Revista de Derecho, Nº 42 2022 pp. 55-79

DOCTRINA

COMPLIANCE - IMPORTANCIA DE LOS MODELOS DE PREVENCIÓN DE LOS DELITOS

Mario Morales Díaz[1]

RESUMEN: *El Compliance o cumplimiento normativo es definido como el cumplimiento o conformidad con las normas, leyes, estándares y políticas. También implica un sentido de responsabilidad, la obligación de respetar los códigos de conducta pertinentes, contar con un sistema interno formal de políticas, procedimientos, controles y acciones para detectar y prevenir incumplimiento de leyes, reglamentos y normas. En consecuencia, implementar un programa de Compliance es fundamental para las organizaciones, públicas y privadas, en la tarea permanente de prevención de ilícitos que puedan poner en riesgo su integridad, así como su reputación.*

La tendencia actual es transitar desde el cumplimiento, como requisito preventivo derivado de normas legales, hacia un modo de gestión basado en el respeto a las obligaciones y compromisos asumidos como valor fundamental. Importa más el comportamiento organizacional basado en una ética y conducta acendrada en la cultura institucional. El primer paso para formular un modelo de Compliance o de prevención de delitos consiste en identificar los riesgos legales y reputacionales que debe afrontar una organización determinada a partir de los cuales corresponde adoptar medidas de mitigación. Para contar con modelos de Compliance efectivos, estos deben integrarse con fluidez en la estructura de la organización que se trata, especialmente en lo que dice relación con el rol y las funciones que desempeña el oficial de cumplimiento. En el caso de una organización pública un sistema de Compliance ampliado

[1] **MARIO MORALES DÍAZ.** Auditor y Contador Público por la Universidad de Santiago de Chile, MBA Loyola College por Maryland. Jefe Finanzas Consejo de Defensa del Estado.

que no tenga por límite el sistema de prevención de lavado de activos, financiamiento del terrorismo y delitos funcionarios, constituye una oportunidad al cooperar en establecer un proceso continuo que dará como resultado que la entidad cumpla con sus obligaciones y fortalezca su reputación.

PALABRAS CLAVES: *Cumplimiento - Códigos de ética - Códigos de conducta - Modelos de prevención - Prevención - Riesgos (mitigación) - Oficial de cumplimiento*

ABSTRACT (Compliance – Importance of crime prevention models): *Compliance or regulatory compliance is defined as: "compliance or conformity with regulations, laws, standards and policies." It also implies a sense of responsibility, the obligation to respect relevant codes of conduct, having a formal internal system of policies, procedures, controls and actions to detect and prevent non-compliance with laws, regulations and standards. Consequently, implementing a Compliance program is essential for organizations, public and private, in the permanent task of preventing crimes that may put their integrity, as well as their reputation, at risk.*

The current trend is to move from compliance, as a preventive requirement derived from legal regulations, towards a management mode based on respect for the obligations and commitments assumed as a fundamental value. Organizational behavior based on ethics and conduct rooted in the institutional culture is more important. The first step in formulating a Compliance or crime prevention model consists of identifying the legal and reputational risks that a given organization must face, from which mitigation measures must be adopted. To have effective Compliance models, these must be fluidly integrated into the structure of the organization in question, especially in relation to the role and functions performed by the compliance officer. In the case of a public organization, an expanded Compliance system that is not limited to the system for preventing money laundering, financing of terrorism and official crimes, constitutes an opportunity to cooperate in establishing a continuous process that will result in the entity fulfill your obligations and strengthen your reputation.

KEYWORDS: *Codes of conduct - Compliance - Crime prevention model - Integrity - Risks (policies and regulations)*

1. INTRODUCCIÓN

Compliance es uno de los términos emergentes en el ámbito de la gestión de riesgos utilizado actualmente en la literatura técnica especializada en el desarrollo de modelos de prevención de delitos corporativos. Hoy se entiende que las materias cubiertas por el *Compliance* no se agotan en aquellas consagradas en la normativa, de manera que el riesgo de cumplimiento es concebido también como la posibilidad de que una organización padezca pérdidas económicas o de reputación generadas a consecuencia del incumplimiento de normas o de códigos de conducta aplicables a su negocio.

El *Compliance* o cumplimiento normativo es definido por Nitish Singh y Thomas Bussen, como "el cumplimiento o conformidad con las normas, leyes, estándares y políticas". También implica un sentido de responsabilidad y la obligación de respetar los códigos de conducta pertinentes. Desde una perspectiva más legalista, el *Compliance c*orporativo implica la elaboración de un sistema interno formal de políticas, procedimientos, controles y acciones para detectar y prevenir violaciones de leyes, reglamentos y normas. Si bien el código de conducta ayuda a establecer el tono corporativo general hacia las expectativas de cumplimiento, el programa de una compañía debe comprender una serie de mecanismos integrados, diseñados para abordar todos los aspectos en materia de cumplimiento. Estos componentes clave del programa incluyen el compromiso de los directivos con mayor jerarquía de la organización en la implementación de estos modelos, definición de estándares y procedimientos para detectar y prevenir fraudes. De tal manera, el contar con un programa de *Compliance* es fundamental para las organizaciones, públicas y privadas, para prevenir delitos que puedan poner en riesgo su integridad, así como su reputación.

Los programas de cumplimiento normativo adquieren una importancia creciente en los Estados Unidos durante el siglo XXI a partir de escándalos financieros de alta connotación pública, como lo fue el caso Enron, World Com, FTX, entre otros; no obstante que desde mediados del siglo pasado se contaba con regulaciones para la prevención de conductas contrarias a la corrupción. A la sazón, nuestro país no ha estado exento de estos

escándalos, estando aún en la retina los casos de La Polar, Cascadas, Caval, por nombrar algunos.

En Chile, los modelos de cumplimiento normativo nacieron vinculados a la prevención del lavado de activos, con la vigencia de la Ley Nº 19.913, que crea la Unidad de Análisis Financiero (UAF) y con posterioridad, a partir de diversos casos de connotación pública, el *Compliance* ha ido adquiriendo una dimensión más compleja, de modo que hoy las organizaciones pueden verse enfrentadas al diseño y puesta en marcha de modelos que abarcan una diversidad de materias, como el lavado de activos, delitos funcionarios, financiamiento del terrorismo, receptación, negociación incompatible, corrupción entre particulares, apropiación indebida, administración desleal, delitos sobre responsabilidad penal de las personas jurídicas, medio ambiente, libre competencia, entre otras. En suma, en nuestro país, la incorporación de los sistemas de *Compliance* va tomando importancia en relación con la incorporación de normas, más allá de la Ley N° 20.393 de Responsabilidad Penal de Personas Jurídicas, en donde las medidas de prevención se consideran como elementos importantes al momento de determinar las penas aplicables en caso de infracción administrativa o delito.

En general, el cumplimiento normativo ha ganado relevancia en los actuales entornos regulados, donde la gran cantidad de leyes que se publican generan en grandes organizaciones un complejo contexto para gestionar todos los requerimientos y obligaciones que vienen exigidas por la normativa. La tendencia actual es transitar desde el cumplimiento, como requisito preventivo derivado de normas legales, hacia un modo de gestión basado en el respeto a las obligaciones y compromisos asumidos como valor fundamental que da cuenta de la actuación de los miembros de una organización, es decir, importa más el comportamiento organizacional basado en una ética y conducta acendrada en la cultura institucional, lo que explica por qué las labores de *Compliance* estén siendo desarrolladas, con mayor frecuencia, por los denominados *Chiefs Ethics and Compliance Officers.*

En un escenario como el descrito, el cumplimiento normativo puede convertirse en una tarea compleja de asumir, desde el punto de vista de los recursos que se requieren para satisfacer cada uno de los requerimientos

establecidos en el ordenamiento jurídico y por la organización como objetivos de *Compliance.* Un aspecto que puede facilitar esta labor radica en entender que el cumplimiento normativo se concreta a través de la formulación de modelos que cuentan con elementos básicos comunes y donde prevalezca una visión sistémica, amplia e integral con independencia del tipo de norma cuyo incumplimiento se pretenda evitar o administrar. Por lo tanto, el análisis de estos elementos comunes puede contribuir a la construcción de programas de *Compliance* que integren adecuadamente la gestión de los diversos riesgos normativos que afronta una organización, tal como el recomendado por la Comisión para el Mercado Financiero que insta a las entidades que regula, a elaborar códigos de autorregulación que contengan normas de gobierno corporativo, ética empresarial, transparencia y competencia leal.

2. EL SISTEMA O MODELO DE PREVENCIÓN DE DELITOS

2.1. Aspectos Generales

El primer paso para formular un modelo de *Compliance* o de prevención de delitos consiste en identificar los riesgos legales y reputacionales que debe afrontar una organización determinada a partir de los cuales corresponde adoptar medidas de mitigación. Estos riesgos dependen, entre otros factores, del giro, el tamaño, la ubicación geográfica y los productos o servicios ofrecidos por una empresa, así como de la forma jurídica que adopta la organización, de modo que no existe un modelo de cumplimiento idéntico a otro.

De esta manera habrá organizaciones comprendidas simultáneamente en el ámbito de aplicación de más de un modelo de *Compliance,* como puede ocurrir, por ejemplo, con aquellas sociedades que están obligadas debido a su giro, a implementar un modelo de prevención de lavado de activos y contra el financiamiento del terrorismo cumpliendo con lo dispuesto en la Ley Nº 19.193 y que, además, pueden adoptar el modelo voluntario de prevención de delitos contemplado en la Ley Nº 20.393. Para contar con modelos de *Compliance* efectivos, estos deben integrarse con fluidez en la estructura de la organización especialmente en lo que dice relación con el rol y las funciones que desempeña el

oficial de cumplimiento. En el caso de una organización pública un sistema de *Compliance* ampliado que no tenga por límite el sistema de prevención de lavado de activos, financiamiento del terrorismo y delitos funcionarios, constituye una oportunidad al cooperar en establecer un proceso continuo que dará como resultado que la entidad cumpla con sus obligaciones y fortalezca su reputación. El desafío que presenta no es menor pues las prácticas deben integrarse a la cultura organizacional y en el comportamiento de las personas que la integran.

2.2. Elementos Fundamentales del Sistema o Modelo

Para que un Sistema, Modelo de Prevención de Delitos o Programa de Cumplimiento sea eficaz debe considerar al menos cuatro de los siguientes elementos fundamentales: a) prevención, b) detección, c) respuesta y d) mejora continua, teniendo como foco la cultura organizacional y la gestión de riesgos.

2.2.1. Elementos de Prevención

En los elementos de prevención el modelo conocido de "las tres líneas de defensa" resulta importante de considerar, toda vez que asigna a cada línea un rol esencial e irremplazable. Así, los organismos que participan en la primera línea de defensa, tales como las gerencias operacionales y divisiones similares, deben contar con sistemas de control interno capaces de detectar y neutralizar eventuales amenazas al cumplimiento de sus objetivos; del mismo modo, la segunda línea de defensa revela el papel del Compliance y la gestión de riesgos, en su tarea de supervisar los procesos operacionales y establecer instrumentos de monitoreo que mitiguen riesgos y por último, en la tercera línea, corresponderá una tarea insustituible a los órganos de auditoría interna que, gozando de autonomía e independencia de las áreas operacionales y ejecutivas, buscan el aseguramiento de los sistemas de control.

EL MODELO DE LAS TRES LÍNEAS DE DEFENSA

Adaptado de la Guía emitida por ECIIA/FERMA sobre la
8va Directiva de Derecho de Sociedades de la Unión Europea, artículo 41

Los elementos de prevención diseñados buscan prescribir la conducta de los miembros de la organización y señalan las consecuencias de su incumplimiento. De aquí la importancia de la elaboración de los diversos tipos de normas internas que las organizaciones desarrollan, tales como códigos de ética, políticas, procedimientos, instructivos o protocolos.

Los protocolos y programas de cumplimiento deben ser aprobados por las más altas autoridades de la organización, siguiendo una hoja de ruta piramidal desde los instructivos o protocolos hasta el código de ética. Es central que estos aspectos normativos internos tengan las características de ser realistas, medibles y aplicables, con un uso de lenguaje simple y preciso, auditables, consistentes con otras normas internas, estableciendo responsables claros y accesibles a todo el personal.

En la formulación, desarrollo y publicación del código de ética debe invertirse todo el tiempo necesario para que goce de aplicabilidad, sea efectivo y, especialmente, representativo de los valores que la organización desea plasmar en su gestión. El código de ética debe considerarse como piedra fundacional del programa de cumplimiento pues trata de la postura valórica de la institución, debe desarrollarse en base a principios o conductas, teniendo como límite el respeto a los derechos del personal, sus infracciones deben ser sancionables y su diseño atractivo y amigable.

Dado que las normas no crean cultura por sí mismas, es fundamental internalizar las conductas deseables a través de programas de capacitación, difusión y concientización. En consecuencia, la capacitación y entrenamiento debe tener un lugar de relevancia en el proceso de prevención, generando los incentivos adecuados y asociados a metas de desempeño medibles. Un buen programa de capacitación en *Compliance* debiera considerar como contenidos mínimos: normas internas, legislación vigente, casos reales, lecciones aprendidas, entre otras materias y tener un alcance a la totalidad del personal, con especial atención en los cargos expuestos y terceros relacionados, como proveedores, representantes, distribuidores y clientes. El tipo o modalidad de capacitación a utilizar debe obedecer a un diseño flexible de carácter presencial o telemático y su frecuencia debiera ser de carácter anual y cada vez que la legislación establezca nuevas regulaciones. La organización debe llevar registro de las capacitaciones efectuadas incorporándolas en la hoja de vida del personal, demostrando los tipos de prueba efectuados y sus resultados.

2.2.2. Elementos de Detección

Los elementos de detección de un sistema o modelo de prevención de delitos tienen como objetivo central la manifestación de una actitud diligente de la organización en verificar que el estándar de conducta prescrito en las normas internas se está efectivamente cumpliendo. De aquí fluye la necesidad de contar con un canal de denuncias, auditorías, monitoreo y seguimiento, como encuestas de percepción.

El canal de denuncias no es solo un email o un teléfono. Es un sistema integrado que debe estar constituido de medios de captación de denuncias, proceso de gestión de denuncias, proceso de investigaciones internas, proceso disciplinario y mecanismos de tratamiento de datos y reportería.

Entre los medios de captación directa de denuncias se encuentran: el email, teléfono, casilla de correo, buzón, el oficial de cumplimiento. Entre aquellos de captación indirecta pueden señalarse las denuncias recibidas por otros ejecutivos de la empresa. Todos estos casos deben ser accesibles, abiertos a terceros, garantizar la confidencialidad, el anonimato y una adecuada relación entre reacción y respuesta.

El proceso de gestión de denuncias debe estar formalizado como un procedimiento, definiendo perfiles de responsables, plazos y criterios de admisión o derivación de denuncias. El proceso de investigaciones internas, a su vez, debe también definir el perfil de investigadores, plazos, medidas objeto de investigación, de resguardo, informe de hallazgos y estar debidamente formalizado. Debe garantizar confidencialidad, anonimato y objetividad, auditabilidad, recoger principios de debido proceso y tener especial cuidado de no transgredir las garantías laborales.

En cuanto al proceso sancionatorio o disciplinario, debe admitirse el principio de inocencia, la objetividad e imparcialidad, dando garantías de no represalias y estando formalizado en un procedimiento interno de conocimiento de toda la organización. Como los anteriores procesos debe garantizar confidencialidad y anonimato. Respecto de las medidas disciplinarias estas deben extenderse a todo el personal sin distinción y los tipos de medidas pueden ser de carácter conservador (amonestación verbal, por escrito, multa) y de carácter extintiva, como el despido disciplinario.

El proceso de tratamiento de datos y reportería tiene la función de registrar todas las denuncias recibidas, derivadas, investigadas y los hallazgos (infracciones verificadas). Asimismo, debe llevar el registro de medidas disciplinarias recomendadas y aplicadas, garantizando el debido anonimato.

2.2.3. Elementos de Respuesta

Se trata de constituir la forma en que la organización reacciona una vez verificado un incumplimiento, sea aplicando medidas disciplinarias, adoptando un plan de acción que contenga el análisis de causas para identificar controles que fallaron, de qué manera incide en la cultura organizacional. Los tipos de planes de acción que pueden llevarse a cabo corresponden a una revisión y ajuste de políticas y procedimientos, un nuevo plan de comunicaciones y concientización, la revisión y ajuste de capacitaciones y entrenamientos, reparación del daño causado y la revisión y ajustes de los incentivos, entre otros.

2.2.4. Elementos de Mejora Continua

Los programas de cumplimiento deben actualizarse cada vez que se producen cambios internos, tales como crecimiento de la organización, modificación a la estructura organizacional, nuevas operaciones o líneas de negocios, nuevos países o áreas geográficas en operación. Los cambios externos también influyen en la actualización tales como cambios normativos, en el mercado relevante, cambios socio-económicos, etc.

Asimismo, estos programas deben evaluarse periódicamente respecto a su efectividad a través de métricas o indicadores de gestión.

En suma, de los elementos fundamentales tratados en este punto se espera que el sistema o modelo preventivo (programa de cumplimiento) a implementar cumpla al menos con los siguientes estándares: normas de conductas escritas, capacitación y entrenamiento, auditorías y evaluaciones para monitorear el programa, implementación de un sistema de reporte de reclamos y denuncias, aplicación de medidas disciplinarias e incentivos, sistemas de investigación y solución de denuncias y designación de un oficial de cumplimiento.

3. SISTEMA DE PREVENCIÓN SECTOR PÚBLICO

3.1. Antecedentes

Con el objetivo de prevenir que el sector público sea utilizado para la comisión de ciertos delitos, la Ley Nº 20.818 modificó la Ley Nº 19.913, incorporando a las superintendencias y los demás servicios y órganos públicos como instituciones obligadas a informar operaciones sospechosas a la Unidad de Análisis Financiero (UAF), agregando el siguiente artículo a la señalada ley: “Las superintendencias y los demás servicios y órganos públicos señalados en el inciso segundo del artículo 1º de la Ley Nº 18.575, orgánica constitucional de Bases Generales de la Administración del Estado estarán obligados a informar sobre operaciones sospechosas que adviertan en el ejercicio de sus funciones”.

Para la materialización de la normativa legal señalada, el Ministerio de Hacienda dictó el Oficio Circular N° 20, de 15 de mayo de 2015, y la Guía de Recomendaciones año 2015. La norma ordenó que las entidades públicas se inscribieran en el Registro de Entidades Reportantes de la Unidad de Análisis Financiero (UAF), designando un funcionario responsable de relacionarse con la UAF, que tiene por función analizar desde una perspectiva financiera todos los actos, operaciones o transacciones que se realizan para determinar cuáles de estas deben ser informadas bajo la modalidad de operación sospechosa. Además, en tal ocasión se impartieron recomendaciones para el diseño e implementación del sistema de prevención de delitos.

En el marco de estos antecedentes, la UAF efectuó las siguientes principales recomendaciones a considerar en el sistema de prevención de delitos:

- Designar un funcionario responsable de relacionarse con la UAF, y de coordinar las políticas y procedimientos de prevención y detección de delitos conforme a las características organizacionales propias de la entidad pública y de reportar eventuales operaciones sospechosas que se adviertan.

- Diseñar e implementar políticas y procedimientos para la construcción de un Sistema Preventivo contra los Delitos Funcionarios, el Lavado de Activos y el Financiamiento del Terrorismo que contendrá todas las políticas, procedimientos que se definan y principales señales de alerta.

- Elaborar una matriz de riesgo institucional con los procesos del negocio con riesgo de comisión de delitos funcionarios, lavado de activos y financiamiento del terrorismo.

- Establecer mecanismos para la supervisión del riesgo detectado y el monitoreo del programa ya sea continuo, regular o selectivo.

- Evaluar el diseño e implementación de declaraciones de conformidad.

- Diseñar un sistema y procedimientos de denuncias y consultas o comunicación, que cumpla estándares internacionales de transparencia, debido proceso, efectividad, ausencia de represalias y otras buenas prácticas.

En términos referenciales, para los efectos de apoyar el desarrollo e implementación de un Sistema de *Compliance* Público, en el punto siguiente se describe el Modelo de Prevención de Delitos establecido en la Ley Nº 20.393.

3.2. Modelo de Prevención de Delitos de la Ley Nº 20.393

Como ya se ha señalado, en Chile, la Ley Nº 20.393 establece la responsabilidad penal de las personas jurídicas frente a determinados delitos, cumplidas determinadas circunstancias. Como es sabido, su establecimiento encuentra su razón de ser en exigencias para el ingreso de nuestro país a la OCDE. Se establece en la ley la opción de crear modelos de prevención de estos delitos y definir un encargado de prevención de ellos. Los requisitos del modelo de prevención están contemplados en el artículo 4 de la ley, que define su estructura de cuatro elementos mínimos:

3.2.1. Designación de un Encargado de Prevención

Los aspectos esenciales a satisfacer respecto de este punto son los siguientes:

- Su nominación debe provenir de la máxima autoridad administrativa de la persona jurídica.

- El nominado durará en su cargo hasta tres años, lapso prorrogable por períodos de igual extensión.

- El encargado de prevención debe contar con autonomía respecto de la administración de la persona jurídica, de sus dueños, de sus socios, de sus accionistas o de sus controladores. No obstante, podrá ejercer labores de contraloría o auditoría interna.

3.2.2. Definición de Medios y Facultades del Encargado de Prevención

Es la propia ley la que determina qué se entiende por medio y facultades suficientes. Estos son, conforme al texto legal, a lo menos, los siguientes:

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

- Acceso directo a la administración de la persona jurídica para informarla oportunamente por un medio idóneo, de las medidas y planes implementados en el cumplimiento de su cometido y para rendir cuenta de su gestión y reportar a lo menos semestralmente.

3.2.3. Establecimiento de un Sistema de Prevención de Delitos

La ley fija el estándar, al precisar que este deberá contemplar a lo menos lo siguiente:

- La identificación de las actividades o procesos de la entidad, sean habituales o esporádicos, en cuyo contexto se genere o incremente el riesgo de comisión de delitos.

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

- La identificación de los procedimientos administrativos y de auditoría de los recursos financieros que permitan a la entidad prevenir sean utilizados en los eventuales delitos.

- La existencia de sanciones administrativas internas, así como de procedimientos de denuncia o persecución de responsabilidades pecuniarias en contra de las personas que incumplan el sistema de prevención de delitos.

3.2.4. Supervisión y Certificación del Sistema de Prevención de Delitos

- Se establece la obligación de coordinar medidas de control y supervisión del modelo con el objetivo de garantizar su permanente adecuación a las mejoras prácticas en la materia.

- Se confiere a las personas jurídicas la opción de certificar la suficiencia y operatividad de su modelo de prevención de delitos.

4. ASPECTOS CENTRALES DE LA FUNCIÓN *COMPLIANCE*

Los asuntos relacionados con la autonomía, independencia, responsabilidades y perfil del encargado de prevención o *Compliance* officer, constituyen elementos esenciales en la implementación y éxito de un sistema de prevención de delitos y que se revisan a continuación.

4.1. Autonomía e Independencia

La normativa señala que el encargado de prevención deberá contar con autonomía respecto de la administración de la Persona Jurídica, de sus dueños, de sus socios, de sus accionistas o de sus controladores. La autonomía hace referencia a la capacidad del órgano de Compliance de actuar por iniciativa propia, sin necesidad de estar recibiendo órdenes o mandatos específicos. La independencia supone neutralidad de juicio que garantiza un recto proceder de la función de *Compliance*. Se refiere a la distancia respecto de los objetivos del negocio y ausencia de represalias por el desarrollo de sus cometidos.

Para desarrollar su función con libertad y neutralidad el oficial de cumplimiento debe tener libre acceso a personas y documentos, como a grupos de trabajos o comités donde se debaten o toman decisiones susceptibles de entrañar riesgos de *Compliance*. En consecuencia, es relevante que la administración de la persona jurídica haga públicas las facultades como el nombramiento y la comunicación, de dotarlo de representación para actuar ante terceros, como de asignar los recursos (presupuesto, equipo, materiales, etc.) para desarrollar sus cometidos.

Como amenazas a la autonomía e independencia se tienen las siguientes situaciones:

- Dependencia funcional de administradores ejecutivos.
- Dependencia temprana de cargos de áreas financieras o de gestión de riesgos que debieran estar separadas.
- Carencia de recursos. Es importante que exista capacidad real de asignar presupuesto.
- Falta de empoderamiento. Debe ser respetado y con capacidad para sostener su opinión.

4.2. Responsabilidades del *Compliance* Officer

Las funciones del *Compliance* Officer son de supervisión (tiene deberes propios de vigilancia y control) y no necesariamente de decisión. Se espera que desempeñe correctamente y con la debida diligencia la función informando de los resultados al Directorio o Gobierno Corporativo. Debe velar por los daños que pueda sufrir la organización (incluye daños reputacionales) o por los daños que pueda causar a terceros.

En suma, el *Compliance* Officer debe actuar diligentemente y desarrollar correctamente: a) las actividades del modelo de prevención, b) los procedimientos establecidos, c) reportar a la administración, d) escalar comunicación de riesgos para evitar su materialización, e) velar por la implementación efectiva del programa, f) velar por la permanente adecuación y actualización del programa, g) velar porque empleados sean entrenados y formados.

4.3. Perfil del *Compliance* Officer

Se requiere, evidentemente, una formación apropiada y preferentemente acreditada por órganos especializados en *Compliance* o entidades universitarias que desarrollan programas de cumplimiento o

modelo de prevención de delitos. Asimismo, resulta clave que el nominado acredite experiencia en estas materias y tenga una visión amplia de la organización y, además, cuente con las competencias "blandas" necesarias para interactuar con todos los niveles de la organización, especialmente, en la relación directa con ejecutivos, gerentes y directores.

En cuanto a la profesión, dado el carácter multidisciplinario de las funciones del *Compliance* Officer, en la práctica estas podrían corresponden a: abogado, auditor, economista, profesional de gestión de riesgos, psicólogo organizacional y otras profesiones afines.

5. GESTIÓN DE RIESGOS Y *COMPLIANCE*

5.1. Aspectos Generales

La gestión del riesgo consiste en identificar, analizar y valorar los focos de riesgo que amenazan a la organización, para determinar así el modo de gestionarlos dentro de parámetros aceptables. Existen diversos tipos de riesgos susceptibles de provocar tanto daños económicos como reputacionales, incluyendo el incumplimiento de las obligaciones de *Compliance*.

Existe una evidente relación entre gestión de riesgos y *Compliance*. Esta última vela por el cumplimiento de las directrices autoimpuestas de gobernanzas y, por otra parte, tanto para estas como para el resto de las obligaciones, se recurre a técnicas de gestión de riesgos.

Del mismo modo, *Compliance* está relacionado íntimamente con gobernanza en la organización, instancia en que surgen principios como buenas prácticas y que luego se incorporan en derecho. Muchas disfunciones de modelos de *Compliance* obedecen realmente a esquemas de gobernanza deficientes, y un buen modelo no tendrá eficacia si está ubicado en un mal entorno de gobernanza.

5.2. Enfoque basado en Riesgos

De acuerdo con el Grupo de acción Financiera para América Latina (GAFILAT), el riesgo es definido como "una función que se encuentra determinada por la interacción de tres variables: amenaza, vulnerabilidad y consecuencia o impacto".

En el enfoque basado en riesgos, la amenaza la representa una persona, un grupo de personas, cuyo objeto o actividad tiene el potencial de afectar el normal devenir de un Estado, una sociedad o una economía.

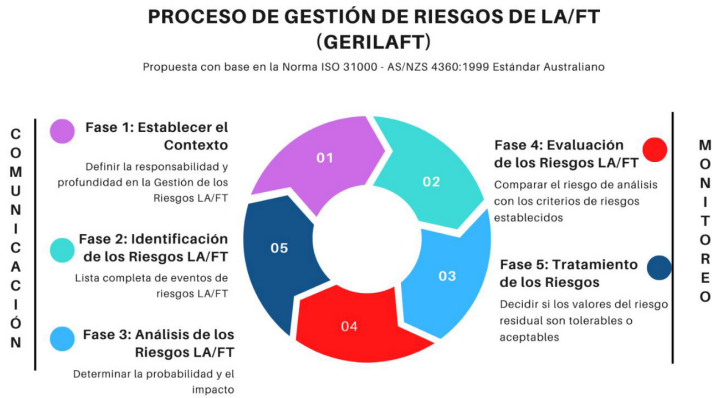
Como factor determinante del riesgo, la evaluación de la amenaza requiere del conocimiento del ambiente donde se desarrollan los delitos determinantes y cuáles serían los ingresos generados por las actividades criminales. Las vulnerabilidades comprenden aquellas debilidades que pueden ser explotadas por la amenaza o que pueden facilitar y/o permitir sus actividades. En el contexto de la evaluación de riesgos y apreciando las vulnerabilidades como concepto absolutamente distinto al de amenaza, se debe focalizar la atención en los factores que significan debilidades en el sistema o en los controles estatales. Mientras la amenaza es algo extrínseco al sistema, la vulnerabilidad es un aspecto intrínseco del mismo que facilita la actuación de la primera. Por su parte, las consecuencias se refieren al impacto o daño que los delitos perpetrados pueden causar e incluye los efectos de la actividad delictual y terrorista en el sistema, en las instituciones, así como en la economía y en toda la sociedad. Las consecuencias a su vez pueden ser consideradas a corto y a largo plazo y relacionarse con determinados intereses nacionales, regionales y locales, reputación internacional, sectores de negocios, comunidades, etc.

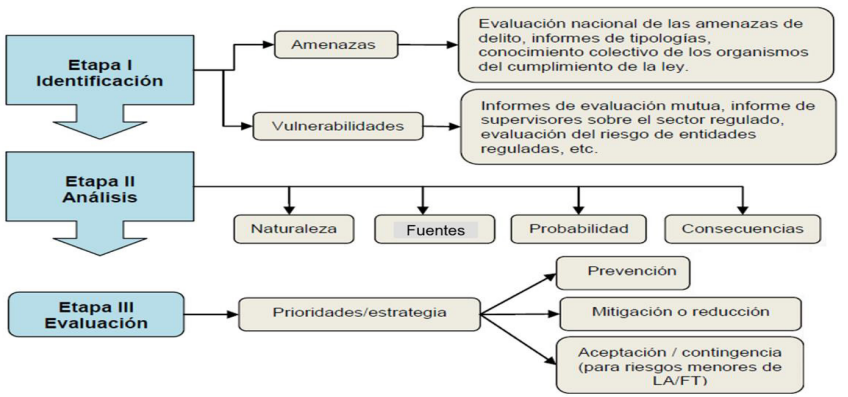
5.3. Administración del Riesgo

La administración del riesgo es un término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. La administración de riesgo es tanto identificar oportunidades como evitar o mitigar pérdidas y

puede ser aplicado a todas las etapas de la vida de una actividad, función, proyecto o producto.

Un esquema clarificador del concepto de administración de riesgo lo representa adecuadamente la Norma ISO 31000, que incorpora las etapas señaladas en la Guía del GAFI (2013), constituyéndose en una adecuada propuesta para evaluar los riesgos que se presenta en los gráficos siguientes:





Fuente: GUÍA GAFILAT – Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Diciembre 2020.

5.4. Matriz de Riesgo – Diseño de un Mapa de Riesgo

El diseño de un Mapa de Riesgos pretende identificar procesos, actividades, funciones o tareas riesgosas, cuantificando su probabilidad de ocurrencia y la medición del daño potencial asociado a su ocurrencia. La idea es sintetizar la información relativa a las indeterminaciones que afronta la organización y colaborar en las estrategias destinadas a mitigar la exposición y daños potenciales. En esta tarea es central identificar los factores de riesgos considerando en la matriz de riesgos los eventos asociados a clientes, productos y servicios, zonas geográficas de operación y canales de distribución, como se ejemplifica en el gráfico siguiente:

Fuente: GUÍA GAFILAT – Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Diciembre 2020.

En la elaboración de un Mapa de Riesgo se pueden identificar determinadas fases. A saber:

- Contexto
- Identificación de riesgos
- Análisis, asignación y valoración de los riesgos
- Identificación de controles
- Análisis, asignación y valoración de controles
- Establecimiento de opciones de tratamiento de los riesgos
- Monitoreo de los riesgos
- Revisión

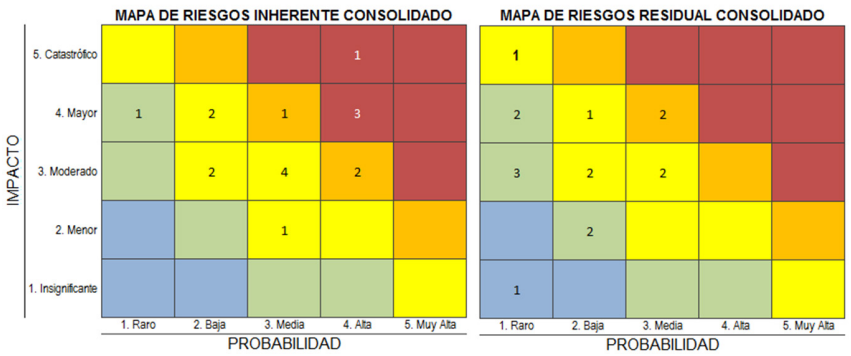
En el punto siguiente se analizan las fases de mayor relevancia.

5.4.1. Identificación de Riesgos

Identificar los riesgos posibilita conocer los eventos potenciales que pueden afectar el logro de los objetivos estratégicos de la organización. Se trata de establecer los agentes generadores de riesgos, las causas y los efectos de su ocurrencia, para lo cual se utilizan metodologías de recolección de información y determinación de riesgos existentes y potenciales como entrevistas con expertos, dueños de procesos, revisión de registros, lluvia de ideas, cuestionarios, encuestas de percepción, entre otras.

5.4.2. Valoración de Riesgos

El riesgo debe ser asignado a uno o varios procesos de la organización, en los cuales tendremos identificados los departamentos o áreas que intervienen. De no contarse con la identificación de procesos será necesario elaborar un mapa de los procesos más significativos identificando a un responsable de estos. Para la valoración es útil apoyarse en una matriz de doble entrada: probabilidad/frecuencia e impacto. La matriz más utilizada es la de 5x5 como se exhibe en la figura siguiente.

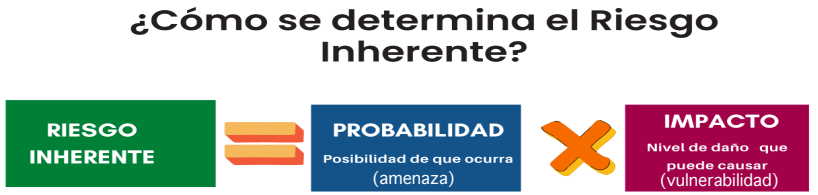


Fuente: GUÍA GAFILAT – Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Diciembre 2020.

Evaluar la probabilidad e impacto de los potenciales riesgos es un proceso en el que hay que contar con algunos factores económicos, financieros, operacionales, reputacionales y legales. No todos los riesgos potenciales tienen la misma probabilidad y el mismo impacto en todos los casos. Las medidas de probabilidad pueden ir desde niveles "muy improbable" hasta "altamente probable", cuyos rangos asignan porcentajes de 1% hasta 100%.

Respecto del impacto, esto es, el daño que supondría para los objetivos estratégicos de la organización que el riesgo se concretara en un suceso cierto, se deberán también considerar factores de orden financiero, operacionales, reducción del rendimiento de la actividad, pérdida de imagen, reputación, aspectos legales y regulatorios. Al igual que la probabilidad el impacto se categoriza en diversas medidas desde "insignificante", cuya materialización no genera pérdidas financieras ni compromete de ninguna forma la imagen pública de la organización, hasta "catastrófico", cuya materialización puede generar pérdidas financieras que tendrán un enorme impacto en su viabilidad económica y/o comprometen totalmente la imagen pública de la entidad.

Finalizado el proceso de valoración se obtiene la severidad del riesgo inherente (sin mitigantes):



Fuente: GUÍA GAFILAT – Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Diciembre 2020.

5.4.3. Valoración de Controles

Antes de valorar los controles existentes es preciso identificarlos con los documentos internos que los aprueban. En caso de no existir debe recomendarse su formalización. Estos controles son los que permitirán, en última instancia, o bien reducir la probabilidad de ocurrencia de un suceso o, si este se produce, minimizar su impacto.

Identificados los controles, es posible calcular el riesgo, esta vez considerando el nivel de vulnerabilidad de los controles disponibles en la organización, surgiendo el concepto de riesgo residual, que es aquel que subsiste, después de haber implementado los controles. Estos podrán ser más o menos efectivos, dependiendo de su tipología que pueden tener el carácter de preventivos, detectivos, correctivos, frecuencia, etc.

El grado de efectividad del control determinará el grado de reducción que proporciona ese control sobre un determinado riesgo. Estas metodologías de cálculo deben estar previamente definidas y procedimentadas.

5.4.4. Monitoreo de los Riesgos

El monitoreo de los riesgos es necesario, permite determinar si todos los componentes del plan de prevención operan efectivamente y si el

resultado de los controles identificados es reportado oportunamente al órgano de *Compliance.* Para el monitoreo de los riesgos se definirán indicadores cuantitativos o cualitativos, así como los controles asignados, lo que constituye el plan de acción. En caso de que un indicador supere la tolerancia fijada, serán los propietarios de los riesgos los encargados de analizar las causas. La efectiva labor de monitoreo no solo contribuye a realizar análisis de causa, sino que permite identificar qué procesos son vulnerables a estos riesgos y con base a ello desarrollar nuevos planes de acción.

6. CONCLUSIONES

El desafío principal que enfrenta la función *Compliance* y los sistemas o modelos de prevención es abandonar los archivos y estanterías legalistas donde se encuentran reposando y, en consecuencia, está la gran y no fácil tarea de incorporarla en la base y centro de la organización, a través de la gestión del cambio cultural.

Si bien se desconocen estudios estadísticos de la penetración del *Compliance* en las empresas chilenas, asiste la convicción, certificaciones de modelos mediante, que las empresas que cotizan en bolsa, el sector bancario y mediana empresas de diversas industrias han incorporado gradualmente esta función teniendo como referencia el modelo de prevención de delitos que establece la Ley Nº 20.393. A contrario sensu, las organizaciones de menor tamaño están lejos de iniciar este camino. En el ámbito del sector público se observa con interés que, al menos, la autoridad del Ministerio de Hacienda se ha ocupado de instruir a los órganos de la administración centralizada y descentralizada de cumplir con requisitos mínimos en la tarea de prevención de delitos de lavado de activos. Del sector municipal, se asume, al igual que las organizaciones de tipo pyme, estarían a la zaga de esta iniciativa. En atención a las iniciativas anticorrupción que han promovido los últimos gobiernos, se esperaría que, en el siguiente lustro, los organismos del Estado exhiban sistemas robustos de *Compliance*.

En cuanto a la estructura de la función *Compliance* se observa la figura emergente de un responsable bajo la denominación de *Compliance*

Officer o un departamento específico que depende mayoritariamente del Consejo de Administración o del Comité de Auditoría, teniendo por encargo principal la supervisión y monitorización del programa de *Compliance* y, en algunos casos, cuentan con un presupuesto específico que se dirige principalmente para cubrir los gastos relacionados con los recursos humanos (retribuciones y acciones de formación del personal).

Es deseable y del mayor interés de la sociedad que las motivaciones e incentivos para establecer un sistema de *Compliance* puedan corresponderse con el compromiso ético de la dirección de las organizaciones y no tanto o exclusivamente de la exención o atenuación de la responsabilidad penal y la preocupación por no perder oportunidades de negocio. Por tanto, atendiendo al alcance y contenido del sistema de *Compliance*, se espera que la gran mayoría de las organizaciones cuenten con los elementos imprescindibles de un sistema de gestión de *Compliance*: código ético o de conducta, canal de denuncias, mapa de riesgos y controles de cumplimiento, plan de monitoreo e informes periódicos al órgano de administración.

7. BIBLIOGRAFÍA

Compliance: ¿Por qué? Y ¿Para qué? Claves para su gestión – Patricio Véliz Moller, Yoab Bitran Hasson

Compliance. Visión general desde una perspectiva penal y comercial – Gustavo Balmaceda Hoyos, Rodrigo Andrés Guerra Espinosa, María Fernanda Juppet Ewing

Fuente: GUÍA GAFILAT – Estándares Internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Diciembre 2020.

La Responsabilidad Penal del *Compliance* Officer. Alejandro Turienzo.

Compliance Management: A How to Guide for Executives, Lawyers and Other *Compliance* Profesionals – Nitish Singh, Tomas Bussen.

Ley Nº 20.393. Sobre Responsabilidad Penal de las Personas Jurídicas.

Ley Nº 19.913 y sus modificaciones. Crea la Unidad de Análisis Financiero.