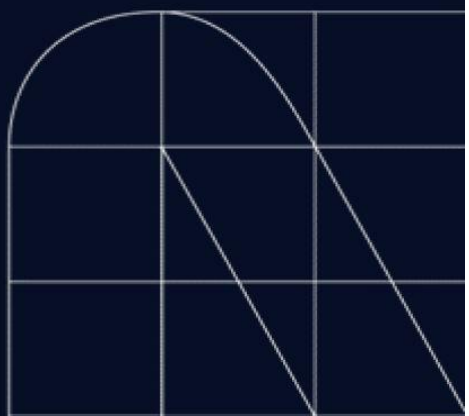
MANUAL DE PREVENCIÓN DE DELITOS

LEY N°20.393 DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

ÍNDICE DE CONTENIDO



1. INTRODUCCIÓN, ÁMBITO Y ALCANCE DE APLICACIÓN DE ESTE MANUAL

La Ley 20.393, que entró en vigencia en Chile el año 2009, establece y regula la responsabilidad penal de las personas jurídicas en relación con los delitos especificados en su primer artículo. Posteriormente, la publicación de la Ley N°21.595 sobre Delitos Económicos y Medioambientales introdujo un marco legal más estricto en el ámbito económico, aumentando tanto la cantidad como la severidad de los riesgos legales, y endureciendo las sanciones para los incumplimientos normativos de personas y empresas.

Las personas jurídicas son penalmente responsables de los delitos mencionados cuando éstos son cometidos en el contexto de su actividad por, o con la intervención de una persona natural que tenga un cargo, función, posición en ella, o le preste servicios gestionando asuntos suyos ante terceros con o sin su representación. Esto aplica siempre y cuando la comisión del delito se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de delitos por parte de la persona jurídica. En consecuencia, la ley exime de responsabilidad penal a las personas jurídicas que implementen oportunamente un Modelo de Prevención de Delitos, es decir, un modelo de organización, administración y supervisión destinado a prevenir, evitar y detectar la comisión de delitos.

Cabe destacar que la responsabilidad penal de la persona natural que comete el acto indebido es perseguida individualmente por el Ministerio Público, independientemente del proceso penal al que pueda ser sometida la persona jurídica.

La persona jurídica no será penalmente responsable cuando el hecho punible se perpetre exclusivamente en contra de la propia persona jurídica.

Ante la expansión de las conductas que pueden conllevar responsabilidad penal para una empresa, se ha llevado a cabo un análisis de las operaciones de NTT DATA CHILE S.A. (en adelante, "La Empresa") y se ha estudiado la industria en la que opera, con el fin de identificar los riesgos relevantes de incumplimiento y establecer controles mitigantes efectivos. De este modo, se busca proporcionar una base sólida para las actividades de adaptación de la empresa a este cambio legislativo, fomentando una cultura en la que la integridad sea un componente esencial de su operación.

Como aproximación metodológica y tras el análisis de los antecedentes, se definieron las contingencias penales que pueden afectar con mayor probabilidad al giro y actividad

de NTT DATA CHILE S.A.: corrupción entre particulares, cohecho, delitos informáticos, lavado de activos, receptación, delitos tributarios, laborales y previsionales, apropiación indebida, delitos contra la libre competencia, secretos comerciales, delitos contemplados en la Ley de Sociedades Anónimas y riesgos comunes a las actividades económicas en general como la administración desleal, falsedades documentales, entre otros.

Forman parte integral del Modelo de Prevención de NTT DATA Chile S.A. las sociedades relacionadas NTT DATA Chile Centers Ltda. y NTT DATA Chile BPO Servicios Profesionales, Técnicos y Tecnológicos Ltda., en adelante conjuntamente como "las Sociedades", NTT DATA CHILE o la "persona jurídica".

2. ELEMENTOS CENTRALES DEL MODELO DE PREVENCIÓN

De acuerdo con el artículo 4° de la Ley N°20.393, se entenderá que un Modelo de Prevención de Delitos efectivamente implementado por la persona jurídica es adecuado para los efectos de eximirla de responsabilidad penal cuando, en la medida exigible a su objeto social, giro, tamaño, complejidad, recursos y a las actividades que desarrolle, considere seria y razonablemente los siguientes aspectos:

- La identificación de las actividades o procesos de la persona jurídica que impliquen riesgo de conducta delictiva.

- El establecimiento de protocolos y procedimientos para prevenir y detectar conductas delictivas en el contexto de las actividades a que se refiere el punto anterior, los que deben considerar necesariamente canales seguros de denuncia y sanciones internas para el caso de incumplimiento.

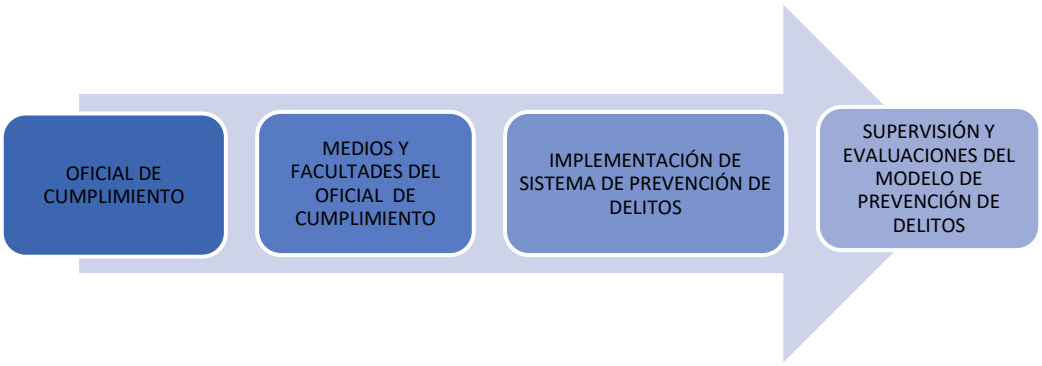
- Estos protocolos y procedimientos, incluyendo las sanciones internas, deberán comunicarse a todos los trabajadores e incorporarse expresamente en los respectivos contratos de trabajo y de prestación de servicios de todos los trabajadores, empleados y prestadores de servicios de la persona jurídica, incluidos sus máximos ejecutivos.

- La asignación de uno o más sujetos responsables de la aplicación de dichos protocolos, con la adecuada independencia, dotados de facultades efectivas de dirección y supervisión, acceso directo a la administración de la persona jurídica para informarla oportunamente de las medidas y planes implementados en el cumplimiento de su cometido, y para rendir cuenta de su gestión y requerir la adopción de medidas necesarias para su cometido que pudieran ir más allá de su competencia. La persona jurídica deberá proveer al o a los responsables de los

recursos y medios materiales e inmateriales necesarios para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la persona jurídica.

- La previsión de evaluaciones periódicas por terceros independientes y mecanismos de perfeccionamiento o actualización a partir de tales evaluaciones.

CUADRO 1: SINOPSIS DE UNA PREVENCIÓN DE DELITOS EFECTIVA



En conformidad con dicha normativa, NTT DATA CHILE, S.A. ha implementado un Modelo de Prevención de Delitos, en adelante también referido como el "Modelo de Prevención" o el "Modelo", para asegurar el cumplimiento de las regulaciones nacionales e internacionales sobre políticas de prevención de delitos, especialmente aquellas contenidas en la Ley N° 20.393. Este Modelo de Prevención, incluye las siguientes herramientas principales:

1. Protocolos, políticas y procedimientos definidos para ejercer como controles mitigantes de los riesgos de comisión de delitos identificados en la matriz de riesgos de las Sociedades.
2. Una Matriz de riesgos de delitos y sus controles asociados.
3. El Código de Ética y Conducta Profesional y las Políticas globales de cumplimiento normativo de Grupo NTT DATA..
4. Un Título relativo al Modelo de Prevención en el Reglamento Interno de Orden, Higiene y Seguridad.
5. Cláusulas contractuales especiales en contratos de trabajo y contratos con proveedores.
6. Plan de capacitación y comunicación dirigido a todos los trabajadores y

colaboradores de NTT DATA CHILE.
7. Plan de seguimiento y monitoreo del Modelo de Prevención de Delitos.
8. Un canal de denuncias (Whistleblowing System) y procedimientos asociados.
9. El presente Manual, que contiene el Modelo de Prevención de NTT DATA CHILE frente a los delitos contemplados en el artículo 1° de la Ley 20.393, diseñado para asegurar que la Compañía cumple con la normativa nacional e internacional sobre políticas de prevención de delitos.

Los objetivos de este Manual son:

1. Dar a conocer las actividades y procedimientos necesarios para la efectiva implementación y operación del Modelo de Prevención de Delitos de NTT DATA CHILE.
2. Dar a conocer las pautas para la prevención y mitigación de los riesgos de delitos a los cuales NTT DATA CHILE se encuentra expuesta.
3. Dar a conocer las actividades del Modelo de Prevención de Delitos, bajo responsabilidad del Encargado de Prevención de Delitos en cumplimiento de sus funciones de supervisión, las cuales deben orientarse a la eficacia y eficiencia del Modelo en el tiempo.
4. Dar cumplimiento estricto a los requisitos establecidos por la Ley 20.393 para los modelos de prevención de delitos. En este sentido, busca establecer los principales procedimientos y actividades conducentes a la efectiva implementación del modelo descrito, y la sostenibilidad de éste en el tiempo.
5. Instaurar una cultura de respeto a los derechos fundamentales de los colaboradores y la transparencia en todos los procesos de NTT DATA CHILE.
6. En general, entregar normas respecto de las mejores prácticas para prevenir la realización de actividades que puedan constituir alguno de los delitos contemplados en el artículo 1° de la Ley 20.393.

3. MARCO LEGAL DE LA LEY N°20.393 DE RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

La Ley N°20.393 establece la responsabilidad penal de las personas jurídicas respecto de los delitos señalados en su artículo primero y regula el procedimiento aplicable a la investigación y establecimiento de la responsabilidad penal de una persona jurídica, la determinación de las sanciones procedentes y la ejecución de éstas.

Por su parte, la Ley N°21.595 de Delitos Económicos que modifica la Ley N°20.393 y otros cuerpos legales, sistematiza los delitos económicos y los atentados contra el medio ambiente, adecúa las penas aplicables y establece un nuevo estatuto normativo para este tipo de delitos.

Se debe hacer especial mención respecto a que en el concepto de persona jurídica caben no sólo las entidades de derecho privado con o sin fines de lucro, sino que también las empresas públicas creadas por ley; las empresas, sociedades y universidades del Estado; los partidos políticos; las fundaciones y las personas jurídicas religiosas de derecho público.

ACTIVIDADES CON RIESGOS RELEVANTES PARA NTT DATA CHILE

- **LAVADO DE ACTIVOS**

  El delito de lavado de activos está tipificado en el artículo 27 de la ley 19.913 y requiere de un delito precedente que genere los fondos que se intentan lavar. El lavado de activos consiste en ocultar o disimular el origen ilícito de dinero o bienes, por provenir éstos de un delito anterior, o de mantener tales activos, de origen ilícito, en su poder.

  Para que exista la figura penal de lavado de activos se requiere que los activos que se pretenden lavar provengan de algunos de los delitos señalados en el artículo 27 de la Ley N°19.913.

- **COHECHO A EMPLEADO PÚBLICO**

  El cohecho a empleado público nacional, tipificado en el artículo 251 bis del Código Penal, es la acción de ofrecer, dar o consentir en dar un beneficio económico o de otra naturaleza a un empleado público, en razón de su cargo o para que realice ciertas acciones u omisiones, o por haberlas realizado. Este acto está sancionado con penas de multa e inhabilitación, y, dependiendo de la gravedad, con reclusión.

  El cohecho a funcionario público extranjero, tipificado en el artículo 251 bis del Código Penal, es el acto de ofrecer, prometer, dar o consentir en dar un beneficio económico o de otra naturaleza a un funcionario público extranjero para obtener o mantener una ventaja en cualesquiera transacciones internacionales de una actividad económica desempeñada en el extranjero. Ambos tipos de cohecho comparten normas comunes, que establecen inhabilitaciones y penas agravadas para ciertos casos y excluyen los mínimos de las penas en situaciones específicas. Además, se excluyen como delitos los donativos oficiales o protocolares de escaso

valor autorizados por la costumbre, salvo en ciertos casos relacionados con funcionarios públicos extranjeros.

- **CORRUPCIÓN ENTRE PARTICULARES**

  La corrupción entre particulares o soborno entre particulares, sancionada en los artículos 287 bis y 287 ter del Código Penal, es el delito que sanciona a los que soliciten, acepten recibir, den, ofrezcan o consientan en dar un beneficio económico o de otra naturaleza para favorecer, en el ejercicio de sus labores, la contratación con un oferente sobre otro. En términos simples, se trata de una figura muy similar a la del cohecho, pero en la que no participa un funcionario público, si no que se da entre dos particulares. Por ejemplo, en un proceso de negociación entre dos empresas, el ejecutivo de la empresa A da dinero al ejecutivo de la empresa B para cerrar un contrato.

- **APROPIACIÓN INDEBIDA**

  La apropiación indebida está contemplada en el artículo 470 N° 1 del Código Penal y corresponde, esencialmente, a la conducta de apropiarse o no restituir bienes muebles que han sido recibidos en administración u otro título que obligue a devolverlos o entregarlos.

- **ADMINISTRACIÓN DESLEAL**

  La Ley N° 21.121 incorporó el delito de administración desleal al Código Penal y lo agregó como un delito base de la Ley N° 20.393. Este delito, tipificado en el numeral 11 del artículo 470 del Código Penal, se comete cuando una persona a cargo de la salvaguarda o gestión del patrimonio de otra causa perjuicio a dicho patrimonio.
  Esto ocurre si se abusan de las facultades para disponer por cuenta del titular del patrimonio o para obligarlo, o si se realiza u omite cualquier acción de manera claramente contraria a los intereses del titular del patrimonio afectado.

- **DELITOS INFORMATICOS**

  La Ley N° 21.459, incorporó nuevos delitos al artículo 1 de la Ley N° 20.393. Esta Ley moderniza los tipos penales para adaptarlos a las nuevas formas de delitos

informáticos y avances tecnológicos, cubriendo riesgos no contemplados por la legislación anterior.

Los delitos contemplados en esta ley son los tipificados en sus artículos 1° a 8° y corresponden a los siguientes:

1. Ataque a la integridad de un sistema informático: Consiste en obstaculizar o impedir el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos.

2. Acceso ilícito: Acceder a un sistema informático, sin autorización o excediendo la autorización y superando barreras técnicas o medidas tecnológicas de seguridad.

3. Interceptación ilícita: Interceptar, interrumpir o interferir indebidamente, por medios técnicos, la transmisión no pública de información en un sistema informático. También se tipifica la captación de datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, sin la debida autorización.

4. Ataque a la integridad de los datos informáticos: Alterar, dañar o suprimir datos informáticos, siempre que cause un grave daño a su titular.

5. Falsificación informática: Considera el introducir, alterar, dañar o suprimir indebidamente datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.

6. Receptación de datos informáticos: Se refiere a comercializar, transferir o almacenar, con un fin ilícito, datos informáticos, conociendo o debiendo conocer su origen, provenientes de la realización de las conductas descritas en a), b) y e), anteriores.

7. Fraude informático: Manipular un sistema informático, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático.

8. Abuso de los dispositivos: Entregar u obtener para su utilización, importar, difundir o poner a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o

adaptados para la perpetración de los delitos previstos en los artículos a), b), c) y d), señalados precedentemente, y las conductas señaladas en el artículo 7° de la ley N° 20.009 (aquellas que constituyen delito de uso fraudulento de tarjetas de pago y transacciones electrónicas).

- **DELITOS CONTEMPLADOS EN LA LEY DE SOCIEDADES ANÓNIMAS (LEY n°18.046)**

  Los delitos contemplados en la Ley de Sociedades Anónimas, entre otros, incluyen la entrega o aprobación de información falsa en memorias, balances u otros documentos destinados a socios, terceros o a la administración. Además, se considera delito colaborar con terceros que entreguen dicha información falsa en los mismos tipos de documentos. También se tipifica como delito adoptar acuerdos abusivos para beneficio personal o de otros en particular, sin reportar un beneficio a las sociedades.

- **DELITOS CONTRA LA LIBRE COMPETENCIA DE LOS MERCADOS (DL 211)**

  El Decreto Ley 211 fija normas para la defensa de la libre competencia con el fin de supervisar los mercados y promover una competencia activa. Para ello, establece restricciones a la libertad de actuación de los agentes del mercado, quienes, en su búsqueda de maximizar ganancias, pueden ignorar el marco legal para obtener mayores beneficios. Estas prácticas distorsionan el funcionamiento normal de los mercados, fomentan la concentración de la riqueza, limitan la libertad de otros participantes y perjudican el bienestar de los consumidores. La regulación en libre competencia busca prevenir conductas perjudiciales, como acuerdos entre competidores para fijar precios, limitar la producción, dividir mercados y afectar licitaciones.

- **DELITOS TRIBUTARIOS**

  Como todas las personas jurídicas de derecho privado, NTT DATA CHILE puede incurrir en delitos tributarios que incluyen, entre otros, la presentación engañosa de declaraciones, emisión de información falsa para evadir impuestos, manipulación de registros contables, uso indebido de documentos tributarios, operaciones ilegales, violación de clausuras tributarias, destrucción de sellos

tributarios, y acciones para obtener beneficios tributarios de manera fraudulenta, entre otras.

4. RESPONSABILIDAD PENAL DE LA EMPRESA Y MODELOS DE PREVENCIÓN

Finalmente, y respecto de la imputación de responsabilidad penal a la persona jurídica, el artículo 3° de la Ley N° 20.393 dispone que: "Una persona jurídica será penalmente responsable por cualquiera de los delitos señalados en el artículo 1°, perpetrado en el marco de su actividad por o con la intervención de alguna persona natural que ocupe un cargo, función o posición en ella, o le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, siempre que la perpetración del hecho se vea favorecida o facilitada por la falta de implementación efectiva de un modelo adecuado de prevención de tales delitos, por parte de la persona jurídica".

"Si concurrieren los requisitos previstos en el inciso anterior, una persona jurídica también será responsable por el hecho perpetrado por o con la intervención de una persona natural relacionada en los términos previstos por dicho inciso con una persona jurídica distinta, siempre que ésta le preste servicios gestionando asuntos suyos ante terceros, con o sin su representación, o carezca de autonomía operativa a su respecto, cuando entre ellas existan relaciones de propiedad o participación. Lo dispuesto en este artículo no tendrá aplicación cuando el hecho punible se perpetre exclusivamente en contra de la persona jurídica".

SANCIONES PENALES EN LA LEY N°20.393

La Ley N°20.393, establece penas a las personas jurídicas para los casos en que se establezca su responsabilidad penal en alguno de los delitos contemplados expresamente por ella, sanciones que pueden ir desde la pérdida de beneficios fiscales, altas multas bajo el sistema de días-multa, o prohibición de celebrar contratos con el Estado u organismos del Estado, hasta la disolución o cancelación de la personalidad jurídica.

5. EL ENCARGADO DE PREVENCIÓN

5.1. DESIGNACIÓN

El numeral 3 del artículo 4° de la Ley N°20.393 señala que, se entenderá que un modelo de prevención de delitos efectivamente implementado por la persona jurídica es adecuado para eximirla de responsabilidad penal cuando, considere seria y razonablemente la

asignación de "*uno o más sujetos responsables de la aplicación de los protocolos, con la adecuada independencia, dotados de facultades efectivas de dirección y supervisión y acceso directo a la administración de la persona jurídica para informarla oportunamente de las medidas y planes implementados en el cumplimiento de su cometido, para rendir cuenta de su gestión y requerir la adopción de medidas necesarias para su cometido que pudieran ir más allá de su competencia (…)*"

En NTT DATA CHILE, las funciones del sujeto responsable recaerán en el Encargado de Prevención de Delitos (EPD), quien deberá cumplir con los siguientes requisitos:

- Haber sido designado por el directorio.
- Contar con autonomía en su actuar.
- Contar con recursos y medios materiales e inmateriales provistos por la dirección para realizar adecuadamente sus labores, en consideración al tamaño y capacidad económica de la persona jurídica.
- Contar con acceso directo al directorio.

El directorio de NTT DATA CHILE designará a su Encargado de Prevención, el que durará hasta tres años en el cargo, pudiendo ser reelegido por periodos de igual duración.

El Encargado de Prevención designado poseerá cabal conocimiento de:

- Las funciones y los responsables de cada área de la empresa
- La legislación y la normativa emanada de las autoridades reguladoras
- El presente Manual de Prevención
- El Reglamento Interno de Orden, Higiene y Seguridad
- La matriz de riesgos de los delitos contemplados en la Ley N°20.393
- El plan de capacitación y difusión dirigido a todos los trabajadores y colaboradores de NTT DATA CHILE, el plan de seguimiento y monitoreo de las actividades propias del Modelo de Prevención.

- El plan de seguimiento y monitoreo de las actividades propias del Modelo de Prevención.

5.2. MEDIOS, FACULTADES Y FUNCIONES DEL ENCARGADO DE PREVENCIÓN

El Encargado de Prevención gozará, en el ejercicio de sus funciones, de autonomía respecto del directorio y las gerencias de la empresa. Para mantener dicha cualidad como característica esencial de su cargo, el Encargado de Prevención contará con un presupuesto especialmente asignado para llevar a efecto sus funciones.

Por otra parte, el Encargado de Prevención de NTT DATA CHILE, tendrá las siguientes facultades y funciones:

1. Ejercer el rol de Encargado de Prevención de acuerdo a lo establecido en la Ley N°20.393.
2. Proponer al directorio un modelo de prevención de aquellos delitos a los cuales se refiere la Ley N° 20.393, que contemple, a lo menos, los elementos establecidos en el artículo 4° número 3, de dicha ley.
3. Determinar, y requerir al directorio, los medios y recursos necesarios para lograr cumplir con su rol y responsabilidades.

4. Liderar el correcto establecimiento y operación del Modelo de Prevención de Delitos desarrollado e implementado por la Empresa.
5. Identificar los riesgos asociados a los delitos de la Ley Nº 20.393, así como definir los controles que permitan prevenir la comisión de éstos.
6. Reportar al directorio, a lo menos semestralmente y/o cuando las circunstancias lo ameriten, informando, a través del medio que se considere más adecuado, de las medidas y planes implementados en el cumplimiento de sus funciones.
7. Velar que se dé cumplimiento, por las áreas correspondientes, a los controles y se desarrollen las políticas y procedimientos necesarios requeridos por el Modelo de Prevención de Delitos y sugerir, desarrollar e implementar cualquier otra política y/o procedimiento que estime necesario para complementar el modelo existente.
8. Fomentar que los procesos con riesgo de comisión de delitos en NTT DATA CHILE cuenten con controles de prevención y mantener evidencia del cumplimiento y ejecución de estos controles.
9. Velar por la existencia de procesos de administración de recursos financieros y de procedimientos de auditoría de éstos.
10. Evaluar, permanentemente, la eficacia y vigencia del Modelo de Prevención de Delitos adoptado y su conformidad con las leyes y demás regulaciones, informando al directorio respecto de la necesidad o conveniencia de su modificación.
11. Velar por la actualización de este Manual y del Modelo de Prevención de Delitos, de acuerdo con los cambios normativos y el entorno de negocios de la persona jurídica.
12. Proponer al directorio los métodos más idóneos para la aplicación efectiva del

Modelo de Prevención de Delitos y su supervisión, tales como:

- Actividades de difusión y de capacitación a los trabajadores de la Empresa, respecto del Modelo de Prevención de Delitos, sus componentes, así como las materias bajo el alcance de la Ley N° 20.393.
- Seguimiento de los resultados de acciones relacionadas con el catálogo de delitos de la Ley N° 20.393.
- Revisiones periódicas de los procesos y documentación de aquellas áreas que revisten mayor riesgo de incumplimiento, dejando testimonio escrito de cada una de sus actuaciones, priorizando aquellos procesos con mayor probabilidad de ocurrencia o impacto según la respectiva matriz de riesgo.

13. Tomar conocimiento, y efectuar un análisis, de todo caso sospechoso de constituir delito de la Ley N°20.393 y, de considerarlo necesario, elevar dicho caso al directorio. A efectos del análisis, deberá recabar toda la documentación relacionada con esa operación, generando para tales efectos un archivo de antecedentes.
14. Documentar y custodiar la evidencia relativa a las actividades de prevención de delitos.
15. Liderar el proceso de revisión del Modelo de Prevención de Delitos por parte de un tercero independiente.
16. Efectuar la implementación o el seguimiento de las recomendaciones que emanen del proceso de revisión del tercero independiente.
17. Intervenir, cuando corresponda, en las demandas, denuncias o gestiones judiciales que decida emprender NTT DATA CHILE en relación a los delitos señalados en la Ley N° 20.393 y aportar todos los antecedentes que mantenga en su poder o de los cuales tuviere conocimiento en razón de su función.
18. Realizar trabajos especiales que el directorio le encomiende en relación con las materias de su competencia.
19. Capacitarse continuamente en términos de actualizar y perfeccionar sus conocimientos y otras habilidades, especialmente en cuanto a modificaciones en las leyes nacionales y buenas prácticas empresariales.

6. ÁREAS DE APOYO AL ENCARGADO DE PREVENCIÓN

El objetivo de las áreas de apoyo es entregar asistencia y soporte al Encargado de Prevención en las actividades de prevención, detección, respuesta y monitoreo que componen el Modelo de Prevención de NTT DATA CHILE. Esto se puede materializar mediante la asesoría en la toma de decisiones, apoyo en la coordinación de actividades, entrega de información, entre otros. De vital importancia como apoyo al Encargado de Prevención se encuentran los siguientes órganos y áreas:

- Comité Global de Cumplimiento Normativo y Prevención Legal (Comité Global de Cumplimiento)
- Comisión de Auditoría
- Área Legal & Tax Advisory
- Área Financial Services
- Área de Seguridad de la información
- Área de Ciberseguridad

7. DIAGNÓSTICO DE RIESGOS

El diagnóstico de riesgos es el proceso a través del cual se identifican las actividades, procesos y negocios expuestos al riesgo de la comisión de los delitos contemplados en el artículo 1° de la Ley 20.393. Las actividades y procesos de riesgo identificados son vaciados en una Matriz de Riesgos, en la cual se muestra también el nivel de riesgo que se ha determinado para cada uno de estos procesos o actividades identificados.

7.1 MATRIZ DE RIESGOS

La matriz de riesgo es una herramienta que identifica los potenciales riesgos de comisión de los delitos contemplados en la Ley N°20.393 en las que NTT DATA CHILE, potencialmente, podría verse involucrada durante el desarrollo normal de sus actividades.

La identificación de riesgos es liderada por el Encargado de Prevención quien, con la participación de los cargos más altos de la administración de la Empresa, deberá analizar los principales escenarios de riesgo de comisión de los delitos señalados en la Ley Nº20.393.

CUADRO 2: PROCEDIMIENTO DE IDENTIFICACIÓN Y REACCIÓN ANTE RIESGOS

La identificación, análisis y evaluación del riesgo de comisión de dichos delitos deberán quedar plasmados en una Matriz de Riesgos que deberá ser revisada anualmente o cuando sucedan modificaciones importantes en la regulación o las condiciones de operación de la Empresa.

El proceso de diagnóstico de riesgos comprende también el análisis de la probabilidad de que se produzca un evento de riesgo y el impacto que esto tendría para la organización. La probabilidad de ocurrencia y el impacto se combinan indicando el nivel o severidad del riesgo.

Para el análisis de riesgos de los procesos de NTT DATA CHILE se han utilizado las tablas de valores que se muestran a continuación:

TABLA 1: VALORACIÓN DE PROBABILIDAD

TABLA DE VALORACIÓN DE PROBABILIDAD		
Categoría	Valor	Descripción
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente. (90% a 100%).
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente.

TABLA 2: VALORACIÓN DE IMPACTO

TABLA DE VALORACIÓN DE IMPACTO		
Categoría	Valor	Descripción
Catastrófico	5	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto catastrófico en el presupuesto y/o comprometen totalmente la imagen pública de la organización. Su materialización dañaría gravemente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo finalmente que estos se logren.
Mayor	4	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto importante en el presupuesto y/o comprometen fuertemente la imagen pública de la organización. Su materialización dañaría significativamente el desarrollo del proceso y el cumplimiento de los objetivos, impidiendo que se desarrollen total o parcialmente en forma normal.
Moderado	3	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto moderado en el presupuesto y/o comprometen moderadamente la imagen pública de la organización. Su materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle parcialmente en forma normal.
Menor	2	Riesgo cuya materialización puede generar pérdidas financieras ($) que tendrán un impacto menor en el presupuesto y/o comprometen de forma menor la imagen pública de la organización. Su materialización causaría un bajo daño en el desarrollo del proceso y no afectaría el cumplimiento de los objetivos.
Insignificante	1	Riesgo cuya materialización no genera pérdidas financieras ($) ni compromete de ninguna forma la imagen pública de la organización. Su materialización puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afectaría el cumplimiento de los objetivos.

Por otra parte, la combinación de probabilidad e impacto permite definir la severidad (o

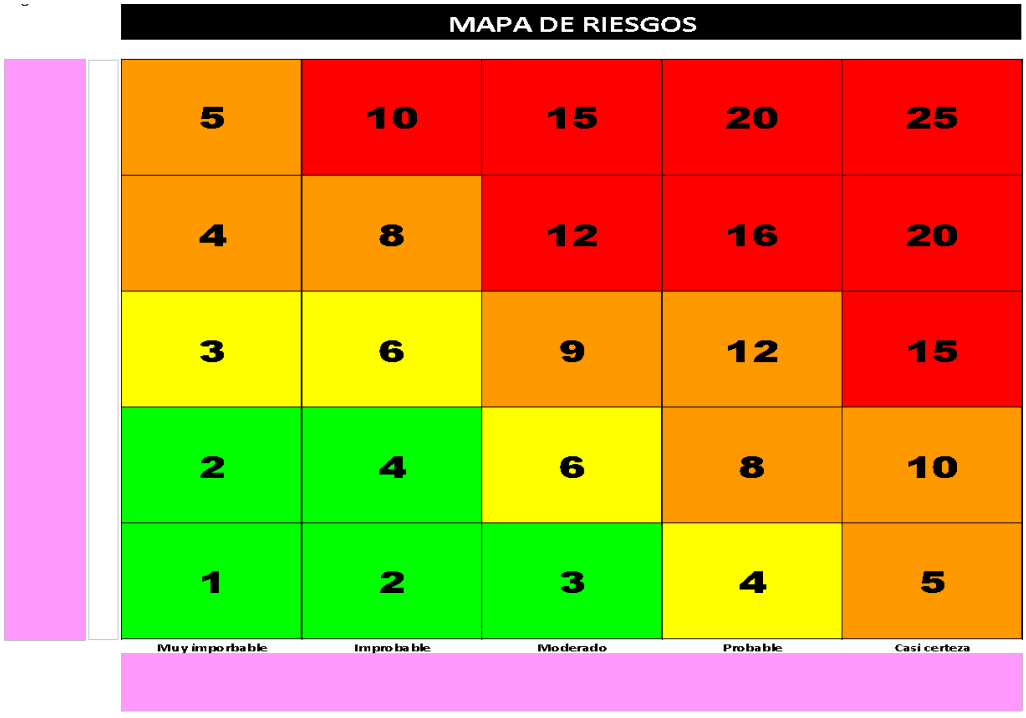
nivel de severidad) con que el evento de riesgo afectaría a NTT DATA CHILE, lo que luego puede graficarse de acuerdo a la siguiente tabla y mapa de riesgos:

TABLA 3: NIVEL DE SEVERIDAD DEL RIESGO

Nivel de severidad del riesgo

Nivel Probabilidad		Nivel Impacto		Severidad del Riesgo	
Casi Certeza	5	Catastrófico	5	Extremo	25
Casi Certeza	5	Mayor	4	Extremo	20
Casi Certeza	5	Moderado	3	Extremo	15
Casi Certeza	5	Menor	2	Alto	10
Casi Certeza	5	Insignificante	1	Alto	5
Probable	4	Catastrófico	5	Extremo	20
Probable	4	Mayor	4	Extremo	16
Probable	4	Moderado	3	Alto	12
Probable	4	Menor	2	Alto	8
Probable	4	Insignificante	1	Moderado	4
Moderado	3	Catastrófico	5	Extremo	15
Moderado	3	Mayor	4	Extremo	12
Moderado	3	Moderado	3	Alto	9
Moderado	3	Menor	2	Moderado	6
Moderado	3	Insignificante	1	Bajo	3
Improbable	2	Catastrófico	5	Extremo	10
Improbable	2	Mayor	4	Alto	8
Improbable	2	Moderado	3	Moderado	6
Improbable	2	Menor	2	Bajo	4
Improbable	2	Insignificante	1	Bajo	2
Muy improbable	1	Catastrófico	5	Alto	5
Muy improbable	1	Mayor	4	Alto	4
Muy improbable	1	Moderado	3	Moderado	3
Muy improbable	1	Menor	2	Bajo	2
Muy improbable	1	Insignificante	1	Bajo	1

TABLA 4: MAPA DE RIESGOS



Adicionalmente, la matriz de riesgos de NTT DATA CHILE contiene los controles mitigantes respectivos para cada uno de los riesgos descritos, las áreas de riesgo y los cargos expuestos.

7.2 MEDIDAS DE PREVENCIÓN

NTT DATA CHILE cuenta con diversas normas, políticas y prácticas de prevención de conductas que pueden generar responsabilidad penal a la persona jurídica. Entre ellas podemos encontrar:

7.2.1 CÓDIGO DE ÉTICA Y CONDUCTA PROFESIONAL DEL GRUPO NTT DATA.

El "Código de Ética Empresarial de NTT DATA" es un valioso apoyo a todos los trabajadores y colaboradores de NTT DATA CHILE al momento de tomar decisiones, ya que establece distintos principios y valores, todos de especial interés para reforzar el Modelo de Prevención de Delitos. Dicho Código regula, entre otras, las siguientes materias:

- Los Valores de la empresa (Generosidad Exigente, Libertad Responsable, Energía Creativa y Transparencia y Coherencia)
- Principio de Objetividad y Conflictos de intereses
- Gestión de la información
- Uso de activos y marca NTT DATA
- Relaciones con clientes y proveedores
- Relaciones con funcionarios públicos
- Relación con competidores
- Relación con la comunidad y medio ambiente
- Sanciones a incumplimientos éticos.

En definitiva, el Código de Ética y Conducta Profesional del Grupo es uno de los instrumentos en el que se plasman la actitud y cultura que la empresa ha elegido para caracterizar su actuación en el mercado. Por otra parte, la violación de las normas contenidas en el Código de Ética y Conducta Profesional por parte de los colaboradores de la compañía pueden derivar en la imposición de sanciones y/o en la adopción de las acciones legales correspondientes.

En particular, si en el contexto de un procedimiento resultante de una denuncia interpuesta a través del Sistema de Alertas, el Comité Global de Cumplimiento determina

que un profesional del Grupo ha realizado actividades contraviniendo lo establecido en dicho Código o en Procedimientos y Políticas corporativas de la Compañía, lo elevará a la Comisión de Auditoría para que decida sobre la aplicación de las medidas disciplinarias, conforme al régimen de faltas y sanciones previsto en la legislación laboral aplicable, ello sin perjuicio de cualesquiera otras responsabilidades civiles, penales o administrativas que resulten legalmente exigibles.

Por último, el Código recalca que ningún profesional del Grupo podrá requerir a otro, independientemente de encontrarse en una posición jerárquica superior, que cometa un acto que contravenga lo previsto en el mismo o, en general, que sea impropia o ilegal. En idéntico sentido, ningún profesional puede justificar una conducta contraria al Código de Ética y Conducta Profesional amparándose en las órdenes o indicaciones de un superior.

7.2.2. PRINCIPIO DE OBJETIVIDAD Y POLÍTICA GLOBAL ANTE CONFLICTOS DE INTERÉS DE GRUPO NTT DATA

Los profesionales del Grupo deben ser imparciales y no estar condicionados por elementos externos o presiones (ya sea de tipo económico, político, etc.) que puedan desvirtuar el ejercicio de su actividad profesional. Así, la aplicación de criterios objetivos es imprescindible en todos los trabajos que se lleven a cabo en el Grupo.

En este sentido, se exige demostrar imparcialidad frente a terceros, evitando situaciones que puedan llevar consigo conflictos de interés o suponer un menoscabo de la lealtad a la compañía en favor de intereses propios, perjudicando la objetividad, independencia e imparcialidad con que se debe desempeñar el trabajo.

Los conflictos de intereses pueden ser personales o profesionales. Se entiende que existe un conflicto de interés personal cuando cualquier beneficio que se pueda percibir directa o indirectamente como consecuencia de relaciones de parentesco, afectividad, propiedad, gestión y/o inversiones o actividades de los profesionales del Grupo NTT DATA (incluyendo personas físicas y/o jurídicas directamente o indirectamente vinculadas a ellos) colisionen con los intereses de la empresa o de las actividades realizadas por dichos profesionales a favor de terceros. Por su parte, se entiende que existe un conflicto de interés profesional cuando la prestación de servicios a un cliente imposibilite, por cualquier causa, la prestación de servicios a otro cliente, debiendo establecerse las medidas oportunas que resuelvan tal impedimento. En caso de existir cualquier conflicto de interés, el profesional de NTT DATA implicado debe informar a su responsable de forma inmediata en el momento en que éste se produzca y remitir la pertinente comunicación de

dicha situación al Área de Compliance a través del buzón All.Compliance_ev@nttdata.com. El Área de Compliance podrá dar traslado del mismo al Comité Global de Cumplimiento y se arbitrarán las medidas necesarias para resolver el conflicto, atendiendo a las circunstancias de cada caso concreto.

En caso de que cualquier profesional se vea involucrado en un procedimiento judicial, penal o administrativo de carácter sancionador, que pueda afectarle en el ejercicio de sus funciones, o acepte un cargo público, ejerza un cargo de administración o dirección en otras sociedades o adquiera acciones/participaciones o cualquier interés en un competidor, deberá comunicarlo a la compañía siguiendo el mismo procedimiento descrito en el apartado anterior.

Finalmente, los profesionales de las Sociedades deben evitar encontrarse situaciones de incompatibilidad, prohibición o conflicto de interés, que impida, restrinja o limite la prestación de sus servicios y/o asesoramiento a la compañía.

7.2.2.1 DECLARACIÓN DE CONFLICTO DE INTERÉS

En conformidad con la Política Global ante Conflictos de Interés del Grupo NTT DATA, NTT DATA CHILE ha dispuesto una declaración dirigida a los colaboradores y otra a los proveedores con los que la compañía entabla relaciones comerciales, con el objeto de conocer cuándo pudiera producirse un conflicto de interés, permitiendo prevenir y evitar dichas situaciones o bien, si el conflicto de interés no pudiera evitarse, con el objeto de abordar la situación mediante la implementación de estrategias necesarias para mitigar los riesgos relacionados al conflicto de interés detectado. La declaración que sea suscrita por el colaborador o el proveedor será resguardada por el Área de People o de Compras, respectivamente, bajo estrictos estándares de confidencialidad y se registrará en la carpeta personal de cada colaborador o en la del proveedor, según corresponda.

La Declaración de Conflicto de Interés dirigida a los colaboradores deberá ser presentada al Área de People al momento de su ingreso a NTT DATA CHILE. Los colaboradores que tengan los cargos de socios, directores y altos ejecutivos de NTT DATA CHILE deberán presentar esta declaración anualmente y en el plazo de 10 días contados desde la asunción de alguno de los cargos mencionados. Asimismo, se deberá presentar esta Declaración cuando el colaborador tome conocimiento de alguna modificación de la información presentada en su última declaración.

Para el caso de los proveedores, esta declaración formará parte de los documentos necesarios para su homologación, que serán remitidos al proveedor por el Área de Compras al inicio de dicho proceso.

7.2.3. POLÍTICA ANTICORRUPCIÓN DE GRUPO NTT DATA

Con el objeto de proteger a la organización, la Política Global Anticorrupción del Grupo exige el cumplimiento de las siguientes reglas y principios:

1. Todos los profesionales del Grupo deben observar un comportamiento ético e íntegro y cumplir con las Leyes Anticorrupción. Lo contrario será entendido por la organización como un incumplimiento de los deberes/funciones del cargo o posición y como una actuación injusta y desleal.
2. Todos los profesionales del Grupo habrán de cumplir con lo dispuesto en el Código de Ética y Conducta Profesional, así como en todas las políticas, protocolos y demás procedimientos internos que, en cada momento, se encuentren en vigor.
3. Determinadas áreas en las que el riesgo de corrupción pueda ser mayor (como pudieran ser las áreas Financiera o de Compras) deben cumplir expresamente con las acciones/medidas anticorrupción, de carácter específico, que la organización considere oportunas en cada momento, entre otras, las de información y formación a cargo del responsable del área, o las de prevención y consideración de la normativa anticorrupción existente en caso de desarrollo o expansión de cierta actividad en los países considerados conflictivos a nivel internacional.
4. No se llevará a cabo actuación alguna por parte de los profesionales del Grupo que pueda implicar un conflicto de interés, generando un beneficio personal en detrimento de los intereses de la organización o de su reputación.
5. Verificar en cada caso, con el soporte del área de Compliance, si fuere necesario, la correspondiente due diligence de todo tercero con quien se quiera entablar una relación contractual. En el marco de esta due diligence podrán realizarse actuaciones de investigación o “screening” del tercero con el fin de comprobar si se encuentra inmerso en un procedimiento judicial, ha resultado condenado por algún delito en virtud de sentencia firme, se encuentra relacionado con personas asociadas a corrupción, etc. A través del procedimiento de due diligence de terceros, el Grupo NTT DATA se compromete a evaluar los riesgos de posible soborno y corrupción en el tercero y en el marco de cualquier potencial relación con el mismo, adoptando las medidas que resulten precisas con carácter previo a entablar dicha relación.
6. En el evento de suministrar información confidencial del Grupo a terceros, se debe firmar previo al suministro, el correspondiente Acuerdo de Confidencialidad, o bien

incluir la correspondiente cláusula de Confidencialidad en el contrato que corresponda suscribir, a fin de que dicha información quede legal y debidamente protegida.

7. Todo acuerdo a suscribir por cualquier entidad del Grupo debe formalizarse por escrito. Por consiguiente, la organización no autoriza la celebración de acuerdos verbales.
8. Utilizar siempre, sea cual fuere la relación contractual, los modelos de contrato que se encuentren vigentes en cada momento y que hayan sido elaborados por el área de Legal & Tax Advisory. Estos modelos reflejarán, al menos, el objeto y causa de la relación, prestaciones a realizar/cumplir, el precio/retribución y su beneficiario final, así como la forma de pago, de manera que no implique corrupción de ningún tipo.
9. Siempre que proceda por procedimiento interno, así como en todos aquellos supuestos en los que el proveedor, cliente o tercero imponga su modelo de contrato, consultar al área de Legal & Tax Advisory.
10. Los acuerdos que se quiera suscribir con terceros (principalmente agentes, mediadores, distribuidores, comisionistas y asesores externos) deberán ajustarse a los modelos de contrato de Negocio que tenga elaborados el área de Legal & Tax Advisory y que se encuentren en vigor. Dichos modelos de contrato habrán de incluir el Compromiso Anticorrupción, a firmar por el tercero, que haya facilitado el área de Compliance.
11. El profesional del Grupo o el tercero que actúe en nombre del mismo, cuando le sea requerido que asuma un compromiso económico o de otro tipo, o que apruebe o realice un pago, deberá asegurarse antes que entiende completamente la razón del mismo, así como que el mismo es legal. En caso de duda, podrá elevar la consulta al área de Compliance, a través del buzón de correo electrónico ibbiol.compliance@emeal.nttdata.com

12. Sólo se aceptará el cobro o pago de comisiones que se ajusten a la legalidad vigente y que resulten práctica común en operaciones de intermediación o similar, bajo un objeto y causa legal, así como éticamente procedentes y adecuados al Código de Ética y Conducta Profesional.
13. Todas las operaciones en la organización que impliquen cobros y pagos deben recogerse fiel, ordenada y puntualmente en la contabilidad o en los registros correspondientes. Asimismo, se prohíben los pagos que puedan tener el carácter de ilícitos o irregulares. Cualquier gasto en la organización debe estar debidamente justificado y ser aprobado por el responsable que corresponda, registrándose y contabilizándose adecuadamente.
14. En todo caso, cualquier posible delito de corrupción o conducta ilegal en este ámbito podrá denunciarse por los profesionales del Grupo a través del Sistema de Alertas Profesionales (Whistleblowing System).
15. Los profesionales del Grupo siempre podrán dirigir sus consultas, en materia anticorrupción, al área de Compliance, a través del buzón de correo electrónico ibbiol.compliance@emeal.nttdata.com

7.2.4. POLÍTICA DE COMPRAS (PROCUREMENT) Y RELACIÓN CON PROVEEDORES

Los departamentos de Procurement son los responsables del desarrollo e implementación de la estrategia de compras del Grupo NTT DATA, en colaboración con todas aquellas áreas corporativas y departamentos cuya involucración fuese necesaria. De acuerdo a esta Política, la estrategia de compras debe velar por el cumplimiento de cuatro aspectos clave: Calidad en la Compra/Creación de Valor, Agilidad, Control y Medición de Resultados y el objetivo fundamental de dicha estrategia es el de garantizar la calidad en la compra y maximizar el valor generado en las compras y contratos de los productos y servicios necesarios para abastecer las necesidades de NTT DATA CHILE, además de asegurar los plazos de entrega contratados.

Por otra parte, todo proveedor que inicie una relación comercial con una entidad del Grupo NTT DATA debe ser previamente homologado siguiendo las pautas establecidas en el Procedimiento de homologación en vigor, aplicable a ese tipo de proveedor/material/servicio. Asimismo, para asegurar la calidad de los productos y servicios contratados, el Área de Compras podrá realizar una evaluación expost.

7.2.5. POLÍTICA DE REGALOS Y HOSPITALIDAD

Los profesionales del Grupo NTT DATA, en el contexto de su trabajo y en cualquier interactuación con clientes, proveedores o terceros, habrán de tener presente en todo momento y seguir las pautas del Código de Ética y Conducta Profesional, así como de la Política global de Regalos y Hospitalidad.

En el sector privado, queda expresamente prohibido, aceptar, obtener, ofrecer, prometer, otorgar o autorizar la entrega de dinero, favores, promesas de ventajas o ningún tipo de regalo, hospitalidad o beneficio a/o de los clientes, proveedores o terceros, directa o indirectamente, que, por su valor, pudiera tener una interpretación distinta del mero detalle o pudiera provocar conflicto entre los intereses personales o los intereses del Grupo. Se considera que la atención recibida y otorgada excede de la mera cortesía o detalle cuando ésta sea diferente y mayor que las que se concedan habitualmente en los usos comerciales. De igual forma, todo profesional del Grupo deberá informar a nivel superior cuando el regalo/atención/obsequio exceda determinados valores.

En el sector público, queda expresamente prohibido a todo profesional del Grupo ofrecer, prometer, otorgar o autorizar la entrega de dinero, regalos, favores, contribuciones o aportaciones a cualquier funcionario para la obtención de un beneficio, concesión, subvención o ventaja a favor del Grupo. En particular, el profesional debe abstenerse, así como suspender automáticamente, toda relación ante cualquier indicio de corrupción que pueda determinar un trato preferencial o que pueda dar lugar a una influencia, trato de favor, o que esté ligado a cualquier extorsión o soborno.

7.2.6. POLÍTICA DE DONACIONES

Las contribuciones o aportaciones que las entidades del Grupo quieran realizar, en su caso, a fundaciones o entidades benéficas o sin fin de lucro deberá ajustarse a las pautas internas que, en cada momento, existan en la organización. En cualquier caso, toda donación, dineraria o en especie, requerirá, con el soporte del área de Compliance, la previa investigación de la organización o institución.

7.2.7. CAPACITACIÓN PERMANENTE Y PLAN DE DIFUSIÓN DEL MODELO DE PREVENCIÓN

NTT DATA CHILE estima que la comunicación oportuna y capacitación permanente son maneras eficaces de prevenir la comisión de los delitos señalados en el artículo 1° de la Ley 20.393, como, asimismo, el cumplimiento de la normativa interna vigente. Por ello, los colaboradores de NTT DATA CHILE deben estar oportuna y debidamente informados y capacitarse periódicamente.

En este sentido, el Encargado de Prevención está a cargo de diseñar y coordinar Programa Anual de Difusión y Capacitación sobre prevención de los delitos de la Ley N°20.393. Dicho Programa Anual debe indicar las materias objeto de la capacitación, metodologías mínimas a usar, los medios que se emplearán para su ejecución y los procedimientos de evaluación obligatoria.

La participación de los colaboradores de la Empresa en los programas de capacitación es obligatoria y se llevará control de asistencia y aprobación de los cursos impartidos.

7.2.8. MONITOREO Y CONTROLES

NTT DATA CHILE considera que el monitoreo y control del cumplimiento de sus políticas, normas y procesos internos es una actividad que debe desarrollarse de manera permanente y continua a fin de asegurar su debida implementación y cumplimiento, detectar brechas, falencias, mitigar o gestionar el riego a fin de lograr una mejora continua.

El control tiene como propósito detectar y reportar las actividades que se pretendan realizar o que se hayan realizado, así como también, mitigar o gestionar el riego, buscando aumentar la probabilidad de que los procesos logren sus metas y objetivos en la prevención de los delitos señalados en el artículo 1° de la Ley 20.393.

7.2.9. AUDITORÍA

El Encargado de Prevención cuenta con la facultad de solicitar el apoyo del área de Finanzas. Por su parte y con el fin de resguardar los recursos financieros de la Empresa y de velar por la prevención de su utilización en toda clase de delitos, Administración y Finanzas podrá efectuar los siguientes procedimientos:

a. Auditorías programadas relacionadas a aspectos operacionales, de contratos y/o proyectos relevantes en base al marco legal y regulatorio vigente.
b. Auditorías no programadas de investigación, a fin de determinar el adecuado resguardo de los activos financieros de la Empresa.

7.2.10. REPORTES

De acuerdo con el artículo cuarto de la Ley N°20.393 y lo señalado en el numeral 3.2 de este Manual, el Encargado de Prevención debe reportar al directorio de NTT DATA CHILE, a lo menos semestralmente y/o cuando las circunstancias lo ameriten, de las medidas y planes implementados en el cumplimiento de sus funciones y rindiendo cuenta de su gestión.

7.2.11. POLÍTICAS Y PROCEDIMIENTOS DE ADMINISTRACIÓN DE RECURSOS FINANCIEROS

NTT DATA CHILE cuenta con procedimientos que sus distintas áreas están obligadas a cumplir en la ejecución de los procesos que involucren la gestión de recursos financieros, entre otros:

- Proceso de Pago a Proveedores nacionales.
- Proceso de Pagos de Proveedores extranjeros e intercompañía.
- Política General de Reembolso de Gastos.
- Proceso de Posiciones de Caja diarios.
- Manual de Apoderados Comercio Exterior.
- Política Global de Compras.

Sin perjuicio de la importancia y constante aplicación de los procedimientos antes señalados, NTT DATA CHILE se encuentra en permanente revisión y desarrollo de políticas que sean útiles al control de los recursos financieros.

7.3. PROGRAMAS DE AUDITORÍA INTERNA Y DEL MODELO DE PREVENCIÓN

Según lo establece el artículo 4°, de la Ley 20.393, el Encargado de Prevención, en conjunto con la Administración de la persona jurídica, debe establecer protocolos y procedimientos para prevenir y detectar conductas delictivas referidas a las actividades o procesos de las Sociedades en donde se hayan identificado riesgos. Por otra parte, establecer procesos para la aplicación efectiva del Modelo de Prevención a fin de detectar y corregir sus fallas y actualizarlo de acuerdo a los requerimientos regulatorios.

En este sentido y con la finalidad de asegurar una efectiva implementación del Modelo, el Encargado de Prevención debe coordinar un programa periódico de auditorías que asegure:

1. El cumplimiento de las políticas y procedimientos de administración de los recursos financieros.
2. El cumplimiento de las políticas y procedimientos establecidos para prevenir los riesgos identificados.
3. El desarrollo de un programa de auditoría interna, aplicable a todas las áreas de NTT DATA CHILE, en relación a los elementos que componen el Modelo de Prevención,

con el objetivo de validar que éstos se encuentren operativos y que son actualizados con la periodicidad que se requiere.

Los resultados de dichas revisiones deben ser puestos en conocimiento del Encargado de Prevención, de tal modo que se tomen las medidas correctivas necesarias y se realicen las actualizaciones a la matriz de riesgo y/o a las políticas y procedimientos establecidos, según corresponda, en atención a los hallazgos o debilidades que dichas auditorías revelen. Los resultados deben también ser incorporados por el Encargado de Prevención en los reportes que éste debe realizar al directorio.

Los elementos del Modelo de Prevención de la Ley N°20.393 que deben ser auditados son los siguientes:

1. La designación del Encargado de Prevención en los términos prescritos en la ley, así como la asignación de sus medios y facultades.
2. La realización de los reportes semestrales por parte del Encargado de Prevención al directorio de NTT DATA CHILE . Deberá controlarse que el informe contenga a lo menos:
    i. Resultados y hallazgos de evaluación de auditoría interna (control financiero y modelo).
    ii. Actualizaciones del Modelo si se requieren.
    iii. Actividades de entrenamiento y difusión.
    iv. Análisis presupuestario del área.
    v. Resumen de denuncias y medidas adoptadas.
3. La realización y registro de las actividades de difusión y capacitación.
4. La actualización anual de la Matriz de Riesgos del Modelo.
5. La incorporación de las cláusulas definidas para el Modelo en los contratos de trabajo.
6. La incorporación de las cláusulas definidas para el Modelo en los contratos de adquisición de bienes o contratación servicios.
7. La actualización oportuna del Reglamento Interno de Orden, Higiene y Seguridad, de forma tal que incorpore las obligaciones y prohibiciones que se requieran como consecuencia de las actualizaciones del Modelo.
8. El cumplimiento de los procedimientos de denuncias establecidos por la Empresa para la prevención de los delitos contemplados en la Ley N°20.393.

8. OBLIGACIONES, PROHIBICIONES Y SANCIONES

En virtud de lo establecido por la Ley N°20.393, NTT DATA CHILE ha establecido obligaciones y prohibiciones a las que están sujetos sus colaboradores, las que se han agregado a su Reglamento Interno de Orden, Higiene y Seguridad, a los contratos de trabajo y a los contratos con proveedores. El incumplimiento de dicha normativa es sancionado en los términos establecidos en el mismo Reglamento Interno de Orden, Higiene y Seguridad.

8.1. REGLAMENTO INTERNO DE ORDEN, HIGIENE Y SEGURIDAD

De acuerdo con la Ley N°20.393, las personas jurídicas deben incorporar las obligaciones, prohibiciones y sanciones administrativas internas que se establezcan como parte del Modelo de Prevención, expresamente en el Reglamento Interno de Orden, Higiene y Seguridad (RIOHS).

Sin perjuicio de los cambios o ajustes en el marco del mejoramiento constante del Modelo de Prevención de NTT DATA CHILE , dichas obligaciones y prohibiciones se encuentran incorporadas en el RIOHS, en particular en el Título VI: Código de Ética y Modelo de Prevención del Delito.

8.2. CONTRATOS DE TRABAJO

Los contratos de trabajo de NTT DATA CHILE deberán contener las obligaciones y prohibiciones a que estarán sometidos los trabajadores, de idéntico tenor a las dispuestas en el Reglamento Interno de Orden, Higiene y Seguridad recién referenciadas, las que se les incorporarán ya sea como addendum para el caso de los contratos existentes, o bien como cláusulas especiales a los nuevos contratos de los trabajadores que se incorporen a la empresa en el futuro.

8.3. CONTRATOS CON PROVEEDORES

Asimismo, los principios del Modelo de Prevención deben incorporarse en los contratos con proveedores. Es por ello que NTT DATA CHILE incorpora en los contratos con sus proveedores cláusulas especiales -o anexos según corresponda- referidas al Modelo de Prevención de Delitos.

9. CANAL DE DENUNCIAS, PROCEDIMIENTO DE INVESTIGACIÓN Y SANCIONES

9.1. CANAL DE DENUNCIAS

Como compañía global, que forma parte del Grupo NTT DATA, la compañía propugna el cumplimiento de todas las leyes y reglamentos, tanto a nivel internacional como nacional en las jurisdicciones en las que desarrolla sus actividades, así como un comportamiento y actitud conforme a los valores de compañía, esto es, Generosidad Exigente, Libertad Responsable, Energía Creativa y Transparencia y Coherencia, de forma que el logro de su visión se lleve a cabo a través de una práctica correcta e íntegra, aplicando los apropiados estándares de ética en los negocios.

A tal efecto, y de conformidad con lo dispuesto en el Código de Ética y Conducta Profesional (que incluye la Global Compliance Policy del Grupo), junto a otros canales regulares de comunicación previstos internamente (por ejemplo, la comunicación espontánea al Comité Global de Cumplimiento Normativo y Prevención Legal o a los responsables superiores), se cuenta con un canal global de denuncias o "Sistema Whistleblowing", al que se puede acceder mediante el siguiente link: disponible para estos efectos en el siguiente link:

https://cl.nttdata.com/report-ethical-concern

La información que pueda obtenerse a través de este canal ayuda a que la compañía pueda sostener, a nivel global, el cumplimiento de las obligaciones de Compliance, así como prevenir y detectar riesgos de cumplimiento normativo o de otro tipo.

A través de este canal de denuncias se pueden reportar:

- Cualquier infracción a los valores, principios de actuación o normas de conducta de los trabajadores que se recogen en el Código o en políticas y normativa interna.
- Cualquier infracción de las normas, principios y pautas del Código de Conducta y de Buen Gobierno de NTT DATA CHILE.
- Cualquier incumplimiento de la legislación internacional o local vigente.
- Cualquier contingencia que pueda suponer un riesgo para la reputación y el negocio de la Compañía.
- Cualquier otra conducta que pueda ser considerada generadora de un dilema ético.
- Cualquier otro hecho o circunstancia que pueda suponer un incremento relevante del riesgo empresarial de la compañía.

La información comunicada por este canal se mantendrá bajo estrictos criterios de confidencialidad y anonimato, manteniéndose su integridad y seguridad. Conforme a estos criterios, cuando se proporciona la misma, se encripta de forma automática y permanece como estrictamente confidencial.

Asimismo, NTT DATA CHILE se compromete a no adoptar ninguna forma de represalia, directa o indirecta, contra de aquellos que sin mantener su anonimato, formulen una comunicación a través de dicho canal.

Este Sistema de Whistleblowing puede ser utilizado por todos los profesionales que forman el Grupo, así como por cualquier tercero que pueda mantener algún tipo de interés o relación con el Grupo, o que actúe en su nombre o colabore con ellos (clientes, proveedores, agentes, otros terceros relacionados, etc.).

Se considerará, violación del Modelo de Prevención la acusación falsa o efectuada de mala fe o la negativa a cooperar en una investigación relacionada a una falta o infracción a este Manual. En este sentido, NTT DATA CHILE garantiza que no habrá represalia alguna contra aquellas personas que efectúen denuncias de buena fe.

9.2. PROCEDIMIENTO DE INVESTIGACIÓN

El Canal de Denuncias o Sistema Whistleblowing tiene como finalidad recibir toda denuncia por infracción o incumplimiento a las obligaciones de Compliance, al Código de Ética, al presente Manual de Prevención del Delito, y/o a la normativa vigente y en este sentido, en cumplimiento de la Ley N°20.393, se establece el siguiente Procedimiento de Denuncia:

PROCEDIMIENTO DE DENUNCIA, INVESTIGACIÓN Y SANCIONES DEL MODELO PREVENCIÓN DE DELITOS

Artículo 1. Las denuncias serán recepcionadas a través del Sistema Whistleblowing del Grupo NTT DATA por el Comité Global de Cumplimiento Normativo y Prevención Legal de Grupo NTT DATA y por el Encargado de Prevención de Delitos.

Artículo 2. Toda denuncia deberá efectuarse de buena fe y debidamente fundamentada, indicando en lo posible hechos, lugares, fechas referenciales y nombres o cargos de los implicados.

Artículo 3. La Empresa garantiza que todas las denuncias que formalmente sean presentadas serán investigadas en forma seria, responsable y con la estricta confidencialidad requerida para resguardar la identidad del denunciante.

Artículo 4. La Empresa se obliga a respetar en todo momento los derechos fundamentales de los trabajadores en el curso de ésta.

Artículo 5. Recibida una denuncia mediante el Sistema Whistleblowing, el Encargado de Prevención de Delitos o la persona designada para estos efectos, iniciará la etapa de investigación.

Artículo 6. Las denuncias relativas al incumplimiento del Modelo de Prevención o conductas relacionadas a la Ley 20.393 serán investigadas por el Encargado de Prevención de Delitos, quien recabará todos los antecedentes que estime pertinentes y adoptará las medidas conducentes al esclarecimiento de los hechos. Sin perjuicio de lo anterior, no podrán adoptarse medidas que directa o indirectamente afecten la dignidad del empleo del trabajador afectado por la respectiva investigación.

Artículo 7. El proceso de investigación constará por escrito, dejándose constancia de las acciones realizadas por el investigador, de las declaraciones efectuadas por los involucrados, de los testigos y las pruebas que aportaran.

Artículo 8. El Encargado de Prevención de Delitos tendrá un plazo de 30 días para la recopilación de antecedentes, y una vez transcurrido dicho plazo, emitirá un Informe Preliminar sobre los resultados de su investigación.

Artículo 9. Dicho Informe Preliminar será puesto en conocimiento de los implicados, quienes tendrán el plazo de 10 días para presentar sus descargos, observaciones y aportar todos los antecedentes pertinentes para el esclarecimiento de los hechos.

Artículo 10. Presentados los descargos, el Encargado de Prevención de Delitos podrá realizar nuevas diligencias, fijando para ello un plazo máximo de 10 días.

Artículo 11. Agotado el término a que se refiere el artículo anterior o transcurridos 15 días desde la presentación de los descargos, el Encargado de Prevención de Delitos emitirá un Informe Final en que expresarán las conclusiones de su investigación.

Artículo 12. El Informe Final se referirá expresamente a la eventual responsabilidad de los implicados en los hechos, propondrá las medidas adecuadas y/o la sanción pertinente, la necesidad de efectuar las respectivas denuncias ante los Tribunales Ordinarios de Justicia y, si fuere necesario, las medidas necesarias para corregir internamente las irregularidades. El Encargado de Prevención de Delitos deberá

incluir en sus conclusiones tantos los elementos que agravan la responsabilidad de los implicados, como aquellos que la atenúan.

Artículo 13. El Informe Final del Encargado de Prevención de Delitos será puesto en conocimiento del directorio de NTT DATA CHILE.

Artículo 14. Las decisiones relacionadas con las eventuales sanciones, absolución y/o adopción de medidas correctivas en la organización, serán exclusivamente adoptadas por el directorio de NTT DATA CHILE en conjunto con el Departamento Jurídico.

Artículo 15. En el caso de que el hecho denunciando involucre a un trabajador y en conformidad con lo establecido en el N° 10 del artículo 154 del Código del Trabajo, el directorio de NTT DATA CHILE, por resolución fundada, podrá aplicar una de las siguientes sanciones internas:

I) Amonestación verbal.
II) Amonestación escrita
III) Multa de hasta 25% de la remuneración diaria del infractor.

Las sanciones que decida aplicar el directorio no implican una renuncia a su facultad de denunciar a los Tribunales Ordinarios de Justicia en los casos que estime necesario.

9.3. SANCIONES

La violación por parte de los trabajadores de NTT DATA CHILE de lo establecido en este Manual, así como a las políticas asociadas al mismo, podría resultar en las acciones correctivas y sanciones, de carácter progresiva y fundada, determinadas en el Reglamento Interno de Orden, Higiene y Seguridad y que podrán incluir, entre otras que se estimen pertinentes, las de amonestación, registro de los hechos para su consideración en el desarrollo profesional futuro de la persona infractora al interior de la Empresa, el eventual despido de la persona infractora y la posible denuncia de los hechos a las autoridades correspondientes, todo lo anterior en atención a la naturaleza y gravedad de los hechos.

Asimismo, la violación de lo establecido en este Manual y documentos relacionados al mismo, tales como anexos de contratos, contratos y políticas, por parte de un tercero con el que la compañía tiene una relación comercial (como por ejemplo, proveedores, clientes, profesionales externos, entre otros) facultará a NTT DATA CHILE a poner término a dicha relación contractual, sin perjuicio de las acciones legales que pueda, además, emprender en contra del infractor.

NTT DATA CHILE prestará toda la colaboración necesaria que sea requerida por el Ministerio Público y/o por autoridad administrativa o judicial con el objeto investigar, perseguir y sancionar los delitos pertinentes.

10. EVALUACIÓN POR TERCERO INDEPENDIENTE

En conformidad a la ley N°20.393, un Modelo de Prevención no solo debe cumplir con las exigencias legales, sino que también se debe asegurar la mejora continua y la eficacia de éste a través de evaluaciones periódicas por parte de terceros independientes que permitan mecanismos de perfeccionamiento o actualización.

Hasta ahora, la certificación de los Modelos de Prevención de Delitos en las empresas era voluntaria, sin embargo, la nueva normativa impone la obligación de prever evaluaciones periódicas efectuadas por terceros independientes. La implementación de estas evaluaciones es esencial porque refuerza una buena práctica internacional que busca la mejora continua a través de la revisión imparcial de un tercero. Este tercero debe ser realmente independiente, sin conflictos de interés o relaciones comerciales que puedan comprometer la objetividad de su evaluación. Por lo tanto, cualquier relación previa o concurrente entre la empresa evaluada y el evaluador puede ser cuestionada en sede penal, poniendo en riesgo la validez de la evaluación.

Las Sociedades, harán evaluaciones periódicas de su Modelo de Prevención de Delitos por parte de un tercero independientes cada dos años, con el propósito de que dicho modelo se vaya perfeccionando en el tiempo.

La independencia del evaluador garantiza que las evaluaciones no estén contaminadas por intereses comerciales y que se enfoquen en la objetividad y veracidad de los hallazgos. La evaluación debe ir más allá de una simple verificación formal y constar en informes detallados que demuestren una mejora continua. Esto implica actualizaciones permanentes del Modelo de Prevención de Delitos, integrando nuevos delitos, señales de alerta, riesgos, estándares y controles más eficientes. Un modelo inalterable a lo largo del tiempo indicaría una gestión inadecuada del programa de compliance penal. Lo que se requiere es evidencia tangible de una mejora continua virtuosa, validada por la opinión de un tercero verdaderamente independiente. Esto es fundamental para eximir a una empresa de responsabilidad penal.