Deloitte.

Compliance*Trends*

by Deloitte

Edición I

Indice

Editorial: Más allá del cumplimiento 04

ISO 37301: Reconocimiento del ecosistema de cumplimiento Consideraciones claves luego de su publicación 05

Características y utilidad de los instrumentos que componen los Programas de Cumplimiento 07

Proyecto de ley refundido: Que sistematiza los delitos económicos y modifica extensamente la responsabilidad penal de las personas jurídicas (Ley N°20.393) 09

Alta Gerencia y riesgos de ciberseguridad 11

Principales consecuencias: En la Incorporación de empresas automotoras como sujetos obligados de la Unidad de Análisis Financiero 13

Proyecto de Ley pro-consumidor artículo 15 bis respecto de los datos personales de los consumidores 15

Editorial

Más allá del cumplimiento

Manuel Gálvez | Socio Risk Advisory - Verónica Benedetti | Directora Risk Advisory & Compliance

Dentro de una organización es fundamental contar con principios, valores, lineamientos y un sistema de cumplimiento que garantice el actuar de todos de acuerdo a la ley vigente y de manera íntegra.

A fin de seguir aportando en temas de ética y cumplimiento, y contribuir a una mejor cultura ética de las empresas y de nuestra sociedad, en Deloitte decimos lanzar “Compliance Trends”, una serie de breves artículos referidos a últimas tendencias y buenas prácticas en esta materia aplicable para todas las industrias.

Esperamos que puedan disfrutar la primera edición de esta publicación y que sus contenidos sean útiles y desencadenen conversaciones relevantes, que ayuden al crecimiento sostenible y a mantener la reputación de sus organizaciones.

Equipo Editorial

ISO 37301:

Reconocimiento del ecosistema de cumplimiento Consideraciones claves luego de su publicación

Por Oscar Martínez | Manager Risk Advisory

El 13 de abril de 2021 se publicó un nuevo estándar internacional para los sistemas de gestión de cumplimiento (“CMS”). Conocido como ISO 37301, el estándar internacional reemplaza a la ISO 19600 que brindaba orientación para establecer, desarrollar, implementar, mantener y mejorar sistemas de gestión de cumplimiento efectivos.

¿Qué significa para las funciones de cumplimiento?

La ISO 37301 posiciona la gestión del riesgo de cumplimiento en un siguiente nivel e introduce el concepto de ecosistema de cumplimiento y enfatiza que la gestión del riesgo de cumplimiento involucra varios elementos comunes interrelacionados en toda la organización, estableciendo objetivos y principios para un sistema de gestión de cumplimiento integrado, con fuerte foco en construir una cultura de cumplimiento positiva, alineada con prácticas comerciales sostenibles. Se explicará a continuación los aspectos relativos de cada uno de estos aspectos:

1 Ecosistema de cumplimiento:

El estándar hace hincapié en la interrelación de los diferentes instrumentos organizacionales que permiten gestionar los riesgos de cumplimiento de ámbitos normativos específicos (por ejemplo, protección de datos personales, protección de los derechos de los consumidores, responsabilidad penal de las personas jurídicas, entre otras) bajo una visión holística, y reconoce que la gestión de riesgos de cumplimiento es un ciclo de mejora continua totalmente integrado.

2 Gobierno y liderazgo:

Los lineamientos dispuestos en la norma enfatizan el papel y la importancia de las unidades de gestión de riesgos que se encuentran supeditadas a la Alta Dirección, impulsando la participación en la gestión de los deberes de cumplimiento y en la generación de lineamientos, procesos y estructuras integradas, adecuadas y proporcionales para lograr los objetivos del CMS. También, promueve un mayor enfoque hacia la transparencia, la clara comunicación y la generación de reportes continuos.

3 Contexto organizacional:

La ISO 37301 promueve la identificación de situaciones relevantes que pudiesen afectar el propósito de cumplimiento y la capacidad de lograr los resultados previstos en el sistema de gestión (por ejemplo, el impacto y posición social y económica de la organización).

4 Conducta:

Acentúa la importancia de actividades e instrumentos comunes que guíen e impulsen los comportamientos deseados que se requieren en toda la organización, a efectos de respaldar el cumplimiento y mejorando la relación con todos los stakeholders (clientes, empleados, proveedores, mercados y comunidades).

5 Cultura de cumplimiento:

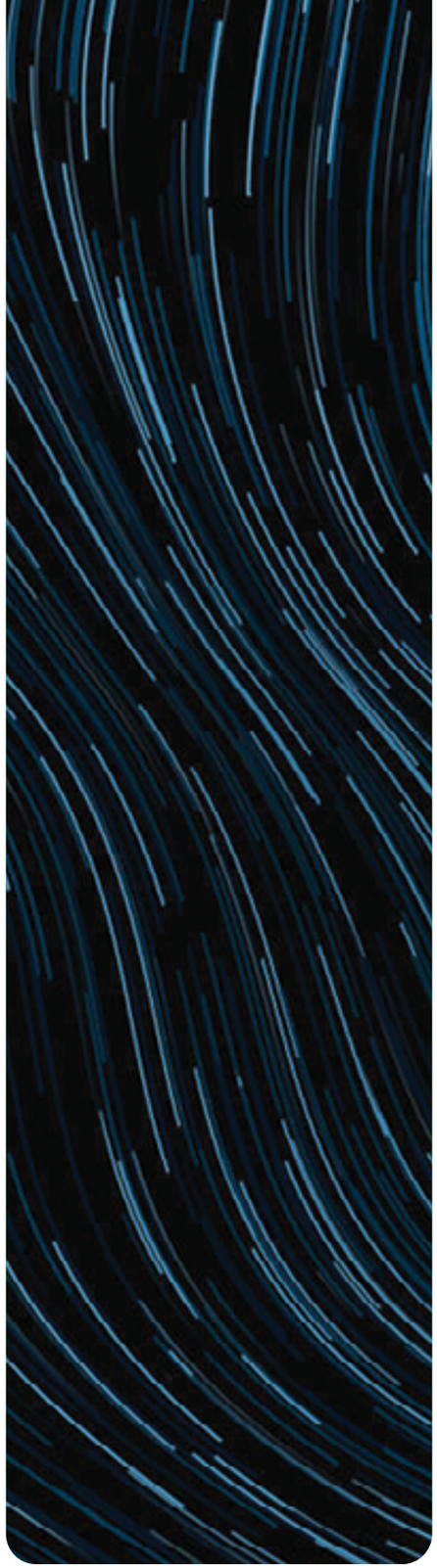
El estándar exalta en que el CMS debe promover, desarrollar, mantener y propender a una cultura de cumplimiento en todos los niveles dentro de la organización. El directorio y la Alta Dirección deben demostrar un compromiso activo, visible, coherente y sostenido bajo un estándar común de comportamiento. Destaca además que la cultura de cumplimiento debe ser presentada con instrumentos y herramientas metodológicas comprensibles.

6 Certificación:

la ISO 37301 es una norma de Tipo A, lo que significa que está articulada en un lenguaje directivo usando la palabra “deberá”. Esto significa que el nuevo estándar es “certificable”, y tanto los reguladores como los expertos independientes pueden utilizar el estándar para evaluar el sistema de gestión de cumplimiento de una organización.

La certificación permite que una organización demuestre a sus clientes, socios comerciales y reguladores que sus prácticas, procesos, estructuras y sistemas se alinean con los estándares aceptados a nivel mundial.

Como se observó anteriormente, la ISO 37301 incorpora consideraciones para construir una cultura de cumplimiento positiva alineada con prácticas comerciales sostenibles. Sin duda, la adopción de este estándar representa un importante desafío para todas las organizaciones, independientemente del nivel de madurez de su función de cumplimiento y del CMS implementado, dado que los responsables de cumplimiento deben asegurar la coherencia y la responsabilidad en cada etapa de implementación, generar confianza a las partes interesadas, tanto internas y externas; y de forma paralela, ayudar a cumplir con los objetivos de cumplimiento durante su evolución.



Características y utilidad de los instrumentos que componen los Programas de Cumplimiento

Por Sebastián Orellana | Consultor Senior, Risk Advisory & Compliance

Desde la dictación de la Ley No.20.393 que establece la responsabilidad penal de las personas jurídicas, la cultura de “compliance” ha ido fortaleciéndose al interior de las organizaciones, sobre todo si consideramos que desde el año 2009 hasta la fecha, se han dictado diversas normas que consagran la posibilidad de que las compañías diseñen e implementen programas o modelos de cumplimiento en diversas materias, como por ejemplo, en responsabilidad penal, prevención del lavado de activos y financiamiento del terrorismo, libre competencia, y protección de los derechos de los consumidores.

Sin embargo, las normas que conforman los programas o modelos de cumplimiento no suelen definir aquellos instrumentos que lo componen, quedando esta labor, por una parte, en manos de entes reguladores que a través de normas de carácter interpretativas precisan los instrumentos que deben considerar los programas o modelos (como por ejemplo el SERNAC respecto de los programas de cumplimiento en materia de protección de los derechos de los consumidores); o a través de normas y estándares internacionales referentes a esta materia (como lo son las ISO 19600 y 37301).

En este mismo sentido, los instrumentos, canales o mecanismos disponibles para las denuncias que componen los programas o modelos de cumplimiento, tomando de referencia los estándares nacionales e internacionales son, al menos, los siguientes: Política de compliance, Procedimiento de compliance, Matriz de riesgos, e Instrumentos legales. A continuación, revisaremos las características y utilidad de cada uno de ellos:

a) Política de compliance:

Se constituye como un elemento central en la adopción de los programas o modelos de cumplimiento, ya que por medio de ella se formalizan sus lineamientos generales, se establecen sus principales elementos y se definen los responsables de su adopción. Resulta un documento especialmente relevante pues proporciona un marco de referencia para el establecimiento de los objetivos de compliance y el compromiso de la organización para lograr esos objetivos mediante acciones[1]. Para lo anterior, es necesario que la Política sea aprobada por el máximo órgano social al interior de la compañía, a efecto de transmitir liderazgo y compromiso en la adopción del programa o modelo de cumplimiento.

b) Procedimiento de compliance:

Es el documento que describe las acciones o actividades concretas que la organización deberá llevar a cabo para dar cumplimiento a la Política (por ejemplo: actividades de prevención, detección y de respuesta), detallando los roles y responsabilidades de cada una de las áreas involucradas. Producto de los constantes cambios regulatorios, es posible que este Procedimiento deba sufrir modificaciones y/o actualizaciones periódicas para garantizar la correcta adecuación de los programas o modelos de cumplimiento implementados a los nuevos requerimientos normativos.

[1] Organización Internacional de Normalización. Sistemas de Gestión de Compliance (ISO 19600:2014)

c) Matriz de Riesgos y Controles:

El diseño e implementación de un programa o modelo de cumplimiento requiere que la organización identifique y evalúe sus riesgos de *compliance*[2]. Esta apreciación de los riesgos a los que se ve expuesta la organización constituye la base para implementar un programa o modelo de cumplimiento, y sirve para planificar la asignación de recursos y procesos para la gestión de esos riesgos previamente identificados. Dado que las organizaciones pueden verse expuestas a múltiples riesgos, es necesario contar con una herramienta que le permita al líder de la función de *compliance* -y a quienes apoyen esta labor al interior de la organización- gestionar debidamente estos riesgos.
La Matriz de Riesgos y Controles es precisamente la herramienta que cumple con el propósito antes mencionado, pues una vez identificados los riesgos de *compliance* permite documentarlos en ella para posteriormente priorizarlos, con el objeto de destinar mayores recursos a aquellos riesgos más críticos. Asimismo, permite documentar las actividades de control presentes en la organización (que mitigan la ocurrencia de los riesgos identificados) y evaluarlos desde una perspectiva de su diseño. Finalmente, la Matriz de Riesgos y Controles puede incorporar otros elementos que ayudarán en la gestión de los riesgos, como lo son: mapas de calor, gráficos, fórmulas de automatización, entre otros.

d) Instrumentos legales:

Son todas aquellas cláusulas contractuales que deberán incorporarse en los contratos que celebre la organización con terceros con los que se relacione (proveedores, clientes, asesores, trabajadores, etc.). Estos instrumentos establecen prohibiciones y obligaciones que deberán observar los terceros para dar estricto cumplimiento al programa o modelo implementado.

Finalmente, es preciso señalar que los programas o modelos de cumplimiento deben considerar la elaboración y/o adecuación de otros instrumentos tales como: políticas, normas y códigos internos a fin de robustecer su ambiente de control interno, y con ello, mejorar sus programas o modelos de cumplimiento.

[2] Organización Internacional de Normalización. Sistemas de Gestión de Compliance (ISO 19600:2014)

Proyecto de ley refundido

Que sistematiza los delitos económicos y modifica extensamente la responsabilidad penal de las personas jurídicas (Ley N°20.393)

Por Victoria Aylwin | Consultor Senior, Risk Advisory & Compliance

El Proyecto de Ley sobre Delitos Económicos, Boletines refundidos N°13204-07 y N°13.205-07, en adelante el "Proyecto", constituirá un cambio sin parangón en la Ley No. 20.393. Entre las principales modificaciones se destaca la masiva ampliación del catálogo de delitos que hacen procedente la responsabilidad penal de las personas jurídicas. Según el Proyecto, la nueva sistematización de delitos económicos diferenciará cuatro categorías. La primera categoría la constituyen los delitos que tienen el carácter de económicos cualesquiera que sean las circunstancias de su comisión, como, por ejemplo, los delitos sobre mercado de valores, en contra de la libre competencia y de la ley general de bancos, así como la corrupción en el ámbito privado. La segunda categoría la compone un extenso listado de delitos que se consideran económicos cuando han sido cometidos por un sujeto al interior de una empresa o en beneficio de ella, acá se encuentran los delitos aduaneros y medioambientales, la estafa y la administración desleal, entre otros. La tercera categoría la integra un listado de delitos especiales, es decir, cometidos por funcionarios públicos u otros autores que tienen una calidad personal especial, que se consideran económicos cuando en su comisión ha intervenido un sujeto al interior de la empresa o son cometidos en su beneficio de la corporación. La cuarta la configuran los delitos de receptación o blanqueo de activos cuando recaen sobre bienes originados por delitos económicos o cuando en su comisión se cumplen las condiciones de la segunda categoría de delitos económicos ya explicada.

> El Proyecto establece la autonomía de la responsabilidad penal de la persona jurídica de forma independiente

Además de la ampliación y sistematización de las figuras penales resumidas en lo precedente, el Proyecto instaura una ampliación de las personas jurídicas susceptibles de incurrir en responsabilidad penal de la Ley No. 20.393, incluyendo a las universidades del Estado, los partidos políticos y las personas jurídicas religiosas de Derecho Público. Lo anterior, junto con una modificación de los criterios para imputar responsabilidad, ampliando sustancialmente el círculo de personas al que se puede vincular su responsabilidad y la eliminación del beneficio económico como criterio de imputación. En cuanto a la ampliación de los criterios de imputación, el Proyecto vincula la responsabilidad de la empresa u organización no solo a los delitos cometidos por aquellos que se encuentran en la cima de la estructura corporativa, sino que además aquellos cometidos por o con la intervención de alguna persona natural que ocupare un cargo, función o posición en ella, o le prestare servicios gestionando asuntos suyos ante terceros, con o sin su representación.
Lo anterior ampliará los requerimientos propios de los modelos de prevención de delitos a todo tipo de intermediarios y representantes. Sumado a lo anterior, el Proyecto establece la autonomía de la responsabilidad penal de la persona jurídica de forma independiente, y a pesar, de que no se determine la responsabilidad penal de la persona natural.

El Proyecto simplifica la regulación de los requisitos de los programas de cumplimiento, suprimiendo el reconocimiento legal de la certificación de estos programas; se incluye la nueva figura del supervisor, se regula detalladamente la ejecución de las penas, desarrolla la ampliación del comiso[1], y establece una nueva forma de determinación de las multas.

El Proyecto sigue un estándar internacional[2] que busca responsabilizar efectivamente a la empresa en materia penal. A nivel local, constituye un cambio paradigmático que inducirá un cambio cultural hacia la ética e integridad corporativa en forma acelerada. La transformación cultural deberá partir desde los gobiernos corporativos "*tone from the top*", generando, desde ya, conciencia organizacional, pues a la fecha no se sabe con claridad si existirá un periodo de adecuación para las organizaciones. La alta administración, junto con contribuir en la ética e integridad de todas las unidades de gestión, deberá ocuparse en dirigir acertadamente el desarrollo de nuevos sistemas integrales de prevención sobre este nuevo universo de delitos, que permitan detectar cabalmente la complejidad de los nuevos riesgos legales e incluir controles que permitan contener dichos riesgos de forma efectiva y evidenciable.

[1] Comiso de ganancias. Por el comiso de ganancias se priva a una persona de activos patrimoniales cuyo valor corresponde a la cuantía de las ganancias obtenidas a través del hecho, y se los transfiere al fisco. El comiso de ganancias se deriva del artículo 31 del Código Penal chileno.
[2] Otras jurisdicciones especialmente EE.UU y Europa.

Alta Gerencia y riesgos de ciberseguridad

Por Juan Pablo González Gutiérrez | Senior Manager Risk Advisory

En un entorno globalizado que cada vez exige estar más digitalizado y dependiente de nuevas tecnologías al interior de las organizaciones, comienzan a surgir diversos riesgos de carácter cibernéticos que no solo influyen en las actividades cotidianas de las organizaciones, sino que también necesariamente en los portafolios de riesgos de éstas, debiendo ser atendidas oportunamente por la Alta Gerencia de las Compañías.

Es importante mencionar una serie de normativas en el sector financiero, seguros, casinos y juegos, entre otros; que han establecido diversas obligaciones respecto del reporte de los incidentes de ciberseguridad, la necesidad de evaluar este tipo de riesgos en sus organizaciones, el establecimiento de políticas, procedimientos y planes de acción frente a los riesgos de ciberseguridad detectados, como también, contar con áreas especializadas en materia de ciberseguridad, a fin de tener una visión integral de esta materia. Su incumplimiento puede conllevar a que sean multadas como también afectar la confianza de los usuarios, así como su reputación.

En línea con este enfoque de integrar nuevas materias a los sistemas tradicionales de riesgos normativos, viene apoyado por la reforma en curso de la legislación respecto de los delitos informáticos (Boletín Nº 12.192-25)[1], que además de adecuar nuestra legislación al Convenio sobre Ciberdelincuencia (Budapest), agrega una serie de obligaciones para las empresas, particularmente modificando la Ley No. 20.393 sobre responsabilidad penal de las personas jurídicas, incorporando a los delitos informáticos como aquellos ilícitos contenidos en el artículo 1º de la mencionada norma. Ello, necesariamente repercutirá en la forma en que se adecuen los actuales programas de cumplimiento vigentes, particularmente aquellos instrumentos que lo conforman.

Especial atención revisten las matrices de riesgos, en que la actividad de una organización será de vital importancia tenerla presente para detectar la exposición a los riesgos cibernéticos, debiendo relacionarse intrínsecamente con

[1] Actualmente en tercer trámite constitucional, Comisión Mixta, Senado.

otras obligaciones normativas ya existentes, y que por su dependencia a ciertas tecnologías, no configuren el ilícito en sí, pero si sirvan para que se produzcan alguno de los otros tipos penales de la normativa y con ello, quede en evidencia una debilidad en el modelo de cumplimiento implementado.

La necesidad de actualizar e integrar políticas propias en materia de ciberseguridad al modelo de cumplimiento, tales como aquellas relativas al control de accesos a los servidores, al uso de los dispositivos electrónicos de la organización como autorizados por los colaboradores, el registro de actividades en los sistemas informáticos, la segregación de las funciones y otras medidas concretas para resguardar la confidencialidad, disponibilidad e integridad de la información, se tornarán esenciales para acreditar que se ha gestionado adecuadamente este tipo de riesgo. El rol de la Gerencia de la Seguridad de la Información o Ciberseguridad será preponderante en su relación con las áreas de Riesgos, Legal y Compliance.

Finalmente, la importancia de prepararse frente a estas obligaciones no es baladí, sobre todo si se tiene en cuenta las multas asociadas por parte de los reguladores en caso de incumplimientos, especialmente, en el caso de infracción a los deberes de dirección y supervisión de la Alta Gerencia para efectos de comprobar que se han adoptados las medidas solicitadas por la ley para prevenir que la organización sea defectuosa y que producto de ello, se cometan los respectivos ilícitos, por ejemplo los informáticos.

Principales consecuencias:

En la Incorporación de empresas automotoras como sujetos obligados de la Unidad de Análisis Financiero

Por Marianne Walker Acosta | Analista Risk Advisory

Con el objetivo de mejorar la persecución del narcotráfico y del crimen organizado en nuestro país, se está discutiendo en el Congreso Nacional un proyecto de ley (Boletín N°12.680-07)[1] que incorpora a las empresas automotoras entre aquellas obligadas a reportar las operaciones sospechosas y operaciones en efectivo a la Unidad de Análisis Financiero, en adelante "UAF". De aprobarse esta iniciativa, se determinarán importantes exigencias a los nuevos sujetos obligados, las cuales serán expuestas a continuación.

En primer lugar, las automotoras deberán implementar un Sistema de Prevención de Lavado de Activos y Financiamiento (LA/FT) del Terrorismo, el cual deberá contener a lo menos los siguientes elementos:

Designación de un Oficial de Cumplimiento, quién tendrá por función principal la coordinación de las políticas y procedimientos de prevención y detección de operaciones sospechosas, como, asimismo, responsabilizarse por el cumplimiento de las obligaciones contenidas en la Ley N°19.913 y circulares emitidas por la UAF. El Oficial de Cumplimiento deberá ostentar un cargo de alta responsabilidad dentro de la automotora, con el objeto de asegurar una debida independencia en el ejercicio de su labor.

Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo: Documento que deberá contener las políticas y procedimientos implementados para evitar que las automotoras sean utilizadas o puedan participar en una eventual comisión de los delitos de lavado de activos y financiamiento del terrorismo.

Capacitación del personal: las automotoras deberán desarrollar y ejecutar programas de capacitación e instrucción permanentes a sus empleados respecto al Sistema de Prevención de LA/FT, actividades a las que deberán asistir a lo menos una vez al año.

[1] Primer trámite constitucional/ Cámara de Diputados.

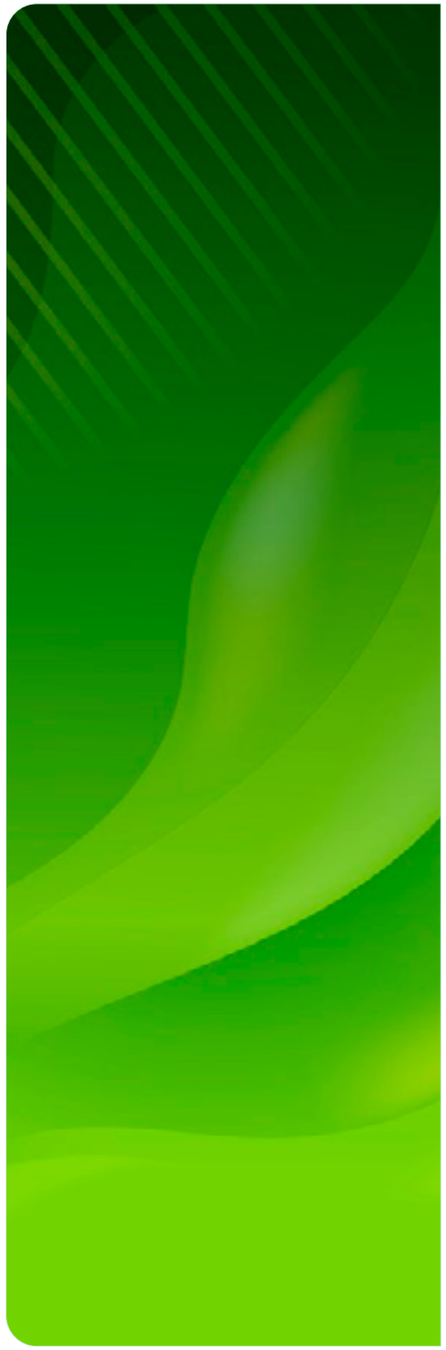
Conjuntamente con la implementación de un Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo, las empresas pertenecientes a la industria automotriz, deberán contemplar estrategias de gestión de riesgos de lavado de activos y financiamiento al terrorismo, por lo que deberán adoptar medidas de debida diligencia y conocimiento del cliente (DDC), las cuales se deberán emplear según el perfil de riesgo que hayan fijado tanto para sus clientes como para los productos y servicios que ofrecen. En caso de que el cliente sea una persona jurídica, deberán solicitar una declaración (proporcionada por la UAF) que contenga los datos de identificación suficiente respecto de la identidad de sus beneficiarios finales.

En el marco del cumplimiento de la obligación de debida diligencia y conocimiento del cliente (DDC), las automotoras deberán crear y mantener por un plazo mínimo de cinco años, los siguientes cuatro registros, ya sea en formato electrónico o físico:

- Registro de Operaciones en Efectivo (ROE).
- Registro de Debida Diligencia y Conocimiento del Cliente (DDC).
- Registro de Operaciones realizadas por Personas Políticamente Expuestas (PEP).
- Registro de Operaciones Electrónicas de Fondos.

Por último, las automotoras deberán informar y reportar a la UAF en el menor tiempo posible las operaciones sospechosas de las que tengan conocimiento en el ejercicio de su actividad, así como acompañar la documentación fundante necesaria. Asimismo, deberán informar semestralmente, durante los primeros 10 días hábiles de los meses de enero y julio de cada año, las operaciones en efectivo que realicen en el ámbito propio de su actividad y que superen los USD 10.000 o su equivalente en pesos chilenos. En el evento de que la automotora no tenga operaciones en efectivo que reportar, deberá enviar un "Registro de Operaciones en Efectivo Negativo".

En conclusión, la creación de un área de Cumplimiento y la designación de un Oficial de Cumplimiento, serán fundamentales para la implementación de un Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo eficaz, que se ocupe de velar por el cumplimiento de la totalidad de las exigencias normativas mencionadas anteriormente. Para lograr dicho cometido, las empresas automotoras deberán establecer un presupuesto anual para el funcionamiento de dicha área, así como proveer los medios tecnológicos y humanos requeridos para una correcta ejecución de la labor de prevenir que la empresa sea utilizada para lavar activos y/o financiar el terrorismo.



Proyecto de Ley pro-consumidor artículo 15 bis respecto de los datos personales de los consumidores

Por Camila Jaureguiberry Bravo | Consultor Risk Advisory

El Proyecto de Ley Pro-Consumidor (Boletín Nº 12.409-03) incluye una batería de modificaciones a considerar en esta materia. Una de éstas, es la inclusión del artículo 15 bis, a la normativa sobre Protección de los Derechos de los Consumidores. Esto constituye un hito relevante para efectos de explicitar la competencia que tiene el Servicio Nacional del Consumidor (SERNAC) en estas materias.

El texto del artículo sería el siguiente: *"Las disposiciones contenidas en los artículos 2 bis letra b), 58 y 58 bis de la presente ley, serán aplicables respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo, salvo que las facultades contenidas en dichos artículos se encuentren en el ámbito de competencias legales de otro órgano."*

Esto debe relacionarse directamente cuando existen intereses difusos o colectivos en materia de consumidor y, por ende, otorga facultades al SERNAC para iniciar mecanismos de fiscalización como eventuales acciones judiciales en caso de que se encuentre involucrado el interés difuso o colectivo de los consumidores, en el supuesto de que existiese afectación a los datos personales de estos. Es importante, señalar que solo es aplicable la norma en cuanto existan relaciones de carácter contractual.

Con este artículo se zanja una antigua discusión respecto de las posibles facultades del SERNAC en materia de protección de datos personales, ya que lo reconoce expresamente. Esta situación impacta en el funcionamiento de las Compañías, porque requerirá una mayor proactividad por parte de los proveedores ante actividades tales como la recolección y tratamiento de datos personales, provocando que las empresas deban volver a identificar las actividades riesgosas, sobre todo en un contexto de comercio electrónico.

En consecuencia, es recomendable implementar los **Programas de Cumplimiento de Ley de Protección al Consumidor**, que permitirán beneficiar de diversas formas a los proveedores, a saber:

1) Desarrollo de medidas preventivas, correctivas y de detección en eventuales incumplimientos.

2) Existencia de ambientes de control y estructuración de los riesgos en este ámbito.

3) Adecuada preparación ante una posible fiscalización del SERNAC.

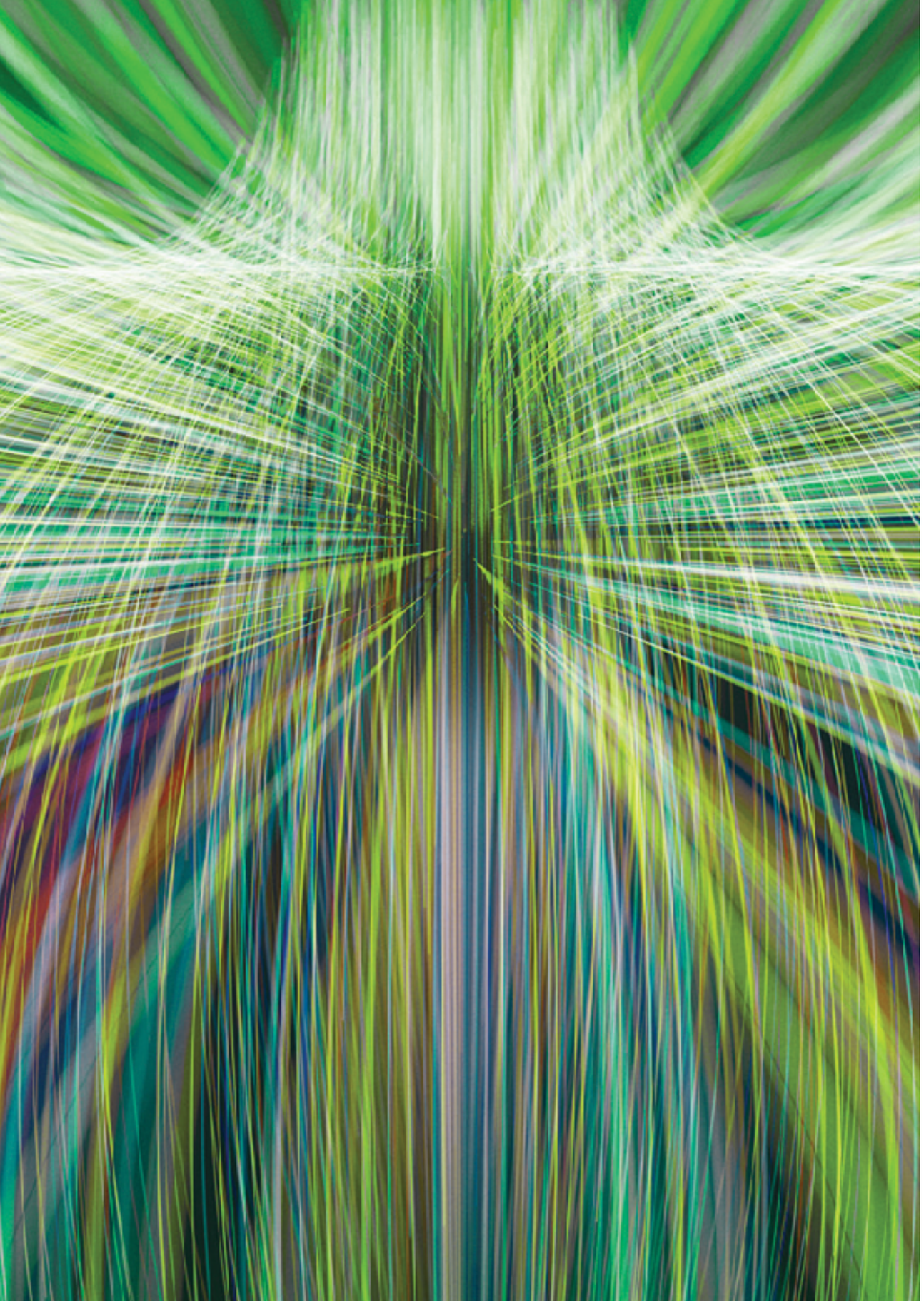
4) Circunstancia atenuante de la responsabilidad, entendiéndose que hay colaboración sustancial del proveedor, cuando se cumpla con los requisitos fijados por ley.

5) Evidencia una actitud proactiva en la protección de los Derechos del Consumidor por parte de la organización.

6) Constituye una buena práctica de gestión corporativa.

7) Modelo de cumplimiento complementario a las otras regulaciones a la que están sujetos los proveedores o empresas.

Finalmente, en una concepción moderna de los que es el Derecho, la regulación y la empresa, la autorregulación cobra más valor para actuar de manera proactiva ante posibles incumplimientos, ya no solo prima lo normativo, sino que también los riesgos que pueden afectar la reputación de la organización.



Rosario Norte 407
Las Condes, Santiago
Chile
Phone: (56) 227 297 000
Fax: (56) 223 749 177
deloittechile@deloitte.com

Av. Grecia 860
3rd floor
Antofagasta
Chile
Phone: (56) 552 449 660
Fax: (56) 552 449 662
antofagasta@deloitte.com

Alvares 646
Office 906
Viña del Mar
Chile
Phone: (56) 322 882 026
Fax: (56) 322 975 625
vregionchile@deloitte.com

Chacabuco 485
7th floor
Concepción
Chile
Phone: (56) 412 914 055
Fax: (56) 412 914 066
concepcionchile@deloitte.com

Quillota 175
Office 1107
Puerto Montt
Chile
Phone: (56) 652 268 600
Fax: (56) 652 288 600
puertomontt@deloitte.com

Deloitte.

www.deloitte.com