servicios a la empresa, cualquiera sea su nivel jerárquico, el dar cumplimiento a las obligaciones, instrucciones y deberes que impone el Marco Normativo y el presente Manual. Todos los colaboradores antes descritos tendrán el deber de reportar oportunamente al Encargado de Prevención del Delito o EPD cualquier transacción sospechosa o inusual, atendida las Señales de Alerta que se puedan desprender de la misma. Sin perjuicio de las demás funciones que le correspondan, el Encargado de Prevención del Delito o EPD deberá velar por la observancia de lo establecido en el presente Manual, y será el encargado de tomar contacto con la Unidad de Análisis Financiero cuando corresponda.

5. ACTOS ILÍCITOS SANCIONADOS POR LA LEY 20.393

Previo al desarrollo del sistema de prevención de delitos, aparece claramente la necesidad de identificación y adecuado conocimiento de los supuestos de responsabilidad establecidos por la Ley N° 20.393. En virtud de lo anterior, el presente capítulo busca ilustrar y presentar en forma breve pero sistemática, los supuestos delitos que de acuerdo a lo establecido en el Artículo 1° de la Ley N° 20.393, pudieren atribuir responsabilidad penal a Tecnodata S.A., siendo por lo tanto, el objetivo principal de la presente Política y del Modelo de Prevención de Delitos, el evitar la perpetración de estos actos ilícitos.

5.1. La existencia de un hecho punible cometido por alguna de las personas que realicen actividades de administración y dirección de Tecnodata S.A. o por una persona natural que esté bajo la dirección o supervisión de alguno de estos sujetos.

En relación a lo anterior, y según lo dispuesto por el Artículo 3° de la Ley 20.393, cabe señalar que una institución o empresa es legalmente responsable de los delitos que fueren cometidos directa e inmediatamente en su interés o para su provecho, por:

- a) Sus dueños, controladores, responsables, ejecutivos principales, representantes o quienes realicen actividades de administración y supervisión;
- b) Personas naturales que estén bajo la dirección o supervisión directa de alguno de los sujetos mencionados en el inciso anterior.

5.2. Incumplimiento por parte de la persona jurídica, con su deber de dirección y supervisión, y que esto haga posible la comisión del delito.

Para efectos de la citada Ley se considerará que los deberes de dirección y supervisión se han cumplido cuando, con anterioridad a la comisión del delito, la persona jurídica hubiere adoptado e implementado modelos de organización, administración y supervisión para prevenir delitos como el cometido.

5.3. Comisión del delito en interés o para el provecho de la persona jurídica.

La Ley N° 20.393 exige que el delito sea cometido en interés o beneficio de la persona jurídica, en sentido contrario, las personas jurídicas no serán responsables en los casos en que las personas naturales, indicadas precedentemente, hubieren cometido el delito exclusivamente en ventaja propia o a favor de un tercero.

5.4. Comisión de alguno de los delitos expresamente sancionados por el Artículo 1° de la Ley 20.393.

A continuación, se detallan los tipos penales sancionados: Política de Prevención de Delitos Material de Uso Interno de Tecnodata S.A. Página 7 de 16

- a) Delitos de Lavado y Blanqueo de Activos previstos en el Artículo 27° de la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones sobre la materia.
- b) Delitos de Financiamiento del Terrorismo previstos en el Artículo 8° de la ley N° 18.314.
- c) Delitos de Cohecho de funcionario público nacional y extranjero previstos en los Artículos 250° y 251° bis del Código Penal.
- d) Delito de Receptación previsto en el Artículo 456 bis A del Código Penal.

6. SANCIONES A LA PERSONA JURÍDICA

En caso de verificarse la comisión de un delito en los términos sancionados por la Ley N° 20.393, ésta hace aplicables a las personas jurídicas una o más de las siguientes penas:

6.1.) Disolución de la persona jurídica o cancelación de la personalidad jurídica. La disolución o cancelación producirá la pérdida definitiva de la personalidad jurídica. Para Tecnodata S.A., esta sanción no sería aplicable de acuerdo a la excepción establecida en el Artículo 8º de la Ley N° 20.393, la que establece que esta pena no se aplicará a personas jurídicas de derecho privado que presten un servicio de utilidad pública cuya interrupción pudiere causar graves consecuencias sociales y económicas o daños serios a la comunidad.

6.2.) Prohibición temporal o perpetua de celebrar actos y contratos con los organismos del Estado. Esta prohibición consiste en la pérdida del derecho a participar como proveedor de bienes y servicios de los organismos del Estado.

6.3.) Pérdida parcial o total de beneficios fiscales o prohibición absoluta de recepción de los mismos por un período determinado. Se entiende, para efectos de la Ley N° 20.393, por beneficios fiscales aquellos que otorga el Estado o sus organismos por concepto de subvenciones sin prestación recíproca de bienes o servicios y en especial, subsidios para financiamiento de actividades específicas o programas especiales y gastos inherentes o asociados a la realización de éstos, sea que tales recursos se asignen a través de fondos concursables o en virtud de leyes permanentes o subsidios, subvenciones en áreas especiales o contraprestaciones establecidas en estatutos especiales y otras de similar naturaleza.

6.4.) Multa a beneficio fiscal

6.5.) Otras penas accesorias. Dichas penas están señaladas en el Artículo 13º de la Ley N° 20.393. El detalle de las penas accesorias señaladas en el punto anterior, es el siguiente:

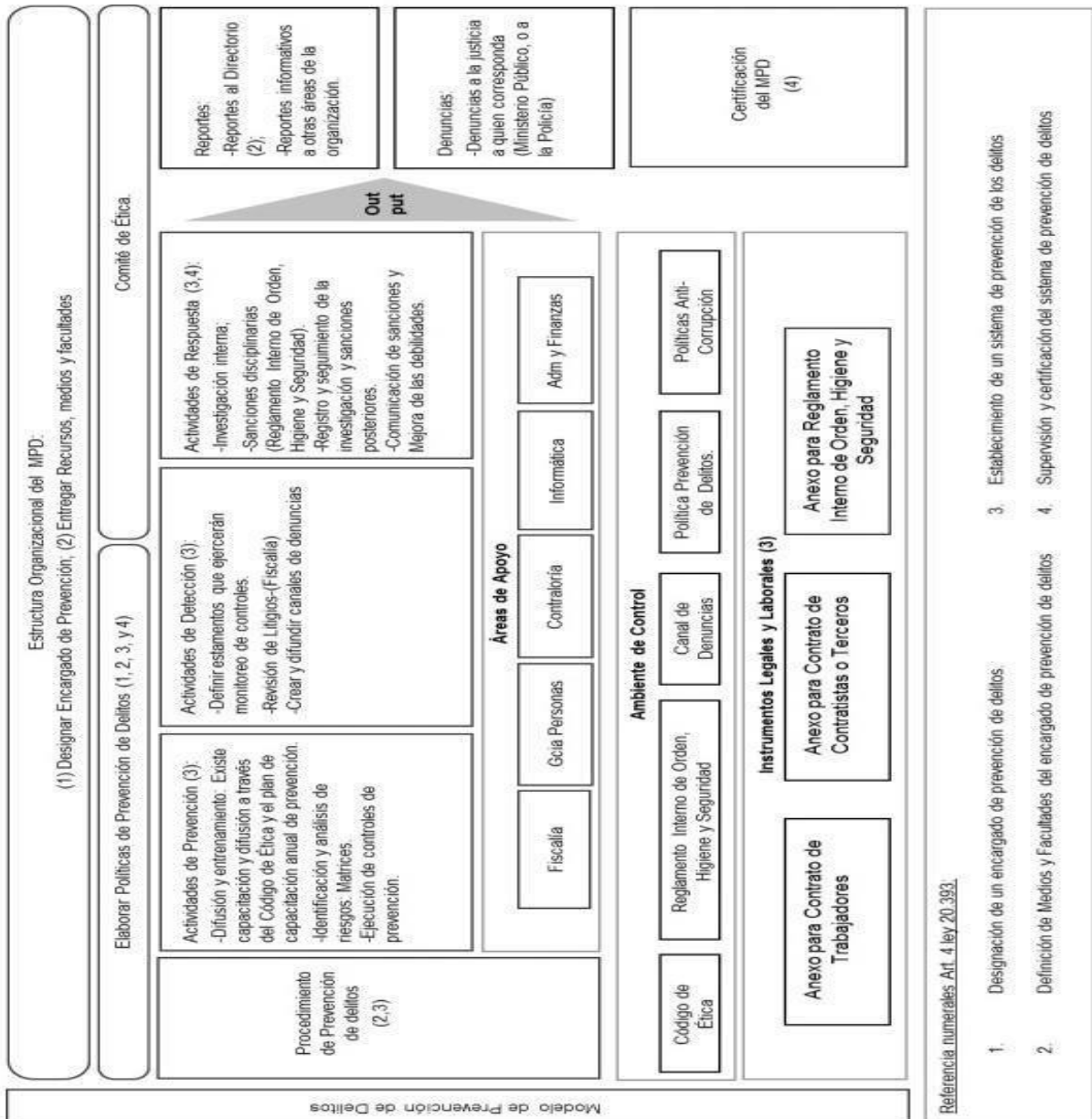
6.5.1.) Publicación de un extracto de la sentencia. El tribunal ordenará la publicación de un extracto de la parte resolutive de la sentencia condenatoria en el Diario Oficial u otro diario de circulación nacional.

6.5.2.) Comiso. El producto del delito y demás bienes, efectos, objetos, documentos e instrumentos del mismo serán decomisados.

6.5.3.) Multa accesoria con entero en arcas fiscales. En los casos que el delito cometido suponga la inversión de recursos de la persona jurídica superiores a los ingresos que ella genera, se impondrá como pena accesoria el entero en arcas fiscales de una cantidad equivalente a la inversión realizada.

7. MODELO DE PREVENCIÓN DE DELITOS

El Modelo de Prevención de Delitos, consiste en un proceso preventivo y de monitoreo, a través de la ejecución de diversas tareas de control, sobre los procesos o actividades que se encuentran expuestas a los riesgos de comisión de los delitos señalados en la Ley N°20.393 y adicionalmente a lo estipulado en el DS211. El MPD de Tecnodata S.A., está diagramado de la siguiente forma:



7.1. ESTRUCTURA ORGÁNICA DEL MODELO DE PREVENCIÓN DE DELITOS

Tecnodata S.A. cuenta con una estructura para administrar el MPD, la que incluye al Directorio como máxima autoridad administrativa de Tecnodata S.A, el Comité de Ética y el Encargado de Prevención de Delitos (EPD). Además, para su funcionamiento requiere el apoyo de las gerencias de la organización, los colaboradores y los prestadores de servicios.

7.1.1. DIRECTORIO

El Directorio es el responsable de velar por la correcta implementación y efectiva operación del MPD. Es su función designar y revocar al Encargado de Prevención de Delitos (EPD), ratificar y prorrogar dicho nombramiento cada tres años, y definir sus medios y facultades para que ejerza su cargo, en conformidad a lo establecido en el Artículo 4° de la Ley N° 20.393. Asimismo, el Directorio será responsable de:

- Proporcionar los medios y recursos necesarios para que el Encargado de Prevención de Delitos (EPD) logre cumplir con sus roles y responsabilidades.
- Aprobar la política y procedimiento de prevención de delitos, y sus correspondientes actualizaciones.
- Recibir y evaluar los informes de gestión y funcionamiento del MPD generados por el Encargado de Prevención de Delitos, al menos cada seis meses.
- Informar al Encargado de Prevención de Delitos cualquier situación observada, que tenga relación al incumplimiento de la Ley N°20.393 y las gestiones relacionadas al MPD. Por otra parte, de acuerdo a lo establecido en el Artículo N° 4, numeral 3 de la Ley N° 20.393, el Directorio, en conjunto con el Encargado de Prevención de Delitos, deberá establecer un sistema de prevención de delitos, el que deberá contemplar a lo menos los siguientes aspectos:
 - Identificación de actividades o procesos con riesgo de comisión de delitos de lavado de activos, financiamiento del terrorismo y de cohecho (Artículo 4º, N° 3, letra a).
 - Establecimiento de protocolos, reglas y procedimientos que permitan prevenir la comisión de delitos (Artículo 4º, N° 3, letra b).
 - Identificación de procedimientos de administración y auditoría a los recursos financieros, a fin de prevenir su utilización en los delitos (Artículo 4º, N° 3, letra c).
 - Establecimiento de sanciones administrativas internas y procedimientos de denuncias por incumplimiento del sistema de prevención de delitos (Artículo 4º, N° 3, letra d).

7.1.2. COMITÉ DE ÉTICA

El Comité de Ética tendrá las siguientes funciones en relación a la prevención de delitos de lavado de activos, financiamiento del terrorismo y cohecho:

- Apoyar al EPD en el proceso de análisis de denuncias que tengan relación con el cumplimiento de Ley N° 20.393.
- Definir, en conjunto con el EPD, la decisión y designación de responsables de efectuar investigaciones y otros procedimientos, según la complejidad del caso y el grado de incumplimiento al MPD.
- En conjunto con el EPD, proponer recomendaciones y sanciones, producto de informes de investigación por las denuncias recepcionadas.
- Ante la detección de un hecho que pueda tipificarse como un probable delito, el Comité de Ética deberá presentar el caso al Directorio para que éste evalúe el envío de la información al Ministerio Público.

7.1.3. COLABORADORES Y PRESTADORES DE SERVICIOS

Todos los colaboradores, asesores y contratistas, deberán cumplir con lo siguiente:

- Cumplir con lo dispuesto en esta política y con lo establecido en el MPD.
- Informar por los canales definidos los hechos que pudieren contravenir la ley y/o las instrucciones contenidas en la presente política.
- Consultar al EPD en caso de necesitar discriminar si está frente a un riesgo de comisión de alguno de los delitos estipulados en la ley. PROGRAMA DE CAPACITACIÓN Una finalidad esencial del MPD es la de fomentar el cumplimiento al más alto nivel de normas profesionales y éticas, así como de todas las leyes y regulaciones aplicables, con el objeto de prevenir la comisión de cualquier conducta que revista caracteres de ilicitud en el marco de la actividad de Tecnodata S.A.

Con objeto de tener la seguridad de que todos los colaboradores estén plenamente familiarizados con las conductas prohibidas tipificadas como delito por la legislación chilena, se contará con programas y recursos educativos y de capacitación.

En el Encargado de Prevención de Delitos recae la responsabilidad principal de implementar tal programa. La intención de éste es la de proporcionar un nivel apropiado de información e instrucción para cada colaborador.

7.1.4. GERENCIAS DE LA EMPRESA Las Gerencias de Unidades de Negocios y Operacionales, serán responsables de las siguientes funciones:

- Apoyar al EPD, asegurando su acceso irrestricto a la información y a las personas, así como también en la coordinación de las actividades propias del MPD en las áreas que se requiera informar al EPD cualquier situación observada, que tenga relación al incumplimiento de la Ley N° 20.393 y las gestiones relacionadas al MPD.
- Velar por el cumplimiento de los controles establecidos para prevenir la comisión de los delitos tipificados en la ley N° 20.393, e implementar los controles que sean necesarios para mitigar los riesgos identificados producto de las investigaciones realizadas en relación al MPD, o surgidos de cualquier riesgo nuevo identificado.
- Informar sobre la aparición de nuevos riesgos al EPD.

El Sistema de Prevención de Delitos de IMPORTACIONES Y EXPORTACIONES TECNODATA S.A., en materia de instrumentos legales y laborales contempla los siguientes aspectos:

7.2. POLÍTICAS Y PROCEDIMIENTOS DE CONOCIMIENTO DEL CLIENTE

7.2.1. Identificación de los Clientes

En el marco de la debida diligencia, es necesario tomar las siguientes medidas destinadas al conocimiento del Cliente, de las actividades generadoras de sus recursos y las características más relevantes de sus operaciones:

- a. Identificar al Cliente y verificar la identidad del mismo a través de los documentos expedidos por las autoridades de su país para dicho propósito.
- b. Identificar al beneficiario final, de manera tal que La Empresa esté convencida de quién se trata. En el caso de las personas jurídicas y otras estructuras jurídicas, se debe entender la titularidad y control que el Cliente tiene en las mismas.
- c. Entender y, cuando corresponda, obtener información sobre el propósito y el carácter que se pretende dar a la relación comercial.
- d. Realizar una debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esta relación para asegurar que las mismas sean consistentes con el conocimiento que tiene La Empresa de su Cliente,

su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos.

En base a la información recabada, se generará una ficha por cada Cliente, la cual deberá mantenerse actualizada.

En el evento que el Cliente se niegue a entregar todo o parte de la información solicitada, dicha negativa deberá ser considerada como una Señal de Alerta, a objeto de analizar la procedencia del envío de un reporte de Operación Sospechosa a la Unidad de Análisis Financiero.

7.2.2. Sistema de Evaluación de los Riesgos asociados al Lavado de Activos y Financiamiento del Terrorismo

La Empresa ha implementado una metodología de evaluación del Riesgo basados en las normativas vigentes y buenas prácticas de la industria, con el objeto de identificar, evaluar, monitorear, administrar y mitigar los riesgos de Lavado de Activos y financiamiento del terrorismo. Esta metodología permite aplicar medidas y procedimientos atendiendo al riesgo que pueda implicar la relación con el Cliente, tanto al inicio como durante la relación contractual.

Los Clientes serán clasificados como de **alto o bajo riesgo**. Los factores que se tienen en cuenta para realizar la evaluación son los siguientes:

- a. **Actividad económica:** Se considerarán todas las actividades realizadas por el Cliente, y no solo la principal, con el objeto de verificar si alguna de ellas puede ser considerada una actividad riesgosa.
- b. **Personas Expuestas Políticamente:** Toda actividad con un PEP debe ser identificada como una actividad de alto riesgo. Asimismo, los actos, operaciones o transacciones con personas que hayan desempeñado funciones públicas destacadas en un país y hayan cesado en las mismas hace más de un año, serán considerados de alto riesgo.
- c. **Vehículos de inversión:** Existen personas jurídicas o estructuras jurídicas que pueden ser vehículos de tenencia de activos personales, de tal forma que algunas de ellas pueden ser consideradas más riesgosas que otras, según cómo se manifiesta la transparencia en la propiedad de los recursos y/o si ellos se encuentran normados.
- d. **Países de mayor riesgo:** Se deben aplicar medidas de debida diligencia intensificada a las relaciones comerciales y transaccionales con personas naturales o jurídicas procedentes de países calificados como de mayor riesgo, conforme a la pauta elaborada.

e. **Factores de riesgo con respecto a productos, servicios, transacciones o canales de envío:** Algunas de estas operaciones revisten mayor riesgo, de acuerdo a una serie de factores tales como el tratarse de una transacción anónima o en la que no se estable un contacto físico con el Cliente.

Todos los Clientes que presenten un alto riesgo deberán ser informados al Encargado de Prevención del Delito o EPD, al cual deberán ser remitidos todos los antecedentes. Asimismo, estos Clientes serán objeto de medidas intensificadas de debida diligencia, las cuales se realizarán frecuentemente. Se considerarán Clientes de Alto Riesgo, por ejemplo; persona definidas como PEP, personas cuya actividad está considerada de Alto Riesgo, personas que operan principalmente con efectivo, personas que operan con países de mayor riesgo.

7.2.3. Revisión de Clientes

Como parte de la política de La Empresa, y con el objeto de hacer más efectivo la Evaluación del Riesgo, todos los nuevos Clientes deberán ser analizados a través de algún índice de riesgo o servicio proporcionado por proveedores de bases de datos fidedignas. Esta revisión será visada por la Subgerencia de Cumplimiento, cuando exista coincidencia con alguna persona identificada en alguna de las bases de datos mencionadas, durante la introducción de un nuevo Cliente y no se abrirá cuenta alguna sino hasta que la revisión haya finalizado. La información negativa obtenida a través de esta revisión, deberá ser analizada en el contexto de la evaluación de riesgo del Cliente y formará parte del historial de información del Cliente.

7.2.4. Personas Expuestas Políticamente

Son Personas Expuestas Políticamente los chilenos o extranjeros que desempeñan o hayan desempeñado funciones públicas destacadas en un país hasta a lo menos un año de finalizado el ejercicio de la misma. Asimismo, para los efectos del presente Manual, se considerará que son PEP las personas que hayan desempeñado las funciones antes mencionadas, aunque hayan cesado en las mismas con anterioridad a un año. Se incluyen en la categoría de PEP a jefes de estado o de un gobierno, políticos de alta jerarquía (entre ellos, a los miembros de mesas directivas de partidos políticos), funcionarios gubernamentales, judiciales o militares de alta jerarquía, altos ejecutivos de empresas estatales, así como sus cónyuges, sus parientes hasta el segundo grado de consanguinidad y las personas naturales con las que hayan celebrado un pacto de actuación conjunta mediante el cual tengan poder de voto suficiente para influir en sociedades constituidas en Chile.

El Marco Normativo establece que en Chile, a lo menos, deberán estar calificados como PEP quienes desempeñen los siguientes cargos:

a. Presidente de la República;

- b. Los senadores, diputados y alcaldes;
- c. Los ministros de estados, subsecretarios, intendentes, gobernadores, secretarios regionales ministeriales, y embajadores, jefes superiores de servicios tanto centralizados como descentralizados y el directivo superior inmediato que debe subrogar a cada uno de ellos; d. Ministros de la Corte Suprema y Cortes de Apelaciones;
- e. Los Comandantes en Jefe de las Fuerzas Armadas, el Director General de Carabineros, y el Director General de Investigaciones, y el superior inmediato que deba subrogar a cada uno de ellos;
- f. Fiscal Nacional del Ministerio Público y los Fiscales Regionales;
- g. Los directores y ejecutivos principales de empresas estatales, según lo definido en la Ley N° 18.045 sobre Mercado de Valores;
- h. Directores de sociedades anónimas nombradas por el Estado o sus organismos;
- i. Miembros de las directivas de los partidos políticos;
- j. Contralor General de la República;
- k. Consejeros del Banco Central;
- l. Consejeros del Consejo de Defensa del Estado;
- m. Ministros del Tribunal Constitucional;
- n. Ministros del Tribunal de la Libre Competencia;
- o. Integrantes titulares y suplentes del Tribunal de Contratación Pública; y,
- p. Consejeros del Consejo de Alta Dirección Pública. Para establecer relaciones comerciales con un PEP (incluyendo en dicho concepto a los familiares y socios cercanos a los mismos), o con un Cliente que adquiera dicha calidad con posterioridad, se deberá obtener y exigir:
 - a. la aprobación de la Subgerencia de Cumplimiento;
 - b. tomar medidas para establecer la fuente de riqueza y la fuente de los fondos; y
 - c. llevar a cabo un monitoreo continuo intensificado de la relación comercial.

Las Personas Políticamente Expuestas serán clasificadas como Clientes de alto riesgo. Asimismo, cualquier operación en que esté involucrada alguna persona que deba ser calificada como PEP,

deberá ser registrada e informada por el Encargado de Prevención del Delito a la Unidad de Análisis Financiero a la brevedad posible, cuando se considere que se está en presencia de una Operación Sospechosa

7.2.5. Identificación de sujetos incorporados al Listado del Consejo de Seguridad de las Naciones Unidas

El Encargado de Prevención del Delito deberá revisar y chequear, permanentemente, las listas confeccionadas por el Comité establecido en las resoluciones números 1.267, de 1999; 1.333, de 2000; 1.390, de 2002, y 1.988, de 2011 del Consejo de Seguridad de las Naciones Unidas y sus subsecuentes resoluciones o cualquiera otra que las adicione o reemplace.

En el caso que se registren actos, transacciones u operaciones realizadas o que intente realizar alguna de las personas naturales o jurídicas individualizadas en las listas antes mencionadas, deberán ser informados a la Unidad de Análisis Financiero a través de los procedimientos que la misma determine.

7.2.6. Identificación de sujetos que pertenezcan a países no cooperantes o paraísos fiscales

El Encargado de Prevención del Delito deberá efectuar revisiones periódicas de las transacciones realizadas con países, territorios o jurisdicciones que, de acuerdo al Grupo de Acción Financiera Internacional (GAFI) y a la Organización de Cooperación y Desarrollo Económico (OCDE), se encuentren calificados como no cooperantes o paraísos fiscales. La información obtenida, derivada del proceso de revisión de los datos, deberá ser analizada a objeto de determinar si procede informar de la operación a la Unidad de Análisis Financiero. Con todo, La Empresa no tendrá relaciones comerciales con Clientes que tengan jurisdicción o domicilio en un país no cooperante o de paraísos fiscales.

7.2.7. Revisión de otros listados

El Encargado de Prevención del Delito revisará las listas de la OFAC (Office of Foreign Assets Control), del Departamento del Tesoro de los Estados Unidos de América, respecto de todos los Clientes y beneficiarios finales.

7.2.8. Países de Alto Riesgo

Algunos países están asociados a delitos de tráfico de drogas, fraude, corrupción, etc., por lo que representan un alto riesgo para La Empresa. Por lo anterior, se hace necesario emplear una debida diligencia acentuada respecto de entidades o personas que tengan su

sede en estos países, así como tomar precauciones respecto de la documentación presentada y/o emitida en los mismos.

7.2.9. De los Bancos Pantalla (Shell Banks)

Un Banco Pantalla es aquel que no tiene una presencia física en el país en el que es constituido y recibe licencia, y que no está afiliado a un grupo financiero regulado que esté sujeto a una supervisión consolidada eficaz. Se entiende por “presencia física” cuando dentro de un país está ubicada la cabeza y la gestión principal. La existencia simplemente de un agente local o personal de bajo nivel no constituye una presencia física.

La Empresa no entrará en, ni continuará, una relación de banca corresponsal con bancos pantalla. Asimismo, La Empresa no entablará relaciones con estos bancos ni con instituciones que permitan que sus cuentas sean utilizadas por ellos.

8. PROCEDIMIENTOS INTERNOS DE CONTROL

8.1 Ambiente de control

El Ambiente de Control es el conjunto de documentos y valores éticos que rigen la organización, y que forman la base en la que se sustenta el Sistema de Prevención de Delitos, ya que proporciona los lineamientos fundamentales respecto de su estructura y funcionamiento. En este sentido, la actuación de los Directores, Ejecutivos y Colaboradores, debe efectuarse de conformidad con los principios, políticas, normas y procedimientos establecidos en los siguientes documentos:

- a) Política de Prevención de Delitos de Tecnodata S.A.
- b) Reglamento Interno de Orden, Higiene y Seguridad de Tecnodata S.A.
- c) Código de Ética y Conducta Empresarial de Tecnodata S.A.
- d) Las Disposiciones del Modelo de Prevención de Delitos.

Queda estrictamente prohibido a cualquier Director, Ejecutivo o Colaborador, planificar, desarrollar o ejercer directa o indirectamente, individual o concertadamente, cualquier tipo de iniciativa o acto, que tenga por finalidad obtener cualquier tipo de beneficio o ventaja en favor de la Empresa que sea acreditado como un acto delictivo establecido en la Ley N° 20.393. Las jefaturas deberán velar por la permanente difusión a sus colaboradores respecto de las presentes disposiciones y la exigencia de su cumplimiento íntegro y estricto.

8.2. Áreas de Apoyo

El objetivo de las áreas de apoyo es entregar soporte al Encargado de Prevención de Delitos (EPD), en temas específicos, que componen las actividades de prevención, detección, respuesta, supervisión y monitoreo del Sistema de Prevención de Delitos.

Esto se puede materializar mediante la asesoría en la toma de decisiones, coordinación de actividades relacionadas al Modelo y la entrega de información, entre otros. Entre las principales áreas de apoyo al Modelo se encuentran: Fiscalía, Auditoría Interna, Riesgos y Recursos Humanos.

8.3. Actividades de Prevención

La prevención eficaz ayuda a evitar conductas u omisiones impropias desde su origen o inicio. El objetivo de las actividades de prevención es evitar incumplimientos o violaciones al MPD y prevenir la comisión de los delitos señalados en la Ley N° 20.393. Entre ellas encontramos:

a) Matriz de Riesgos: el área de Cumplimiento, en conjunto con las áreas de apoyo, identificará las actividades de riesgo de comisión de los delitos contenidos en la Ley N° 20.393, las que serán documentadas en una Matriz de Riesgos de Delitos.

El objetivo de la Matriz de Riesgos de Delitos, será evaluar los riesgos existentes en los distintos procesos de la Empresa, 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. 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.

b) Capacitación del Personal: el EPD implementará programas de capacitación anuales que tengan por objeto:

- Capacitar a los colaboradores respecto del funcionamiento del MPD de la Empresa.
- Inducción de nuevos empleados en los alcances y contenidos del MPD y la Ley N° 20.393.
- Difusión de información actualizada del MPD hacia todos los colaboradores.

c) Difusión del Modelo: con la finalidad de difundir cada uno de los conceptos contenidos en el MPD de la Empresa entre todo el personal y terceras partes interesadas, el EPD deberá:

- Comunicar a todos los Directores, Ejecutivos y Colaboradores de la Empresa sobre la puesta en vigencia del Modelo, así como las modificaciones y/o actualizaciones del mismo.
- Gestionar la publicación y difusión del MPD en la web corporativa y en la intranet de la Empresa, así como mediante cualquier otro medio idóneo.

8.4. Actividades de Detección

El objetivo de estas actividades es efectuar acciones que detecten incumplimientos al MPD o posibles escenarios de comisión de los delitos señalados en la Ley N° 20.393. Con este fin, se establecen las siguientes actividades:

a) Mecanismos de Denuncias: la Empresa asegurará la existencia de canales de denuncia disponibles para todos sus colaboradores, clientes, proveedores y terceras personas interesadas que deseen efectuar denuncias sobre posibles violaciones al MPD y la Ley N° 20.393, o reportar infracciones al Código de Ética y Conducta Empresarial. Los medios habilitados para realizar estas denuncias son:

- Canal de Denuncias, al cual se accede a través de la intranet y web corporativa de la Empresa.
- Denuncia directa, por escrito o vía mail, al EPD de la Empresa. El EPD deberá garantizar una adecuada investigación de las denuncias recibidas, así como la confidencialidad, transparencia, facilidad de acceso, anonimato e inexistencia de represalias en contra de quienes realicen denuncias de buena fe, y la objetividad en el tratamiento y análisis de los casos recepcionados.

b) Auditorías al Modelo: el EPD en conjunto con Auditoría Interna deberá estructurar anualmente un plan de monitoreo que tenga por objeto verificar que los controles establecidos por el Modelo operan conforme su diseño. El objetivo de las auditorías será acreditar la operación del MPD e identificar deficiencias que pudieran afectar su funcionamiento.

c) Revisión de Litigios: el EPD en conjunto con Fiscalía Interna deberá revisar y analizar, cada vez que ocurra, demandas, juicios, multas, infracciones y cualquier acción legal o actividad fiscalizadora que involucre a Tecnodata S.A. en algún escenario de delito relacionado a la Ley N° 20.393, con objeto de detectar incumplimientos al MPD y evaluar las medidas necesarias para su tratamiento.

8.5. Actividades de Respuesta

El objetivo de estas actividades es establecer resoluciones, medidas disciplinarias y/o sanciones a quienes incumplan el MPD de la Empresa o ante la detección de infracciones a los delitos señalados en la Ley N° 20.393.

a) Sanciones Disciplinarias: Las infracciones a las normas que constituyen el MPD serán consideradas como una falta grave a las obligaciones que impone el Reglamento Interno de Orden, Higiene y Seguridad; el Código de Ética y Conducta Empresarial y el Contrato de Trabajo. La Empresa podrá aplicar 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 N° 20.393, tomando en consideración lo siguiente:

- Las sanciones deben ser proporcionales a la falta cometida.
- Las sanciones deben ser consistentes con los procedimientos internos de la Empresa.
- Las sanciones deben ser aplicables a todas las personas involucradas. La sanción a ser aplicada deberá ser determinada por el Encargado de Prevención de Delitos en conjunto con el Comité de Ética y Cumplimiento.

b) Denuncias a la Justicia: Ante la detección de un hecho que pueda tipificarse como delito de la Ley N° 20.393, el EPD deberá evaluar, en conjunto con el Comité de Ética y Cumplimiento, la posibilidad de efectuar acciones de denuncia ante el Ministerio Público o la Policía, para realizar la persecución legal de quienes resulten responsables, aplicando las sanciones civiles y penales que determinen los Tribunales de Justicia conforme a la legislación vigente.

c) Mejoras de Actividades de Control: El EPD deberá evaluar los riesgos y actividades de control vulnerados en cada uno de los casos sancionados, para determinar la necesidad de establecer nuevas actividades de control o mejoras en las actividades que no operan efectivamente o cuyo diseño no es el adecuado. El EPD será responsable de asesorar a las áreas involucradas en la definición e implementación de las medidas correctivas adoptadas. La responsabilidad de la implementación de las acciones correctivas será del área correspondiente.

8.6. Instrumentos Legales y Laborales

a) Capítulo Reglamento Interno de Orden, Higiene y Seguridad: el MPD contempla modificaciones en la normativa interna de la Empresa, debiéndose incorporar

expresamente las obligaciones, prohibiciones y sanciones internas del Modelo en el Reglamento Interno de la Empresa.

b) Contratos de Trabajo: los contratos de trabajo de todos los empleados de la Empresa deberán contener cláusulas que exijan el cumplimiento del Modelo de Prevención de Delitos y de las disposiciones legales, regulatorias e internas referidas a la Ley N° 20.393; y comuniquen los alcances y obligaciones internas derivadas de su cumplimiento.

c) Contratos de Prestación de Servicios: el MPD contempla modificaciones en la normativa interna de la Empresa así como en los vínculos jurídicos y contractuales con terceros, debiéndose incorporar expresamente cláusulas en los contratos con proveedores, que definan las obligaciones, prohibiciones y sanciones derivadas del MPD de la Empresa.

8.7. Reporte a Directorio

El EPD deberá reportar a Directorio, al menos semestralmente, respecto de las medidas y planes implementados en el cumplimiento de su cometido, así como para rendir cuenta de su gestión. El Directorio podrá delegar la función de dicho reporte en el Comité de Ética y Cumplimiento, no obstante, el EPD siempre tendrá acceso directo para reportar sus labores al Directorio, cada vez que él o el Directorio lo estimen pertinente.

Así, conforme lo establecido por la Ley N° 20.393 que establece responsabilidad penal para personas jurídicas, la Empresa ha definido voluntariamente la adopción de un Modelo de Prevención de Delitos que considera los siguientes elementos:

8.8. Designación de un Encargado de Prevención de Delitos (EPD)

El Directorio de la Empresa deberá designar un responsable denominado “Encargado de Prevención de Delitos” (EPD), el que tendrá como principal función implementar un modelo de organización, administración y supervisión para prevenir los delitos contenidos en la Ley N° 20.393, y que durará en su cargo hasta tres años, pudiendo prorrogarse su designación por períodos de igual duración.

Para cumplir su cometido, el Encargado de Prevención deberá contar con autonomía respecto de la Administración de la Empresa, de sus dueños, de sus socios, de sus accionistas y/o de sus controladores.

8.9. Del Encargado de Prevención del Delito o (EPD)

El Encargado de Prevención del Delito será el funcionario responsable de la coordinación de las políticas y procedimientos de Prevención de Lavado de Activos y Financiamiento del Terrorismo al interior de La Empresa, y de gestionar el cumplimiento a las obligaciones contenidas en el citado Marco Normativo. El Encargado de Prevención del Delito ostentará

un cargo de alta responsabilidad en la empresa, tales como gerente de área o división, la cual lo proveerá de los recursos humanos y tecnológicos necesarios para cumplir con su misión. El Encargado de Prevención del Delito será independiente de las áreas de negocios, auditoría y riesgo de La Empresa.

8.9.1. Nombramiento y duración

En cumplimiento a lo establecido en el Artículo N° 4, numeral 1 de la Ley N° 20.393, Tecnodata S.A. contará con un Encargado de Prevención de Delitos nombrado por el Directorio, quien durará en su cargo hasta tres años, pudiendo prorrogarse su designación por períodos de igual duración.

8.9.2. Deberes y responsabilidades

El EPD será responsable de mantener y llevar a cabo el programa institucional tendiente a evitar la comisión de actos ilícitos que puedan afectar la responsabilidad de Tecnodata S.A. en los términos dispuestos en la Ley N° 20.393. Los deberes y responsabilidades del EPD incluirán:

- a. Reportar a la Unidad de Análisis Financiero cualquier Operación Sospechosa de la que tenga conocimiento, acompañando los antecedentes que sean necesarios para su acertada revisión.
- b. Informar a la Unidad de Análisis Financiero de toda Operación en Efectivo que supere los diez mil dólares de los Estados Unidos de América, o su equivalente en pesos chilenos según el valor del dólar observado el día en que se realizó la operación, a través del Reporte de Operaciones en Efectivo, establecido por la Unidad de Análisis Financiero.
- c. Informar y proporcionar a la Unidad de Análisis Financiero toda la información, antecedentes y documentos que ésta requiera para la revisión de una Operación Sospechosa.
- d. Informar a la Unidad de Análisis Financiero de todos los actos, transacciones u operaciones realizadas o que intente realizar alguna persona natural o jurídica que haya cometido, cometa o intente cometer actos de terrorismo o participar en ellos o facilitar su comisión.
- e. Velar porque La Empresa cumpla con sus obligaciones de capacitar a su personal periódicamente, dejando constancia de las capacitaciones efectuadas.
- f. Relacionarse con la Unidad de Análisis Financiero y cumplir las instrucciones que se impartan cuando exista una medida decretada por el Ministro de la Corte de Apelaciones de Santiago respectivo, tendiente a

evitar el uso, aprovechamiento, beneficio o destino de bienes, valores o dinero materia del acto, transacción u operación.

g. Realizar la supervigilancia del MPD sancionados por la ley N° 20.393 adoptado por Tecnodata S.A., y velar por su aplicación efectiva y el establecimiento de métodos para tal fin;

h. Dirigir y supervisar la identificación de las actividades o procesos en cuyo contexto se genere o incremente el riesgo de comisión de delitos sancionados por la ley N° 20.393;

i. Supervisar la aplicación de sanciones administrativas internas, y la existencia de procedimientos de denuncia y persecución de responsabilidades en contra de las personas que incumplan el sistema de prevención de delitos;

j. Coordinar la revisión y actualización del MPD, de acuerdo al cambio de circunstancias en Tecnodata S.A.;

k. Dirigir el establecimiento de protocolos, reglas y procedimientos específicos de prevención de delitos;

l. Prestar funciones de asistencia y asesoría a las diferentes áreas de Tecnodata S.A. dentro del marco legal establecido;

m. Resolver consultas de los colaboradores relacionadas con cualquier aspecto relativo a la prevención de delitos;

n. Capacitar al colaborador de Tecnodata S.A. en materias bajo el alcance de la Ley 20.393;

o. Rendir cuenta de su gestión al Directorio al menos semestralmente, sin perjuicio de hacerlo cada vez que alguna situación particular lo amerite.

p. Las demás obligaciones establecidas en la legislación vigente, instrucciones de los órganos administrativos y en el presente Manual

La Ley N° 19.913, establece que la información proporcionada de buena fe por el Encargado de Prevención del Delito, en conformidad a la ley, lo exime de toda responsabilidad legal y, como se señalará más adelante, se encuentra prohibido a los funcionarios y/o personas que presten servicios a La Empresa, informar al afectado, o a terceras personas, acerca de haberse requerido o remitido esta información.

8.9.3. Medios y facultades del Encargado de Prevención de Delitos

El EPD contará con la adecuada autonomía que el ejercicio de su función requiere, ya sea respecto del propio Directorio, como de la Administración de Tecnodata S.A. y, actuará de manera independiente en relación a las demás gerencias, reportando directamente al Directorio, de acuerdo a lo establecido en el Artículo 4º de la Ley N° 20.393. De acuerdo a lo establecido en el Artículo N° 4, numeral 2 de la Ley N° 20.393, Tecnodata S.A, a través del Directorio, proveerá al EPD los recursos y medios materiales necesarios para el desempeño de sus funciones. Asimismo, el EPD contará con amplias facultades de acceso a la información y documentación de Tecnodata S.A, tanto física como aquella almacenada en medios electrónicos, relacionada con su ámbito de acción, El Encargado de Prevención de Delitos tendrá derecho a concurrir a las sesiones del Directorio con derecho a voz, pero sin derecho a voto, y deberá hacerlo siempre que sea necesario para mantener informado a éste de las medidas y planes implementados en el cumplimiento de su cometido, para rendir cuenta o informar de su gestión.

8.9.4. Definición de Medios y Facultades del EPD

La Administración de la Empresa deberá proveer al Encargado de Prevención de Delitos, los medios y facultades suficientes para el desempeño de sus funciones, entre los que se consideran:

- Los recursos y medios materiales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la Empresa.
- Acceso directo a la Alta Administración para informarla oportunamente de las medidas y planes implementados en el cumplimiento de su cometido y para rendir cuentas de su gestión.
- Acceso y apoyo del Comité de Ética y Cumplimiento, para las diferentes actividades derivadas de la implementación y funcionamiento del Modelo de Prevención de Delitos.

8.9.5. Establecimiento de un Sistema de Prevención de Delitos

El Encargado de Prevención, en conjunto con la Administración de la Empresa, deberá establecer un Sistema de Prevención de los delitos sancionados por la Ley N° 20.393, que deberá contemplar a lo menos lo siguiente:

- Identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de los delitos contemplados en la Ley.

- El establecimiento de protocolos, reglas y procedimientos específicos 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 los delitos de la Ley N° 20.393.
- La identificación de los procedimientos de administración y auditoría de los recursos financieros que permitan a la Empresa prevenir su utilización en los delitos de la Ley N° 20.393.
- La existencia de sanciones administrativas internas, así como de mecanismos de denuncia y/o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el Sistema de Prevención de Delitos.

8.9.6. Supervisión y Certificación

- El EPD deberá establecer métodos para la aplicación efectiva del Modelo de Prevención de Delitos, y su supervisión, a fin de detectar y corregir sus fallas, así como actualizarlo de acuerdo al cambio de circunstancias que enfrente la Empresa.
- La Empresa podrá realizar la Certificación del MPD con el fin de corroborar su adecuado diseño e implementación. El proceso de certificación permitirá a la Administración de la Empresa objetivar la fortaleza del MPD y su habilidad para prevenir la ocurrencia de los delitos contenidos en la Ley N° 20.393. Para este efecto, la certificación deberá ser llevada a cabo por una entidad registrada y autorizada por la Superintendencia de Valores y Seguros para cumplir con esta labor.

8.9.7. PROGRAMA DE CAPACITACIÓN

Una finalidad esencial del MPD es la de fomentar el cumplimiento al más alto nivel de normas profesionales y éticas, así como de todas las leyes y regulaciones aplicables, con el objeto de prevenir la comisión de cualquier conducta que revista caracteres de ilicitud en el marco de la actividad de Tecnodata S.A.. Con objeto de tener la seguridad de que todos los colaboradores estén plenamente familiarizados con las conductas prohibidas tipificadas como delito por la legislación chilena, se contará con programas y recursos educativos y de capacitación.

En el Encargado de Prevención de Delitos recae la responsabilidad principal de implementar tal programa. La intención de éste es la de proporcionar un nivel apropiado de información e instrucción para cada colaborador en lo que se refiere a conductas prohibidas y a normativa en materia criminal. También contemplará, si fuere procedente, el informar de estas materias a proveedores o personal externo.

El Encargado de Prevención de Delitos usará los siguientes métodos al implementar el programa educativo de capacitación:

- a. Con apoyo de medios proporcionados por Tecnodata S.A. como por asesoría externa, preparará actividades de capacitación que incluirán en su contenido la responsabilidad penal de las personas jurídicas y su sistema de prevención. El material se pondrá a disposición de los colaboradores y si corresponde de los proveedores. Estas capacitaciones serán obligatorias para determinados colaboradores. El Encargado de Prevención de Delitos actualizará y revisará el material según lo considere apropiado.
- b. Además de la capacitación antes señalada, las materias de importancia se encuentran contenidas en la presente Política y en los documentos que forman parte integrante de la misma, sin perjuicio de que pueda prepararse y enviarse otras comunicaciones sobre la materia.
- c. El Encargado de Prevención de Delitos podrá recomendar que ciertos colaboradores asistan a seminarios a disposición del público que cubran determinadas áreas de las leyes en materia penal.
- d. El Programa de orientación e inducción de Tecnodata S.A. para colaboradores nuevos, incluirá información del Programa de Prevención y de la obligación de un colaborador de mantener los más altos niveles de conducta y normas de ética.

8.10. Modificaciones en la información de Clientes y revisión de la información

El Agente Colocador, o Asesor Comercial, es el encargado de mantener con los Clientes una comunicación permanente. Cualquier cambio en la información de los Clientes o en su perfil de inversión, debe encontrarse documentado y registrarse. El Ejecutivo Comercial será el encargado de efectuar una revisión anual al registro de cada Cliente, con el objeto de verificar la información de los mismos y que la documentación se encuentre al día. Asimismo, deberá confirmar la clasificación del riesgo de cada Cliente. El Encargado de Prevención del Delito deberá verificar que se cumpla con el procedimiento interno de revisión de la información.

8.11. De las Operaciones Sospechosas y Operaciones en Efectivo

Para detectar una Operación Sospechosa, es preciso tener en consideración los antecedentes del Cliente, tales como su giro o actividad, la documentación allegada, la modificación de antecedentes presentados, la información proporcionada o falta de ésta, etc. Resulta de importancia el considerar las Señales de Alerta, de las que se tratará en el numeral siguiente. Además de las operaciones que puedan ser calificadas como

sospechosas, la ley establece que deben ser objeto de un especial escrutinio, de un registro especial y de reporte a la Unidad de Análisis Financiero, aquellas que realicen personas naturales o jurídicas de cualquier naturaleza, que involucren el pago a la entidad de un monto en efectivo, en moneda de curso legal o moneda extranjera, que exceda a diez mil dólares de los Estados Unidos de América, o su equivalente en pesos chilenos según el valor del dólar observado el día en que se realizó la operación. Sin perjuicio de las obligaciones de reporte y registro que establece la ley, las cuales deben ser cumplidas por el Encargado de Prevención del Delito, La Empresa no realiza Operaciones en Efectivo

9. Señales de Alerta

Existen innumerables operaciones y transacciones que posibilitan el proceso de blanqueo de activos, sin embargo, es posible sostener que el carácter sospechoso de una operación proviene, ya sea de la forma inusual en que se realice, en relación a un comportamiento habitual y/o esperable del Cliente, o bien, de la naturaleza misma o de las características propias de la operación. Se debe prestar especial atención a aquellas operaciones que presenten elementos o características inusuales, irregulares o anormales, en relación con las actividades o giro del Cliente o de cualquiera de los que participan en ella, y/o que por su gestación, diseño financiero, estructura, presentación, documentación utilizada, modificación de antecedentes ya registrados, información proporcionada o falta de ésta, por la reiteración o cuantía de las mismas o la intervención inusual de terceros o desconocidos, puedan ser calificadas como sospechosas.

Quienes se relacionen con los Clientes deberán dar especial atención a las señales de alerta publicadas en el sitio web de la Unidad de Análisis Financiero, www.uaf.gob.cl. Algunas Señales de Alerta relacionadas con el comportamiento del Cliente son las siguientes:

- 1.1 Operaciones que no se condicen con la capacidad económica y perfil del Cliente.
- 1.2 Cambio repentino del comportamiento financiero de un Cliente.
- 1.3 Cliente indica una dirección que coincide con el domicilio de otro negocio diferente al que declaró desarrollar, o no se ajusta a la ocupación declarada.
- 1.4 Cliente que al momento de realizar una operación se rehúsa o evita entregar información acerca de su actividad, acreencias o capacidad financiera
- 1.5 Cliente que realiza transacciones de elevado monto y no declara un empleo remunerado o actividad acorde, que justifique los montos involucrados.
- 1.6 Cliente que presiona e insiste en que una determinada operación se realice con extrema rapidez, evitando trámites predefinidos y sin justificar el motivo de su apremio.
- 1.7 Cliente que sin justificación evita presentarse personalmente en la entidad con la que está realizando una operación, llegando incluso a nombrar representantes o intermediarios encargados del manejo de sus inversiones.

1.8 Cambios de propiedad de instrumentos financieros entre personas o sociedades que no cuentan con antecedentes que justifiquen esas operaciones, y que eludan proporcionar o actualizar su información financiera.

1.9 Incremento inusual e injustificado de la facturación del negocio de un Cliente, observado a partir de la actividad económica consignada en sus cuentas y perfil.

1.10 Cliente que en un corto período aparece como dueño de nuevos negocios o empresas, constituidas con capitales iniciales relevantes.

1.11 Cliente que en un corto período aparece como dueño de activos, los cuales representan un alto valor patrimonial.

1.12 Cliente que realiza reiteradas operaciones a nombre de terceras personas.

1.13. Constitución de empresas con capitales o socios provenientes de países considerados no cooperantes por GAFI, o regímenes fiscales preferenciales nocivos según clasificación de la OCDE (Paraísos Fiscales).

1.14 Cambio repentino en la propiedad de una sociedad, cuyos nuevos socios presentan un perfil comercial que no se ajusta a la información histórica de la entidad, o que se muestran reacios a presentar información personal o financiera

1.15. Cliente que entrega documentación incompleta, inconsistente o falsa al momento de realizar una determinada operación

1.16 Clientes que presenten documentos de identificación inusuales o en mal estado.

1.17 Cualquier individuo que presione o intente presionar para no presentar los antecedentes requeridos en una determinada transacción.

1.18 Existencia de varias cuentas corrientes en moneda nacional y extranjera sin que exista una razón de negocio que lo justifique.

1.19 Apertura de múltiples cuentas con una persona en común a todas ellas.

1.20 Clientes que realizan compras y ventas consecutivas o simultáneas de instrumentos financieros, con el propósito de simular un alto nivel de inversiones o capital.

Por su parte, son Señales de Alerta relacionadas con el funcionamiento de Empresa, entre otras, las siguientes:

1.1 Operaciones contractuales por parte de personas y/o clientes que forman parte de un proceso judicial.

1.2 Operaciones concertadas a precios que no guardan relación con las condiciones del mercado.

1.3 Cliente que realiza operaciones que no se condicen con sus condiciones financieras, pudiendo estar actuando en representación de un tercero, respecto del cual no se aportan antecedentes.

1.4 Operaciones realizadas de forma reiterada entre las mismas partes, existiendo ganancias o pérdidas permanentes para alguna de ellas.

1.5 Cliente o proveedor tiene dificultades en bancos, con el SII. O con Tesorería General de la República, no reconociendo pagos o no declarándolos.

1.6 En cuanto al pago a subcontratistas, se exigen anticipos y no se inician trabajos, las obras no están terminadas o los avances de las obras son inexistentes, generándose un pago a dicho subcontratista sin respaldo real.

1.7 Cliente o ejecutivo tanto externos a la empresa como internos, presiona al personal de la empresa para aprobar el ingreso de dicho cliente sin contar con los antecedentes adecuados para su revisión.

1.8 Cliente solicita pagar con documentos bancarios de terceros.

1.9 Trabajador solicite pago de remuneración en cuenta de una tercera persona.

1.10 solicitud por parte de trabajador de comisiones, bonos y horas extras no correspondiéndole.

1.11 Al momento de confeccionar planilla de ingreso de nuevo trabajador, se entregue información no verídica.

1.12 Que trabajador altere fraudulentamente documentación académica en relación a sus capacidades para el cargo a postular, mostrando documentación falsa.

1.13 Personas naturales o jurídicas que demuestran gran solvencia económica y sin embargo les resulta difícil la consecución o suministro de información sobre referencias comerciales o financieras al momento de llenar los formularios de vinculación y/o apertura.

1.14 Transacciones que no se comportan de acuerdo a las prácticas del mercado.

1.15 Cuando un ejecutivo insiste en reiteradas ocasiones que se compre un producto a un proveedor puntual, aun cuando el valor de dicho producto es mayor en comparación a otros proveedores.

1.16 Cuando se insiste en comprar un producto a un proveedor determinado, antes de que llegue la orden de compra por parte del cliente, sobre todo si es fin de mes.

1.17 Cuando recibida la nota de venta, esta no contiene la misma información a la orden de compra del cliente.

1.18 Cuando un ejecutivo comprar un producto por cuenta propia y se lo entrega en forma directa al cliente, sin pasar por bodega y sin orden de compra.

1.19 Cuando se solicita una compra o realizar algo de manera urgente y para conseguirlo, se saltan todos los protocolos de ventas y adquisiciones.

1.20 Cuando ponen una orden de compra en forma directa desde Gerencia comercial, sin pasar por el departamento de compras, donde el gerente del área asume, para salvar la contingencia.

1.21 Cliente hace visible su intención de recibir incentivos fuera del marco legal para así obtener un beneficio.

1.22 Ejecutivo de la empresa manifiesta su intención de entregar incentivos a un cliente para obtener beneficios y asegurar el cierre de un negocio.

1.23 Ejecutivo comercial realice actos indebidos con el fin de adulterar valores de productos y/o servicios para generar ganancias ilícitas, exponiendo a la empresa a riesgos de pérdidas.

1.24 Cuando en el proceso de despachar equipos contratados, se genera despacho por sobre la cantidad pactada, con el objeto de que el cliente reciba más equipos, con la intención de adquirirlos para reventa externa, generándose una pérdida no contemplada en los costos.

1.25 Cuando se confeccionan notas de venta y generar cobros de forma correcta, se genere cohecho para adulterar valores de los productos y/o servicios asociados a la facturación, generando ganancias ilícitas, exponiendo a la empresa a pérdidas y a problemas legales con la justicia.

10. DEL PAGO A TERCEROS

La Empresa sólo se relacionará contractualmente con sus Clientes, por lo cual no realizará pagos ni efectuará transacción alguna, por ningún concepto, a terceros. La única excepción a lo anterior estará dada por pago a terceros que tengan la calidad de socios o accionistas de Clientes personas jurídicas, siempre que conste la orden escrita, emitida por quien tenga poder para representarla, en este sentido. Lo anterior se hará efectivo tras la revisión de los antecedentes legales que se encuentren en poder de La Empresa, donde deberá constar la calidad de socio o accionista de la persona a quién se efectúa el pago y el poder de su representante para emitir dicha orden.

11. PROCEDIMIENTOS DE REPORTE DE LA INFORMACIÓN

11.1. Procedimiento interno de reporte

Cualquier trabajador o colaborador que preste servicios a La Empresa, que detecte una transacción inusual o una Señal de Alerta, deberá comunicarla al Encargado de Prevención del Delito de forma confidencial, indicando los fundamentos de la apreciación realizada, los antecedentes de la operación y toda otra información relevante de la que disponga o que le sea solicitada por este último. De verificarse una Señal de Alerta en una transacción, se deberá obtener toda la información del Cliente referida a:

- a. Naturaleza de la operación y copia de los documentos o antecedentes que la respaldan.
- b. Nombre y apellidos, RUT o su equivalente para los extranjeros no residentes, nacionalidad, profesión, giro, domicilio, número telefónico y correo electrónico del inversionista, Cliente o parte de la operación, copia del mandato si opera para un tercero o, en ausencia de tal contrato, constancia de actuar para un tercero y la completa identificación de aquél, con inclusión de los datos suficientes para poder contactarle. Para las personas jurídicas, deberá dejarse copia de sus antecedentes legales y la individualización de sus representantes.
- c. Aquella documentación que permita determinar la extensión de relaciones que una empresa pueda tener con otras, esto es, determinar si un determinado objetivo es parte de un holding empresarial o de un grupo de empresas. Y, por tanto, aquella que permita la determinación de los miembros del grupo empresarial.
- d. Origen inmediato de los recursos con los que se efectúa la transacción.

Recibida la comunicación, y con la información necesaria para analizar la operación, el Encargado de Prevención del Delito verificará la procedencia de catalogarla como una Operación Sospechosa, caso en el cual procederá conforme a lo dispuesto en el apartado siguiente.

11.2. PROCEDIMIENTOS DE REGISTRO DE LA INFORMACIÓN

Con el objeto de detectar indicios que permitan identificar comportamientos sospechosos o poco habituales por parte de los Clientes y generar los perfiles de riesgo de los mismos que permitan detectar Operaciones Sospechosas, La Empresa llevará registros con la información de cada uno de sus Clientes, conforme a las Fichas de Clientes y a los demás antecedentes que obren en su poder. Con todo, los registros deberán contar con, a lo menos, los siguientes antecedentes:

- a. Nombre o razón social: En el caso de las personas jurídicas se debe agregar el nombre de fantasía de la empresa, de ser procedente.
- b. Número de cédula nacional de identidad o número de pasaporte cuando se trate de ciudadanos extranjeros. En el caso de personas jurídicas, se deberá solicitar su RUT o su equivalente, si es extranjera.
- c. Número de boleta, factura o documento emitido.
- d. Domicilio o dirección en Chile, o en el país de origen o de residencia.
- e. Correo electrónico y teléfono de contacto.
- f. Giro comercial registrado ante el Servicio de Impuestos Internos, si corresponde. En razón de lo anterior, La Empresa deberá mantener el Registro de las Operaciones Efectivo que se realicen.

12. PROCEDIMIENTO DE DENUNCIAS E INVESTIGACIÓN

El procedimiento de denuncias e investigación aplicable a Tecnodata S.A., forma parte integrante de esta Política. Su objetivo es establecer los pasos para **repcionar, investigar y determinar la forma de actuar de Tecnodata S.A.** en caso de denuncias directas o anónimas de colaboradores, clientes, proveedores y terceros, en general, en relación a hechos que revistan carácter de delito, en especial de los sancionados por el Artículo 1° de la Ley N° 20.393. SISTEMA DE SANCIONES Se distinguen dos grupos de infracciones:

a) al MPD y su normativa; y

b) aquellas que digan relación con la comisión de ilícitos. El Comité de Ética, a iniciativa y proposición exclusiva del Encargado de Prevención de Delitos de Tecnodata S.A., tendrá siempre la facultad de proponer y supervisar la aplicación de sanciones, determinar o pronunciarse sobre su procedencia, y revisar o reconsiderar las sanciones cursadas.

El procedimiento de denuncia es el siguiente:

- En caso de denuncia directa, la persona debe acercarse al jefe del área respectiva, con toda la información acerca del asunto a denunciar, para que este pase los antecedentes al encargado de prevención del delito.

- En caso de denuncia anónima, la persona deberá llenar un formulario de denuncia, que se encuentra disponible en www.tecnodatasa.cl/denuncia, donde deberá ingresar la información que en los campos se le soliciten, para así dichos antecedentes puedan ser conocidos por el encargado de prevención del delito.

- Un vez el encargado de prevención del delito recepcione la denuncia con los antecedentes, procederá a investigar los hechos dentro del plazo más breve posible. Dependiendo del resultado de las indagaciones, podrán suceder dos cosas: **A)** que el hecho denunciado no constituya uno de los delitos enmarcados en el modelo de prevención del delito, ni una infracción al reglamento interno, con lo cual no habrán medias de ningún tipo, comunicándole este resultado a la jefatura respectiva. **B)** que efectivamente el hecho denunciado constituya una infracción al modelo de prevención del delito y/o al reglamento interno de Tecnodata S.A., con lo cual el encargado de prevención del delito procederá a informar a la jefatura correspondiente, junto con el archivo de todos los antecedentes recopilados, para así tomar las medidas respectivas, las cuales pueden ser, desde la aplicación de multas y sanciones que contempla el reglamento interno de la empresa, o informar los antecedentes al ministerio público en el caso que dicho actuar investigado constituya un delito.

Todo esto se enmarca además dentro de los lineamientos de los procedimientos de reporte de la información y el procedimiento de registro de la información, ya descritos en el presente modelo.

12.1) Infracción al Modelo de Prevención de Delitos

Será motivo de sanción, la falta de colaboración en la implementación y cumplimiento de los lineamientos del programa de prevención de delitos por parte de los colaboradores, quienes estarán sujetos a las acciones disciplinarias que el Comité de Ética estime proponer. Entre las acciones u omisiones que harán que un colaborador esté sujeto a disciplina por esta razón están, a título enunciativo pero no limitativo, lo siguiente:

- I. Contravenir las normas de la Política de Prevención de delitos;
- II. No informar de un hecho o conducta que revista caracteres de delito;
- III. Infringir los principios generales de comportamiento y actuación;
- IV. No hacer o falsificar cualquier certificación exigida bajo el programa de prevención;
- V. Falta de atención o de diligencia por parte del personal de supervisión que, directa o indirectamente, ocasione la realización de hechos o conductas que revistan caracteres de delito;
- VI. Represalias directas o indirectas contra un colaborador que informa sobre la presunta comisión de un acto o conducta que revista caracteres de delito.

Si un colaborador contraviene cualquier norma contenida en la presente Política y/o sus documentos integrantes, dependiendo el tipo de falta, podrá ser amonestado en forma verbal o escrita, previa evaluación del caso por parte del Comité de Ética, generando un plan de acción respecto al hecho ocurrido, definiendo un plazo para su normalización. Copia del plan de acción, con la firma del Supervisor y del colaborador, será incorporada a la carpeta personal de éste. Dependiendo de la situación, se podrá enviar una copia a la Inspección del Trabajo.

Las acciones antes descritas se entenderán sin perjuicio de las multas previstas en el Artículo 157º del Código del Trabajo o de otras sanciones legalmente procedentes.

Cuando un Supervisor constate una falta, la informará a su superior debiendo dar cuenta al Encargado de Prevención de Delitos de Tecnodata S.A., quien a su vez reportará el evento al Comité de Ética, el cual en base a los antecedentes y resultados de la investigación, propondrá a la Alta Administración y/o al Directorio la sanción correspondiente.

Lo descrito precedentemente, se entiende sin perjuicio de la facultad de Tecnodata S.A. de poner término al Contrato de Trabajo, cuando la situación lo justifique.

13. MONITOREO Y SUPERVISIÓN

El objetivo del monitoreo y supervisión será verificar el adecuado funcionamiento de las actividades de control definidas por el MPD y evaluar la necesidad de efectuar mejoras en el Sistema de Prevención de Delitos. El Encargado de Prevención de Delitos podrá efectuar las siguientes actividades de monitoreo y supervisión:

- Elaborar un plan de trabajo anual, que tenga por objeto medir la eficacia del MPD, así como detectar y corregir sus fallas.
- Revisar documentación que respalde las pruebas efectuadas por las áreas de apoyo.
- Auditar actividades de control (mediante muestreo).
- Realizar análisis de razonabilidad de transacciones.
- Verificar el cumplimiento de las restricciones establecidas en los procedimientos internos.
- Conocer nuevas normativas aplicables.
- Evaluar cambios relevantes en la organización y/o industria de seguros.
- Establecer seguimiento de las mejoras implementadas a las actividades de control.
- Otras actividades que el Encargado de Prevención de Delitos estime convenientes.

14. INFRACCIÓN DE LA LEY EN MATERIA PENAL.

La participación penal de algún colaborador en cualquier clase de delito, en especial de los delitos sancionados por el Artículo 1° de la Ley N° 20.393, realizada en el desempeño de sus funciones o con ocasión de éstas, se considerará como falta de probidad grave del colaborador.

En caso de verificarse hechos o conductas que revistan caracteres de los ilícitos referidos, comprobando razonablemente la veracidad de ellos, Tecnodata S.A. procederá a la desvinculación inmediata del colaborador, sin derecho a indemnización, en virtud de verificarse las conductas graves señaladas como causal de despido en el Artículo 160° del Código del Trabajo, numeral 1°, letras a) y e); y procederá a citar al Comité de Ética para que se pronuncie sobre la procedencia de denuncia o presentación de querrela criminal en contra de los supuestos responsables del hecho delictivo, previo informe del Encargado de Prevención de Delitos

15. ACTUALIZACIÓN

El Modelo de Prevención de Delitos deberá ser controlado permanentemente y revisado cada año por el Encargado de Prevención de Delitos, quien deberá proponer al Directorio su actualización en función de las circunstancias y necesidades que enfrente la Empresa o de los cambios normativos que puedan afectar a la Ley N° 20.393.

ANEXO SOBRE ACTUALIZACIONES A LA LEY 20.393 Sobre responsabilidad penal de las personas jurídicas

Por medio del presente anexo, se pone en conocimiento de los trabajadores de Importaciones y Exportaciones Tecnodata S.A., las actualizaciones que atañen a la ley 20.393 y a nuestro modelo de prevención del delito, anexo el cual se considera parte integral del mismo.

Delitos que atribuyen responsabilidad penal a las personas jurídicas (primeros cuatro delitos ya definidos, y a modo de recordatorio).

- Lavado o blanqueamiento de activos (art. 27 de la Ley nº19.913).
- Financiamiento del terrorismo (art. 8, ley nº18.314).
- Cohecho activo a funcionarios nacionales (art. 250 Código Penal).
- Cohecho activo a funcionarios extranjeros (art. 251 bis Código Penal).

La Ley N°20.931 del 2016, incorpora el delito de Receptación:

“El que conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies hurtadas, robadas u objeto de abigeato, de receptación o de apropiación indebida, las transporte, compre, venda, transforme o comercialice en cualquier forma, aun cuando ya hubiese dispuesto de ellas”.

La Ley N°21.121 del 2018, incorpora 4 delitos:

- **Negociación Incompatible** (art. 240 Código Penal). El que tenga a su cargo la salvaguarda o la gestión de todo o parte de los bienes o patrimonio de otra persona, sea esta natural o jurídica; y directa o indirectamente se interese en cualquier negociación, actuación, contrato, operación o gestión en la cual hubiere de intervenir en relación con los bienes o patrimonio que tiene a su cargo, comete el delito de negociación incompatible.
- **Corrupción entre privados** (artículos 287 bis y 287 ter del Código Penal). Comete el delito de corrupción entre particulares: - El empleado o mandatario del sector privado que solicitare o aceptare 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 (Definición de acuerdo al artículo 287 bis del Código Penal). - El que diere, ofreciere o consintiere en dar, a un empleado o mandatario del sector privado, 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.
- **Apropiación indebida** (art. 470 N°1 del Código Penal). Comete este delito todo aquel que en perjuicio de otro se apropiare o distrajere dinero, efectos o cualquiera otra cosa

mueble que hubiere recibido en depósito, comisión o administración, o por otro título que produzca obligación de entregarla o devolverla.

- **Administración desleal** (art. 470 N°11 del Código Penal). Comete Administración Desleal el que teniendo a su cargo la salvaguardia o la gestión del patrimonio de otra persona, o de alguna parte de éste, en virtud de la Ley, de una orden de la autoridad o de un acto o contrato, le irrogare perjuicio, sea ejerciendo abusivamente facultades para disponer por cuenta de ella u obligarla, sea ejecutando u omitiendo cualquier otra acción de modo manifiestamente contrario al interés del titular del patrimonio afectado.

La Ley N°21.132 del 2019, incorpora 4 delitos, pero que no tienen relación con el giro de nuestra institución:

- Contaminación de aguas (art. 136 Ley de Pesca).
- Comercialización de productos vedados (art. 139 Ley de Pesca).
- Pesca ilegal de recursos del fondo marino (art. 139 bis Ley de Pesca).
- Procesamiento, almacenamiento o utilización de recursos escasos (art. 139 ter Ley de Pesca).

La Ley N°21.240 del 20 de junio de 2020, incorpora delito sobre incumplimiento de medidas sanitarias:

- Delito detallado en Artículo 318 Ter del Código Penal: “ 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, será castigado con presidio menor en sus grados mínimo a medio y una multa de diez a doscientas unidades tributarias mensuales por cada trabajador al que se le hubiere ordenado concurrir. ”

De La Ley N°21.240 del 20 de junio de 2020, Consideraciones.

1. La presente modificación afecta a todas las Personas Jurídicas de Derecho Privado y a las Empresas del Estado, que no cuenten con autorización sanitaria para trabajar.
2. La referida Ley tiene por objeto elevar las sanciones establecidas, para aquellos que infrinjan las normas dictadas por la autoridad sanitaria. En este sentido:

“Se debe poner especial énfasis en el área de recursos humanos o en aquellas personas a cargo de los equipos de trabajo, toda vez que la Ley se refiere a una “orden” dirigida al trabajador, no siendo necesario que este último concorra al lugar de trabajo”.