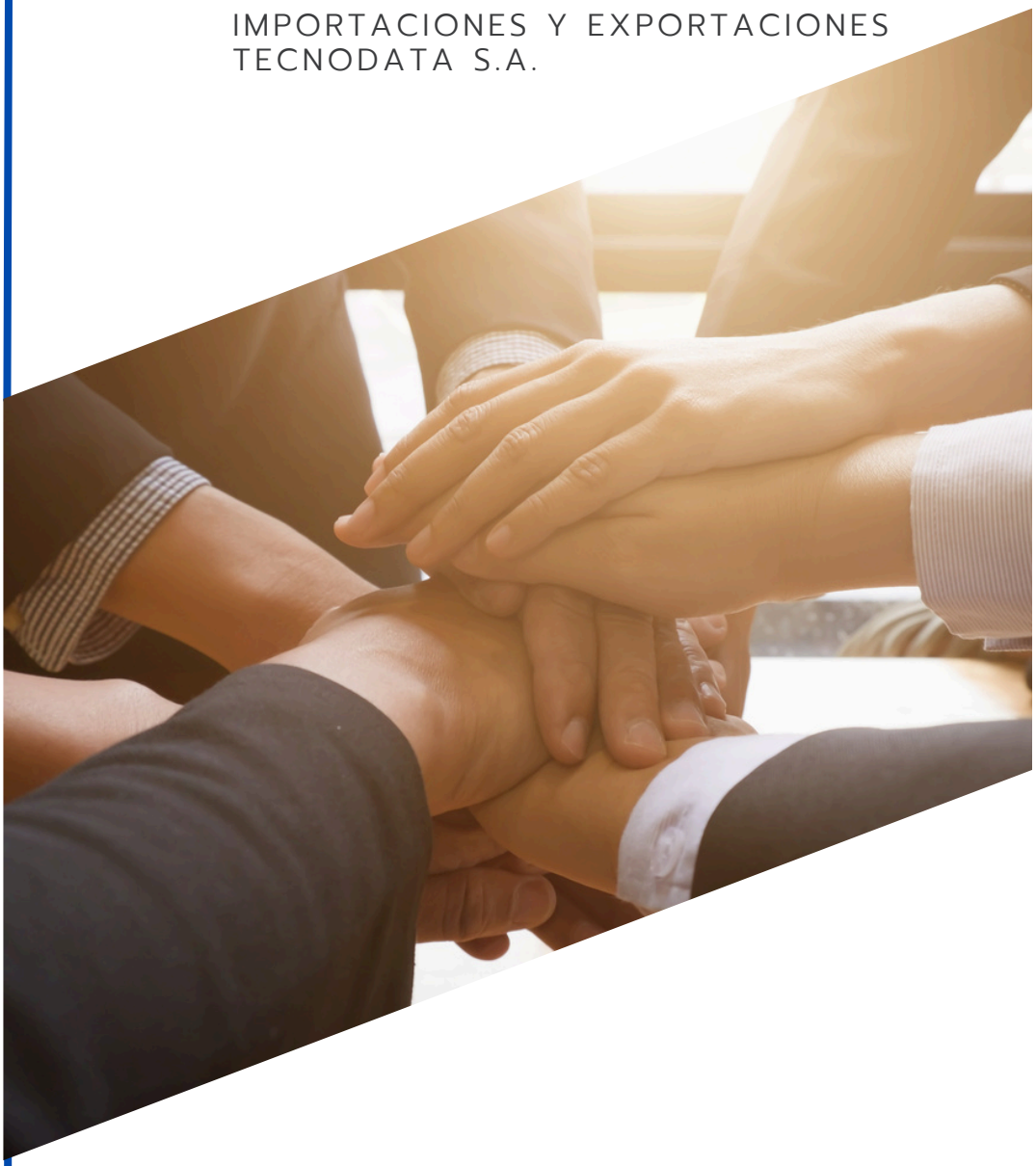
MODELO PREVENCION DEL DELITO

IMPORTACIONES Y EXPORTACIONES
TECNODATA S.A.



Febrero 2024

Palabras del Gerente General:

En Importaciones y Exportaciones Tecnodata S.A., estamos comprometidos con la más alta integridad y ética corporativa en todas nuestras operaciones y relaciones comerciales. Como parte de este lineamiento, deseamos comunicar nuestra adhesión y compromiso con la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas.

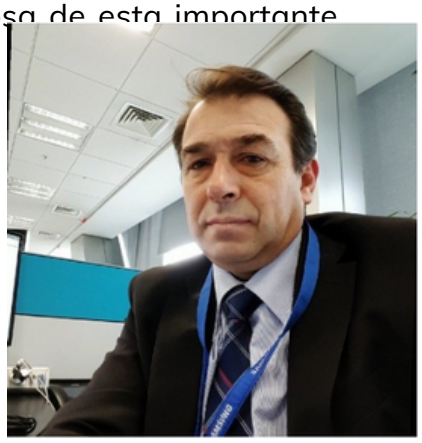
Nuestra empresa reconoce la importancia de cumplir con las regulaciones legales y contribuir a un entorno empresarial ético y responsable. En este sentido, hemos decidido implementar un **Modelo de Integridad y Ética y Prevención del Delito** que cumpla con los requisitos establecidos en la ley 20.393. Este modelo no solo es un requisito legal, sino que también es una parte esencial de nuestra cultura corporativa, que promueve la integridad en todas nuestras actividades empresariales.

Se espera que todos nuestros colaboradores y empleados sigan y cumplan con este modelo, ya que es una responsabilidad compartida garantizar que nuestra empresa opere de manera legal y ética en todo momento. Para lograr este compromiso, hemos establecido un equipo encargado de supervisar y mantener actualizado nuestro modelo de prevención de delitos y nuestra política de Compliance. Este equipo será el punto de contacto para cualquier consulta o preocupación relacionada con la aplicación de este modelo.

Como empresa, trabajaremos de manera conjunta para garantizar que nuestro modelo de prevención de delitos sea implementado y seguido rigurosamente por todos los miembros de nuestra organización.

Dentro de este contexto, nos comprometemos a mantener, comunicar y mejorar continuamente nuestro sistema de compliance, a objeto de ser un apoyo a nuestras soluciones basadas en productos y servicios de excelencia, así como también gestionar los riesgos y oportunidades, promover las relaciones que fomenten el crecimiento, proteger el medio ambiente y cumplir con los requisitos pactados, legales y reglamentarios.

Agradecemos su compromiso continuo con nuestros valores y principios, y esperamos contar con su apoyo en la implementación exitosa de esta importante iniciativa.



Fabrizio Montagna Muñoz.
Gerente General
Importaciones y Exportaciones
Tecnodata S.A.

Introducción:

> Con fecha 2 de diciembre de 2009, se publicó en el Diario Oficial la Ley N°20.393, (indistintamente la "Ley" o "Ley 20.393"), en virtud de la cual se estableció, por primera vez en nuestro país, la posibilidad que las personas jurídicas respondan criminalmente en caso de que ciertas personas vinculadas a éstas cometan alguno de los delitos en ella establecidos.

En conformidad con lo dispuesto en la Ley, las personas jurídicas responden penalmente por la comisión de ciertos delitos, los cuales están descritos en la norma y corresponden a los siguientes:

1. Lavado de activos.
2. Financiamiento del terrorismo.
3. Cohecho de funcionario público nacional o extranjero.
4. Receptación.
5. Negociación incompatible.
6. Administración desleal.
7. Corrupción entre privados (soborno).
8. Apropiación indebida.
9. Daños a recursos hidrobiológicos existentes en mar, ríos, lagos o cualquier otro cuerpo de agua, como
consecuencia de la contaminación de éstos.
10. Aprovechamiento de recursos hidrobiológicos en veda.
11. Extracción y explotación ilegal de recursos bentónicos.
12. Procesamiento, elaboración o almacenamiento ilegal de recursos hidrobiológicos sobrexplotados o productos derivados de ellos, y;
13. Inobservancia de medidas decretadas por autoridad sanitaria en caso de epidemia o pandemia

Además de la comisión de alguno de los ilícitos descritos, para que se genere la responsabilidad de la empresa, es necesario cumplir además con una serie de otros requisitos establecidos en la Ley:

01 El delito debe ser cometido por personas que forman parte de la organización. En particular, por 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.	**02** El delito debe cometerse en interés de la persona jurídica o para el beneficio de ésta.	**03** La comisión del delito debe ser resultado del incumplimiento, por parte de la persona jurídica, de sus deberes de dirección y supervisión.

TECNODATA cumple con sus deberes de dirección y supervisión cuando cuenta con un Modelo de Prevención de Delitos (indistintamente "MPD" o "Modelo"), que se aplica efectivamente en la persona jurídica, de forma tal que le permite prevenir la ocurrencia de cualquier ilícito de aquellos que activan la responsabilidad penal en su contra.

El presente Manual establece la operativa de las diversas actividades de prevención y mitigación de los potenciales riesgos de comisión de delitos, en el marco de los distintos procesos de la empresa que se han identificado e integrado al Modelo.

Objetivo:

El propósito del presente Modelo de Integridad y Ética y Prevención del Delito (en adelante, el “Manual”, MPD o MIE) 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° 20.393 y 19.913. 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.

Se busca establecer las actividades del MPD a cargo del Encargado de Prevención de Delitos en cumplimiento de sus funciones de supervisión del Modelo y dar cabal cumplimiento a los requerimientos establecidos al amparo de la Ley 20.393, así como la demás normativa que sea aplicable en la materia.

Alcance:

El presente Manual es aplicable a todos quienes prestan servicios directos e indirectos a Importaciones Y exportaciones Tecnodata S.A., en adelante “Tecnodata”.

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)..

Por la naturaleza de sus actividades. Tecnodata esta expuesta a riesgos asociados a la eventual comisión de alguno de los delitos contemplados en la Ley 20.393, o al menos, evaluados con un distinto nivel de criticidad. Por consiguiente, este Manual deber ser tomado como lineamiento base, ante la necesidad de creación de procedimientos específicos, de manera que se garantice el cumplimiento de su fin último, consistente en prevenir la comisión de los referidos delitos.

Todos los colaboradores antes descritos tendrán el deber de reportar oportunamente al Encargado de Prevención del Delito o EPD cualquier transacción sospechosa o procedimiento inusual. 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

Actos Ilícitos Sancionados por la ley 20.393

Delitos y Marco Jurídico:

La Ley 20.393 ha establecido un catálogo restringido de delitos que pueden generar responsabilidad penal corporativa. Asimismo, la esta misma entrega un marco general de aplicabilidad de los deberes de dirección y supervisión. A continuación, se incorpora una breve explicación de cada uno de los ilícitos incluidos en la norma:

- **Lavado de Activos:**

El delito de lavado de activos, tipificado en el artículo 27 de la Ley N°19.913 castiga a quienes, conociendo su origen ilícito, de cualquier forma, busquen disimular u ocultar la naturaleza, origen, ubicación, propiedad o control de dinero y/o bienes, o bien, los adquieran, tengan o posean de cualquier forma. Este delito sanciona la introducción en la economía de activos de procedencia ilícita, otorgándoles la apariencia de legalidad al valerse de actividades lícitas, lo que faculta a delincuentes y organizaciones criminales a encubrir el origen ilegal de su producto, sin poner en peligro su fuente.

Para que se configure el lavado de activos, se requiere que los fondos que se ocultan, disimulan o mantienen, provengan de ciertas actividades ilícitas enumeradas en la Ley 19.913, y que por ello se les conoce como “delitos base”. En otras palabras, el dinero que se intenta “blanquear” debe venir de la comisión de uno de los siguientes delitos.

Los siguientes constituyen en la actualidad los delitos base del lavado de activos en nuestro ordenamiento:

Cabe señalar que el delito no solo sanciona a quienes conocen el origen ilícito de los activos o bienes, sino también a quienes, por negligencia inexcusable, no tuvieron conocimiento de la procedencia delictiva.

1. Conductas terroristas (Ley N° 18.314).
2. Tráfico de armas (Ley N°17.798).
3. Trafico de drogas (Ley N° 20.000).
4. Algunos delitos bancarios (Ley General de Bancos).
5. Algunos delitos de mercado de valores (Ley N° 18.045).
6. Delitos de contrabando (Ordenanza de Aduanas).
7. Delitos funcionarios, especialmente el cohecho y el fraude al fisco.
8. Asociaciones ilícitas (Código Penal).
9. Estafa, apropiación indebida, administración desleal y fraude de subvenciones al Estado (Código Penal).
10. Producción, comercialización, distribución y difusión de material pornográfico infantil (Código Penal).
11. Promoción de la prostitución (Código Penal).
12. Trata de personas y tráfico de migrantes (Código Penal).
13. Secuestro y sustracción de menores (Código Penal).
14. Delitos contra la propiedad intelectual (Ley N°17.736).
15. Delitos de fabricación y circulación de billetes falsos (Ley N°18.840).
16. Algunos delitos tributarios (Código Tributario).
17. Delitos de uso fraudulento de tarjetas de pago y transacciones electrónicas (Ley N°20.009).

> El delito podría configurarse en caso de que Tecnodata contrate como proveedor a una empresa de asesorías contables que en realidad se dedica a actividades asociadas a la comercialización de estupefacientes, habiendo contratado el servicio sin realizar ninguna acción que permitiera conocer el origen ilícito de las actividades del proveedor. Esta sería una forma de “limpiar” activos que provienen de actividades delictivas.

- **Cohecho o Soborno a Funcionario Público Nacional o Extranjero:**

La Ley 20.393 recoge las situaciones de cohecho tanto respecto de funcionarios públicos nacionales (artículo 250 del Código Penal) como extranjeros (artículo 251 bis del Código Penal). Sanciona a quien *dé, ofrezca o consienta en dar a un empleado público un beneficio económico o de otra naturaleza, en provecho de éste o de un tercero, en virtud de las siguientes justificaciones*:

1. En razón de su cargo.
2. Para que el funcionario público desarrolle u omita algunos actos que son propios de su cargo.
3. Por haber realizado u omitido actos propios de su cargo.
4. Para que ejerza influencia sobre otro empleado público, beneficiando a un tercero.
5. Para que cometa ciertos delitos.

En el caso del cohecho a funcionario público extranjero , la conducta sancionable consiste en ofrecer, prometer, dar o consentir en dar a un funcionario público extranjero, un beneficio económico o de otra naturaleza, en provecho de éste o de un tercero, en razón de su cargo, o para que realice una acción o incurra en una omisión con miras a la obtención o mantención, para sí u otro, de cualquier negocio o ventaja indebidos en el ámbito de una transacción internacional o de cualquier actividad económica desempeñada en el extranjero.

Si bien el delito de cohecho sanciona a quien ofrece o consiente en dar a un empleado público un beneficio económico o de otra naturaleza, no es necesario que ese beneficio económico vaya en provecho del propio funcionario público, sino que puede procurar beneficio a un tercero.

Además, basta con el mero ofrecimiento para que se cometa el delito, no es necesario ni que se haya efectivamente pagado ni que se haya aceptado o recibido el beneficio económico.

En el caso del cohecho a funcionario público extranjero, es importante señalar que aun cuando se haya perpetrado fuera del territorio de la República, por expresa disposición legal debe ser conocido y juzgado por los Tribunales Chilenos. Lo anterior, siempre que haya sido cometido por un nacional chileno o bien por un extranjero con residencia habitual en Chile.

Algunos Ejemplos:

- La contratación de una persona por petición exclusiva de un funcionario público, como forma de pago por un beneficio que otorgó a Tecnodata en el ejercicio de sus funciones.

- El pago, por parte de un colaborador, a algún empleado público para evitar o modificar los resultados de las fiscalizaciones que se hagan a Tecnodata.

- Un caso de cohecho internacional lo constituye aquella situación en la que un representante de Tecnodata en el extranjero, le pague a un funcionario público de ese país para obtener un permiso que necesita para su funcionamiento en dicha localidad.

Respecto a qué sujetos la Ley califica como funcionarios públicos, se consideran las siguientes definiciones:

FUNCIONARIO PÚBLICO NACIONAL

Corresponde a toda persona que desempeñe un cargo o función pública, sea en la administración central o en instituciones o empresas semifiscales, municipales, autónomas u organismos creados por el Estado o dependientes de éste, aunque no sean de nombramiento del Presidente de la República ni reciban sueldo del Estado, incluyéndose aquellos cargos de elección popular.

FUNCIONARIO PÚBLICO EXTRANJERO

El Código Penal considera empleado público extranjero a toda persona que tenga un cargo legislativo, administrativo o judicial en un país extranjero, haya sido nombrada o elegida, así como cualquier persona que ejerza una función pública para un país extranjero, sea dentro de un organismo público o de una empresa pública. Asimismo, se entenderá que tiene la calidad señalada con anterioridad cualquier agente de una organización pública internacional.

- **Financiamiento al Terrorismo:**

El financiamiento del terrorismo, consagrado en el artículo 8° de la Ley N°18.314, sanciona a quienes de cualquier forma soliciten, recauden o provean fondos con la finalidad de que se utilicen para cometer los delitos terroristas establecidos en la misma Ley.
A diferencia del lavado de activos, en el financiamiento del terrorismo el foco de vulnerabilidad no está en el origen de los recursos, sino en el destino de éstos.

- El delito podría configurarse a partir de donaciones que se hicieran a organizaciones no gubernamentales (ONG) que, si bien parecieran tener fines lícitos, verdaderamente financian o se vinculan con actividades terroristas.

- También, por ejemplo, Tecnodata podría entregar activos fijos dados de baja a una persona natural o jurídica desconocida, la cual podría estar relacionada con la realización de actos de carácter terrorista.

- **Corrupción entre Particulares:**

El delito de corrupción entre particulares se encuentra tipificado en los artículos 287 bis y 287 ter del Código Penal. La conducta sancionada es similar a la establecida en el cohecho, con la diferencia que no requiere la intervención de funcionarios públicos, ya que se castiga la afectación de imparcialidad en los procesos de contratación privados

El ilícito castiga a las dos partes de la relación corrupta, sancionando:

1. Al empleado o mandatario 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 de un oferente sobre otro.

2. Al que diere, ofreciere o consintiere en dar a un empleado o mandatario un beneficio económico o de otra naturaleza, para sí o un tercero, para que favorezca o por haber favorecido la contratación con un oferente sobre otro.

Ejemplo:

- Este delito podría configurarse en aquellos casos en que Tecnodata solicite servicios específicos y pida cotización a varias empresas y un empleado o mandatario de una de ellas hace llegar un obsequio a una de las personas encargadas del proceso, siendo ese regalo aceptado por el responsable de contratación y decidiendo a favor de la empresa que le entregó el presente En este caso, será penalmente responsable, el trabajador que acepta el referido beneficio.

El delito puede ser cometido, primordialmente, por cualquier trabajador o mandatario de una empresa, que se encuentre a cargo del área de compras y deba decidir respecto a las compras directas que realice Tecnodata.

La conducta se da típicamente dentro de procesos de contratación en el que existan al menos tres empresas involucradas, una que se encuentra en posición de favorecer, y otras que tomarán la posición de empresa favorecida y/o perjudicada, dependiendo de la decisión que adopte la empresa en posición de favorecer.

El o los trabajadores de Tecnodata que se encuentren a cargo de decidir la el proveedor de la Compañía en formatos de compra de la empresa, serán autores del delito cuando prefieran a un oferente por sobre otro, producto de haber aceptado o recibido un beneficio económico o de otra naturaleza, para sí o para un tercero, entregado u ofrecido por el potencial proveedor.

Es muy importante que sepas que este ilícito se consuma con la mera aceptación que el trabajador de Tecnodata haga del beneficio económico, sin que sea necesario que se haga una entrega efectiva del mismo o que la decisión haya causado una pérdida a la Compañía.

- **Administración Desleal:**

Este delito, establecido en el artículo 470 N°11 del Código Penal, consiste en la conducta del que, teniendo a su cargo la salvaguardia o la gestión del patrimonio de un tercero, le irrogue perjuicio, ejerciendo abusivamente sus facultades de representación, o ejecutando u omitiendo cualquier otra acción de modo manifiestamente contrario al interés del titular del patrimonio afectado.

La norma sanciona la conducta de una serie de sujetos que tienen a su cargo la gestión del patrimonio, en particular, aquellos que se encuentran a cargo del patrimonio de una sociedad anónima abierta o especial.

En este caso, y dependiendo de la fuente de los deberes de resguardo que se tengan sobre el patrimonio de un tercero, el delito puede cometerse:

1. Por aquella persona que, en virtud de un contrato o un mandato, tiene a su cargo, con facultades de disposición, la gestión del patrimonio ajeno, y en ese encargo, le irroga perjuicio abusando de dichas facultades.

2. Por aquella persona que ejecuta u omite intencionalmente cualquier acción contraria al interés del titular del patrimonio. En este segundo caso no es necesario que el autor de la conducta sea mandatario o posea facultades de disposición del patrimonio. Lo que se sanciona es la infracción a los deberes de fidelidad, es decir, los deberes generales de cuidado y salvaguarda del patrimonio de otra persona.

- Un ejemplo de la primera situación descrita se daría en caso de que un ejecutivo principal de Tecnodata. que, en virtud de un mandato, administra el patrimonio de la empresa, decida invertir parte de dicho patrimonio en actividades que le generan perjuicio a la empresa, y que en cambio le otorgan un beneficio personal. En este caso, será penalmente responsable, el trabajador que toma la decisión de inversión en perjuicio de la Compañía.

- Respecto a la segunda forma de comisión del delito, esta podría configurarse en el caso que, teniendo un contrato con una empresa en el que se pactó que Tecnodata administrará las compras necesarias para la prestación del servicio, el encargado del proyecto comience mes a mes a demorar el pago de los reembolsos por dichas compras, debido a que se han generado sobrecostos, esto para efectos de disminuir las pérdidas de Tecnodata y mostrar mejores resultados.

- **Apropiación Indebida:**

El Código Penal establece, en el artículo 470 N°1, el delito de apropiación indebida, el cual sanciona a quien se apropie o distraiga dinero o especies de un tercero, que se encuentran en su poder en virtud de un título de mera tenencia, es decir, que obliga a su devolución dentro de un tiempo determinado.

Para que se configure el delito, el dueño de los bienes muebles debe entregarlos al tercero que se los apropia o distrae mediante un título que no transfiere el dominio. Luego, el autor del delito se apropia o distrae las especies dándoles un uso distinto al acordado, o bien no haciendo entrega de ellas al dueño de acuerdo a lo pactado.

El requisito fundamental para que se configure el delito es que la apropiación o distracción de los bienes cause perjuicio patrimonial a la víctima.

Ejemplos:

- Podría incurrirse en una apropiación indebida cuando un trabajador de Tecnodata a cargo de efectuar el pago a los proveedores no los realice, y en su lugar destine el dinero a un fin distinto.

- Podría configurarse el delito en el caso de que Tecnodata firme un contrato de equipos electrónicos, y estos sean registrados como activos propios en la contabilidad de la Compañía, y vencido el plazo no se restituyan a su dueño.

- **Receptación:**

El delito de receptación, consagrado en el artículo 456 bis A del Código Penal, sanciona a quien, conociendo su origen o no pudiendo menos que conocerlo, tenga en su poder, a cualquier título, especies hurtadas, robadas u objeto de abigeato (hurto de ganado), de receptación o de apropiación indebida, las transporte, compre, venda, transforme o comercialice en cualquier forma, aun cuando ya hubiese dispuesto de ellas.

Es importante notar que la propia norma señala que solo se puede sancionar por receptación a la persona que haya tenido o que debía tener conocimiento del origen ilícito de los bienes. En otras palabras, si el posible autor de la conducta no tuvo conocimiento de dicha procedencia, y dicho desconocimiento está justificado, no es posible sancionarlo.

Ejemplos:

Si Tecnodata compra bienes que un proveedor obtuvo mediante un robo.

- **Negociación Incompatible:**

La negociación incompatible, tipificada en el artículo 240 N°7 del Código Penal, es la regulación a nivel penal de los conflictos de intereses. Este delito sanciona a un conjunto de sujetos que tienen como característica común la capacidad para tomar decisiones respecto del patrimonio de otras personas y, en particular, a los directores, gerentes y ejecutivos principales de una sociedad anónima que se interesen en cualquier negociación, actuación, contrato, operación o gestión que, por su posición o por su relación con el patrimonio que tienen a cargo, debieron haberse abstenido.

La negociación incompatible se califica como un delito de peligro abstracto, por lo que no requiere resultado para que se sancione. Por interés, debe entenderse la acción de participar en la toma de decisión sobre una operación comercial en la que la existencia de un conflicto de interés obligaba a abstenerse. Así, se trata de una hipótesis de grave conflicto de interés.

El interés en este caso tiene que ser de índole económica. A su vez, el negocio en el que toma parte el autor debe interpretarse en un sentido amplio, referido a cualquier acuerdo de voluntades, cualquier trabajo o negocio en donde el sujeto tenga intervención en virtud de su cargo, sin distinción de su naturaleza.

Ejemplos:

Cuando un gerente de Tecnodata decide hacer una donación a una organización no gubernamental en la que uno de sus hijos es director, sin advertir dicha circunstancia al Directorio.

La contratación, por parte de algún ejecutivo de Tecnodata, de un servicio a una empresa proveedora que resulte ser de propiedad de su esposa, o de algún otro familiar, sin advertir de dicha circunstancia oportunamente.

Dentro de quienes pueden cometer este delito, como se señaló, están los directores, gerentes y ejecutivos principales de una sociedad anónima, los que incurrirán en el ilícito si se interesan en una transacción o en un contrato que pudiese representar un beneficio para sí o para personas naturales o jurídicas con la que se encuentren relacionados, infringiendo así las obligaciones establecidas en la Ley N°18.046 sobre sociedades anónimas que obliga, en general, a poner estas transacciones en conocimiento del directorio para su aprobación, y porsobre todos que sean ejecutadas en condiciones de mercado

- **Infracción a las medidas decretadas por la autoridad sanitaria en contexto de epidemia o pandemia:**

Este delito se encuentra regulado en el artículo 318 ter del Código Penal y sanciona a quien, teniendo autoridad para disponer del 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 decretado por la autoridad sanitaria.

De esta manera, se sanciona la conducta de un trabajador que, teniendo la autoridad, les ordene a sus subordinados concurrir a su lugar de trabajo, a sabiendas de que dichos colaboradores se encuentran residiendo en una zona declarada en cuarentena por la autoridad sanitaria, o hayan sido obligados por dicha autoridad a guardar aislamiento sanitario, por constituir un peligro a la salud pública.

Pueden existir excepciones a esta obligación, por ejemplo, cuando la empresa, conforme a la normativa establecida para ello, obtenga y entregue a sus trabajadores, el permiso necesario para movilizarse en zonas de cuarentena, el que debe ser otorgado por la autoridad correspondiente.

Ejemplos:

- Podría cometerse el delito cuando un trabajador de Tecnodata que, teniendo la autoridad, le ordene a uno o más trabajadores subordinados concurrir a las dependencias de la empresa, a sabiendas de que dichos trabajadores residen en una zona declarada en cuarentena, sin haberles proporcionado el respectivo permiso obtenido conforme a la normativa vigente.

- También se cometería el delito si un trabajador de Tecnodata que, teniendo la autoridad, le ordena a uno de sus trabajadores dirigirse a su lugar de trabajo, y al dar esa orden no tenía menos que saber que el referido trabajador se encontraba cumpliendo alguna medida de aislamiento sanitario, decretado por la autoridad, por encontrarse cursando una enfermedad con efectos en la salud pública

- **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:

- Disolución de la persona jurídica o cancelación de la personalidad jurídica. La disolución o cancelación producirá la pérdida definitiva de la personalidad jurídica.

- 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.

- 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.

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

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

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

    - 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.

- Multa a beneficio fiscal.

Modelo de Prevención de Delitos:

De acuerdo con lo establecido en el artículo 4° de la Ley 20.393 Tecnodata ha determinado voluntariamente la implementación de un Modelo de Prevención de Delitos, sobre la base de los establecido en este Manual y que considera, entre otros, los siguientes elementos:

1. Designación del Encargado de Prevención de Delitos ("EPD").
2. Definición de medios y facultades del EPD.
3. Establecimiento de un sistema de prevención de los Delitos de la Ley.
4. Supervisión y certificación del sistema de prevención de los Delitos de la Ley.

Diagrama del modelo de prevención de delitos de Tecnodata

Encargado de prevención del delito (EPD)

MODELO DE PREVENCION DE DELITOS

MATRIZ DE RIESGO	ÁREAS DE APOYO	AMBIENTE DE CONTROL	LEGALES LABORALES
• Identificación de riesgo de delitos • Definición de controles Evaluación de Cumplimiento • Actividad de respuesta	• Gerencia General • Recursos Humanos • Finanzas y Contabilidad • Comité de Ética	• Código de Ética • Canal de Denuncia • Reglamento Interno • Política de Integridad y Compliance • Capacitaciones y difusión	• Anexo Contrato Trabajadores, y Proveedores • Cláusula anexo al reglamento interno

OUTPUT

- Reportes semestrales al directorio
- Reportes informativos a otras áreas
- Actualización y monitoreo del MPD
- Denuncias a la justicia

Supervisión y Monitoreo:

Encargado de prevención del delito (EPD)

El MPD de Tecnodata consiste en un sistema preventivo y de supervisión, a través de diversas actividades de control, sobre los procesos o actividades de negocio que se encuentran o encontrarán expuestas a los riesgos de comisión de los delitos señalados, y que tienen el propósito de evitar su ocurrencia. La responsabilidad de implementación y mantención del MPD corresponde al Directorio, al Gerente General, al Encargado de Prevención de Delitos de (el "EPD"), y a todas las áreas responsables de los controles asociados a él.

Encargado de Prevención del Delito (EPD) ó Compliance Officer.

La Ley 20.393, en su artículo 4°, describe los elementos mínimos que debe contener un Modelo de Prevención de Delitos, siendo uno de ellos que la empresa debe contar una persona designada especialmente para asumir la responsabilidad de administrar el Modelo; es decir, un Encargado de Prevención (EPD) quien, en el caso de nuestra empresa, es el colaborador especialmente designado por el Directorio de Importaciones y Exportaciones Tecnodata S.A., para que, en conjunto con la administración de la empresa, diseñe, implemente y supervise el Modelo.

La duración del Encargado de Prevención en el ejercicio de su cargo lo definirá el Directorio de Tecnodata. Sin embargo, y en cumplimiento de la ley, no podrá mantenerse más de tres años en sus funciones, período prorrogable por otro de igual duración.

Medios, Facultades y Responsabilidades Del Encargado De Prevención De Delitos:

- **Medios y facultades EPD:**

Los medios y facultades del Encargado de Prevención para la ejecución de sus labores serán:

1. Independencia respecto de la administración de Tecnodata, para ello, por una parte, accederá y reportará directamente al Directorio y por otra, al Gerente General con el fin de rendir cuenta de su gestión, así como para reportar sus hallazgos.

2. El EPD contará con línea directa y libre de obstáculos a las distintas áreas de la organización, con el fin de ejecutar las siguientes actividades:

- a. Investigaciones específicas.
- b. Monitoreo del sistema de prevención de delitos.
- c. Revisar y requerir información para la ejecución de sus funciones.

3. Acceso ilimitado a toda la información necesaria para el correcto desempeño de sus funciones, y a la que se pueda tener acceso conforme a la Ley.

4. Recurso presupuestario anual aprobado por el Directorio de Tecnodata, el cual debe ser suficiente para la ejecución de revisiones de monitoreo continuo del MPD, así como para la realización de mejoras y auditorías según corresponda.

5. Infraestructura básica y apropiada para el adecuado desempeño de sus roles y responsabilidades, es decir, de ser necesario, se le deberá dotar de herramientas tecnológicas, infraestructura física y recursos humanos.

- **Responsabilidades del EPD:**

Sus actividades, atribuciones y obligaciones podrán principalmente resumirse como sigue:

1. Velar por la adecuada implementación, ejecución y operación del MPD.

2. Modificar el MPD cuando corresponda, de acuerdo a los cambios que experimente la normativa en virtud de la cual éste se genera, y/o cuando estos tengan lugar en la estructura de negocios de la Compañía.

3. Reportar su gestión en forma periódica al Directorio. En particular, deberá reportar sobre el estado del MPD y todos los temas que se relacionen con la correcta implementación y fiscalización del MPD, así como cualquier otra materia sobre la que el Directorio deba tomar conocimiento, y que deba tomar medidas oportunamente.

4. Requerir al Directorio y al Gerente General los medios, recursos y facultades necesarias para el cumplimiento de su labor.

5. Encargarse de las investigaciones cuando exista una denuncia válida o una situación sospechosa por casos de infracción al MPD, reuniendo toda la información necesaria, y conforme a lo establecido en el Procedimiento de Denuncias e Investigaciones.
6. Establecer auditorías específicas para la verificación del cumplimiento de las actividades del MPD. Consecuentemente, determinar su alcance y cobertura.

7. Diseñar y ejecutar un programa de difusión y capacitación para el cumplimiento del MPD, dirigido a todos los trabajadores, colaboradores, proveedores y contratistas respectivamente.

8. Revisar según corresponda, sea de acuerdo a una periodicidad establecida, o en virtud de circunstancias sobrevinientes, las actividades o procesos de la Compañía en los cuales la exposición a riesgos de comisión de delitos se incremente.

9. Requerir a las correspondientes áreas las evidencias o respaldos de la ejecución y cumplimiento de los controles críticos a su cargo; establecer brechas y concertar con dichas áreas planes de acción para su cierre.

10. Recomendar implementar a las áreas responsables o dueñas de procesos críticos, políticas, procedimientos y/o actividades de control que considere necesarios para añadir al MPD.

11. Asesorar y resolver consultas o dudas que puedan emanar de parte de los empleados y colaboradores, relativas a cualquier aspecto referente a la prevención de los delitos dispuestos en la Ley 20.393.

El Encargado de Prevención de Delitos podrá actuar en forma individual o a través del personal a su cargo, o alguien específicamente designado por el EPD para estas labores, y también incluir otras actividades, atribuciones y obligaciones de las señaladas anteriormente sin que estas sean limitadas. Para estos efectos, al menos semestralmente,
reportará al Directorio una presentación de situaciones de riesgo que pudiera haber detectado, conclusiones y planes de acción, así como la idoneidad y efectividad del MPD.

Sistema de Prevención de Delitos:

El EPD, en conjunto con el directorio y la alta gerencia, dispondrá de un Sistema de Prevención de Delitos, cuyos procesos principales son:

1. La identificación de los procesos o actividades, sean éstos habituales o esporádicos, en virtud de los cuales aumente la exposición a riesgos de comisión de delitos contemplados en la Ley 20.393.

2. El establecimiento de protocolos, reglas y procedimientos específicos que permitan a las personas que intervengan en las actividades o procesos indicados anteriormente, programar y ejecutar sus tareas o labores de una manera que prevenga la comisión de los mencionados delitos.

3. La identificación de los procedimientos de administración y auditoría de los recursos financieros que permitan a la entidad prevenir su utilización en los delitos dispuestos en la Ley 20.393.

4. La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el Sistema de Prevención de Delitos.

El Sistema de Prevención de Delitos se sostiene sobre cuatro actividades o pilares que aseguran su funcionamiento y cumplimiento, todas insertas sobre un adecuado ambiente de control. Estas actividades, que se desarrollarán con mayor profundidad en otros documentos adicionales a éste, son las siguientes:

- **Actividades de Prevención.**
- **Actividades de Detección.**
- **Actividades de Respuesta.**
- **Actividades de Supervisión y monitoreo.**

Ambiente de Control:

Es el conjunto de documentos y cultura, incluyendo valores éticos, que norman a la organización, y conforman la base en la que se respalda el Sistema de Prevención de Delitos, puesto que facilitan el establecimiento los pilares fundamentales respecto de su estructura y funcionamiento.

Los siguientes elementos son relevantes para el adecuado funcionamiento del mismo, sin que sean taxativos o limitantes:

A) Políticas y procedimientos del programa de compliance.

Corresponden a todos aquellos documentos o procesos del Programa que establecen definiciones, medidas y controles para Tecnodata S.A.

En este sentido, es relevante considerar que atendidas las actividades que fundan el negocio, estas podrán considerar documentos o procesos distintos en la línea de asegurar el debido control de sus riesgos, siempre cumpliendo con los lineamientos entregados en este Manual.

Teniendo en consideración lo anterior, se considerarán para Tecnodata S.A:

- Código de Ética.
- Procedimiento de Denuncias e Investigaciones.
- Reglamento Interno Tecnodata.

B) Políticas y procedimientos de conocimiento del cliente y de administración de recursos financiaros:

Comprenden todos aquellos procesos internos que establecen medidas y controles para la administración de recursos financieros y evaluación de clientes y que, a partir de ello, permiten prevenir la utilización de los recursos de la Compañía para la comisión de los delitos dispuestos en la Ley 20.393, además de permitir detectar potenciales clientes fraudulentos. En este contexto, Tecnodata podrá considerar distintos documentos o procesos de control de acuerdo con su estructura de negocios.

Para el caso de Tecnodata S.A., se considerarán los siguientes procesos:

- Procedimiento para la aprobación y control de Clientes.
- Procedimiento para la aprobación, registro e imputación de gastos.
- Procedimiento de aprobación de clientes.

Identificación de 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 por el área de Finanzas .

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, y como recomendación se indica que se suspende toda relación comercial con el mismo hasta poder verificar la información solicitada.

Procedimiento de reporte de la información:

- **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.

Procedimiento 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, el área de Finanzas deberá contar con 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.

Canal de Denuncias e Integridad:

El canal de integridad o denuncias, es un sistema implementado por Tecnodata que tiene como propósito principal proporcionar un canal de consultas, reclamos y/o denuncias. Mediante esta herramienta, los trabajadores, colaboradores, proveedores, socios comerciales, clientes y terceras personas interesadas de alguna de las empresas del Grupo pueden efectuar consultas, reclamos o denuncias respecto a conductas que podrían suponer un incumplimiento legal, del MPD, del Código de Ética o una posible comisión de alguno de los delitos referidos en la Ley 20.393.

- **Procedimiento de denuncia 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 recepcionar, 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.

- **Resultado de las Indagaciones:**

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 de 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.

Instrumentos Legales:

En el marco de las relaciones establecidas entre Tecnodata y sus trabajadores, deberán incluirse determinadas cláusulas en los instrumentos que las regulan, esto es, en los contratos de trabajo y en el Reglamento Interno de Orden, Higiene y Seguridad. La misma directriz aplicará a aquellos contratos que se suscriban con proveedores.

- **Cláusulas de Contrato de Trabajo:**

Todos los contratos de trabajo sean de carácter temporal o indefinido, deben necesariamente contar con una cláusula de cumplimiento, en virtud de la cual se verifique que los trabajadores conocen y se comprometen a no incurrir en las conductas constitutivas de aquellos delitos previstos en la Ley 20.393 y a actuar siempre en el desempeño de sus funciones, conforme a los principios y valores de CAP declarados en su Código de Integridad, cumpliendo la ley y la normativa interna.

- **Contratos de Prestación de Servicios:**

En los contratos de prestación de servicios con proveedores y/o contratistas se establecerá, mediante una cláusula o un anexo de contrato, que el cumplimiento al MPD y especialmente la prohibición de incurrir en las conductas constitutivas de los delitos previstos en la Ley 20.393 y la consiguiente adopción de medidas en orden a prevenirlas, es una más de sus obligaciones. Además, se establecerá que éstos deberán actuar conforme a la normativa vigente en materia de prevención de delitos, entre otras, y de acuerdo a las Bases Generales de Contratación de Servicios de Tecnodata S.A. (BGCS), así como la obligación de comunicar o denunciar cualquier hecho que pudiese ser relevante para efectos de prevenir la comisión de delitos de la Ley 20.393.

- **Reglamento Interno de Orden, Higiene y Seguridad ("RIOHS"):**

Es el documento que contiene obligaciones, prohibiciones y sanciones, al que deben sujetarse todos los trabajadores, en relación con sus labores, permanencia y vida en la empresa. En este contexto, el RIOHS deberá incorporar los referidos elementos en orden a prevenir los delitos previstos por la Ley 20.393. Debe hacer mención, además, a las políticas, procedimientos y estructuras que conforman el Sistema de Prevención de Delitos, como documentos cuyas directrices los trabajadores están obligados a cumplir.

Actividades de Prevención:

La finalidad de estas actividades es precaver eventuales incumplimientos al MPD y sus políticas y procedimientos relacionados, con el fin de prevenir conductas u omisiones inapropiadas que pudieran afectar su cumplimiento, por corresponderse con los delitos contemplados en la Ley 20.393

Formarán parte de las actividades de prevención:

- **Capacitación y Difusión:**

Es importante que todos los trabajadores comprendan y tengan claro los principales aspectos de la Ley 20.393 y el Programa de Cumplimiento de Tecnodata para implementar correctamente el Modelo de Prevención de Delitos (MPD). El MPD será comunicado y explicado a todo el personal, y se incluirá una cláusula relacionada en los contratos de trabajo y prestación de servicios.

Se llevarán a cabo capacitaciones periódicas para transmitir los conocimientos necesarios mínimos y se deja en manos del EPD la definición de la frecuencia de estas capacitaciones, considerando las necesidades específicas de la empresa, esto con la finalidad de integrar a la cultura corporativa el programa de integridad y cumplimiento que trae implícito el MPD.

Así el EPD en conjunto con la Subgerencia de Recursos Humanos, deberá velar por:

- La capacitación al menos anual de todos los trabajadores y colaboradores responsables de procesos en los cuales se identifiquen riesgos de comisión de los delitos contemplados en la Ley 20.393,respecto del funcionamiento del MPD, con sus correspondientes registros.
- La comunicación a todos los directores, ejecutivos, gerentes y colaboradores de la Compañía sobre la vigencia del MPD, así como sus posteriores modificaciones.
- El diseño e implementación de una estrategia de comunicación que permita difundir el MPD dentro de la Compañía, la cual además tendrá un fuerte foco en fomentar una cultura de integridad basada en valores.

La capacitación contendrá (sin que este listado sea taxativo) a lo menos los siguientes tópicos:

1. Definición de los delitos contemplados en la Ley 20.393.
2. Legislación sobre esta materia.
3. Rol y conocimiento del EPD.
4. Casos prácticos.
5. Referencia a políticas y/o procedimientos que forman parte del Sistema de Prevención de Delitos (por ejemplo, viajes, regalos, donaciones, conflictos de interés).
6. Cualquier otro que el EPD considere necesario.

El Encargado de Prevención de Delitos podrá usar a su arbitrio, sin ser obligatorio, los siguientes métodos al implementar el programa educativo de capacitación:

A. Con apoyo de medios proporcionados por Tecnodata S.A. como por asesoría externa de ser necesario, 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 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.

Gestión y Análisis de los Riesgos:

El EPD , solicitando apoyo de a las áreas críticas, identificará, analizará y evaluará los procesos o actividades de mayor riesgo o exposición a la comisión de los delitos indicados en la Ley N° 20.393, los que deberán quedar contemplados en una Matriz de Riesgos de Delitos (“MRD” o “Matriz”), la cual pertenece a sus funciones internas y la que se refleja en la Matriz de Riesgos de Tecnodata.

La identificación de las actividades y procesos expuestos a dichos riesgos se realizará a través de reuniones con todas las áreas clave y cargos de relevancia de la Empresa, incluyendo al EPD. Para esto, se deberá desarrollar un listado con los principales escenarios de riesgo de comisión de delitos contenidos en la Ley 20.393, los que serán incluidos en la MRD.

Esta Matriz tendrá como propósito visibilizar la evaluación de los riesgos existentes en la Compañía, incluyendo la estimación de su probabilidad, de ocurrencia y su impacto, los que determinarán el nivel de severidad del riesgo, tanto inherente, como residual, en este caso, una vez aplicados los controles mitigantes existentes que se incorporarán también a la Matriz, para finalmente y sobre la base de este, incorporar actividades de mejora continua, en caso de ser necesario

Para la gestión de riesgos comprendidos en la Matriz se deberá usar la metodología indicada bajo el estándar ISO 31.000 considerando las siguientes etapas:

- **Identificación de Riesgos:**

La identificación de las principales fuentes de riesgos de comisión de delitos de la Ley, así como aquellos roles y funciones en donde dicha exposición aumenta.

- **Evaluación de Riesgos:**

Basado en la norma ISO 31.000 los riesgos identificados deben evaluarse con el objetivo de determinar mayores exposiciones.

- **Identificación y Evaluación de Controles:**

Posterior a la identificación de riesgos se deberá identificar las actividades de control existentes que tengan un efecto compensatorio de riesgo. Esta actividad supone una interacción con las distintas áreas y funciones dentro de la Compañía para no solo obtener la descripción del control crítico, sino también la evidencia de su existencia. Se deberá, luego, evaluar la efectividad del diseño y control en relación con la exposición al riesgo. Dicha evaluación la hará el EPD con la gerencia, dueño o área responsable del control crítico.

Cabe señalar además, que los siguientes elementos deben considerarse en forma holística, para ver si mitigan razonablemente el riesgo inherente que resulta de la probabilidad de impacto y ocurrencia. Para cada control se debe identificar:

- Descripción de la actividad de control.
- Frecuencia.
- Responsable de la ejecución.
- Evidencia de sustento.
- Tipo de control (manual o automático).

La evaluación realizada permitirá concluir que el control:

- Mitiga razonablemente el riesgo de delito.
- No mitiga razonablemente el riesgo de delito.

Para todos los controles evaluados como “No mitiga razonablemente el riesgo de delito”, se debe implementar una actividad de control mitigante adicional. El diseño de una actividad de control, en cuyo proceso o actividad existe el riesgo, será implementado por el área dueña de dicha actividad o proceso, en conjunto con el EPD, siendo el área la responsable de su ejecución y aplicación. Con todo, en el diseño de las referidas actividades de control, deberá considerarse este Manual como documento de referencia.

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 20.393.

Entre las actividades de detección del MPD encontramos, a modo ejemplar, las siguientes:

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.

Recibida una denuncia, el EPD deberá realizar un análisis de ella, para identificar si está bajo el alcance del Modelo de Prevención de Delitos o se encuentra asociadas a escenarios de posible comisión de ilícitos de la Ley N°20.393.

b) Auditorías al Modelo: el EPD deberá, como parte de sus funciones propias, realizar anualmente un monitoreo que tenga por objeto verificar que los controles establecidos por el Modelo operan conforme su diseño. El objetivo de dicho monitoreo será acreditar la operación del MPD e identificar deficiencias que pudieran afectar su funcionamiento.

c) Revisión de Litigios: el EPD 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.

Los medios dispuestos son:
Canal de denuncias, al cual se accede por:
https://www.tecnodatasa.cl/denuncias/
Correo habilitado para denuncia directa a la siguiente casilla:
denuncias@tecnodatasa.cl

Actividades de respuesta:

El objetivo de las actividades de respuesta es establecer resoluciones, medidas disciplinarias y/o sanciones a quienes incumplan el MPD o bien ante la detección de indicadores de delitos de la Ley 20.393.
Como parte de las actividades de respuesta se debe contemplar la revisión de las actividades de control vulneradas, a fin de fortalecerlas o reemplazarlas por nuevas actividades de control. Además, el EPD deberá reevaluar, respecto del riesgo inherente, el grado de mitigación del mismo de forma posterior al incumplimiento de los controles.

A modo de ejemplo, las siguientes se consideran actividades de respuesta:

A) Denuncias a los órganos competentes:

Ante la detección de un hecho que pueda tipificarse como delito, el Encargado de Prevención de Delitos deberá evaluar, en conjunto con la Gerencia Legal de la Compañía, la posibilidad de efectuar acciones de denuncia ante los Tribunales de Justicia, Ministerio Público o Policía, con el fin de ejecutar las acciones legales en contra de quienes resulten responsables, con las sanciones penales y civiles que fijen los Tribunales de Justicia conforme a la legislación vigente.

B) Sanciones disciplinarias:

Las infracciones al MPD podrán ser categorizadas como una falta grave a las obligaciones que impone el Código de Integridad, el RIOHS y/o el Contrato de Trabajo. La Compañía podrá aplicar medidas disciplinarias ante el incumplimiento de las políticas y procedimientos de prevención de delitos o la detección de indicadores de potenciales ilícitos, tomando en consideración, además de lo permitido por la legislación laboral vigente, lo siguiente respecto de las medidas disciplinarias:

- Las sanciones deben ser proporcionales a la gravedad de la infracción comprobada.
- Deben ser consistentes con las políticas y procedimientos disciplinarios de Tecnodata, por ejemplo, el RIOHS.
- Las sanciones aplicadas lo serán a todas las personas o áreas involucradas en forma universal y uniforme.

C) Registro y seguimiento de denuncias y sanciones:

El EPD debe mantener un registro actualizado de denuncias, investigaciones (en curso y cerradas) y medidas disciplinarias aplicadas en relación con el incumplimiento al MPD o la detección de delitos (Ley 20.393), de acuerdo a lo que se establezca en el “Procedimiento de Denuncias”. Además, al menos semestralmente, el EPD o quien éste designe, debe efectuar un seguimiento a las denuncias.

D) Comunicación de sanciones y mejora de actividades de control del MPD, que presenten debilidades:

Como resultado de la investigación y resolución de los incumplimientos detectados del MPD, el EPD debe realizar lo siguiente:

- Evaluar la comunicación de las medidas disciplinarias adoptadas a todos los integrantes de la Compañía, respetando siempre el derecho a la privacidad de los involucrados.
- Resolver, en conjunto con el Comité de Integridad y Compliance y las Áreas de Apoyo, la conveniencia de comunicar las medidas disciplinarias a toda la Compañía, con el fin de difundir a los trabajadores y terceros involucrados, su firme compromiso de resguardar los principios y valores éticos declarados.
- Revisar las actividades de control vulneradas, a fin de aplicar mejoras en su diseño o implementar nuevas actividades de control. El EPD debe evaluar los riesgos y actividades de control infringidos en cada uno de los casos resueltos, para determinar la necesidad de establecer:

    - Nuevas actividades de control o,
    - Mejoras en las actividades de control que no operan efectivamente o cuyo diseño no es el adecuado.

Actividades de 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 EPD, dentro de sus funciones de seguimiento y evaluación del Modelo, realizará actividades de monitoreo. Para esto, el EPD puede solicitar apoyo a otras áreas de la organización, siempre que dichas áreas no estén involucradas en la actividad a ser revisada

El EPD puede llevar a cabo las siguientes actividades de monitoreo:

- 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.

En aquellas actividades de monitoreo donde se requiera determinar una muestra, el Encargado de Prevención de Delitos debe determinar y documentar el criterio a utilizar

Actualización del Modelo de Prevención del Delito:

Se debe efectuar, cuando sea pertinente, la actualización del Modelo de Prevención de Delitos luego de la realización del proceso de evaluación anual del diseño y efectividad operativa del mismo.

Para realizar la actualización del MPD, el Encargado de Prevención debe considerar:

- Nueva normativa aplicable.
- Cambios relevantes en la compañía y/o industria en la que se encuentra inserta.
- Seguimiento de las mejoras implementadas a las actividades de control.

En base a la información obtenida, cada el EPD debe actualizar la matriz de riesgos de la empresa y sus controles, así como también las políticas y procedimientos necesarios para garantizar un control efectivo.

Áreas de apoyo al Modelo de Prevención del Delito:

El objetivo de las áreas de apoyo es entregar soporte al EPD en las diligencias de prevención, detección, respuesta, supervisión y monitoreo que componen el MPD. Esto se puede reflejar entre otros, mediante la asesoría en la toma de decisiones, apoyo en la ordenación de actividades, entrega de información, etc.

Las actividades que ejecutará cada área de apoyo, en función de la operación del MPD serán las siguientes:

GERENCIA GENERAL

- Velar por la correcta implementación del Programa y el MPD, así como por su permanente adecuación y actualización.
- Respaldar permanentemente la gestión del EPD, garantizando que pueda acceder a la información y personas necesarias para el desarrollo de sus funciones.
- Informar al EPD de cualquier situación observada que pueda ser constitutiva de delito o bien, incumplimiento al MPD.
- Colaborar con la difusión del MPD, fomentando y creando espacios de comunicación, capacitación y concientización, con el fin de establecer una cultura basada en integridad y valores que parta desde el más alto líder de la Compañía y alcance a todos los trabajadores de Tecnodata.
- Comunicar la obligatoriedad de participar en las capacitaciones y actividades relativas al MPD.

COMITÉ DE ÉTICA

- 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 en 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 evalué el envío de la información al Ministerio Público.

DIRECTORIO

- Aprobar el Manual de Prevención de Delitos y MPD de la Compañía.
- Designar y remover al EPD y proveerle los medios para que cumpla con su cometido.
- Velar por la correcta implementación del Programa de Integridad y Compliance y el MPD.
- Recibir la rendición de cuentas e informe de gestión del EPD.
- Evaluar las eventuales denuncias a los organismos competentes.
- Informar al EPD de cualquier situación observada que pueda ser constitutiva de delito o bien, incumplimiento al MPD.

GERENCIA DE FINANZAS

- Entregar la información que requiera el EPD para el ejercicio de sus funciones.
- Ejecutar controles que sean de su competencia según la Matriz de Riesgos, y documentar y preservar la evidencia relativa a los mismos.
- Elaborar nuevos controles en caso de ser necesario, para superar las brechas identificadas producto de las investigaciones realizadas en relación con el MPD o cualquier riesgo nuevo identificado en el proceso de actualización de la Matriz.
- Presentar al Directorio y al Gerente General, con la asistencia del EPD, políticas, procedimientos o guías relativas a la administración de los recursos financieros, con el fin de evitar su uso en la comisión de delitos de la Ley.
- Definir, en conjunto con el EPD, una serie de controles preventivos vinculados al uso de los recursos financieros que puedan prevenir su mala utilización en la comisión de los delitos dispuestos en la Ley.

OTRAS GERENCIAS / ÁREAS

- Ejecutar controles tanto de carácter preventivo como detectivo, en las áreas que sean de su responsabilidad de acuerdo a la Matriz de Riesgos y, documentar y preservar la evidencia relativa a los mismos.
- Elaborar los controles necesarios para la remediación de las brechas identificadas producto de las investigaciones realizadas en relación al MPD o cualquier riesgo nuevo identificado.

COLABORADORES Y PRESTADORES DE SERVICIOS

- 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.

Actividades de exposición potencialmente riesgosas

En este apartado daremos pauta para tener en consideración algunos de los procedimientos, protocolos, reglas y medidas que conforman las mejores prácticas a las que deben sujetarse todos los trabajadores, colaboradores, ejecutivos, directores Tecnodata, así como los terceros, según se hayan sujetado a estos términos, en los distintos procesos, procedimientos o actividades que se desarrollen en relación con la Compañía que representen un mayor riesgo de comisión de delitos:

- **Conocimiento de terceros:**

Tecnodata desarrolla sus actividades generando interrelaciones con terceras partes, tales como proveedores y contratistas. Cada área respectiva que se relacione con dichos terceros, deberá incorporar en forma previa a la contratación, información que permita ejecutar una investigación o debida diligencia (i.e due diligence) a fin de cerciorarse que la persona o empresa, o alguno de sus dueños o representantes, no esté o haya estado involucrado en una investigación o haya sido sancionado por alguno de los delitos contemplados en la Ley 20.393, o bien, realice operaciones que pudiesen ser constitutivas de dichos delitos, esto con apoyo del Encargado de Prevención del Delito.

Si la relación con los proveedores, contratistas o clientes se hubiese establecido o acordado a través de un contrato, éste deberá incorporar explícitamente una referencia a la obligatoriedad del conocimiento del MPD, el cumplimiento de obligaciones y prohibiciones asociadas a éste en el marco de la ejecución del contrato, y otras declaraciones en relación con la Ley. Si no existiera, por el contrario, un contrato, se solicitará al tercero la firma de una declaración y las órdenes de compra deberán contener una mención del contenido antes señalado.

- **Selección de personal:**

Tecnodata mantendrá en todo momento un exigente procedimiento de selección y contratación de personal. Es política de la Compañía seleccionar y contratar, para los cargos que se encuentren disponibles, a las personas que reúnan los requisitos relativos a conocimientos, experiencia, habilidades, potencial de desarrollo, confiabilidad, probidad, orientación al servicio y que compartan los valores y la cultura organizacional.
Toda persona que ingresa a Tecnodata es sometida a un proceso de selección, administrado por Subgerencia de Recursos Humanos, quien, a su vez, realiza un proceso transparente y técnico de reclutamiento y selección de personal que permite disponer tanto en calidad, cantidad y oportunidad, del personal más idóneo para ocupar las vacantes requeridas.

- **Donaciones, auspicios y proyectos comunitarios:**

Toda actividad relacionada con donaciones, auspicios o proyectos comunitarios deberán ejecutarse evitando la existencia de posibles conflictos de interés con inversionistas, clientes, autoridades, trabajadores o colaboradores.

Además, siempre antes de efectuar una donación, auspicio o aporte para un proyecto comunitario se deberá al menos:

- Identificar los beneficiarios finales.

- Entender la labor que cumple en la comunidad la institución u organización no gubernamental beneficiaria de la donación, señalando, por ejemplo, el objetivo de la actividad y la utilización de los recursos entregados por Tecnodata.

- Revisar que la entidad receptora cuenta con todos los permisos y certificados vigentes como persona jurídica (no se entregarán aportes a personas naturales salvo en casos excepcionales).

- Identificar cualquier riesgo reputacional que se genere para Tecnodata por la entrega de la donación o auspicio. En particular, se deberá poner especial atención a aquellos casos en que los receptores del beneficio estén condenados, estén siendo actualmente investigadas o hayan sido vinculadas a la comisión de alguno de los delitos contemplados en la Ley 20.393.

- **Relación con funcionarios públicos:**

Podemos ocasionalmente compartir información con funcionarios públicos sobre temas que afectan tanto a las operaciones de la Compañía como a la industria en general. Este intercambio de información debe realizarse considerando siempre lo dispuesto en la normativa interna que regula la manera de relacionarnos con autoridades.

Si un colaborador de Tecnodata tiene dudas respecto a la calidad de funcionario público de una determinada persona, debe contactarse con el EPD. En todo caso, cuando existan dudas, debe considerar a la persona como funcionario público.

¿Qué se entiende por funcionario público?

Es cualquier persona que cumpla un cargo o función pública, sea en la administración central o en instituciones, empresas semifiscales, municipales, autónomas u organismos creados por el Estado o dependientes de él, aunque no sean estos nombramientos del Jefe de la República ni reciban sueldos estatales (artículo 260 Código Penal).
Al mismo tiempo, se deben reconocer, para efectos del MPD, no sólo los funcionarios públicos nacionales sino también los extranjeros, entendiendo por éstos últimos aquellos que desempeñan cargos o funciones públicas en otros países o en organismos internacionales (artículo 251 ter del Código Penal).

¿Qué se entiende por persona expuesta políticamente ? (PEP)

Según la Unidad de Análisis Financiero, UAF, en su Circular N°49, define como Personas Expuestas Políticamente (PEP) a "los chilenos o extranjeros que desempeñan o hayan desempeñado funciones públicas destacadas en un país, hasta a lo menos un año de finalizado el ejercicio de las mismas". Se incluyen en esta categoría a jefes de Estado o de un Gobierno, políticos de alta jerarquía, 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

¿Qué se entiende por Persona Influyente?

Es aquella persona que tiene autoridad o poder, y que eventualmente pudiera usarlo en beneficio o perjuicio de Tecnodata. Por ejemplo, presidentes de asociaciones gremiales.

En el marco de la interacción con las personas descritas en este apartado, Tecnodata no entregará contribuciones políticas de ningún tipo ni participará de campañas políticas. Frente a cualquier duda o consulta respecto a estas actividades, se deberá acudir al EPD, quien indicará las pautas mínimas de comportamiento y precisará la procedencia de la situación presentada para su discernimiento. Cada área involucrada en reuniones con funcionarios públicos deberá registrar sus reuniones e informarlas al EPD por medio de un correo donde detalle:

- Individualización de la persona con quien se tiene la reunión.
- Identificación a que entidad pertenece.
- Registro de los temas a tratar.
- Indicación de Fecha y lugar de la reunión.

- **Relación con proveedores y prestadores de servicio:**

Los procesos de contratación de proveedores o prestadores de servicios iniciados por Tecnodata, deberán comprender una debida diligencia, con el objetivo de identificar los riesgos derivados de la contratación con el/los potenciales proveedores que participen en el proceso. De la misma forma, deberán respetarse siempre los términos, plazos y condiciones establecidos en las respectivas bases generales de contratación de servicios, tanto durante el transcurso de los procesos como luego de su contratacion, evitando así cualquier conducta que pudiera ser interpretada como cohecho o corrupción entre particulares, En todo momento se debe dar cumplimiento a lo indicado en el presente MPD sobre relacionamiento tanto con funcionarios públicos, así como con cualquier tercero que pudiera originar un conflicto de interés o una conducta constitutiva de corrupción entre particulares.

Las Bases Generales de Contratación es un documento creado con el fin de apoyar al MPD con regulaciones básicas en lo que comprende el proceso de relacionamiento de Tecnodata con proveedores y prestadores de servicios, siendo su aplicación un complemento al presente modelo y su funcionamiento . Todo prestador de servicios debe aceptar su conocimiento y se adscribirá a el mediante un anexo que deberá quedar digitalizado y archivado en el área legal de la empresa.

- **Operación en contexto de epidemia o pandemia.**

En el marco del desarrollo de una pandemia, epidemia o contagio y mientras deban mantenerse las medidas de seguridad asociadas a su prevención, estas deberán respetarse siempre en el mejor interés de la salud de los trabajadores de Tecnodata.

Para ello, deberán acatarse las instrucciones impartidas por la autoridad sanitaria, muy especialmente en relación a la obligación de cumplimiento de cuarentenas, ya sean obligatorias o preventivas.

De la misma forma, para el caso de la pandemia asociada al COVID 19, la Compañía ha adoptado medidas que deberán ser respetadas por todos los trabajadores con una finalidad preventiva del contagio, y comunicadas de forma clara y oportuna. Entre ellas cuentan, el Procedimiento y Protocolo en caso de COVID-19 positivo, y Protocolo de Notificación de casos positivos , los que se encontrarán vigentes hasta que la emergencia sanitaria haya sido superada y la autoridad competente así lo determine.

En el caso de futuras situaciones de emergencia sanitaria, la Compañía adoptará las medidas preventivas de contagio que resulten pertinentes de acuerdo a las características de la epidemia o pandemia, y que se sujeten al cumplimiento de las directrices que establezca la autoridad sanitaria.

Infracción de la Ley en Materia penal y Sanciones Corporativas:

Es responsabilidad de todos los trabajadores y/o colaboradores de Tecnodata conocer el contenido del Manual, debiendo en todo momento regirse por sus directrices. El EPD procurará el acceso al conocimiento de este Manual. Los trabajadores deberán informar las contravenciones observadas del Modelo de Prevención a sus supervisores o al EPD, a través de los mecanismos de denuncias existentes señalados en este Manual.

Los trabajadores de Tecnodata deberán ser conscientes de que podrían ser objeto de investigaciones internas, si es que existe algún indicio, o se recibió alguna denuncia que diga relación con la comisión de alguno de los delitos contemplados en la Ley 20.393 o con el incumplimiento de la normativa interna de la Compañía en relación con ésta. Los trabajadores deberán prestar toda su colaboración en los procedimientos internos de investigación que sean llevados a cabo dentro del marco de MPD.

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 y sus posteriores actualizaciones, realizada en el desempeño de sus funciones o con ocasión de éstas, se considerará como falta de probidad grave del colaborador. En el caso de los asesores, contratistas o proveedores, el incumplimiento de los términos de este Manual será causal de término inmediato del contrato que se mantenga vigente.

Las sanciones que se apliquen por el incumplimiento del presente Manual serán determinadas por el Encargado de Prevención, conjuntamente con el Comité de Ética, según sea el caso, y siempre de acuerdo a la legislación laboral vigente.

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 querella criminal en contra de los supuestos responsables del hecho delictivo, previo informe del Encargado de Prevención de Delitos

Las políticas y procedimientos indicados en este Manual, en el Código de Integridad y en los demás documentos relacionados con el MPD son de cumplimiento obligatorio y se incorporan tanto a las funciones como a las responsabilidades asignadas a cada colaborador de Tecnodata. Así, su incumplimiento conlleva las sanciones previstas en el RIOHS sin perjuicio de las sanciones civiles y penales que pudieran corresponder en cada caso. La misma obligación de colaboración será exigida a los asesores, proveedores y contratistas, de lo que se dejará constancias en los respectivos contratos o acuerdos que al respecto se puedan suscribir

Vigencia y Actualización del MPD

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.

El presente Manual constituye únicamente una guía y no reemplaza la prudencia y buen criterio de los trabajadores y colaboradores de la Compañía que deban tener en todo momento en el desarrollo de sus funciones.

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

CONTROL DE CAMBIOS	
Número de versión	Fecha
v. Zero	Agosto 2019
v. 01	Agosto 2020
v. 02	Septiembre 2021
v. 03	Septiembre 2022
v. 04	Septiembre 2023
v. 05	Febrero 2024

TECNODATA S.A.