PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

Escuela de Posgrado

El riesgo legal y cómo afrontarlo en la empresa: Propuesta de un modelo de gestión

Trabajo de ınvestigación para obtener el grado académico de Magíster en Derecho de la Empresa que presenta:

Nelson Porras Condori

Asesor:

Bruno Edoardo Debenedetti Lujan

Lima, 2022

RESUMEN EJECUTIVO

La actividad empresarial y el riesgo se encuentran estrechamente relacionados, y uno de los riesgos que adquiere importancia en nuestros días es el denominado “riesgo legal” debido a la creciente normativa que deben cumplir las empresas y la creación y fortalecimiento de agencias gubernamentales cuya finalidad es el cumplimiento de la regulación.

La presente investigación tiene por objetivo entender los alcances del riesgo legal y el diseño de un sistema para la gestión del riesgo legal adaptable a la empresa, debido a que en la actualidad el incumplimiento de las normas jurídicas ha adquirido importancia en la gestión empresarial y requiere una respuesta que tengan un enfoque de prevención de riesgos, en este caso, del ámbito jurídico.

Uno de los principales temas abordados es la definición del riesgo legal, no sólo a partir de la concepción que se tiene del tema en la teoría de la gestión de riesgos, sino con los estudios sobre el sistema jurídico con la intención de adecuar el concepto a nuestra realidad.

Para la investigación se tomó en cuenta bibliografía sobre el tema principalmente en idioma extranjero y los desarrollos sobre el tema en los estudios sobre la gestión de riesgos, usando también como referencia los marcos de gestión de ISO y COSO, por lo que el enfoque de investigación es multidisciplinario.

Como parte de los resultados, se elaboró un modelo de gestión de riesgo legal aplicable a las empresas adecuado a la definición de riesgo legal considerando nuestro sistema jurídico, contemplando no sólo los lineamientos de los estándares mencionados, sino también en el modelo de gestión de riesgos de tres líneas de defensa, que incluye herramientas que pueden servir para quien desee emprender el reto de mejorar la gestión del riesgo legal.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

CAPÍTULO I: INTRODUCCIÓN

La actividad empresarial es conocida como una actividad de riesgo, es así que cuando se dice que una persona ha emprendido o ha decidido iniciar una empresa se entiende que tiene la voluntad de asumir determinados riesgos que de una u otra forma pueden generar beneficios o pérdidas, pero no sólo la decisión de emprender implica riesgo, sino la ejecución de las operaciones de la actividad económica elegida también comprende otros riesgos que varían de acuerdo al sector que se proponga analizar, es así que los riesgos de una empresa minera son distintos a una empresa pesquera o una empresa textil o en una empresa dedicada a la venta de productos para consumo masivo o retail; también son diferentes los riesgos que se tiene cuando los clientes son otras empresas o consumidores finales.

Entre los distintos tipos de riesgo a los que se expone la empresa, hay uno que es común a todos los sectores económicos, y aunque a veces es considerado como un asunto sólo de abogados; con el incremento de leyes, la creación de organismos regulatorios y cada vez más regulación de diverso tipo, la posibilidad de aplicación de sanciones por parte de un aparato estatal, el cierre de un establecimiento comercial por incumplir la regulación de defensa civil o la inhabilitación para ejercer el giro del negocio; hay más de una razón para que los empresarios los tomen en cuenta como riesgos, llevándolos a adoptar medidas para evitar que el incumplimiento de las leyes existentes afecten sus operaciones y también ha hecho frecuente que a través de sus gremios participen en el debate público cuando existe la posibilidad que una reforma legal afecte su actividad económica.

La presencia de este riesgo se hace evidente al observar las relaciones que establecen las empresas en su día a día, con sus clientes, proveedores, trabajadores, y demás personas no sólo de tipo privada sino también entidades públicas, que implican relaciones jurídicas y como tales comprometen normas del sistema jurídico que en caso de incumplimiento puede dar lugar a consecuencias de diversas índole en las empresas, desde el pago de multas, indemnizaciones, honorarios de abogados, gastos en procesos judiciales, hasta la denigración de la imagen, la marca

o sus productos, e incluso es percibido con potencial para afectar la misma existencia de la empresa (Gan@Más, 2016).

La posibilidad que la empresa se vea perjudicada por vulnerar una obligación legal también se encuentra acompañada de una tendencia presente en nuestro país, probablemente compartida con otros países de Latinoamérica, que Brithwaite citado por Martín (2013) denomina regulatory capitalism, entendido como el marco económico en el que el estado tiene cada vez menos servicios, pero con más normativa y agencias administrativas, que tienen como parte del enforcement la aplicación de las sanciones a las empresas en caso de infracción a las disposiciones bajo su supervisión, que se expresa como incremento o reforzamiento de organismos reguladores o supervisores que tienen como finalidad velar por el cumplimiento de determinada regulación aplicable a la actividad empresarial, como es el caso de la Superintendencia Nacional de Fiscalización Laboral (SUNAFIL), Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), la Autoridad Nacional de Protección de Datos Personales (ANPDP), Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), por poner algunos ejemplos; que potencialmente pueden ir acompañados de reclamaciones de terceros, en cuyo caso se incrementa el volumen de pérdidas que se puede sufrir por un incidente.

Pero no sólo se ha incrementado las obligaciones legales y los órganos de tipo administrativo que verifican su cumplimiento, sino también cada vez más se prevén consecuencias más gravosas por incumplimiento como es el caso de la Ley Nº 30424, que establece la responsabilidad administrativa de las personas jurídicas, sin dejar de lado que en determinadas circunstancias los gerentes, directores y demás directivos de la empresa, conocidos como parte de la alta dirección, incluso los propios trabajadores pueden ser objeto de sanciones, investigaciones y demás acciones de tipo legal que también afectan a la empresa, tal como ha sucedido en casos de conocimiento público a nivel nacional como Odebrecht y Graña y Montero, y a nivel internacional los casos de Enron, Lehman Brothers, Siemens entre otros.

Este riesgo emergente, en algunos sectores económicos como el financiero ha sido calificado como riesgo clave (Bejarano, Palencia, Montoya, & Sanchez, págs. 105-107) he incluido con

dicha denominación en la regulación sectorial, pues la Superintendencia de Banca, Seguros y AFP's (2009) en línea con las recomendaciones del Comité de Basilea de Supervisión Bancaria definió el riesgo legal como "posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros.", demostrando que se trata de un riesgo que debe ser tomado en cuenta.

En la medida que las empresas han asumido que su actividad comprende riesgos, desarrollaron herramientas para gestionarlos, en algunas actividades más que en otras, llegando a implementar unidades orgánicas dedicadas a los riesgos, que a nivel internacional se ha reflejado en la normalización técnica o emisión de marcos generales como es el caso del ISO 31000:2018 que comprende los lineamientos o marco general para la gestión de riesgos, y COSO ERM que es el marco integrado para la gestión de riesgo empresarial, sólo por mencionar los más conocidos, y que a su vez han publicado propuestas de lineamientos para la gestión del riesgo legal, como son ISO 31022:2020 y el Compliance Risk Management: Applying the COSO ERM Framework también del año 2020.

En este escenario, en el que se debe dar importancia al riesgo legal y que lleva a la necesidad de gestionarlo a fin que no impacte negativamente en la empresa, no se conoce si es suficiente la contratación de un asesor jurídico interno o habilitar una oficina interna para dicha labor, tampoco se conoce criterios de como priorizar los riesgos, de tal forma que puestos ante el escenario de que obligaciones legales deben ser controladas con mayor cuidado o si amerita la implementación de un programa de cumplimiento, probablemente la respuesta inmediata será lo que instintivamente reconozcan los que dirigen la empresa o los asesores legales a cargo, pero esa respuesta realmente es suficiente y garantiza una adecuada gestión del riesgo legal, será posible que las recientes publicaciones de ISO y COSO nos den una la solución plausible; está situación problemática se resume en la siguiente pregunta ¿Cómo gestionar el riesgo legal en las empresas?

Ante la cuestión formulada, como hipótesis planteamos que la forma más adecuada para evitar que la empresa se vea afectada por el incumplimiento de las normas jurídicas es reconocer que se

trata de un riesgo y la forma de gestionarlo es mediante la implementación de un sistema de gestión de riesgo legal, pues existen lineamientos para la gestión del riesgo en general, e incluso ahora se tienen pautas para la gestión del riesgo legal en particular, emitidas por organizaciones internacionales como ISO y COSO, cuyos lineamientos son generalmente aceptados en los diversos ámbitos de la actividad empresarial.

Para ello se debe partir de la definición del riesgo legal, que no se asimila al incumplimiento de la ley, pues la posibilidad de daños a la empresa también tiene otras fuentes del derecho como los contratos, así como las obligaciones generales de deber de cuidado o debida diligencia, que tienen el potencial de generar efectos similares a la vulneración de una norma jurídica.

El análisis de los estándares ISO 31022:2020 y Compliance Risk Management: Applying the COSO ERM Framework, orientados a organizaciones en general, puede dar puntos de referencia para el diseño de un sistema de gestión del riesgo legal en las empresas que tome en cuenta nuestra realidad y potencialmente sea aplicable en otros países de Latinoamérica por la similitud de nuestros sistemas jurídicos.

La iniciativa de diseñar un sistema de gestión de riesgo legal no se puede limitar a determinar los estándares o lineamientos que se deben cumplir, sino también cómo implementarlo y cómo conocer e informar el avance de la implementación.

Atendiendo a lo expuesto, el objetivo general de la presente investigación es diseñar un modelo de sistema de gestión de riesgo legal que sea aplicable a las empresas, que genere confianza sobre su efectividad, y que sea entendible por quienes están a cargo de la dirección empresarial.

Para alcanzar el fin principal de esta investigación planteamos como objetivos específicos los siguientes:

- Conocer y definir el riesgo legal en la medida que constituye el riesgo que será materia de gestión o control, por lo que, es importante entender sus alcances.

- Analizar los estándares ISO y COSO para la gestión del riesgo legal, a fin de comprender cuáles son sus requerimientos y si estos pueden ser adaptados a la realidad empresarial de nuestro país.
- Diseñar las herramientas que pueden ser utilizadas para asegurar la implementación de un modelo de gestión de riesgos que sea de fácil entendimiento y comunicación a la dirección de la empresa.

Para abordar el objeto de estudio, como enfoque metodológico elegimos el multidisciplinario, dado que no sólo se abordarán conceptos propios del derecho sino prioritariamente de la administración, en específico de la gestión de riesgos, por ello se iniciará por delimitar las definiciones clave, tales como riesgo, gestión de riesgos y modelos de gestión, generalmente utilizados por las disciplinas relacionadas a la gestión empresarial.

Luego, se analizará cómo es entendido el riesgo legal por parte de quienes lo han asumido como objeto de estudio, que por el momento comprende principalmente investigaciones en idioma inglés; así mismo cuál es la concepción que se tiene de dicho riesgo a nivel normativo, en el que como se mencionó anteriormente, ha sido introducido en la regulación del sistema financiero; y en la medida que también se efectuará la revisión de los estándares ISO y COSO, ambos marcos tienen su propia definición de lo que es el riesgo legal que igualmente debe ser analizados para tener un contexto adecuado.

Seguidamente, se analizará los marcos o lineamientos para la gestión de riesgos y como estos pueden ser adaptados para la gestión de riesgo legal, entre ellos las normas técnicas ISO 31000 referido a la gestión de riesgos, ISO 31022 para la gestión del riesgo legal, cuyos lineamientos permitirán tener un panorama más específico sobre el tema que nos ocupa, así como las recomendaciones COSO ERM para la gestión de cumplimiento, cuyas directrices también están relacionadas a la gestión del riesgo legal, y que en conjunto son los marcos de gestión de riesgos más difundidos, por lo que, el uso de su terminología o tenerlos como base para un modelo de gestión facilitará la comunicación con otros profesionales dentro de la empresa y quienes son los que generalmente reciben los informes relacionados al riesgo legal.

Asimismo, se realizará una exploración entre las herramientas de los sistemas de gestión, para identificar los instrumentos que se usan para implementar un sistema de gestión e informar de sus avances, lo que nos permitirá usar aquellas que sean adecuadas para la gestión del riesgo legal.

Finalmente, se procederá con el diseño de una propuesta de sistema de gestión de riesgo legal con la definición de lineamientos o requerimientos mínimos aplicables a empresas.

CAPÍTULO II: ESTADO DEL ARTE

2.1. El riesgo y su clasificación

2.1.1. Definición de riesgo

En el ámbito jurídico el riesgo no es un término nuevo, debido a que es estudiado en el ámbito del derecho civil, específicamente como parte del derecho de las obligaciones, con la denominación de teoría del riesgo. Su objeto es prever las eventualidades que ocurran desde que se asumen obligaciones y tiene por finalidad distribuir razonablemente las consecuencias en caso de incumplimiento de las prestaciones, estableciendo la asignación de responsabilidad sobre el riesgo en diferentes supuestos, pero dicha concepción es limitada para los fines de esta investigación, pues el riesgo que tenemos que abordar está asociado a la actividad empresarial, por ello no podemos auxiliarnos de los estudios realizados en el ámbito jurídico.

Uno de los puntos de partida recurrentes en la explicación del concepto de riesgos es a través de la comprensión de su finalidad. Las empresas existen con la intención de generar valor, a través de la gestión de diversos recursos para la obtención de los bienes o servicios que se ha propuesto ofrecer, y en el camino que recorren para alcanzar ese objetivo asumen riesgos que adecuadamente combinados dan lugar a la generación de beneficios. Desplegadas las actividades, en un contexto optimista se espera que dichos beneficios sean mínimamente tal como han sido planificados, y en sentido contrario, si los riesgos no han sido adecuadamente gestionados o aparecieron algunos no previstos, pueden tener efectos dañinos que no se limitan al interior de la empresa. Dependiendo de su naturaleza las consecuencias del riesgo pueden extenderse a los consumidores o clientes, o demás partes interesadas. Desde esa perspectiva hay una vinculación entre el riesgo y la rentabilidad, e incluso con sostenibilidad de la empresa; es así que se asume al riesgo como un elemento presente en las actividades de la empresa y es visto como una circunstancia o hecho con capacidad potencial de generar daño (Soler Ramos, y otros, 1999, págs. 53-54) (Cabeza & Torra, 2007, págs. 21-22).

Dicha definición resalta la presencia de dos elementos que de forma conjunta permiten entender lo que son los “riesgos”, por un lado, la probabilidad de ocurrencia de un evento dañoso o peligroso, y, por otro lado, que dicha probabilidad está ligada a los objetivos empresariales, combinando la preservación del capital de la empresa y la generación de valor.

Si bien, de forma general, se asume que el riesgo es un evento probable de tipo negativo que tiene potencial de impedir la generación de utilidades, Lizarzaburu (2012) lo define de forma más amplia como “la probabilidad de observar rendimientos diferentes a los esperados” y para determinación de dicha probabilidad es importante la identificación de los factores que generan riesgos, siendo implícito a la actividad empresarial la administración de riesgos, pues no asumir riesgos sería lo mismo que no realizar actividad alguna.

A nivel normativo, el ámbito donde más se ha desarrollado la gestión de riesgos es en el sistema financiero, por lo que el uso del término riesgos es frecuente en la regulación financiera, en la que también se ha definido al riesgo de forma similar a las reseñas efectuadas. La definición de riesgo que figura en la Reglamento de Gobierno Corporativo y Gestión Integral de Riesgos, Resolución SBS Nº 272-2017, que no tiene muchas diferencias con su predecesora la Resolución SBS Nº 037-2008 (aunque referida únicamente a la Gestión Integral de Riesgos) señala que debe ser entendido como la posibilidad de ocurrencia de un hecho externo o interno que genere impacto negativo en los objetivos de la empresa o en su situación financiera. Otra referencia normativa se encuentra en la regulación del mercado de valores, que en el Reglamento de la Gestión Integral de Riesgos (2015) define al riesgo de la misma forma que la regulación financiera mencionada.

A diferencia de la definición normativa, uno de los estándares reconocidos sobre gestión de riesgos, la norma ISO 31000 Gestión de Riesgos-Directrices cuenta con una definición amplia de riesgos, pues lo considera como desviaciones de los objetivos organizacionales generadas por la incertidumbre con efectos positivos (oportunidades) o negativos

(amenazas) o ambos (oportunidades y amenazas) (ISO, 2018), de tal forma que no se centra únicamente en los efectos negativos, incluso contempla la posibilidad que simultáneamente se presente con oportunidades.

Si se toma en cuenta que la empresa tiene en su misma creación la intención de generar beneficios aprovechando las oportunidades y evitando las amenazas, es razonable que los riesgos sean asumidos también como potenciales generadores de beneficios, y si bien en la doctrina no necesariamente existe consenso sobre la definición de lo que es el riesgo, su entendimiento desde un enfoque amplio, que también es compartido por las buenas prácticas resulta ser el más adecuado a la actividad empresarial.

2.1.2. Clasificación de los riesgos

A nivel de los estudios de la materia se encuentran varias clasificaciones, además que consideran diferentes perspectivas, por ejemplo, en función a quien asume el riesgo se dice que existen riesgos empresariales, que son asumidos por la misma empresa en el contexto de sus operaciones, y riesgos financieros, asumidos por quienes realizan las inversiones para fines de las operaciones de la empresa (Soler-Gonzalez, Varela-Lorenzo, Oñate-Andino, & Naranjo-Silva, 2018, pág. 55) (Cabeza & Torra, 2007, págs. 5-7). También hay otra clasificación en función a su origen, que los diferencia como riesgos internos y riesgos externos, siendo los primeros aquellos que se producen al interior de la empresa y los segundos aquellos que dependen de sucesos ajenos a la organización. Otra de las tipologías, es la realizada por Gómez y Partal (2010) que los clasifica los riesgos de acuerdo al factor explicativo, de la siguiente forma:

Tabla 1. Clasificación de los riesgos

Riesgo	**Factor explicativo**
Riesgo de crédito	Incumplimiento del contrato por variación en las condiciones y/o en las características de la contrapartida.
Riesgo de mercado	Cambios en el valor de las posiciones abiertas en activos financieros o sus derivados.

Riesgo de liquidez	Desajustes entre el exigible y la disponibilidad de fondos para un mismo periodo.
Riesgo país	Incumplimiento o retraso en el pago de la deuda adquirida a una entidad o país extranjero.
Riesgo operativo	Falta de adecuación o fallos de los procesos, el personal y los sistemas internos de la entidad.
Riesgo legal	Incumplimiento de la ley de alguna de las partes o inexistencia de marco legal.

Fuente: Albizuri (2015)

La denominación de los riesgos de acuerdo a la tabla, con ciertas diferencias en su concepción es la forma más frecuente de diferenciar los riesgos, que incluso puede incrementar la lista con otros riesgos como el de ciberseguridad o tecnológico, riesgo de tipo de cambio, entre otros, por lo que resulta funcional a nuestro objeto de investigación.

2.1. Riesgo legal

Si bien existe definición del riesgo legal en la regulación, este no se extiende a todas las actividades empresariales que generalmente toman en cuenta los estándares como ISO y COSO como guías de acción, por lo que, para un estudio sobre el riesgo legal debe considerarse dichas definiciones, además de las diversas posiciones de la doctrina, que serán tratados en las siguientes líneas.

2.1.1. El riesgo legal en la regulación y las buenas prácticas

A nivel de la normativa la definición del riesgo legal se encuentra en la regulación financiera, como se mencionó el sector económico que tiene más desarrollada la gestión de riesgos es el sector financiero cuya supervisión se encuentra a cargo de la Superintendencia de Banca, Seguros y AFP's, dicho organismo regulador definió al riesgo legal en la Resolución SBS Nº 2116-2009 como la "posibilidad de ocurrencia de pérdidas financieras debido a la falla en la ejecución de contratos o acuerdos, al incumplimiento no intencional de las normas, así como a factores externos, tales como cambios regulatorios, procesos judiciales, entre otros." siguiendo la concepción de riesgo como potencial generador de

daño, además proporciona luces sobre su alcance a las relaciones contractuales, incumplimiento de las normas, incluyendo factores externos que no son muy precisos al involucrar el término “otros”, siendo pertinente precisar que no existe marco adicional alguno que implique un riesgo para la empresa en el supuesto de no asumir la definición dada por el regulador.

Su incorporación en la normativa del sector financiero tiene influencia en las recomendaciones del Comité de Basilea, que lo considera como parte del riesgo operacional (Nuñez Mora & Chavez Gudiño, 2010) e incluyó una referencia al riesgo legal a pie de página, señalando que incluye “la posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados entre las partes” (Comité de Supervisión Bancaria de Basilea, 2006, pág. 159), con una concepción orientada a la incertidumbre que tiene potencial consecuencia prevista en la norma, como sería una multa, sanción, obligación de indemnización, orientando el origen a la acción del supervisor o relaciones contractuales.

La novísima norma técnica ISO 31022-Directrices para la gestión del riesgo legal también contempla una definición para el riesgo legal, que sigue la concepción general de ISO del riesgo como evento incierto con efectos sobre los objetivos, que se caracteriza como riesgo legal al tener relación con la ley, los contratos, o derechos u obligaciones no contractuales, estos últimos asociados al deber de cuidado (ISO, 2020); definición que incluye no solo los riesgos por el cumplimiento de la ley y de los contratos, sino también aquellas relaciones jurídicas que se generan de forma no contractual, sea por la afectación a los derechos de la empresa, como sería el hecho que un tercero ocasione un incendio en un inmueble de propiedad de la empresa o porque se genere afectación a terceros a partir de acciones o decisiones, como sería el hecho que representantes de la empresa participen en hechos por los cuales los afectados inicien acciones legales por responsabilidad civil contra la empresa.

Por su parte, COSO (2017) tiene la peculiaridad de utilizar la denominación de riesgo de cumplimiento a lo que ISO define como riesgo legal, es así que entiende por riesgo de

cumplimiento a la posibilidad de incumplimiento de leyes, reglamentos, términos contractuales, normas o políticas internas con potencial de generar impactos de tipo financiero o no financiero, que comprende las diferentes materias del derecho, sea civil, penal o de sanciones administrativas u otros efectos de tipo negativos. Siendo una de las primeras diferencias que no lo reduce a los asuntos legales, sino los extiende hasta a las normas o políticas internas, y considera dentro su alcance no sólo a los miembros de la alta dirección sino también al personal, pues a pesar de que los incumplimientos sean efectuados por personas, las infracciones pueden ser atribuibles a la organización si es que se realizaron en el curso habitual de las operaciones de la empresa.

Otro de los aspectos a resaltar en el marco COSO es que expresamente incluye el factor ético como potencial generador de riesgo de cumplimiento, y de forma particular además de los parámetros de conducta o estándares éticos de la organización, da importancia a la gestión de conflicto de interés, debido a esa amplitud señala que las organizaciones tienen la libertad de crear sus propias listas de lo que entienden por riesgo de cumplimiento. Dicha concepción es mucho más amplia que las anteriores con mayor preponderancia del componente ético lo que explica el hecho de contemplar entre las fuentes de riesgo el incumplimiento de las políticas internas.

Como se observa a nivel regulatorio y de las buenas prácticas no existe consenso sobre lo que se debe entender por riesgo legal, incluso en la propia denominación, pues COSO lo denomina riesgo de cumplimiento, no obstante, dan algunos elementos a considerar como el incumplimiento de las normas, contratos, parámetros éticos y la posibilidad de incluir no sólo los impactos de tipo financieros sino también los no financieros.

2.1.2. El riesgo legal en la doctrina

Por lo general la definición del riesgo legal han sido elaboradas en el marco de los estudios sobre riesgos de quienes se dedican a la administración empresarial, sin embargo, a la fecha existen estudios específicos sobre el riesgo legal elaborados por quienes ejercen docencia o la profesión de abogado generalmente al interior de las empresas, los cuales reseñaremos a continuación.

Para su parte López & Sebastián (2008, pág. 230) considera que se trata de una pérdida por la no ejecución de una operación por "incapacidad de una de las partes para cumplir los compromisos asumidos, no existir formalización clara o no ajustarse al marco legal establecido", como se observa es una definición que considera la presencia del riesgo legal en un contexto de relaciones bilaterales, y con el presupuesto que dichas obligaciones son asumidas libremente por las partes, configurándose el riesgo en el supuesto de incumplimiento de compromisos, que se adecua incluso al enfoque de la teoría del riesgo en las obligaciones propio del derecho civil, complementando con los hechos o circunstancias asociadas a la formación o falta de adecuación de los compromisos o formalización conforme al ordenamiento legal, lo que hace apreciar que se trata de una definición muy ligada a las relaciones contractuales.

Una definición similar es realizada por Soler Ramos (1999, pág. 146) en el que aborda el riesgo legal con los aspectos señalados en el párrafo anterior pero incluye las pérdidas que se puedan generar por imposición de multas debido al incumplimiento de las normas que se aplican a las operaciones de la empresa, así como aquellos incumplimientos de la ley que dan lugar al pago de indemnizaciones o impuestos no previstos, además, incluye dentro del riesgo legal la pérdida de reputación por litigios iniciados por terceros, cambios en las disposiciones legales que limiten la competencia o liberalicen el sector de mercado de la empresa, así como la pérdida de opciones de generar negocio.

A decir de Mahler (2010) ante la falta de consenso sobre la definición del riesgo legal, adoptando una posición pragmática, lo más conveniente es seguir la definición prevista en los estándares ISO, que partiendo del supuesto que el riesgo es un efecto de la incertidumbre que con capacidad de influir en los objetivos de la organización o empresa, aunque considera que no está claro si dicha incertidumbre implica que el resultado debe ser incierto o esa incertidumbre debe estar referida a inseguridad jurídica o si la existencia de incertidumbre sobre los hechos es suficiente para tratarlo como riesgo legal; por lo que para efectos prácticos define el riesgo legal como "riesgo relacionado con una decisión en un caso legal".

En dicha definición el enfoque para reconocer al riesgo legal no se encuentra en la causa, sino en la consecuencia, por lo que, el riesgo de tipo legal puede provenir por la deficiencia en la información, comprensión o conocimiento legal para apreciar un hecho, o para la valoración de sus consecuencias o sobre la probabilidad de una decisión que se puede adoptar sobre los hechos sustentado en una o varias normas; en cualquier caso debe impactar en la organización; además, entiende que la decisión puede ser judicial, provenir de autoridades regulatorias o por terceros con capacidad especial sustentada en norma para adoptar una decisión sobre el comportamiento de la organización obligándolo a realizar una determinada conducta; e incluye la propia decisión de la empresa que puede por propia iniciativa adoptar una decisión de cumplimiento por considerar que la norma legal le es vinculante y acepta sus consecuencias, sea de forma positiva, mediante una conducta de cumplimiento o negativa mediante la aceptación de las consecuencias del incumplimiento (Mahler, 2010).

Por su parte Moorhead y Vaughan (2015) en un interesante estudio que comprendió a entrevistas a abogados internos de empresas en Inglaterra, concluyen que existe varias definiciones de riesgo legal, dado que puede comprender sólo el que se origina en las actividades de asesoría legal, y también puede ser entendido como el riesgo que se genera en las operaciones del negocio; y es posible que se extienda sólo a consecuencias legales sino también a impacto en la reputación y la cultura de la empresa en relación con la ley, por lo que debe observar el aspecto ético y comercial de forma más amplia. Además, consideran que el hecho de la ausencia de consenso entre los reguladores y las empresas con relación a la definición del riesgo legal es una ventaja que permite de forma libre su significado y por tanto su forma de gestión.

La incorporación de aspectos éticos y de reputación en la definición del riesgo legal también es compartida por Ceballos (2007) quien señala que en el riesgo legal se debe incluir “la exigibilidad legal, la legalidad de los instrumentos financieros y la exposición a cambios no anticipados en las leyes y regulaciones. Básicamente los efectos del fraude, las malas prácticas (auditoría) y de las regulaciones”, con lo que se entiende el riesgo legal

también puede comprender los efectos de la incertidumbre sobre la conducta de las personas ligadas a la organización que generan efectos negativos o dan lugar a acciones legales contra la empresa con potencialidad con causar pérdidas.

A partir de lo expuesto, podemos asociar el riesgo legal, por un lado, con las operaciones o actividad legal relacionada a las obligaciones que se asumen con terceros, y por otro lado con el cumplimiento de la norma, que propiamente se puede denominar como riesgo de cumplimiento, el mismo que es entendido como el riesgo de incumplimiento de disposiciones de orden legal o normas de conducta, que pueden repercutir incluso en la reputación de la empresa (Quintas, 2007).

Desde visión pragmática atrae la noción de tener libertad para definir el riesgo legal, sin embargo, por un lado debe tenerse en cuenta que al tratarse de un riesgo, siguiendo la concepción amplia del riesgo, no puede restringirse a los efectos negativos, sino también debe ser entendido como oportunidades, y por otro lado, para su calificación como riesgo legal requiere que las consecuencias estén asociadas a la aplicación de una norma jurídica, por lo que si bien existe posiciones que contemplan el factor ético o de conducta, dicho componente no puede ser considerado como determinante para calificar un riesgo como riesgo legal, por lo que, se puede definir como un hecho o evento probable que de ocurrir es capaz de producir efectos positivos o negativos por aplicación o inaplicación de una norma jurídica, siendo posible que involucre a la empresa o quienes actúan en nombre de ella.

2.2. Gestión de riesgos

Seguidamente, definido lo que significa riesgo y su clasificación, y en específico el riesgo legal, toca abordar la gestión de riesgos, para lo cual es importante observar la gestión de las empresas, que son organizaciones que persigue una determina finalidad, o en otros términos son organizaciones que buscan la prestación de bienes y servicios, mediante la utilización de recursos y asumiendo riesgos de forma eficiente, que generan beneficios de tipo social, con la satisfacción de las necesidades sociales y de tipo empresarial con la rentabilidad para los inversionistas, de lo que se advierte que parte importante del proceso de creación de valor en

las empresas está referido al riesgo que deben asumir y gestionar para alcanzar sus objetivos; y para realizar una gestión eficiente se requiere del compromiso de la alta dirección en todos los aspectos, que van desde establecer los lineamientos para la aceptación de riesgos, el análisis y evaluación de los riesgos a nivel de la organización, la toma de decisiones y la evaluación de resultados, sin dejar de lado la disposición o implementación de recursos para todo el proceso (Soler Ramos, y otros, 1999).

A nivel regulatorio la gestión de riesgos no tiene una definición específica, no obstante, es un término frecuentemente utilizado principalmente en el sistema financiero, tal es así que en la regulación emitida por la Superintendencia de Banca, Seguros y AFP's se encuentran disposiciones para los diferentes tipos de riesgos, concentrados principalmente en evitar sus efectos negativos, siguiendo los lineamientos de Basilea (Lizarzaburu, Berggrun, & Quispe, 2012, pág. 96).

Si se toma en cuenta que los riesgos son potenciales generadores no sólo de beneficios sino también de oportunidades, la gestión de riesgos implica una capacidad o habilidad de anticipación a los eventos riesgosos, para aprovechar oportunidades y disminuir los efectos negativos que puedan generar. Para potencial dicha habilidad o capacidad se han elaborado modelos o estándares de gestión, de los cuales los más conocido son es el ISO 31000, el Estándar Australiano AS/MZS 4360:2004 y COSO ERM, que cuyo análisis es útil para el presente trabajo.

2.3. Modelos de gestión de riesgos

En la común intención de mejorar la gestión de las organizaciones, se han elaborado modelos de gestión de riesgos, aunque cuando se mencionan estándares normalizados viene a la mente los ISO, para la gestión de riesgos a otras organizaciones que han diseñado modelos de gestión, entre los que se puede mencionar los Standars de Australia y Nueva Zelanda, COSO, y el Instituto Internacional de Auditores Internos (IIA), que deben ser tratados para entender las tendencias actuales sobre gestión de riesgos.

2.3.1. Modelo de gestión de tres líneas del Instituto Internacional de Auditores

El modelo diseñado por la IIA (2020) está principalmente orientado la distribución de funciones en la gestión del riesgos, partiendo de la premisa que se requiere la intervención de toda la organización y cada órgano desempeña roles específicos, con interrelaciones que también deben tomarse en cuenta, que se representa en la siguiente figura:

Figura 1: Modelo de gestión de las tres líneas del IIA. Fuente: The Institute of Internal Auditors (2020)

De acuerdo a este modelo los roles de primera línea son propietarios y gestores directos del riesgo, mientras que la segunda línea tiene participación en la gestión del riesgo mediante supervisión y asesoramiento generalmente relacionadas con los riesgos, de forma general o por riesgos específicos, como cumplimiento, seguridad de la información, entre otros.

Dicho modelo es de tipo básico pero orientativo en relación a la asignación de roles para evitar la duplicidad de funciones, brinda orientación para el diseño de una estructura de gestión al interior de las empresas.

2.3.2. Estándar Australiano para la administración de riesgos AS/NZS 4360:2004

El modelo que propone el estándar australiano tiene por propósito la implementación de un programa de administración de riesgos, entendiéndolo como un proceso para evitar que se concreten eventos potencialmente dañosos, que tiene como principales elementos los siguientes:

a) Comunicar y consultar
b) Establecer el contexto
c) Identificar riesgos
d) Analizar riesgos
e) Evaluar riesgos
f) Tratar riesgos
g) Monitorear y revisar

Que se reflejan en la siguiente figura:

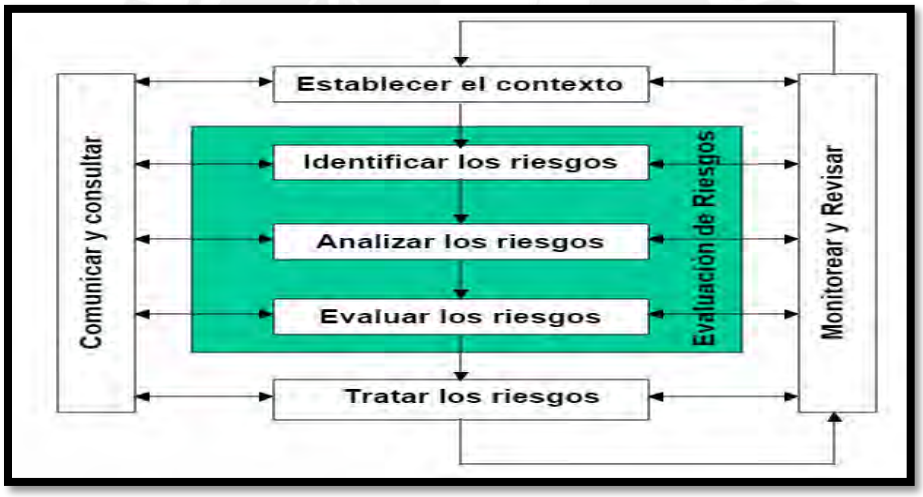


Figura 2: Proceso de administración de riesgos AS/NZS 4360:2004. Adaptado de Bejarano, L., Palencia, C., Montoya, C., & Sanchez, C. (s.f.).

Como se observa de la figura, la identificación, análisis y evaluar el riesgo forman parte de un solo proceso que es la evaluación del riesgo, que requiere de forma precedente la determinación de un contexto y posterior a la evaluación efectuar el tratamiento de los riesgos que luego pasan a actividades de monitoreo y control, siendo esta última actividad transversal a todo el proceso al igual que la comunicación y consulta.

Si bien es un estándar conocido, por su parecido con el ISO 31000, este último es el más aplicado por incluir principios y marco de referencia que deben estar presentes además del proceso, por lo que, sólo se menciona para tener referencia. Cabe mencionar que otra de las similitudes con ISO es que también cuenta con un manual para la gestión de riesgo legal denominado HB 296:2007 Handbook Legal Risk Management.

2.3.3. ISO 31000:2018 Gestión de Riesgos-Directrices e ISO 31022:2020 Gestión de Riesgo Legal - Directrices

Publicada por la Internacional Organization for Standardization (ISO) está diseñada como marco general para la gestión de todo tipo de riesgos, con lineamientos similares a la estándar AS/NZS 4360, pero se diferencia en dedicar apartados a explicar los principios y un marco de referencia necesarios para su aplicación, o en otros términos otorga un marco conceptual previo para llevar adecuadamente el proceso de gestión de riesgos.

En su marco de trabajo parte del compromiso de la alta dirección para llevar adelante los procesos de diseño del modelo de gestión de riesgo, su implementación, seguimiento y revisión, y mejora continua, que relacionado con los principios y procesos tiene como imagen gráfica la siguiente:

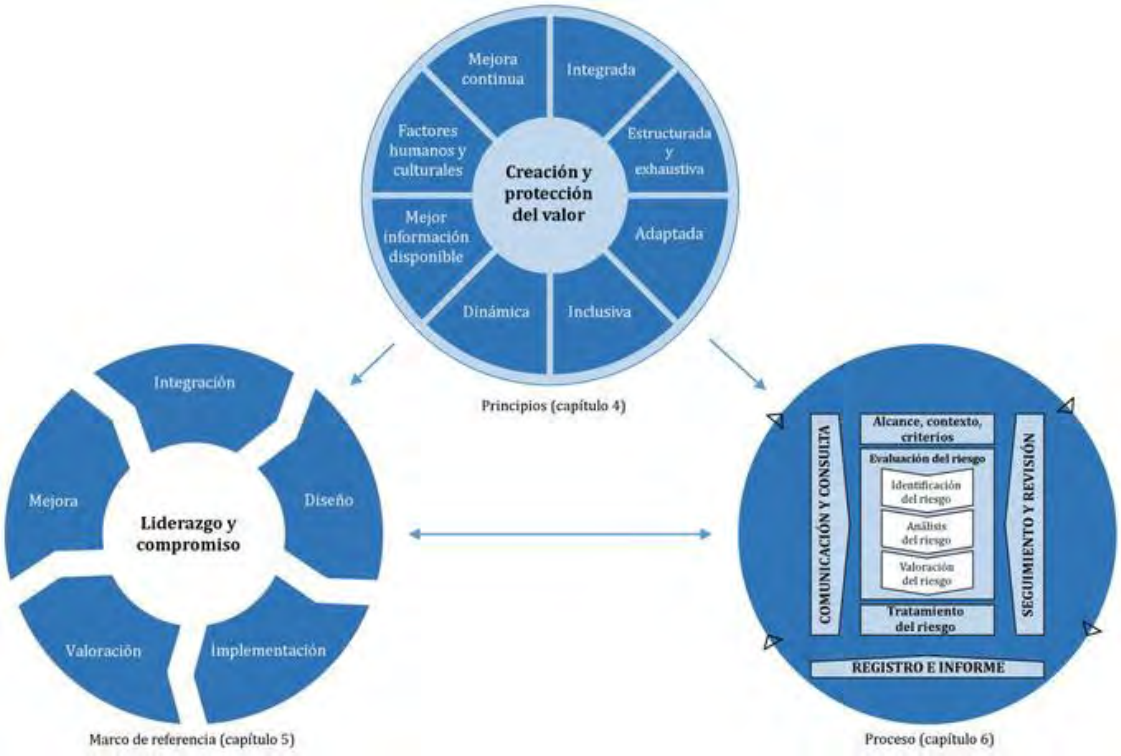


Figura 3: Principios, Marco de referencia y Proceso - ISO 31000:2018. Fuente: ISO (2018)

Como se observa en la figura sus principios, marco de referencia y proceso mismo de gestión de riesgos tiene una interrelación mutua, dando un panorama de que la evaluación de riesgos es una parte importante para la gestión, pero no es la única.

Su posibilidad de adecuación a la gestión del riesgo legal fue advertida por ISO, que publicó el ISO 31022:2020 Directrices para la gestión de riesgo legal, y cuenta con un marco más amplio para el despliegue de la gestión de riesgos, evidenciando que una adecuada gestión requiere más que sólo la determinación del proceso de evaluación, análisis y tratamiento del riesgo.

2.3.4. Gestión del Riesgo Empresarial – Integrando estrategia y desempeño (COSO ERM)

Otra de las organizaciones que elaboró un estándar para la gestión de riesgos es el Committee of Sponsoring Organizations of the Treadway Commission, que publicó el marco de referencia COSO ERM, como una versión revisada y mejorada de los denominados COSO I y COSO II orientados principalmente al control interno.

En el año 1992 COSO presentó el Marco Integrado de Control Interno, orientado a la implementación del proceso de control interno, dicho marco ahora es denominado como COSO I, cuya representación gráfica es la siguiente:

Figura 4: Modelo Coso I de Control Interno. Adoptada de: Abella (2006)

La figura representa la visión integrada de COSO I, que comprende a toda la organización y comprende la gestión de riesgos, además de combinar sus objetivos con los componentes que deben ser tomados en cuenta.

Sus objetivos son:

- Operativos
- Información o reporte financiero
- Cumplimiento

Y sus componentes son:

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y Comunicación
- Supervisión.

Posteriormente, específicamente en el año 2013, se actualizó el marco integrado, atendiendo a las nuevas exigencias del mercado, que ante los escándalos empresariales que requerían mayor transparencia y responsabilidad a las organizaciones en relación con la gestión empresarial, siendo representado de la siguiente forma:

Figura 5: Modelo Coso II de Control Interno. Adaptado de: Abella (2006)

El marco actualizado COSO II sigue el enfoque orientado al control interno, y desarrolla con más amplitud los aspectos sobre la gestión de riesgos que desde COSO I se concibe como parte de la gestión empresarial, siguiendo la concepción que es una parte clave para la administración de una empresa que está estrechamente relacionado con la generación de valor, debido a que si se trata eficazmente la incertidumbre se mejora la capacidad de la empresa para creación de valor.

En COSO II la gestión de riesgos se define como un proceso de toda la empresa y que involucra a todo el personal, cuyo objeto es la identificación de eventos adversos para la organización con miras a gestionarlos de tal forma que se encuentren en niveles aceptables, dando un aseguramiento razonable a la dirección de la empresa sobre el cumplimiento de los objetivos con una adecuada gestión de riesgos. (Abella Rubio, 2006).

Los objetivos en el marco actualizado se incrementan a cuatro (4), que son los siguientes:

- Estratégicos: Vinculados a la misión y visión de la organización.
- Operativos: Relacionados con la eficiencia y eficacia, desempeño y rentabilidad de las operaciones.
- Información: Referida a la información que se brinda no a nivel interno, sino externo y más allá de la información financiera.
- Cumplimiento regulatorio: Vinculado al cumplimiento de la regulación aplicable a la empresa.

Dichos objetivos se interrelacionan con ocho (8) elementos o componentes que deben estar presentes en el proceso de gestión empresarial:

- Ambiente interno: Es la base para la gestión de riesgos, y que influye en los demás elementos al estar vinculado la cultura y el apetito a riesgo.
- Establecimiento de objetivos: Que deben ser determinados de acuerdo a lo misión y visión de la organización, y previstos de forma previa a la identificación de riesgos.

- Identificación de acontecimientos: Que comprende eventos no sólo negativos, sino también los positivos, tanto internos como externos.
- Evaluación de riesgos: Que es la valoración a partir de su impacto y frecuencia, desde una perspectiva cualitativa y cuantitativa, y considerando el riesgo inherente que se observa sin medidas de control y el residual, cuando se aplican medidas de control.
- Respuesta al riesgo: En el que se determina si los riesgos identificados serán evitados, reducidos, compartidos o aceptados.
- Actividades de control: Que comprende las actividades de aseguramiento para evaluar el resultado de la aplicación de las respuestas al riesgo.
- Información y comunicación: Que comprende el tratamiento de los datos o información para la gestión de riesgos, actual e histórica, y que será de uso para la comunicación a las partes interesadas.
- Monitoreo o supervisión: Que comprende los mecanismos para verificar que la metodología está siendo adecuadamente implementada y logra los resultados esperados.

Dicho modelo fue complementado con lo que se conoce como COSO ERM, que tiene por finalidad integrar la gestión de riesgos a la gestión empresarial, entendidos como parte del proceso de creación a de valor, siendo representado de la siguiente forma:

Figura 6: Estructura del modelo Coso ERM. Fuente: COSO (2017)

Como se aprecia en la figura el proceso tiene cinco (5) componentes que a su vez comprenden veinte (20) principios; en este nuevo modelo se prioriza la gestión de riesgos de la empresa, que tiene por finalidad la generación de información que aporte al desarrollo de la estrategia empresarial, no obstante, se dice que no implica dejar de lado el marco integrado COSO II, por lo que deben ser considerados complementarios.

De forma similar a ISO, en el caso de COSO también elaboró un documento sobre la aplicación del modelo COSO ERM para la gestión de cumplimiento, cuya publicación fue efectuada en el año 2020; en el que se establecen las pautas a tener cuenta para su adecuación a lo que denominan riesgo de cumplimiento, que comprende no sólo el incumplimiento de la ley, sino también el incumplimiento de contratos, normas o políticas internas que pueden dar lugar a responsabilidad de tipo financiero, civil, penal, administrativa sea a nivel de la empresa o al personal de la organización.

En el marco de la guía, se contempla al oficial de cumplimiento con un rol importante en la gestión de cumplimiento, y una herramienta que es el programa de cumplimiento, sin definirlos de forma particular pero que serán objeto de análisis en abordar el problema de investigación. Dicha característica es una de las diferencias con el marco ISO pues además de considerar que la gestión de riesgos es una labor transversal a la organización debe establecerse una función que de soporte a la gestión de la organización.

2.4. ¿Cómo saber si la implementación es adecuada? conociendo los modelos de madurez

Los denominados modelos de madurez son entendidos como metodologías que están relacionadas con el grado de evolución de una organización desde la implementación de procesos particulares o específicos hasta su culminación, que permiten observar el avance de una organización desde los aspectos básicos hasta un nivel de optimización avanzado. Son usados no sólo para la determinación del grado de madurez, sino también para elaborar una hoja de ruta que oriente a las empresas en su desarrollo a niveles mayores de desarrollo de sus capacidades de forma incremental, y su uso no hace más que ampliarse desde que se empezaron a ser aplicados en diferentes ramas del conocimiento, como por ejemplo: En los

sistemas de información, procesos de negocios, sistemas de información, entre otros; en cada uno con diferentes versiones con más o menos éxito de difusión y aplicación. (Ochoa, 2016).

Para Crosby (1987), quien es considerado el pionero en la elaboración de los modelos de madurez porque desarrolló un modelo orientado a la gestión de calidad; al tomar la decisión de la mejora de un aspecto de la gestión de la empresa en particular se pueden presentar problemas como la presencia de personas en la alta dirección o en las diferentes áreas que no hayan sido evaluadas para integrarse por lo que no aportarán a su impulso o que tengan ideas preconcebidas sobre el tema, así como estará al frente la imposibilidad de dispensar de algunos miembros por diferentes razones, por lo que hace necesario mostrar el estado de la gestión de calidad con otra perspectiva que no dependa de la buena intención de quien ha sido designado a dirigir la gestión de la calidad, o de su simpatía o su capacidad de disuadir a la alta dirección para adoptar determinar acciones para mejorar la gestión, para superar esas dificultades la herramienta adecuada es un modelo de madurez.

Para Pérez-Melgarejo (2014) en la actualidad se han desarrollado modelos de madurez para diferentes aspectos de la gestión empresarial, siendo aceptado generalmente que se tratan de metodologías o estándares que ayudan a una organización “a mejorar su modo de operar”, permitiendo una evaluación integral de la situación actual comparándola con la situación ideal, cuyo resultado es el fundamento para adoptar decisiones dirigidas directamente a alcanzar los objetivos previstos. Su uso se hizo popular en la industria del software y actualmente tienen varias aplicaciones, siendo frecuentemente utilizadas por empresas que desean mejorar su desempeño, y algunas tienen cierta difusión, como los que se indican a continuación:

Tabla 2.

Modelos de madurez

Modelo de madurez	**Año**	**Desarrollador**
Normas ISO 9004	2009	ISO
Fundación Europea para la Gestión de la Calidad (en inglés, European Fundation for Quality Management, EFQM).	1991	Fundation europea para la Gestión de la Calidad

Modelo Iberoamericano de Excelencia en la Gestión.	1999	Fundation Iberoamericana para la Gestión de la Calidad
CMMI: Capability Maturity Model Integration	2000	SEI: Software Engineering Institute
Modelo de madurez de procesos de negocios.	2004	David Fisher
BPMMM: Modelo de Madurez holístico para BPM.	2005	Michael Rosemann y Tonia de Buin
BPMM: Modelo de madurez de procesos de negocio.	2005-2006	OMG: Charlie Weber, Bill Curtis y Tony Gardier
Modelo de madurez de procesos de Gartner.	2005-2006	Consultora Gartner
PEMM: Modelo de madurez de procesos y empresa.	2006-2007	Michael Hammer

Adaptado de: Melgarejo (2014)

La tabla muestra que hay diferentes modelos de madurez con diversas aplicaciones, siendo las frecuentemente mencionadas las dirigidas a la gestión de calidad y procesos, cuya elaboración es atribuida a diferentes organizaciones que incluyen personas y consultoras, por lo que, se trata de una herramienta que puede ser elaborada de acuerdo a la necesidad de la gestión que se pretende evaluar.

Para entender mejor el tema es conveniente conocer cómo son esos modelos de madurez, para lo cual se puede tomar como ejemplo el modelo desarrollado por Crosby (1987), que se refleja en la siguiente tabla:

Tabla 3.

Modelo de madurez de gestión de calidad - Crosby

Nivel	Descripción
Incertidumbre	Los problemas se resuelven caso por caso, son atribuidos por lo general a los individuos, no se tiene objetivos claros, y los costos de gestión no figuran en los cuadros de mando.
Despertar	Se sigue con la solución a corto plazo, pero se designa un responsable de la función de calidad sin verificar idoneidad técnica y se empieza a calcular el costo de la calidad.

Ilustración	La resolución de problemas no se enfoca en individuos, se llega a un cálculo razonable de los costos de la calidad, la gestión de la calidad no está dirigida por el gerente de calidad.
Sabiduría	Se reducen costos y son calculados con mayor exactitud, se identifican los problemas en sus etapas iniciales, y se considera la gestión de calidad a nivel transversal.
Certeza	Se considera a la gestión de la calidad como esencial para la dirección de la organización, y el sistema de prevención es efectivo.

Adaptado de: Crosby (1987)

Como se observa parte de un nivel básico, que se puede denominar inmaduro, hasta el más desarrollado que es el nivel de certeza, en cuyo proceso hay estadios intermedios con determinadas características asociadas a su objeto de gestión.

Otro de los modelos mencionados es el Capability Maturity Model Integración, asociado a la gestión de software, que se muestra en la siguiente figura:

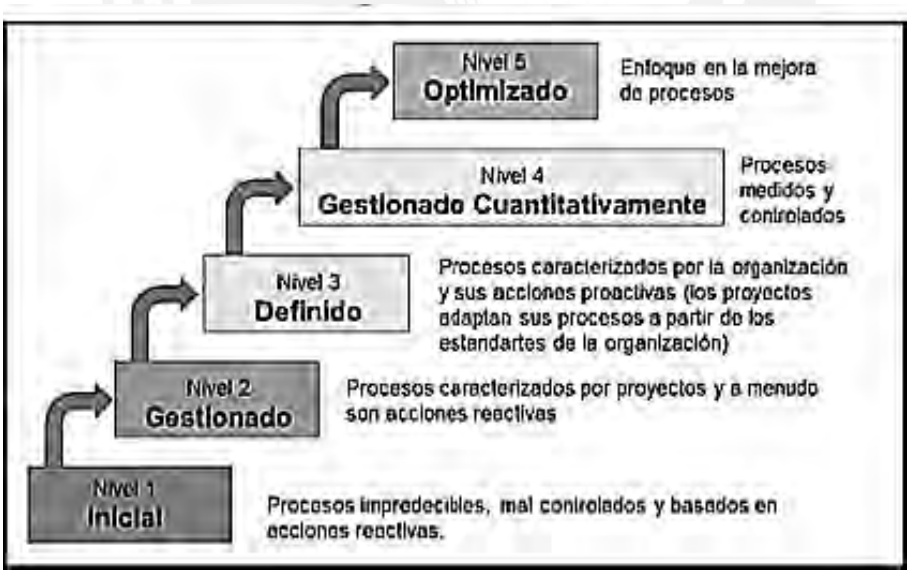


Figura 7. Niveles de Madurez del Modelo Integrado de Madurez de Capacidades (CMMI). Fuente: Ochoa (2016)

Como se observa en la figura, a diferencia del modelo de Crosby, en este caso el CMMI establece los niveles de madurez con números usando términos descriptivos sobre el estado

de los procesos y con algunas diferencias se aplica de la misma forma en otros modelos, como el de calidad ISO 9001 que se detalla a continuación:

Tabla 4.

Descripción del Modelo de la calidad ISO 9001

Nivel de madurez	Nivel de desempeño	Directriz
1	Sin aproximación formal.	No hay una aproximación sistemática evidente; sin resultados, resultados pobres o resultados impredecibles.
2	Aproximación reactiva	Aproximación sistemática basada en el problema o en la prevención; mínimos datos disponibles sobre los resultados de mejora.
3	Aproximación del sistema formal estable	Aproximación sistemática basada en el proceso, etapa temprana de mejoras sistemáticas; datos disponibles sobre la conformidad con los objetivos y existencia de tendencias de mejora
4	Énfasis en la mejora continua	Proceso de mejora en utilización; buenos resultados y tendencia mantenida a la mejora
5	Prestaciones de “mejor en su clase”	Proceso de mejora ampliamente integrado; Resultados demostrados de “mejor en su clase” por medio de benchmarking.

Adaptado de: Melgarejo (2014).

De igual forma que en los anteriores casos, la tabla muestra el patrón de cinco (5) niveles, y de forma similar con características específicas en cada nivel, siendo relevante señalar que esté modelo es un complemento en la implementación del sistema de gestión de calidad.

De la revisión bibliográfica efectuada no se encontró modelos de madurez asociados a la gestión del riesgo legal, no obstante, el diseño de una herramienta con las características que se observan en los diferentes modelos de madurez será de utilidad, para lo cual es necesario la determinación de características o estándares que serán orientativos para la determinación de los distintos niveles.

CAPÍTULO III: PROBLEMA DE INVESTIGACIÓN

Alcance del riesgo legal

Al tratar la definición del riesgo legal concluimos que se trata de un hecho o evento probable que de ocurrir es capaz de producir efectos positivos o negativos por aplicación o inaplicación de una norma jurídica, siendo posible que involucre a la empresa o quienes actúan en nombre de ella; no obstante, es necesaria la determinación de sus alcances, dado que puede comprender los eventos asociados a las relaciones contractuales, el incumplimiento de la ley o la regulación, puede extenderse hasta la dimensión ética y sus efectos no necesariamente se reducen a los de tipos económico, sino también puede tener impacto en la reputación.

A fin de llegar a un alcance razonable sobre el riesgo legal, se debe analizar lo que otorga a un riesgo la peculiaridad de ser calificado como riesgo legal que es la norma jurídica, un concepto básico en el derecho entendido como un complejo sistema de regulación de la conducta en sociedad, que desde un punto de visto lógico comprende un mandato o supuesto de hecho seguido de una consecuencia, cuyo contenido jurídico lo otorga el Estado que tiene la legitimidad del uso de la fuerza en caso de incumplimiento, siendo este último elemento la característica fundamental para diferenciarlo de cualquier otro mandato social (Rubio Correa, 2009, pág. 76).

Al relacionar la concepción de la norma jurídica con la definición de riesgo se puede decir que es la probabilidad que la empresa o quienes actúan en nombre incurran en una conducta que en el ordenamiento jurídico tiene prevista una consecuencia de tipo positivo, negativo o ambos tipos que debe ser asumida por la empresa, no siendo limitativo a la sanción prevista por el sistema jurídico sino la afectación a la imagen o reputación, como sucedió en el caso denominado Pura Vida, que comprendió a los productos similares de las empresas Gloria y Nestlé, quienes además de afrontar las acciones del regulador por incumplimiento de los deberes de información vieron la reducción de sus ingresos (Ruberto, 2017). Pero el problema del alcance del riesgo legal no se resuelve sólo con la definición, pues todavía queda conocer si tiene diferencia con el riesgo de cumplimiento y si comprende o no la dimensión ética, que son aspectos que también deben ser abordados.

Por otro lado, es conocido que la norma jurídica no se limita a ley, si bien es la forma habitual de generación de obligaciones jurídicas no es la única, pues diferenciando entre las fuentes del derecho aquellas que generan normas jurídicas y relacionando con nuestro objeto de investigación, las normas jurídicas que debe cumplir una empresa pueden provenir de la legislación y la autonomía privada, por lo que, en ambos casos se debe analizar su alcance.

3.1.1. Riesgo legal y su relación con la ética

Al hacer referencia a la ética, se hace alusión a las normas morales por las cuales se orienta la conducta de una persona, y el derecho al comprender al conjunto de normas jurídicas que regulan la conducta no puede estar exento de la moral, y no nos vamos a detener a analizar qué tan profunda su relación o sus diferencias, lo que sí no se puede dejar de lado es reconocer la existencia de dicha relación, que lleva a que reconocer normas jurídicas de contenido moral o en otros términos normas morales que se formalizaron como normas jurídicas por su importancia en la convivencia social (Torres Vásquez, 2019, págs. 99-108), por lo que, propiamente la ética no es un componente del riesgo legal pero si un elemento importante para gestionarlo, pues promoción de cumplimiento de normas morales puede traducirse en la reducción de la posibilidad de que los representantes de la empresa o los empleados incurran en conducta con impactos negativos para la empresa.

Es conveniente precisar que lo señalado no significa que la empresa gestione únicamente el comportamiento ético que puede tener impacto en la gestión del riesgo legal, pues un elemento que cada vez más adquiere importancia en la gestión empresarial de nuestros tiempos es el comportamiento ético en los negocios (Morales, 2021), sino por el contrario la gestión del comportamiento ético tiene potencial de aportar a la gestión del riesgo legal, por lo que debe ser tomado en cuenta.

3.1.2. Riesgo legal con origen en la legislación

Si bien la legislación como conjunto de normas jurídicas formalizadas por el estado de manera organizada mediante procedimientos preestablecidos es una de las fuentes de riesgo legal, las que importan para la gestión de riesgos son aquellas que implican mandatos

imperativos, aplicables en las diferentes relaciones jurídicas de la empresa, siendo su incumplimiento la conducta con potencial para generar impacto en la empresa, lo que se adecuada a la denominación de riesgo de cumplimiento, por lo que, se puede decir que este es el ámbito en el que tienen un rol preponderante los programas de cumplimiento, entendidos como herramientas que tienen por finalidad gestionar el riesgo de incumplimiento de determinadas normas jurídicas.

Otro de los aspectos a los que es posible extender el riesgo de cumplimiento es la responsabilidad extracontractual, dado que su finalidad es el resarcimiento principalmente de carácter económico del daño sufrido por una persona ocasionado por el incumplimiento de un deber (De Trazegnies, 1999), por lo que, dicho necesariamente debe ser apartado de la gestión del cumplimiento de la legislación.

3.1.3. Riesgo legal con origen en la autonomía privada

En el derecho es reconocido que la expresión o exteriorización de la voluntad tiene la capacidad de generar normas jurídicas exigibles o vinculantes entre los intervienes, sea de tipo unilateral o bilateral, cuyas condiciones de validez se encuentran detalladas en el artículo 140º del Código Civil, que establece lo siguiente:

El acto jurídico es la manifestación de voluntad destinada a crear, regular, modificar o extinguir relaciones jurídicas. Para su validez requiere:

1. Agente capaz
2. Objeto física y jurídicamente posible
3. Fin lícito
4. Observancia de la forma prescrita bajo sanción de nulidad.

En este ámbito es donde interesa como expresa su voluntad la empresa o sus representantes, las formalidades a través de las cuales se expresa dichas decisiones, y viendo desde su contenido la adecuación de su objeto a la realidad y al ordenamiento jurídico en su conjunto; que no sólo se limitará a sus implicancias en las relaciones

bilaterales, sino en aquellas de tipo unilateral que puede dar a obligaciones autoimpuestas jurídicamente exigibles (Rubio Correa, 2009, págs. 206-209).

Como parte del alcance del riesgo legal derivado de la autonomía privada de la voluntad será necesario considerar la forma en que la empresa expresa su voluntad, no sólo por quien es el representante o apoderado autorizado, sino también el proceso mismo de generación de la decisión, además de los aspectos relacionados a las condiciones y forma de expresión de la voluntad, en particular cuando se realiza de forma bilateral, que en el caso de la actividad empresarial es de tipo patrimonial o contractual.

3.1.4. Riesgo legal y la gestión de litigios

Algunos autores consideran como una categoría del riesgo legal con la denominación de riesgo de disputa el que se relaciona con los litigios, que reconociendo que la causa se encuentra en otro tipo de riesgo como por ejemplo el contractual, estiman que deben ser calificados como tales las decisiones que se adopten desde que se conoce la probabilidad de un litigio (Whalley & Guzelian, 2017). Dicha concepción puede ser reforzada por el hecho que una de las actividades propias del ejercicio profesional de la abogacía es la gestión de litigios, sean estos de tipo administrativo, judicial o arbitral, que probablemente fue una de las primeras formas de relacionamiento entre las empresas y los abogados.

Sin embargo, entendiendo que el proceso, de forma general, es una de las formas de resolución de un conflicto de interés, que entre una de sus categorías tiene a la acción como derecho subjetivo por el cual una persona solicita la intervención del estado para la satisfacción de sus intereses (Monroy Gálvez, 1996, pág. 208); implica que una persona, que puede ser incluso el estado, considera que no se ha cumplido una norma jurídica y por lo tanto es reclamable la sanción, situación que asociado al concepto propiamente se trata de la concretización del evento que se estimaba riesgoso, que por la peculiaridad de la materia requiere de la instrumentalización del derecho a través del proceso.

3.2. Modelos para la gestión del riesgo legal

Dado el contexto que no existe posibilidad de determinar con precisión el alcance del riesgo legal, tampoco es factible determinar con precisión una forma de gestionar dicho riesgo lo que otorga la posibilidad de elaborar un modelo de gestión de riesgo legal de tipo auto regulatorio. Si bien existen estudios sobre la materia como el de Whalley & Guzelian (2017) o Hopkins (2013), la publicación de pautas para la gestión del riesgo legal por parte de ISO y COSO hace factible desarrollar un modelo que sea entendido por profesionales de otras ramas teniendo en cuenta que "si en una organización tiene establecido un marco de gestión de riesgos, es probable que tenga como base COSO ERM o ISO 31000" (Whalley & Guzelian, 2017), por lo que, visto desde un punto de vista práctico, resulta conveniente que un modelo de gestión de riesgo legal tenga su base en dichos marcos de referencia, al ser los generalmente aceptado y con mayor difusión, dejando de lado el estándar australiano HB 296:2007 Legal Risk Management.

3.2.1. Modelo de gestión de riesgo legal – ISO

El marco de gestión ISO, para el caso de la gestión del riesgo legal tiene en cuenta el ISO 31000 e ISO 31022; cabe precisar que una de sus fortalezas y probablemente al que deba su aceptación internacional es su elaboración con participación de varios grupos de interés. Dicho modelo cuya representación gráfica se vio en el capítulo anterior, requiere la integración de un marco de referencia, principios y un proceso, que para el caso de la gestión del riesgo legal tiene sus particularidades.

Asimismo, partiendo de la concepción que la gestión de riesgos no sólo comprende los eventos inciertos con potencialidad de generar pérdida, sino también comprende aquellos que generen oportunidades para la empresa, reconoce que mientras los reguladores no señalen algo al respecto, existe libertad para la definición del riesgo legal, y adoptando una posición amplia sobre el tema extiende sus alcances no sólo al cumplimiento de la ley o de los contratos, sino también a los riesgos que puedan derivarse por relaciones jurídicas extracontractuales, y precisa que entre sus objetivos el apoyar a la función de cumplimiento y sus procesos, involucrar en la gestión del riesgo legal a toda la organización y grupos de

interés; todo ello con la finalidad de asegurar que la organización alcanza sus objetivos gestionando adecuadamente sus obligaciones legales.

Sobre los aspectos que pueden generar riesgo legal, señala que son:

- Los asuntos contractuales o relaciones contractuales: Que a su vez comprende la posibilidad que la organización no cumpla con las obligaciones establecidas contractualmente, no pueda hacer valer o ejecutar los derechos contractualmente establecidos, sea porque existe inadecuada formalización de los contratos o las condiciones contractuales establecidas son onerosas, inadecuadas, irrazonables o inaplicables, aspectos que tienen que ver propiamente con las cláusulas del contrato.
- El incumplimiento de la ley: Que comprende toda norma jurídica que le sea aplicable a la organización, que de acuerdo a nuestro sistema jurídico para su interpretación y alcances debe tener en cuenta no sólo lo establecido en la propia norma, sino también los pronunciamientos que se emitan al respecto por los órganos rectores o por la administración de justicia, y en la medida que la gestión de riesgos comprende la capacidad de anticipación, también incluye los actos políticos o legislativos que pueden dar lugar a la generación de normas que tengan impacto en la empresa.
- Riesgo derivado de relaciones extracontractuales: Que por una parte puede generar derechos para la organización, y por otro implica la posibilidad de asumir obligaciones; en el primer caso relacionados a la imposibilidad de reclamar afectaciones de terceros sobre la propiedad intelectual de la empresa, sus patentes, secretos comerciales, información confidencial; en el segundo caso, comprende los actos o decisiones de la empresa que vulnerando el deber de cuidado, afecten a un tercero dándole la posibilidad de reclamar responsabilidad extracontractual a la organización.

Como se observa de las líneas precedentes, de forma previa a la exposición del modelo de gestión requiere de una delimitación del riesgo legal, labor que hemos realizado en el sub-capitulo anterior, y que tendremos que precisar al momento de elaborar el modelo de gestión de riesgo legal.

3.2. 1.a. Principios y marco de referencia

La gestión de riesgo legal en el modelo ISO requiere el relacionamiento entre los principios, marco de referencia y el proceso mismo de gestión del riesgo.

Con relación a los principios, se contemplan nueve (9) conforme a lo siguiente:

1. Integrada: Que implica comprender la gestión de riesgos como parte de la gestión de la empresa, no sólo en relación a su estructura u organización, sino también en la determinación de la estrategia, los objetivos, planes y procesos operativos, de modo que sea entendido como un asunto de todos y no sólo de los abogados o del área de asesoría legal; y tratándose de un riesgo con ciertas particularidades como es el riesgo legal el enfoque integral también implica que en la evaluación del riesgo y la elaboración del plan de tratamiento se realice con asesoramiento jurídico adecuado.

2. Estructurada y exhaustiva: Relacionado a la necesidad de desplegar el modelo de gestión de forma organizada y planificada que permita el cumplimiento de objetivos con resultados consistentes y comparables en el tiempo.

3. Adaptada: Debido a que cualquier sistema de gestión debe ser personalizada de acuerdo a la situación de la empresa, para lo cual requiere la evaluación del contexto externo e interno, y específicamente con relación al riesgo legal exige que tener un proceso de identificación de normas aplicables a la empresa, que sin lugar a dudas debe tener un registro, además de un proceso de adecuación a las mismas y verificación periódica de su cumplimiento, con participación de asesores legales y los involucrados en los procesos en los que se identificaron los riesgos.

4. Inclusiva: En línea con las exigencias actuales para la gestión de organizaciones, que en el caso de las empresas involucra tener en cuenta a las partes interesadas,

sus puntos de vista y expectativas, la gestión de riesgos legales también debe comprender lo mismo.

5. Dinámica: Considerando que el entorno es cambiante, como lo ha demostrado en nuestro tiempo la pandemia del COVID 19, también la gestión de riesgos debe estar en predisposición de adecuarse a los nuevos escenarios, no sólo a nivel de identificación de los cambios en el entorno, sino inclusive tener la capacidad de anticiparlos, en particular, los cambios en las leyes y las políticas públicas, que puede efectuarse mediante la implementación de alertas tempranas.

6. Mejor información posible: Que exige prever herramientas que permitan que la información para la gestión de riesgos no sea sólo confiable, sino lo más actualizada posible, que en el marco del riesgo legal comprende una base de datos de las normas jurídicas, software o herramientas para la gestión de archivos electrónicos, y aquellas que permitan la elaboración de reportes.

7. Factores humanos y culturales: Principio que exige tener en cuenta que existen puntos de vista emocionales, culturales o sociales, derivados de concepciones o percepciones políticas que pueden dar lugar a riesgos legales, por ello, se debe desarrollar mecanismos para controlar que dichos factores no generen riesgo legal, involucrando en ello a todos los miembros de la organización.

8. Mejora continua: Que implica la predisposición para mejorar la gestión de riesgos, a partir de las lecciones aprendidas o experiencia, e integración de las mejores prácticas que se estén difundiendo.

9. Equidad: Contemplado exclusivamente para la gestión del riesgo legal, por el que la toma de decisiones en la organización debe estar orientada por conceptos como justicia, equidad e igualdad, con una adecuada gestión de conflicto de intereses, por lo que, se incluye el componente ético a la gestión del riesgo legal.

Con relación al marco de referencia, su objetivo es hacer viable y facilitar la incorporación de la gestión de riesgos legales en la organización, pues considera que la posibilidad de su adecuado despliegue y la obtención de los resultados tiene relación directa con la participación de la alta dirección. De forma específica se pide el despliegue de ciertas acciones o actividades que se espera sean realizadas por la alta dirección y los órganos de supervisión, en el caso que estos existan, para la adecuada implementación de la gestión de riesgos. Cabe precisar que no se tiene una definición especifica de lo que se debe entender por alta dirección o por órganos de supervisión, sin embargo, a partir de lo dispuesto por el Artículo 152º de la Ley General de Sociedades, en el que se atribuye la responsabilidad de la administración de la empresa al directorio y la gerencia, entenderemos por alta dirección a los órganos mencionados y dejaremos de lado a los denominados órganos de supervisión para evitar incrementar la complejidad del análisis. Respecto a lo que se espera de la alta dirección tenemos lo siguiente:

- Adoptar acciones para implementar los componentes del marco de referencia para la gestión del riesgo legal.
- Establecer el enfoque o política para la gestión del riesgo legal, así como su adecuada difusión.
- Dotar de recursos suficientes para la gestión del riesgo legal.
- Establecer las responsabilidades, autoridad y línea de reporte en relación con la gestión de riesgos legales.

Asimismo, el marco de referencia tiene cinco (5) componentes, los cuales comparten la necesidad de ser difundidos de la forma más adecuada posible y que se detallan a continuación:

a) Integración: Este componente tiene similitud con el principio de gestión integrada, pues implica que la gestión de riesgos sea incorporada de forma transversal a toda la organización, lo que nos lleva a concluir que su

categorización como componente puede estar motivada en la intención de resaltar la necesidad de considerar la gestión de riesgos como parte integral de la gestión de la empresa para lograr los objetivos esperados.

b) Diseño: Comprende la planificación del modelo de gestión de riesgos, que a su vez tiene varias actividades, que se detallan a continuación:
   - Analizar el contexto externo e interno de la organización en relación con el riesgo que se pretende controlar: En referencia al riesgo legal debe tener en cuenta la regulación relevante para la organización, los recursos con los que cuenta para asesoramiento jurídico, sus grupos de interés, entre otros.
   - Compromiso con la gestión del riesgo legal: Que parte de establecer una política que considere los objetivos para la gestión del riesgo legal, y los demás aspectos involucrados en la etapa de diseño.
   - Determinación de roles, responsabilidades y líneas de reporte para la gestión del riesgo legal.
   - Recursos para la gestión de riesgo legal, no solo el equipo de personas que intervienen sino también las herramientas que se utilizarán, software, procesos, entre otros.
   - Lineamientos para la comunicación y consulta, en la medida que es un requerimiento que debe estar presente a lo largo de todo el proceso.

c) Implementación: Que comprende la elaboración de un plan de trabajo para desplegar el modelo de gestión de riesgo legal de acuerdo con el diseño elaborado.

d) Valoración: Relacionado con la evaluación de desempeño del modelo desplegado.

e) Mejora: Involucrando por un lado la adaptación a los cambios en el entorno y la identificación de aspectos orientados a la mejora continua.

2.2.1.b. Proceso de gestión del riesgo legal

Es el conjunto de actividades destinadas a gestionar los riesgos que han sido calificados como riesgo legal, el proceso general de gestión de riesgo esta descrito en la ISO 31000, sin embargo, al ser articulado con el ISO 31022, el resultado es el siguiente:

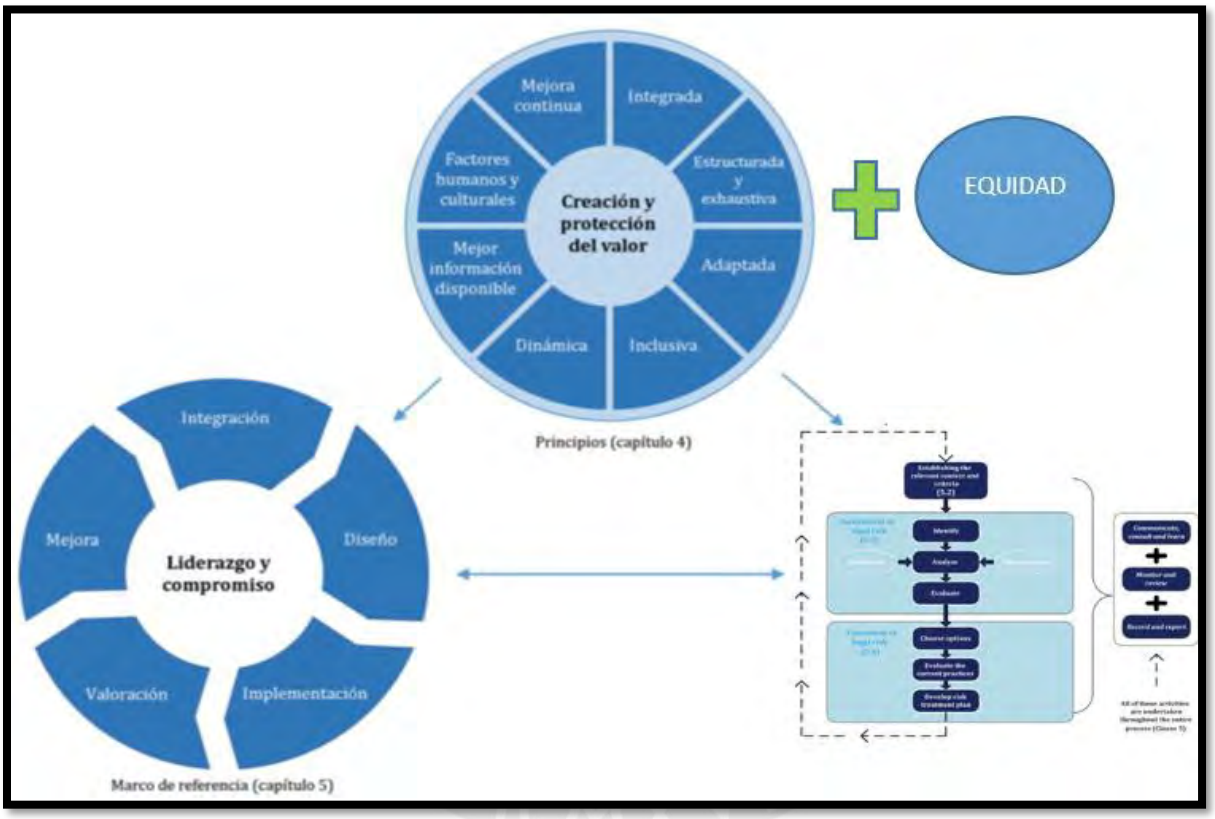


Figura 8. Perspectiva de la gestión del riesgo legal. Adaptado de: ISO (2018)

Como se observa en la figura el punto de partida del proceso de gestión del riesgo legal inicia en la determinación del alcance, contexto y los criterios, que son el resultado de las actividades de diseño del modelo de gestión de riesgo legal, por tal razón, los criterios para identificar, evaluar y tratar el riesgo deben ser definidos en dicha etapa.

Atendiendo al hecho que los estándares solo establecen lineamientos generales, para fines de la identificación de riesgos únicamente se indica que “la organización

debe seleccionar las herramientas y técnicas de identificación de riesgos legales", sin embargo, es importante tener en cuenta que dicha actividad debe efectuarse de forma sistemática, por lo que, requiere de una metodología, de allí que como anexo del ISO 31022 se prevea un ejemplo de método para la identificación de riesgos legales y un modelo de registro de dichos riesgos. Cabe agregar que otro de los elementos importantes para la etapa de identificación de riesgos es implementación de señales de alerta.

Para el análisis de riesgo legal debe tomarse en cuenta la probabilidad de ocurrencia y el impacto o consecuencias, a partir análisis cuantitativo y cualitativo del riesgo legal identificado, además de tomar en cuenta la opinión de los profesionales en derecho; para su valoración nos ofrece algunos criterios tanto para la medición de probabilidad como de impacto asumiendo una valoración de 1 a 5, en esta etapa se recomienda la determinación de indicadores claves de riesgo (KRI) que ayudarán en proceso de determinación de alternativas de tratamiento.

Además, como parte del proceso de evaluación se considera la determinación de la priorización del riesgo identificado, que también debe ser efectuado bajo determinados criterios, y aunque no dice quien efectúa esa labor da a entender que es responsabilidad del dueño del riesgo con aprobación de la alta dirección.

Luego de concluida la evaluación, con la priorización efectuada se debe elaborar el plan de tratamiento del riesgo legal identificado, a partir de la formulación de opciones, y valoración de su eficacia para mitigar el riesgo. En esta etapa requiere la también la evaluación de las prácticas actuales de la organización para el tratamiento del riesgo identificado, siendo relevante que la evaluación de la idoneidad o eficacia del plan de tratamiento, no sólo sea efectuada al momento para la aprobación del plan, sino también sea sujeto a seguimiento.

En relación al seguimiento y revisión se exige la implementación de los siguientes procesos:

- Identificación de nuevas leyes, su modificación o criterios para su aplicación y como se está adecuando la empresa.
- Seguimiento de riesgos que se han concretado.
- Sistema de alertas tempranas para su reporte de acuerdo a las partes interesadas que deben ser informadas.
- Seguimiento a planes de tratamiento de riesgos.

Sobre los registros e informes se pide garantizar el secreto profesional de los abogados que intervinieron en la evaluación de riesgos, además de tener implementadas políticas relacionadas a seguridad de la información y protección de datos personales.

Respecto al proceso de comunicación y consulta, está orientado principalmente a que las partes interesadas comprendan los riesgos a los que está expuesta la organización y su impacto, de tal forma que puedan tomar decisiones de manera informada, siendo otro componente que la función de gestión de riesgo legal tenga comunicación con las partes interesadas externas e internas, así como promover una cultura de gestión de riesgos.

3.2.2. Marco de gestión COSO ERM aplicado al riesgo de cumplimiento

El marco COSO ERM tiene una orientación a la gestión de riesgos que afronta la empresa y los asocia con sus objetivos, compartiendo con ISO la necesidad de integrar la gestión del riesgo a la gestión. Su objeto de atención es lo que denomina riesgo de cumplimiento, entendiendo por tal a lo que se desarrolló en esta investigación como riesgo legal, por tal motivo, el marco de gestión es denomina Gestión de Riesgo de Cumplimiento: Aplicación del marco COSO ERM. A fin de guardar coherencia con el análisis usaremos de forma generar el término de riesgo legal en vez del riesgo de cumplimiento que usa el estándar, en la medida de lo posible.

Este marco está conformado por cinco (5) componentes con veinte (20) principios, tal como se vio en la Figura 6, que, en su aplicación al riesgo legal no varía, aunque contempla

como herramienta de gestión al programa de cumplimiento y ética, además de incluir el rol de oficial de cumplimiento.

De forma similar a ISO, antes de desarrollar los componentes del modelo señala los alcances del riesgo legal, de acuerdo a lo siguiente:

- Incumplimiento de la ley o regulación.
- Vulneración de términos contractuales aplicables.
- Incumplimiento de políticas internas que den lugar a responsabilidad de la empresa o su personal.

En el último caso, comprende entre las políticas, la gestión de conflicto de intereses debido a que su revelación y tratamiento forma parte de estándares profesionales, por lo que deben ser considerados dentro del grupo de los riesgos legales, sin dejar de mencionar que la definición no es exacta y se deja a criterio de las organizaciones.

Otro aspecto resaltante es que la valoración de la consecuencia o impacto no se limita únicamente al factor financiero, pues incluye el daño a la reputación, que puede conllevar a pérdida de clientes, salidas de empleados, entre otros; y no sólo pueden ser generados por acciones o decisiones de la empresa, sino también de proveedores o terceros que de una u otra forma están vinculados a las operaciones de la empresa.

Asimismo, el modelo asocia la gestión del riesgo legal con los programas de cumplimiento y la función de cumplimiento, de reciente desarrollo y cuya independencia no es necesariamente establecida como requisito, pero que se difunde como práctica preferida especialmente por los reguladores, siendo aceptable que forme parte de legal, auditoría interna, riesgos u otra función, así como es factible que sea asumida mediante otros modelos estructurales. Y aunque la función de cumplimiento suele desarrollar el programa de cumplimiento, su ejecución es competencia de la gerencia y la supervisión es responsabilidad del directorio.

En relación al primer componente, requiere compromiso del directorio pues entre otras cosas comprende su participación activa en la supervisión de la gestión del riesgo, con acciones como:

- Prever en la agenda de las sesiones los temas asociados a riesgo de cumplimiento.
- Incorporar en el directorio a miembros con experiencia en gestión de cumplimiento.
- Revisar periódicamente lo relacionado a los recursos, estructura operativa, personal, nivel de empoderamiento de la función de cumplimiento, las politices y procedimientos.
- Revisar los aspectos relacionados a los criterios de retribución y desempeño asociados con la gestión de cumplimiento.
- Establecer los criterios de la debida diligencia para la incorporación de personal.

Cabe mencionar que entre los aspectos relevantes de componente está la recomendación de uso del modelo de tres líneas diseñado por el Instituto de Auditores Internos, actualizado en el año 2020.

Respecto al segundo componente, está relacionado con la definición del contexto empresarial, que comprende:

- La identificación de los riesgos de cumplimiento relevantes para la organización.
- La participación de la gestión de cumplimiento en la definición y modificaciones de la estrategia empresarial.
- La relación del riesgo de cumplimiento con los otros tipos de riesgo.
- La definición de apetito del riesgo, como hecho consiente luego del análisis del contexto, entendido como el riesgo que la organización decide aceptar en busca de sus objetivos, considerando que suele calificarse como no realista reducir la probabilidad de ocurrencia a cero.

El tercer componente comprende la identificación, evaluación, priorización y tratamiento de riesgos, para ello requiere procesos específicos abarca a la organización en

su conjunto, de tal forma que se asignen los recursos los más eficientemente posible; entre los requerimientos que plantea el componente están:

- La elaboración de un inventario de riesgos.
- La evaluación de probabilidad e impacto, un aspecto interesante es la evaluación de los controles implementados, que también deben ser incluidos en una metodología adecuada a la organización.
- Los criterios para el diseño de los planes de tratamiento, que establezca responsabilidades, acciones, plazos para ejecución, seguimiento a la ejecución y a la efectividad de las acciones desplegadas para la mitigación de riesgos, resaltando que de tratarse de riesgos significativos debe incorporar una estrategia de educación y formación.
- La incorporación de los riesgos legales al mapa de riesgos de la empresa para identificar su relación con otros riesgos y su impacto a nivel de la organización.

El componente de seguimiento y revisión está orientado principalmente a identificar los cambios en el entorno, a nivel interno y externo; entre sus requerimientos plantea:

- La revisión periódica de la efectividad del sistema de gestión de riesgo legal por parte del Directorio, que debe comprender la revisión de los riesgos más significativos para la organización.
- El establecimiento de un plan de auditoria; cabe precisar que como alternativas para la evaluación de la efectividad del sistema de gestión de riesgos recomienda autoevaluación, evaluación de auditoria interna o evaluación por un servicio externo.
- La medición de la cultura de cumplimiento, que incluya alguna herramienta para recibir información del personal de todos los niveles de la empresa sobre su percepción del compromiso de la alta dirección con el cumplimiento.
- La implementación de buzón de denuncias con la capacidad de garantizar de la confidencialidad del denunciante, que sirva como herramienta para recibir información sobre posibles incumplimientos que den a lugar a investigaciones y aplicación de sanciones. Dicho mecanismo puede ser complementado con entrevistas a empleados

mediante encuentras periódicas o recepción de comentarios en actividades de capacitación.

- Compromiso con la mejora continua que debe ser un esfuerzo permanente, sobre las brechas y oportunidades de mejora identificadas, con planes de acción y mejoras proactivas para optimizar rendimiento incorporando nuevas herramientas o innovación, que pueden ser evaluadas a partir del benchmarking.

El último componente es información, comunicación y reporte, que requiere entre otras cosas:

- Garantizar que la función de cumplimiento tenga acceso oportuno a la información de cada elemento del programa.
- Utilización de tecnologías para impartir formación.
- Uso de la tecnología para los procesos de cumplimiento, como el análisis de base de datos para la detección de incumplimientos, la posibilidad de elaborar informes automatizados, realizar acciones de revisión de cumplimiento de forma automatiza, generación de tableros de mando o informes personalizados para las distintas partes interesadas, entre otros.
- La entrega de información de calidad a las diferentes partes interesadas, de acuerdo a sus necesidades, con métricas en lo posible y confiables, en especial información sobre las investigaciones realizadas.
- La atención de inquietudes sobre cuestiones de cumplimiento que formulen las unidades de negocio, sobre sus roles y responsabilidades, los protocolos de escala para comprensión del sistema, comunicaciones personalizadas sobre sus responsabilidades y capacitación personalizadas de acuerdo a función.

3.3. Modelo de madurez para la gestión de riesgo legal

Como sucede normalmente con los temas nuevos, no suele existir literatura o estudios sobre la materia, y como vimos en el estado del arte este es el caso, no obstante, llegamos a la conclusión que la herramienta generalmente utilizada para evidenciar el avance respecto de la implementación de estándares de gestión es un modelo de madurez, por lo que es un instrumento complementario que depende de los criterios o estándares a implementar adaptable a diferentes sistema de gestión, cuyo aporte es proporcionar una visión general de

estado de la empresa para la elaboración de una hoja de ruta orientada a la mejora progresiva de la organización.

Siendo así, para fines de elaborar un modelo de madurez para la gestión del riesgo legal, se debe determinar los criterios o estándar que debe cumplir el sistema de gestión que se pretende implementar, cuyo diseño en la presente investigación tiene como base los marcos ISO y COSO, por lo que, una opción práctica es la búsqueda de un modelo de madurez que adapte alguno de dichos marcos de gestión.

En la exploración sobre el tema se encontró que la Contraloría General de la República (2014) realizó una adaptación del Modelo Integrado de Capacidad y Madurez (Capacity Maturity Model Integration-CMMI) para evaluar el avance de la implementación del sistema de control interno en el sector público, que tiene como referencia el marco de gestión de control interno COSO, con seis (6) niveles de madurez, de acuerdo a lo siguiente:

Figura 9. Modelo de madurez para la gestión del riesgo legal. Fuente: Contraloria General de la Republica (2014)

Como se observa en la figura los niveles de maduración son similares a los que se mencionan en el estado del arte, por lo que tienen parecido con las otros modelos de madurez, aunque lo importante no es el número de niveles o su caracterización sino la forma en que se realiza el diagnóstico para ubicar la gestión de una entidad en un determinado nivel.

De acuerdo al modelo citado, el proceso comprende tres etapas:

- La definición de los parámetros de evaluación: Que es el paso inicial, para lo cual utiliza la siguiente tabla:

Tabla 5.

Parámetros de evaluación del modelo de control interno para las entidades publicas

Componente	Puntaje Ponderado	Principio1	Principio2	Principio3	Principio4	Otros…
Ambiente de control	20	20	20	20	20	…
Evaluación de riesgos	20	20	20	20	20	…
Actividades de control	20	20	20	20	20	…
Información y Comunicación	20	20	20	20	20	…
Supervisión	20	20	20	20	20	…
Puntaje total de implementación del Sistema de Control Interno	100					

Adaptado de: Contraloria General de la Republica (2014)

La tabla contiene los criterios fijados, en este caso los del modelo de control interno para las entidades públicas que a cada componente le otorga un puntaje ponderado, compuesto a su vez por principios con sub criterios cuyo cumplimiento se califica con los términos “si”, “no” o “no aplica”.

- La búsqueda de evidencia: Que comprende la compilación de información y registros asociados a cada parámetro.
- Análisis de la información: Donde se realiza la calificación de cumplimiento contrastado la información recibida con los criterios de calificación.

El resultado del proceso se refleja de forma gráfica conforme a lo siguiente:

Figura 10. Reporte de resultados por componente. Fuente Contraloria General de la Republica (2014)

Una vez concluido el proceso la figura reflejará de forma gráfica el nivel de la implementación del sistema de control interno, en un formato que permite apreciar de forma integral los aspectos por trabajar, y, por tanto, con potencial para dar información base para elaborar planes de acción destinados al avance incremental de la gestión.

De lo expuesto, se advierte que es posible la adaptar el modelo a la finalidad de la presente investigación, no sólo por la afinidad de criterios con el modelo COSO que se utiliza de referencia en este trabajo, sino también por su potencial de brindar información en forma práctica para la toma de decisiones de la alta dirección.

CAPÍTULO IV: DISCUSIÓN

Al iniciar la investigación señalamos que la forma de gestionar el riesgo legal en las empresas es a través de la implementación de un sistema de gestión de riesgo legal, cuya elaboración es posible no sólo porque a nivel empresarial el incumplimiento de las normas jurídicas es considerado como riesgo, sino también porque los estándares conocidos ISO y COSO ERM elaboraron pautas para la gestión del riesgo legal.

Y al revisar la literatura encontramos diferentes concepciones sobre riesgo legal, y dado los diversos alcances que podría comprender, desde una perspectiva pragmática se opta por dejar que las empresas determinen lo que entienden por riesgo legal, no obstante, al abordar el problema encontramos que un elemento para la caracterización de un riesgo como riesgo legal es la norma jurídica, cuyo finalidad es la regulación de la conducta en sociedad con mandatos imperativos cuyo incumplimiento faculta la intervención coercitiva del estado, con efectos que en la actividad empresarial no se limitan a la sanción prevista en el ordenamiento jurídica, sino que ahora se extiende a la reputación de la empresa.

Dado que la norma jurídica es el diferenciador del riesgo, se puede categorizar en dos tipos de riesgos legales:

- Riesgo normativo o regulatorio: Que se origina por las normas jurídicas impuestas por la ley o la regulación, que puede ser denominado riesgo de cumplimiento y que a su vez puede dar lugar a obligaciones o derechos extracontractuales, pues su fundamento se encuentra en la obligación de debida diligencia o cumplimiento del deber de cuidado.
- Riesgo contractual: Relacionado a la expresión de la manifestación de voluntad, considerando el proceso de formación de voluntad, a través de quien y mediante que formalidad, además de los aspectos relacionados a las clausulas y forma prescrita por ley, que, si bien lo calificamos como riesgo relacionado a la autonomía privada, debido a que las relaciones jurídicas de la empresa son prioritariamente patrimoniales es práctico denominarlo como riesgo contractual.

Otro tema relevante para el entendimiento del riesgo legal es su conexión con la ética, dado que existen “normas que son simultáneamente jurídicas y morales” (Rubio & Arce, 2017, pág. 58) ,

por lo que al tratarse un componente intrínseco para la gestión de determinados riesgos legales, la gestión del comportamiento ético aporta a la gestión del riesgo legal.

Asimismo, se advirtió que, a gestión de las controversias a través de los procesos o litigios, es la concretización de los riesgos de tipo legal, que de incierto se vuelve en concreto, por lo que no puede ser considerado como una categoría de riesgo legal.

Con la definición del riesgo legal y sus alcances, se tiene el insumo básico para el diseño de un sistema de gestión de riesgo legal con las pautas de los marcos de gestión estandarizados ISO y COSO ERM.

Al abordar los marcos de gestión se encontró similitudes entre ambos, que se pueden observar en la siguiente tabla:

Tabla 6.

Similitudes entre el ISO y el COSO

ISO	COSO
Liderazgo y compromiso (fundamento de marco de referencia)	Gobierno y cultura
Alcance, contexto y criterios	Estrategia y establecimiento de objetivos
Evaluación del riesgo/ Tratamiento del riesgo	Desempeño
Seguimiento y revisión	Revisión y monitorización
Comunicación y consulta	Información, comunicación y reporte

Dicha similitud, también se reflejar en sus requerimientos para implementación, que comparten la generalidad de las pautas, que requieren desarrollo o adecuación a la realidad de nuestro sistema jurídico, no obstante, a partir del entendimiento del riesgo legal es posible proponer los requerimientos para la implementación de un modelo de gestión de riesgo legal.

En ambos casos señalaron la importancia de la definición los roles y responsabilidades, sin embargo, no otorgan lineamientos para dicho fin, por lo que, un complemento adecuado al objeto

es el modelo de gestión de riesgos en tres líneas del IIA, e igualmente otro complemento para evidenciar el avance de implementación del sistema es el diseño de un modelo de madurez.

En relación a sus diferencias, un aporte del marco COSO es la necesidad de una función que oriente la gestión de la organización, que en su caso denomina función de cumplimiento, aunque su alcance comprende lo que se definió como riesgo legal.

A partir de los resultados de la investigación resulta necesario la elaboración de un modelo para la gestión del riesgo legal como estrategia empresarial, que debe comprender cinco (5) pilares:

1. Gobernanza:

   Parte del compromiso que debe asumir la alta dirección respecto del riesgo legal, que puede surgir por interés de sus miembros respecto al cumplimiento de sus deberes fiduciarios de debida diligencia, como también puede ser motivada a partir de quienes están a cargo de la asesoría jurídica de la empresa sea interna o externa, que se expresa mediante la adopción de acciones y tratamiento de los temas del riesgo legal en la agenda de trabajo de la alta dirección.

   Al tratarse de un riesgo de características especiales, que requiere de por medio la intervención de un profesional en derecho, un aspecto clave es la delegación de responsabilidad para el proceso de implementación a un profesional con conocimiento y/o experiencia preferentemente en materia jurídica, rol que puede ser desempeñado por el responsable de asesoría jurídica de la empresa, sea interno o externo, que denominaremos función legal, haciendo un paralelo con lo que el marco COSO denomina función de cumplimiento, con la responsabilidad a nivel de la organización de promover y asegurar a la alta dirección que la adecuada gestión de los riesgos legales en la empresa, lo que encuadra con las nuevas tendencias del ejercicio de la profesión.

   Para que el diseño sea ajustado a la realidad de la empresa y a las expectativas de las partes interesadas, debe fijarse la definición del riesgo legal y sus alcances, la base para dicha labor puede ser la expuesta en este trabajo.

Asimismo, se debe definir el nivel de reporte de la función legal, que puede ser directamente al órgano de dirección máximo o a través de un comité, además que se debe promover que los miembros de la alta dirección tengan experiencia o conocimiento sobre la gestión de riesgo legal.

2. Estrategia:

Para la definición de la estrategia se debe efectuar la evaluación del contexto de la empresa, a nivel interno y externo, apreciado desde el punto de vista del riesgo legal, que no sólo requiere el conocimiento jurídico de la regulación aplicable a la empresa sino también de las condiciones del negocio en el que opera, a partir de dicha evaluación se podrá determinar que programas de cumplimiento se deben implementar, por ejemplo, si la empresa se dedica a la venta de materiales de construcción principalmente a entidades públicas, ante el actual contexto de escándalos de corrupción debe contemplar la implementación de un programa de cumplimiento para la prevención de la corrupción, mientras que si se dedica a venta de productos de consumo masivo, sería pertinente la implementación de programa de cumplimiento en materia de protección al consumidor.

Con la identificación de los riesgos legales de tipo estratégico y el contexto externo e interno de la empresa, se puede proceder con la formalización del diseño de roles y responsabilidades para la gestión del riesgo legal en el que se puede considerar la existencia de funciones de cumplimiento específico para determinadas categorías de riesgo legal o riesgo específicos, así como los lineamientos básicos para la gestión de cada tipo de riesgo, por ejemplo si se considera dentro del alcance al riesgo contractual, se deberán establecer políticas para la gestión del riesgo contractual, que deben comprender los lineamientos de gestión de apoderados y delegación de facultades.

Como propuesta de roles y responsabilidades para la gestión del riesgo legal puede tomarse en cuenta a siguiente tabla:

Tabla 7.

Propuesta de roles y responsabilidades para la gestión del riesgo legal

ROL	RESPONSABILIDAD
Directorio	Determinar la estrategia general para la gestión del riesgo legal
Gerente General	Implementar la gestión del riesgo legal de acuerdo a la estrategia aprobada por el Directorio
Gerente funcional o de división	Asegurar el funcionamiento del sistema de gestión del riesgo legal en su área y que las operaciones su cargo se ejecutan observado las políticas de la empresa.
Función legal	Proponer las políticas y estándares para la gestión del riesgo legal

Asimismo, como parte de la estrategia debe definirse la metodología para la cada etapa del proceso evaluación del riesgo legal, las cuales son identificación, evaluación y tratamiento, considerando lo siguiente:

Identificación: La definición del lenguaje en que será descrito el riesgo y la creación de un registro, en el cual el riesgo este categorizado e individualizando el proceso o línea de negocio en el que fue advertido, como ejemplo con algunos riesgos, sugerimos el siguiente:

Tabla 8.

Registro de riesgos legales identificados

Nro. (1)	PROCESO/LÍNEA DE NEGOCIO/PROYECTO (2)	DESCRIPCIÓN DEL RIESGO LEGAL IDENTIFICADO (3)	TIPO (3)	SUB TIPO (3)
	Gestión de recursos humanos	No registrar la salida de los trabajadores de la oficina principal en el registro de asistencia puede dar lugar a la imposición de una	Riesgo de regulación	Cumplimiento

	multa por infracción del D.S. Nº 728		
Gestión de agencias	No inscribir el contrato de arrendamiento del centro de operaciones 1 puede dar lugar a que en caso de compraventa del bien el nuevo propietario desconozca el contrato.	Riesgo contractual	Formalidades de contrato
Gestión de productos	No registrar la marca “Patito” puede dar lugar a que tercero registren como propio e impidan uso por parte de la empresa.	Riesgos regulatorio	Registro de derechos

Descripción de campos:

(1) El número puede corresponder a la propia definición interna de la organización, por serie, correlativa, etc.

(2) En esta columna debe indicarse el proceso, proyecto o línea de negocio en el que se identificó el riesgo, por lo que, depende de la organización interna o forma de abordar la gestión de riesgos a nivel de la organización.

(3) La descripción del riesgo legal identificado, tipo y sub tipo debe efectuarse de acuerdo a la metodología aprobada por la organización

Además, en la medida que para la identificación de los riesgos regulatorios también se debe implementar un registro de normas legales aplicables a la empresa, con la descripción de las acciones adoptadas para su adecuación, a modo de referencia elaboramos la tabla 9; y un registro de contratos con características similares.

Tabla 9.

Registro de normas legales identificadas

Nro. (1)	TIPO DE NORMA LEGAL (2)	DETALLE DE NORMA LEGAL (3)	IMPACTO EN PROCESO/LÍNEA DE NEGOCIO/PROYECTO (4)	ACCIONES DE ADECUACIÓN (5)	ESTADO DE ACCIONES DE ADECUACIÓN (6)	PLAZO DE ADECUACIÓN (7)

Descripción de campos:

(1) El número puede corresponder a la propia definición interna de la organización, por serie, correlativa, etc.

(2) En esta columna debe indicarse el tipo de norma legal a partir de las definiciones del sistema jurídico: ley, decreto legislativo, etc.

(3) En esta columna debe indicarse el proceso, proyecto o línea de negocio en los que impacta la norma identificada, por lo que, depende de la organización interna o forma de abordar la gestión de riesgos a nivel de la organización.

(4) Se consigna las acciones realizadas por la organización para mitigar el riesgo que iniciar con el plan de adecuación, se recomienda que en las acciones se consigue fecha, así como el registro de los documentos que acreditan dichas acciones.

(5) De acuerdo al estado de implementación de las acciones programadas para adecuación a la norma, siendo habitual definirlo en tres estados: Pendiente, En proceso, Implementado.

(6) De existir acciones pendientes o en proceso para adecuación, es recomendable tener una fecha estimada de implementación.

Evaluación: Tiene que ver principalmente con la probabilidad e impacto, en esta parte seguimos el criterio de la elaboración de matriz de cinco (5) niveles, en relación a la probabilidad los criterios que se pueden considerar son los que se exponen en la tabla 10

Tabla 10.

Probabilidades e impacto en la etapa de evaluación

PROBABILIDAD				
IMPROBABLE	**POCO PROBABLE**	**PROBABLE**	**MUY PROBABLE**	**CASI SEGURO**
No existe afectado No existe supervisor No se conoce sobre acciones legales contra la empresa o en el sector.	De concretarse el riesgo existe una persona afectada con legitimidad para denunciar o demandar.	De concretarse el riesgo existe una persona afectada con legitimidad para denunciar o demandar. Existe organismo supervisor especializado con competencia en caso de concretarse el riesgo.	De concretarse el riesgo existe una persona afectada con legitimidad para denunciar o demandar. Existe organismo supervisor especializado con competencia en caso de concretarse el riesgo. El organismo supervisor ejerce supervisión permanente.	De concretarse el riesgo existe una persona afectada con legitimidad para denunciar o demandar. Existe organismo supervisor especializado con competencia en caso de concretarse el riesgo. El organismo supervisor ejerce supervisión permanente. En el último año se ha presentado por lo menos un evento asociado al riesgo identificado que ha dado lugar a acciones legales contra la empresa. En el último año se conoce de eventos asociados al riesgo que ha dado lugar a acciones legales contra empresas del sector.

En relación al impacto, teniendo en cuenta que la propuesta de definición de riesgo legal considera no sólo el efecto económico, sino también la reputación, dicha concepción debe reflejarse en la valoración de impacto. Cabe mencionar que los valores financieros no pueden ser determinados de forma arbitraria, un criterio que puede ayudar en la labor es el que proporcionan las normas de auditoria, específicamente la NIA 320 que está referida a

la materialidad, dando como lineamiento la posibilidad de considerar como indicadores un porcentaje de las utilidades antes de impuestos o de los ingresos o de los activos totales, como ejemplo de referencia se expone la tabla 11

Tabla 11.

Valoración de impacto económico y la reputación

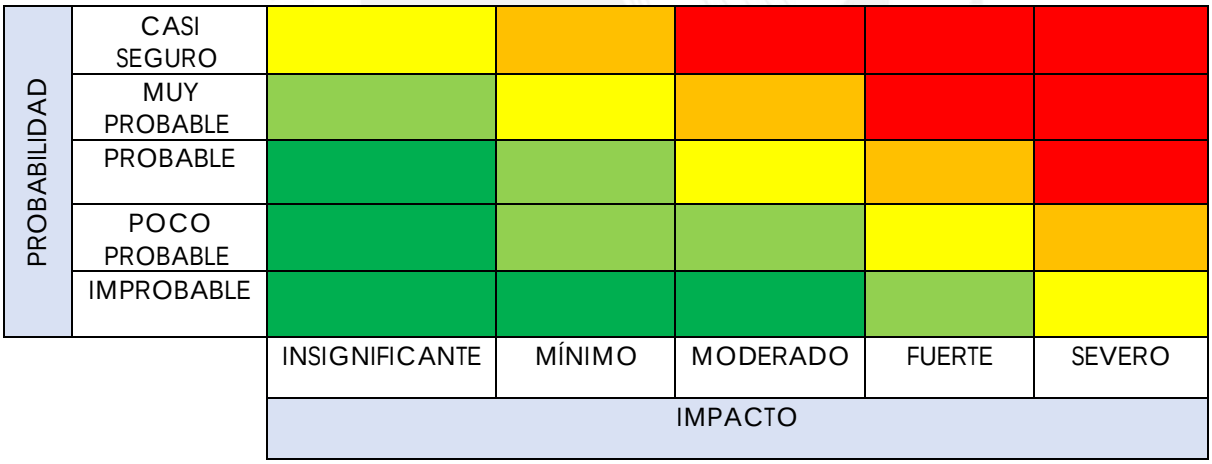
	IMPACTO				
	INSIGNIFICANTE	MÍNIMO	MODERADO	FUERTE	SEVERO
ECONÓMICO	Hasta el 0.5 % de utilidades antes de impuestos. Hasta el 0.1 % de los ingresos. Hasta el 0.1 % del activo total.	Más de 0.5 % hasta 1% de utilidades antes de impuestos. Más de 0.1 y menos del 0.2 % de los ingresos. Más de 0.1 % hasta 0.5 % del activo total.	Más de 1 % hasta 2 % de ganancia antes de impuestos. Más de 0.2 % y menos del 0.5 % de los ingresos. Más de 0.5 % menos del 1 % del activo total.	Más de 2 % hasta 4 % de ganancia antes de impuestos. Más de 0.5 % y menos de 0.9 % de los ingresos. Más de 1 % y menos del 1.5 % del activo total.	Más de 4 % de ganancia antes de impuestos. Más de 0.9 % de los ingresos Más de 1.5 % del activo total.
REPUTACIONAL	Difusión en medios de prensa locales o nacionales, o en redes sociales en periodo de hasta tres (3) días.	Difusión en medios de prensa nacionales o en redes sociales en periodo mayor a (3) y menor a (7) días. Posible incremento de eventos asociados al riesgo hasta 5 % del promedio del último año.	Difusión en medios de prensa nacionales o en redes sociales en periodo mayor a siete (7) y menor a (15) días. Posible incremento de eventos asociados al riesgo mayor a 5 % hasta 10 % del promedio del último año. Posible inicio de acciones por un (1)	Difusión en medios de prensa nacionales, redes sociales en periodo superior a (15) días. Posible incremento de eventos asociados al riesgo mayor a 10 % hasta 20 % del promedio del último año.	Difusión en medios de prensa nacionales o redes sociales en periodo superior a quince (15) días y manifestaciones públicas en instalaciones de la organización. Posible incremento de eventos asociados al riesgo mayor a 20 % del

			organismo regulador.	Posible inicio de acciones por parte de más de un (1) organismo regulador.	promedio del último año. Posible inicio de acciones legales contra miembros de la Alta Dirección

Para fines de la evaluación se requiere la relación entre el resultado de la probabilidad y el impacto, que puede ser efectuado con la tabla 12.

Tabla 12.

Matriz de evaluación del riesgo legal



NIVEL DE RIESGO	OPCIONES DE TRATAMIENTO DE RIESGO
MUY BAJO	Asumir
BAJO	Asumir
MODERADO	Mitigar
ALTO	Mitigar/Evitar/Compartir/Transferir
SEVERO	Mitigar/Evitar/Compartir/Transferir

Tratamiento: A partir del resultado de la evaluación del riesgo legal, cuando se requiera la mitigación del riesgo debe formularse un plan de tratamiento mediante la implementación de controles a fin que el riesgo residual sea aceptable, para lo cual se pueden utilizar las siguientes tablas: tabla 13, tabla 14, tabla 15, tabla 16.

Tabla 13.

Plan de tratamiento de riesgo legal

NRO. (1)	RIESGO LEGAL A TRATAR (2)	PLAN DE TRATAMIENTO O CONTROLES A IMPLEMENTAR	RESPONSABLE	RECURSOS ADICIONALES NECESARIOS	FECHA DE IMPLEMENTACIÓN

Descripción de campos:

(1) El número puede corresponder a la propia definición interna de la organización, por serie, correlativa, etc. Que haya sido consignado en el registro de riesgos.

(2) En esta columna debe indicarse el detalle del riesgo legal que será objeto de tratamiento.

(3) Se debe consignar las actividades y/o acciones para tratar el riesgo identificado.

(4) Se debe consignar la responsabilidad sobre el plan de tratamiento de acuerdo a la determinación de propiedad del riesgo indicados en la política de la organización.

(5) Consignar recursos adicionales que sean necesarios para la mitigación del riesgo legal a tratar.

(6) Consignar fecha prevista para concluir implementación del plan de tratamiento.

Tabla 14.

Modelo de evaluación de control

DETALLE DE CONTROL (1)	TIPO DE CONTROL (2)	EVALUACIÓN DEL CONTROL (3)				RIESGO RESIDUAL (4)
		Se encuentra documentado, con responsable definido y	Se aplica conforme al diseño	Mitiga riesgo identificado	Puntaje Final	

		frecuencia de aplicación				
		2	2	2		

Descripción de campos:

(1) Consignar la descripción del control a aplicar.

(2) Indicar tipo de control, preventivo, detectivo o correctivo.

(3) Se otorga puntuación de acuerdo a criterios y ponderación.

(4) Corresponde a la simulación de la calificación del riesgo luego de la aplicación del control evaluado

Tabla 15.

Criterios de evaluación de control

Por tipo de respuesta	Puntaje
SI	2
NO	0
Parcialmente	1

Por tipo de criterio	Ponderación
Se encuentra documentado, con responsable definido y frecuencia de aplicación	25 %
Se aplica conforme al diseño	25 %
Mitiga riesgo identificado	50 %

Tabla 16.

Calificación de control para riesgo residual

Calificación	Disminución de casillas en probabilidad	Disminución de casillas en impacto
0	0	0
1	1	1
2	2	2

Indica el número de casillas a reducir en ambos ejes de acuerdo a la calificación final del control.

3. Desempeño:

Comprende propiamente la ejecución o puesta en práctica del diseño, este componente está dirigido principalmente a la verificación de la gestión del riesgo de acuerdo a lo planificado, desde el cumplimiento de las políticas, el ejercicio efectivo de los roles y responsabilidades, la evaluación de los riesgos conforme a la metodología, además de su periodicidad y la implementación de los registros y documentos que documenten la gestión.

4. Supervisión:

Como parte de las actividades de supervisión se debe comprender la gestión de los litigios, la implementación de un buzón de denuncias, con políticas y procedimientos formalizados que pueden formar parte de la política de gestión del riesgo legal, así como la definición del mecanismo de aseguramiento de funcionamiento del sistema, que puede ser a través de autoevaluación, auditoria interna, auditoria externa, etc.; que tienen importancia para el proceso de mejora continua del sistema.

5. Información y comunicación

Principalmente asociado a reportes, en el que se define quienes son los destinatarios, que información deben recibir, el establecimiento de planes de capacitación de preferencia adecuado a los procedimientos del personal que recibe la capacitación, así como los canales de consulta para la absolución de inquietudes sobre el sistema de gestión de riesgo legal y la difusión de las personas a acudir en caso de ocurrir incidentes.

De igual forma que los estándares estudiados es posible expresar gráficamente el modelo de tal forma que nos muestre una visión general del mismo e incluso oriente los pasos para su implementación.

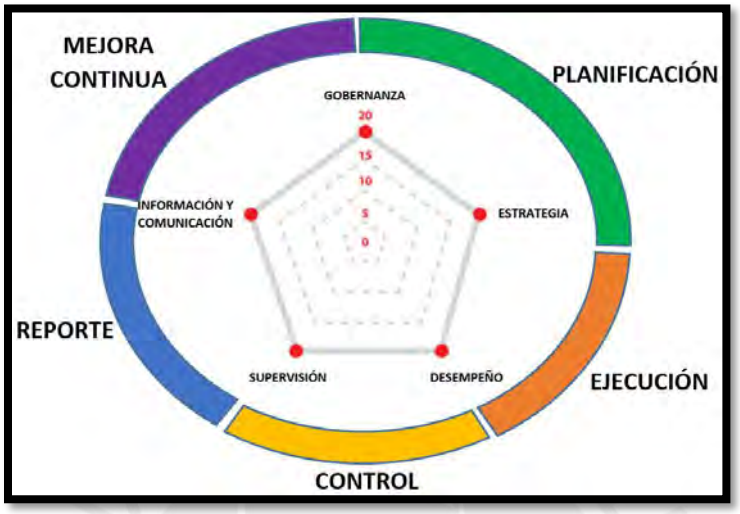


Figura 11. Pilares de modelo propuesto y flujo de implementación

La figura representa no sólo los pilares del modelo que se propone sino también el flujo de su implementación, dando orientación para la determinación de una hoja de ruta a partir de la visión que tenga sobre el tema la alta dirección y condiciones específicas de la empresa.

Por otro lado, para representar el avance de la implementación o aplicación de los estándares para la gestión del riesgo legal, se propone la adecuación al modelo CMMI como herramienta complementaria de que se reflejaría gráficamente en el pentágono de la figura 11 que representa el modelo que también requiere de una tabla para la valoración de cada uno de los criterios, cuya elaboración puede ser personalizada de acuerdo a los estándares de cada empresa.

CONCLUSIONES

El estudio efectuado demuestra que en la gestión empresarial se reconoce como un tipo de riesgo a la probabilidad de ocurrencia de un hecho o suceso relacionado a la regulación que afecte el cumplimiento de los objetivos de la empresa, denominado como “riesgo legal”.

El riesgo legal no tiene definición específica a nivel regulatorio, por lo que para su definición son pertinentes los estudios los estudios sobre gestión de riesgos y los estándares o buenas practicas normalizadas, como es el caso de ISO y COSO, que en ambos casos tienen lineamientos para la gestión del riesgo legal.

El riesgo legal comprende la probabilidad que la empresa o quienes actúan en nombre incurran en una conducta o suceda un hecho que en el ordenamiento jurídico tiene prevista una consecuencia de tipo positivo, negativo o ambos tipos que debe ser asumida por la empresa, no siendo limitativo a la sanción prevista por el sistema jurídico sino la afectación a la imagen o reputación; con la precisión que también tiene contenido ético en la medida que el derecho tiene una relación de conexión con la moral.

El riesgo legal tiene como característica particular su vinculación con las normas jurídicas, y desde la perspectiva del origen de la norma jurídica puede ser clasificado como riesgo regulatorio, que comprende lo que se conoce como riesgo de cumplimiento, el cual está vinculado a la observancia de los mandatos del estado; y riesgo contractual, que comprende los vinculados a la formación de la voluntad contractual y su expresión en las cláusulas contractuales, por lo que tiene relación con el cumplimiento de las condiciones contractuales pactadas con terceros.

A partir de la investigación efectuada es posible la elaboración de un modelo para la gestión del riesgo legal empresarial, de tal forma que la gestión se realice de forma preventiva e integral, con su incorporación a las actividades diarias de la empresa; cuyo fundamento debe partir del entendimiento del riesgo legal y sus alcances, cuya implementación requiere el compromiso de la alta dirección, de forma similar que para la implementación de cualquier sistema de gestión.

Para la elaboración de un sistema de gestión de riesgo legal son de utilidad los marcos de gestión ISO y COSO, que ayudan a establecer los parámetros necesarios para la implementación del modelo de gestión de riesgos, que deben ser complementadas con el modelo de tres líneas de defensa cuyo principal aporte es el entendimiento de los roles y responsabilidades para la gestión de riesgos. También se requiere complementar con el diseño de herramientas como un modelo de madurez que otorgará orientación sobre el nivel de implementación.

Para fines de implementar un sistema de gestión de riesgo legal se puede considerar las etapas de: i) Planificación, ii) Ejecución, iii) Control, iv) reporte y v) mejora continua, que se relacionan con los pilares de gestión: i) Gobernanza, ii) Estrategia, iii) Desempeño, iv) Supervisión y v) Información y comunicación.

Para fines de fortalecer las habilidades para la gestión de riesgo legal se requiere no sólo el entendimiento del derecho sino también de materias como la gestión estratégica, gestión de riesgos, control interno. Dichos aspectos también serán convenientes para futuras investigaciones sobre la gestión del riesgo legal.

REFERENCIAS BIBLIOGRÁFICAS

Abella Rubio, R. (2006). COSO II y la gestión integral de riesgos del negocio. *Estrategia Financiera*(225), 20-24.

Acevedo Sanchez, D. (6 de Abril de 2020). *Transformación organizacional para abogados en tiempos de crisis*. Recuperado el Junio de 2021, de EY Building a better working world: https://www.ey.com/es_co/law/transformacion-organizacional-abogados-tiempos-de-crisis

Balboa, J. M. (2017). El valor añadido de la función jurídica interna. En Lawyerpress, *La abogacía desde dentro: La visión de los abogados in-house sobre los cambios en la profesión* (págs. 44-45). Galapagar.

Bejarano, L., Palencia, C., Montoya, C., & Sanchez, C. (s.f.). Nuevos desafíos en la gestión de riesgos para el sistema financiero. En S. Clavijo, *Regulación y Gestión de Riesgos Financieros: Una visión comparada* (págs. 95-122).

Cabeza, M., & Torra, S. (2007). *El riesgo en la empresa: medida y control mediante @RISK*. New York: Palisade.

Capa, C. (13 de Agosto de 2013). *Abogados 'in house', las nuevas estrellas.* Recuperado el Junio de 2021, de CincoDías: https://cincodias.elpais.com/cincodias/2013/10/21/economia/1382375697_372235.html

Ceballos Homero, D. (2007). Una propuesta de indicador de riesgo legal: Valoración a través de la teoría de seguros del riesgo legal. *2ª Reunión de Investigación en Seguros y Gestión de riesgos.*

Comercio, D. E. (15 de Noviembre de 2019). Una especialidad para asegurar la ética de las empresas. *El Comercio*.

Comité de Supervisión Bancaria de Basilea. (Junio de 2006). Convergencia internacional de medidas y normas de capital. Basilea, Suiza, Suiza.

Committee of Sponsoring Organizations of the Treadway Commision (COSO). (2017). *Compliance Risk Management: Applying the COSO ERM Framework.*

Contraloría General de la República. (2014). *Marco Conceptual del Control Interno.* Lima. Obtenido de

https://apps.contraloria.gob.pe/wcm/control_interno/documentos/Publicaciones/Marco_Conceptual_Control_Interno_CGR.pdf

Crosby, P. (1987). *La calidad no cuesta: el arte de cerciorarse de la calidad.* México: Compañia Editorial Continental S.A.

Dassum Barrera, C. (2 de Diciembre de 2016). *¿Cuál es el rol del abogado in-house?* Recuperado el Junio de 2021, de Pérez Bustamante & Ponce: https://www.pbplaw.com/es/rol-abogado-in-house/

Defilippi, A. (13 de Diciembre de 2019). Compliance en las empresas: una prioridad. *Gestión*.

Martín, A. N. (2013). Regulatory capitalism y cumplimiento normativo. En T. l. blancht, *El derecho penal económico en la era compliance* (págs. 11-30). Valencia: Tirant lo blancht.

Del Rosal, P. (10 de Abril de 2019). *Los abogados internos, ante el reto de cómo aportar valor añadido al negocio*. Recuperado el Junio de 2021, de CincoDías: https://cincodias.elpais.com/cincodias/2019/04/10/legal/1554875988_776305.html

De Trazegnies, F. (1999). "La responsabilidad Extracontractual". Capitulo: Las tendencias en boga en la responsabilidad extracontractual. En A. d. Magistratura, *PROFA Tercer Curso Módulo 4: Derecho Civil* (págs. 464-500). Lima.

Gestión. (31 de Julio de 2018). Corrupción en empresas: Cinco recomendaciones para designar al Compliance Officer. *Gestión*.

Gan@Más. (3 de Agosto de 2016). *El 74% de gerentes considera que los riesgos legales pueden afectar continuidad de una empresa.* Recuperado el Junio de 2021, de Sitio web de Gan@más: https://revistaganamas.com.pe/el-74-de-gerentes-considera-que-los-riesgos-legales-pueden-afectar-continuidad-de-una-empresa/

Garib Market Maker/For Legal. (6 de Enero de 2021). *Pasado, Presente y Futuro: Los Desafíos del Abogado In House para 2021*. Recuperado el Junio de 2021, de Garib Market Maker/For Legal: https://gmarketmaker.com/2021/01/06/pasado-presente-y-futuro-los-desafios-del-abogado-in-house-para-2021/

Hopkins, B. E. (2013). *Legal Risk Management for In-House Counsel and Managers: A Manager's Guide to Legal and Corporate Risk Management.* Trafford Publishing.

ISO. (Febrero de 2018). ISO 31000:2018 Gestión de Riesgos - Directrices. Suiza.

ISO. (Mayo de 2020). ISO 31022:2020 Risk Management-Guidelines for the management of legal risk. Switzerland.

Lizarzaburu, E., Berggrun, L., & Quispe, J. (2012). Gestión de riesgos financieros. Experiencia en un banco latinoamericano. *Estudios Gerenciales, 28*(125), 96-103.

Lopez Pascual, J., & Gonzales Altina, S. (2008). *Gestión bancaria: factores claves en un entorno competitivo.* Madrid: McGraw-Hill.

Mahler, T. (2010). Tool-supported Legal Risk Management: A Roadmap. *European Journal of Legal Studies, 2*(3), 146-167. Recuperado el 30 de Junio de 2021, de http://hdl.handle.net/1814/15122

Monroy Gálvez, J. (1996). *Introduccion al proceso civil. Tomo I.* Santa Fe de Bogotá: Temis.

Morales, O. (21 de Setiembre de 2021). *La ética en tiempos de pandemia.* Recuperado el Noviembre de 2021, de RPP: https://rpp.pe/columnistas/oswaldomorales/la-etica-en-tiempos-de-pandemia-noticia-1355336

Moorhead, R., & Vaughan, S. (2015). *Legal Risk: Definition, management and ethics*. Obtenido de SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594228

Navarro, E. (06 de Junio de 2018). *Abogados "in-house"*. Recuperado el Junio de 2021, de Fuera de la Ley: https://www.expansion.com/blogs/navarro/2018/06/06/abogados-in-house.html

Nuñez Mora, J., & Chavez Gudiño, J. J. (2010). Riesgo operativo: esquema de gestión y modelado del riesgo. *Revista Análisis Económico, XXV*(58), 123-157.

Ochoa, O. L. (Diciembre de 2016). MODELOS DE MADUREZ DIGITAL: ¿EN QUÉ CONSISTEN Y QUÉ PODEMOS APRENDER DE ELLOS? *BOLETIN DE ESTUDIOS ECONOMICOS, LXXI*(219), 573-590. Obtenido de https://www.researchgate.net/publication/313798566_Modelos_de_Madurez_Digital_en_que_consisten_y_que_podemos_aprender_de_ellos

Pérez-Mergarejo, E. P.-V.-R. (Agosto de 2014). *Maturity models and the suitability of its application in small and medium enterprises.* Obtenido de Scielo Cuba: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-59362014000200004&lng=es&tlng=en

Pesce, L. A. (16 de Diciembre de 2016). *El abogado "in house": un profesional clave dentro de la empresa.* Recuperado el Junio de 2021, de Abogados.com.ar: https://abogados.com.ar/el-abogado-in-house-un-profesional-clave-dentro-de-la-empresa/19267

Perez Mergarejo, E., & Perez Vergara, I. y. (mayo de 2014). *Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas.* Recuperado el Junio de 2021, de Scielo Cuba: http://scielo.sld.cu/scielo.php?pid=S1815-59362014000200004&script=sci_arttext&tlng=en

Quintas, S. J. (2007). La gestión de riesgo normativo en el sistema financiero. *Revista Galega de Economía, 16*(extraordinario).

Rubio Correa, M. (2009). *El sistema jurídico: Introducción al Derecho.* Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú.

Ruberto, G. (2 de Agosto de 2017). *Gloria: ventas cayeron, pero utilidad neta creció hasta S/. 236 millones.* Recuperado el Noviembre de 2021, de Semana Económica: https://www.semanaeconomica.pe/sectores-empresas/consumo-masivo/237872-gloria-ventas-cayeron-pero-utilidad-neta-crecio-hasta-s-236-millones

Rubio, M., & Arce, E. (2017). *Teoría Esencial del Ordenamiento Jurídico Peruano.* Lima: Pontificia Universidad Católica del Perú-Fondo Editorial.

San Martin Albizuri, N. (2015). El riesgo en las entidades financieras: una perspectiva práctica. En A. Beraza Garmendia, A. Gilsanz Lopez, R. M. Ahumada Carazo, J. Hoyos Iruarrizaga, M. A. Peña Cerezo, F. J. Ibañez Hernandez, & N. San Martin Albizuri, *Gestión de Entidades Financieras: Un enfoque práctico de la gestión bancaria actual* (págs. 233-280). Madrid: ESIC Editorial.

Soler-Gonzalez, R., Varela-Lorenzo, P., Oñate-Andino, A., & Naranjo-Silva, E. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas. *Revista Ciencia UNEMI, 11*(26), 51-62.

Soler Ramos, J. A., Staking, K. B., Ayuso Calle, A., Beato, P., Botin O'Shea, E., Escrig Melia, M., & Falero Carrasco, B. (1999). *Gestión de riesgos financieros: un enfoque práctico para paises latinoamericanos.* Washigton DC: Banco Interamericano de Desarrollo.

Standards Australia/Standards Nueva Zelanda. (2004). *AS/NZS 4360:2004 Gestión de Riesgos.* Sydney y Wellington: Standards Australia International Ltd.

Superintendencia de Banca, Seguros y Administradoras de Fondos de Pensiones. (2009). Aprueba Reglamento de Riesgo Operacional, Resolución SBS Nº 2116-2009.

The Institute of Internal Auditors. (2020). *El modelo de las tres líneas del IIA 2020: Una actualización de las tres líneas de defensa.*

Torres Vásquez, A. (2019). *Introducción al Derecho.* Lima: Instituto Pacífico.

Valores, S. d. (2015). *Se aprueba el Reglamento de Gestión Integral de Riesgos, Resolución SMV Nº 037-2015.*

Whalley, M., & Guzelian, C. (2017). *The Legal Risk Management Handbook: An International Guide to Protect Your Business from Legal Loss.* Londres: Kogan Page Ltd.