



UNIVERSIDAD
DE PIURA

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

El Compliance Risk Assessment (CRA) como parte de los procesos para identificar y mitigar riesgos normativos en el Banco XYZ supervisado por la Superintendencia de Banca, Seguros y AFP

Trabajo de Suficiencia Profesional para optar el Título de Contador Público

Tania Elizabeth Olivares Sánchez

Revisor(es):
Dr. Julio César Hernández Pajares

Piura, octubre de 2021



A Dios, la Virgen María y mis ángeles de la guarda, Antonio y Luz, que guían mis pasos.

A mis padres, Luis y Manuela, por su amor y motivación constante.

A mis hermanas, Claudia y Alicia, por su apoyo incondicional.

Con especial agradecimiento a mi asesor Dr. Julio Hernández.





Resumen

El propósito de esta investigación es asegurar y proponer oportunidades de mejora que permitan el apropiado cumplimiento de la regulación aplicable a la empresa de estudio. Se plantearon como objetivos las principales obligaciones y responsabilidades que tienen las empresas supervisadas por la SBS para la adecuada implementación de una estructura de cumplimiento normativo; estructura diseñada conforme lo requerido por la regulación correspondiente. Implementar herramientas necesarias para asegurar y plantear oportunidades de mejora.

El estudio se realizó aplicando un enfoque de investigación cualitativo, porque busca describir los procedimientos que se llevaron a cabo en una Entidad Bancaria con la finalidad de identificar riesgos de cumplimiento normativo e implementar controles internos que sirvan para mitigarlos. Aparte de ello, se aplicó la entrevista y encuesta como técnicas de investigación, realizadas al Oficial de Cumplimiento Normativo, Gerente de Control de Cumplimiento y Sub Gerente de Supervisión de Cumplimiento.

El estudio permitió demostrar que si se aplica el *Compliance Risk Assessment* (CRA) se pueden definir los lineamientos y metodologías para evaluar el cumplimiento de las regulaciones externas que tienen impacto directo en la empresa de estudio, a través de la priorización de las normas y/o procesos bajo criterios que determinan el nivel de exposición de estas. Como resultado de ello, se elabora un plan de trabajo a evaluar por este frente, el cual consiste en identificar las obligaciones normativas, evaluar la adecuación en la empresa de estudio y definir planes de acción de identificar brechas respecto a la regulación vigente.

Las enseñanzas y experiencias adquiridas a lo largo de la vida universitaria y profesional del autor han tenido una gran contribución para el desarrollo del presente trabajo. A través de este trabajo de suficiencia profesional se ha logrado demostrar que la aplicación del CRA permite definir los lineamientos y metodologías para prevenir, identificar y/o mitigar los posibles incumplimientos normativos, mediante la ejecución de evaluaciones y/o autoevaluaciones, en las diferentes unidades de la empresa de estudio. Por tal motivo, las empresas que no desarrollen un apropiado programa de cumplimiento normativo se encuentran expuestas a posibles riesgos reputacionales, fraude, lavado de activos y de financiamiento del terrorismo.



Tabla de contenido

Introducción.....	13
Capítulo 1 Aspectos generales	15
1.1 Descripción de la empresa	15
1.1.1 Ubicación	15
1.1.2 Actividad.....	15
1.1.3 Misión y visión de la empresa	15
1.1.4 Organización.....	15
1.2 Descripción general de la experiencia.....	17
1.2.1 Actividad profesional desempeñada.....	17
1.2.2 Propósito del puesto	17
1.2.3 Producto o proceso que es objeto del informe.....	18
1.2.4 Resultados concretos logrados.....	18
Capítulo 2 Fundamentación del tema.....	19
2.1 Teoría y práctica en el desempeño profesional	19
2.1.1 Antecedentes	19
2.1.2 Antecedentes de investigación	20
2.1.3 Bases teóricas.....	21
2.2 Descripción de las acciones, metodologías y procedimientos.....	26
2.2.1 Mapeo regulatorio, priorización y evaluación	26
2.2.2 Metodología del estudio	27
2.2.3 Entrevista de investigación.....	28
Capítulo 3 Aporte y desarrollo de experiencias.....	29
3.1 Aportes	29
3.1.1 Mapeo regulatorio.....	29
3.1.2 Desarrollo de la matriz impacto	29
3.1.3 Evaluación.....	31
3.2 Desarrollo de experiencias	31
Conclusiones	33
Recomendaciones	35
Lista de referencias	37



Lista de tablas

Tabla 1. Tipos de origen de riesgo.....	29
Tabla 2. Criterios para el cálculo de probabilidad e impacto.....	30
Tabla 3. Valoración de nivel de control.....	30
Tabla 4. Cálculo del riesgo residual.....	31





Lista de figuras

Figura 1. Esquema de la gestión del programa de cumplimiento normativo del Banco XYZ	16
Figura 2. Organigrama de la Gerencia de División Cumplimiento y Ética Corporativo.....	17
Figura 3. Ranking de corrupción 2020.....	19
Figura 4. Encuesta sobre la lucha contra la corrupción en el Perú 2019	20
Figura 5. Coso 1992 vs 2013.....	23
Figura 6. Funciones y línea de defensa para la evaluación del riesgo de operación	24
Figura 7. Método para la identificación de un riesgo	25
Figura 8. Mapa semántico de probabilidad / impacto	26





Introducción

Las entidades supervisadas por la Superintendencia de Banca, Seguros y AFP (SBS) tienen el deber de implementar los mecanismos necesarios para garantizar el correcto cumplimiento normativo de acuerdo con las necesidades de cada organización, teniendo como propósito identificar oportunamente a las áreas responsables que tienen impacto directo con las normas externas en relación a las funciones que realizan, al igual que las normas internas relacionadas, con el fin que se tomen las acciones oportunas que permitan cumplir con las disposiciones requeridas. Superintendencia de Banca, Seguros y AFP (SBS) 2017. *Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos*. Cumplimiento Normativo.

La importancia de tener una apropiada gestión de cumplimiento normativo permite prevenir riesgos de cumplimiento normativo y reputacionales al que potencialmente se exponen las empresas, contribuyendo a fortalecer la cultura de cumplimiento en las empresas, y desarrollar un esquema de referencia que impulse el entendimiento y el cumplimiento de la regulación aplicable.

El primer capítulo está enfocado en dar a conocer a la empresa de estudio y las enseñanzas y experiencias adquiridas a lo largo de la vida universitaria y profesional realizadas. El segundo capítulo está enfocado en el marco teórico, así como en las acciones, mecanismos y metodologías de investigación.

Al respecto, el presente trabajo tiene como propósito asegurar y proponer oportunidades de mejora que permitan el apropiado cumplimiento de la regulación aplicable a la empresa de estudio. Se plantearon como objetivos específicos las principales definiciones, obligaciones y responsabilidades que tienen las compañías reguladas y supervisadas por la SBS para la adecuada implementación de una estructura de cumplimiento normativo; estructura diseñada conforme lo requerido por la regulación correspondiente. implementar herramientas necesarias para asegurar y plantear oportunidades de mejora.

Finalmente, el tercer capítulo está enfocado en los aportes, conclusiones y recomendaciones realizados en el trabajo de suficiencia profesional.



Capítulo 1 Aspectos generales

1.1 Descripción de la empresa

El Banco XYZ es una sociedad anónima. Las operaciones de la empresa de estudio están reguladas por la Ley General del Sistema Financiero y de Seguros y Orgánica de la SBS; encontrándose autorizada a realizar operaciones como compañía múltiple por la SBS, de acuerdo con las disposiciones legales vigentes en el Perú.

1.1.1 Ubicación

El domicilio legal del Banco XYZ está ubicado en Lima, Perú. Al 31 de diciembre de 2020, la empresa de estudio tiene 388 sucursales y agencias en el Perú, y 2 sucursales en el exterior.

1.1.2 Actividad

La empresa de estudio está facultada a realizar distintas operaciones y servicios bancarios, tales como recibir depósitos, realizar transacciones, otorgar préstamos y de la misma manera invertirlos junto con su capital. La empresa de estudio puede realizar operaciones como sociedad agente de bolsa, establecer y administrar fondos mutuos, entre otros, a condición de que constituya subsidiarias con ese propósito.

Las actividades realizadas por las distintas áreas, de la empresa de estudio, al ser supervisadas por la SBS, cuentan con un programa de cumplimiento normativo que aseguran la adecuada implementación de la norma y del riesgo de la misma, en tanto les corresponda, y direccionan a su equipo sobre la debida implementación de la misma; de ser necesario, en determinadas oportunidades se forma un equipo multidisciplinario que define el plan de acción, al cual cumplimiento normativo realiza seguimiento, con el fin de mitigar riesgos de cumplimiento normativo y reputacionales.

1.1.3 Misión y visión de la empresa

- **Misión:** ser una compañía que contribuya al desarrollo y superación, alentando y transformando los sueños de sus clientes en realidad.
- **Visión:** ser una compañía peruana referente en gestión empresarial potenciando su liderazgo en la industria financiera en el Perú.

1.1.4 Organización

La empresa de estudio está sujeta al cumplimiento de una variedad de normas legales y reglamentarias emitidas por las entidades que la supervisa, por ello, para asegurar el apropiado cumplimiento de un marco legal complejo y en continua evolución, el directorio de la empresa de estudio aprobó la creación del programa de cumplimiento normativo, el cual está estructurado por las siguientes gerencias como se puede observar en la figura 1 y figura 2.

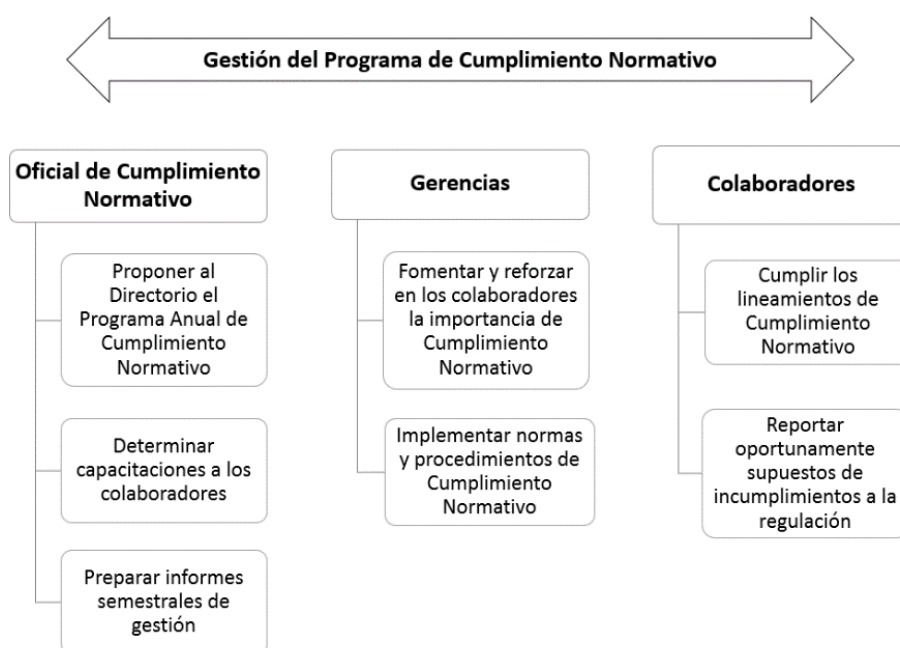
- **Oficial de Cumplimiento Normativo:** su responsabilidad es velar por el cumplimiento de la estructura establecida que permita un diligente desarrollo de su función, logrando así: vigilar el cumplimiento normativo aplicable a la compañía, asegurar la existencia de una estructura que

permita la elaboración de procedimientos y controles que cumplan con las decisiones tomadas y tareas asignadas a los colaboradores de la empresa de estudio.

- **Gerente de Área de Gestión de Cumplimiento:** tiene como principal responsabilidad vigilar el cumplimiento normativo aplicable a la empresa de estudio, y asegurar la existencia de procedimientos y controles que permitan corroborar que los colaboradores cumplen con las decisiones tomadas y tareas asignadas.
- **Coordinadores de Cumplimiento Normativo:** tienen como principal responsabilidad elaborar el plan anual de evaluación por normas existentes a través de la priorización de las normas y/o procesos bajo criterios que determinan el nivel de exposición de estas, así como realizar la evaluación de riesgos de cumplimiento, conforme lo señalado en el procedimiento interno de la compañía.
- **Gerentes de Área:** tienen la responsabilidad de implementar la norma y el riesgo de esta, en tanto les corresponda, y deberán direccionar a su equipo sobre la debida implementación de esta; de ser necesario, en determinadas oportunidades se deberá formar un equipo multidisciplinario que defina el plan de acción, al cual cumplimiento normativo realizará seguimiento, o podrían decidir contratar un consultor externo responsable de liderar la implementación.
- **Colaboradores:** son responsables del cumplimiento de la regulación que le resulte aplicable dentro del ejercicio de sus funciones.

Figura 1

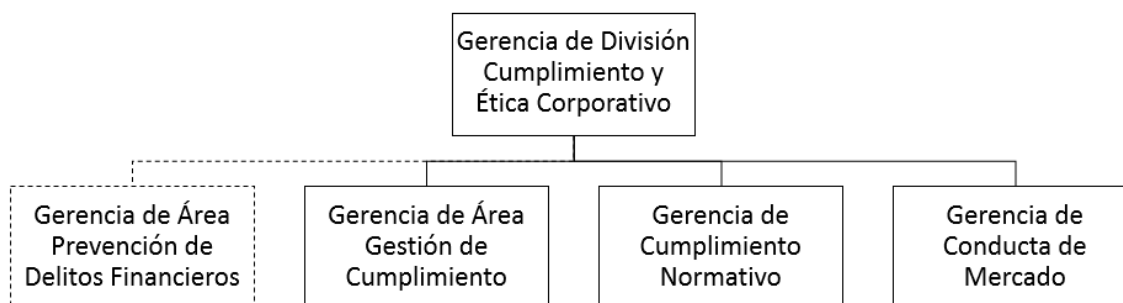
Esquema de la gestión del programa de cumplimiento normativo del Banco XYZ



Nota. Elaboración propia, en base a la información del Banco XYZ.

Figura 2

Organigrama de la Gerencia de División Cumplimiento y Ética Corporativo



Nota. Elaboración propia, en base a la información del Banco XYZ.

1.2 Descripción general de la experiencia

1.2.1 *Actividad profesional desempeñada*

En febrero 2020, se inició la relación laboral en la empresa de estudio como Sub Gerente Adjunto Supervisión de Cumplimiento en su oficina central en la ciudad de Lima. Las principales funciones a cargo que se realizan son:

- Elaborar y/o actualizar la matriz de impacto que contiene el mapeo regulatorio de las regulaciones de impacto para la compañía.
- Elaborar el plan anual de las regulaciones a evaluar.
- Ejecutar las evaluaciones planificadas en el plan anual.
- Identificar riesgos normativos y/u oportunidades de mejora de las regulaciones evaluadas.
- Elaborar informes semestrales.

1.2.2 *Propósito del puesto*

El puesto fue creado con el fin de diseñar los lineamientos y metodologías que permitan prevenir, identificar y mitigar los posibles incumplimientos normativos. Mediante la ejecución de evaluaciones por normas y/o procesos, donde se valida el cumplimiento de las regulaciones aplicables a la empresa de estudio en coordinación con las áreas evaluadas. Las principales responsabilidades desempeñadas son:

- En el periodo de un año, el responsable del puesto realizará como mínimo dos evaluaciones por normas y/o procesos. La revisión se iniciará, previa aprobación del Oficial de Cumplimiento Normativo (en adelante OCN).
- El responsable del puesto debe informar al OCN sobre los avances en el proceso de priorización y/o de revisión a través de los comités bimensuales.
- Proporcionar la información esencial para la elaboración de los informes semestrales a ser presentados al directorio, gerencias u organismos supervisores, según corresponda, asegurando la integridad de la información.

- Participar del comité de cumplimiento normativo, presentando resultados de su gestión y proporcionando datos e información relevante.

1.2.3 Producto o proceso que es objeto del informe

En solución al dinamismo de los procesos en las empresas, existen riesgos potenciales sobre ciertas regulaciones que podrían representar riesgos de cumplimiento.

En tal sentido, con la finalidad de revisar el nivel de cumplimiento de las regulaciones externas que tienen impacto directo en la empresa de estudio, se deberá elaborar un procedimiento de priorización para determinar las regulaciones con score igual a: relevante, alto o crítico, con el fin de determinar la regulación que será evaluada, utilizando drivers diferenciadores.

Por consiguiente, el objeto de este informe es proponer la aplicación del *Compliance Risk Assessment* (CRA) e implementar herramientas necesarias para garantizar el correcto cumplimiento de la normativa adaptable a la compañía de estudio. Se plantearon como objetivos específicos las principales definiciones, obligaciones y responsabilidades que tienen las entidades reguladas por la SBS para la adecuada implementación de una estructura de cumplimiento normativo.

1.2.4 Resultados concretos logrados

Se alcanzó a concretar con la Gerencia de Cumplimiento Normativo de la empresa de estudio, procedimientos que permitan asegurar la correcta adecuación y supervisión del cumplimiento de la regulación adaptable a esta.

Se logró también aplicar el *Compliance Risk Assessment* (CRA) para medir los riesgos de las regulaciones externas que son evaluadas por el responsable del puesto y así proponer planes de acción y/u oportunidades de mejora para mitigarlos.

Se observó también que, los riesgos identificados con criticidad relevante, alto y crítico cuentan con planes de acción y el resultado de la Evaluación es comunicado oportunamente al OCN de la empresa de estudio.

Capítulo 2 Fundamentación del tema

2.1 Teoría y práctica en el desempeño profesional

Para el desarrollo del presente trabajo se ha aplicado el *Compliance Risk Assessment (CRA)* con el fin de identificar y/o mitigar riesgos de cumplimiento normativo al que potencialmente se expone la empresa de estudio. Se han tomado en cuenta los estudios previos que a continuación se expondrán, los cuales han servido como soporte para definir el objeto de estudio.

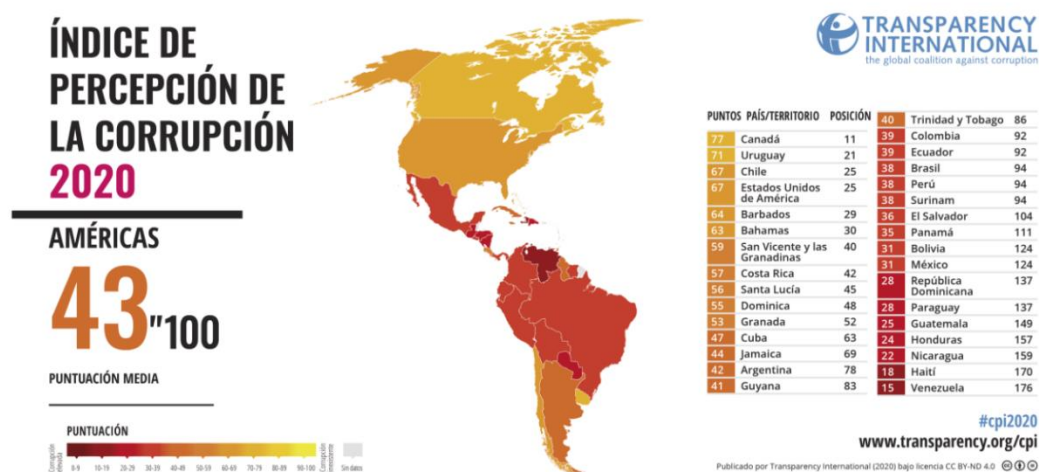
2.1.1 Antecedentes

En el Índice de percepción de la corrupción del año 2020, se puede concluir que, en el año 2018, el Perú se ubicó en el puesto 105 considerándose el indicador más inferior en esta herramienta de evaluación. Sin embargo, entre los años 2019 y 2020, mejoró ligeramente escalando once puntos. Para Samuel Rotta, Director Ejecutivo de Proética, esta puntuación es el resultado de las investigaciones de casos de corrupción y cambios importantes, como por ejemplo la prohibición de postular a cargos políticos a personas sentenciadas y mejoras en el sistema de supervisión. Al mismo tiempo, se progresó con la eliminación de la inmunidad parlamentaria y reforma constitucional. (Proética, s.f.)

Como se puede visualizar en la figura 3, el Perú logró obtener una posición de 38 sobre 100, mejorando dos puntos con respecto al periodo pasado y ocupando actualmente la posición 94 en el estudio realizado por Proética.

Figura 3

Ranking de corrupción 2020



Nota. Proética (s.f.).

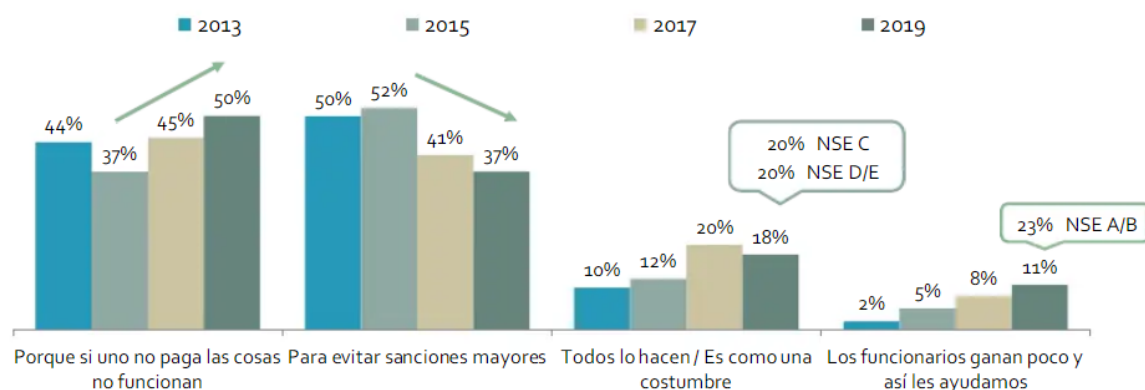
Según la última encuesta nacional sobre la lucha contra la corrupción a nivel institucional, los ciudadanos peruanos ubican en el ranking de las razones para dar una coima o realizar un pago indebido en el año 2019, a la razón “porque si uno no paga las cosas no funcionan” en el primer puesto con un 50%, seguido por el segundo lugar a “para evitar sanciones mayores” con un 37%, mientras que “todos lo hacen” ocupa el tercer puesto con un 18%. (Proética, s.f.)

Figura 4

Encuesta sobre la lucha contra la corrupción en el Perú 2019

¿Por qué lo dio una coima, regalo o pago indebido a dicha institución?

MEDICIÓN COMPARATIVA- RESPUESTA MULTIPLE



Nota. Proética (s.f.).

A partir de la vigencia de la Ley 30424, que regula la responsabilidad administrativa de las personas jurídicas modificada por el Decreto Legislativo 1352 y su reglamento, se recomendó a estas, las cuales operan en el Perú, implementar un programa de prevención alineado a estándares y buenas prácticas internacionales de compliance. Esto con el objetivo de prevenir riesgos de lavado de activos, financiamiento del terrorismo y tráfico de influencias. En adición a estos riesgos, los programas de prevención pueden considerar gestionar otras fuentes de riesgo de cumplimiento relacionadas a la industria del sector de cada empresa.

Las manifestaciones de los riesgos de cumplimiento generan impactos de carácter económico, legal, operativo y reputacional, entre otros. En este contexto surge la necesidad, en el sector empresarial, de incluir dentro de su planilla a colaboradores que cuenten con conocimientos en gestión de riesgos y compliance que les permita implementar herramientas y diseños para mitigar riesgos dentro de la compañía.

2.1.2 Antecedentes de investigación

El compliance, también conocido como cumplimiento normativo, es el grupo de regulaciones, prácticas, políticas y procedimientos que implementan las empresas con el fin de identificar riesgos relacionados con aspectos legales, operativos u otros, prevenirlos y mitigarlos. La importancia de implementar el compliance es evitar y/o sancionar los actos de soborno y corrupción. Al respecto, se

incentiva a las empresas a realizar una adecuada investigación para descubrir y/o prevenir fraudes a los que se encuentran expuestas. Yong (2021).

Cárdenas-Cuba (2019) en su investigación para optar el grado de maestro, destaca la importancia de adecuar un programa de cumplimiento, compliance, dentro de las empresas con el objetivo de mitigar actos y/o delitos de lavado de activos y financiamiento del terrorismo. Asimismo, brinda sugerencias y mecanismos que permiten mejorar los procesos y métodos antes aplicados por las empresas en su gestión de programas de compliance, buenas prácticas o debida diligencia en sus gestiones y operaciones empresariales.

Talavera (2020), en su tesis de maestría, analiza la necesidad de implementar y desarrollar procedimientos de cumplimiento normativo con el fin de evitar actos ilegales. Asimismo, concluye con algunas propuestas de implementación para lograr un adecuado sistema de cumplimiento normativo.

Sanclemente-Arciniegas (2020) *Compliance, empresas y corrupción: una mirada internacional. Derecho PUCP*, (85), 9-40. En la presente revista el autor desarrolla una explicación sobre el entendimiento jurídico de compliance y la lucha contra la corrupción en las organizaciones, a través de una nueva tendencia regulatoria global que propone procedimientos ventajosos para afrontar diferentes hitos, donde se presentan asuntos que están normados y regulados, implementados por las organizaciones con la finalidad de tener en cuenta esas obligaciones. En ese sentido, el autor destaca la manera en la que, al pretender mitigar el riesgo de incumplimiento normativo, las empresas incorporen mecanismos para proteger sus intereses.

2.1.3 Bases teóricas

2.1.3.1 Cumplimiento normativo. En base a los estándares internacionales (ISO 19600 “Compliance Management System” e ISO 37001 “Antibrabery Management System”) podemos definir compliance como “cumplimiento” o “conformidad” de forma genérica ya que engloba diferentes grupos normativos que perjudican a la operación de la empresa, así como las responsabilidades asumidas espontáneamente por estas. (ISO 37001,2016).

Así también, Carrascosa (2018) en el Comité de Basilea para la supervisión bancaria en su presentación “La medición del riesgo de Cumplimiento”, explica al riesgo de cumplimiento normativo como a la pérdida económica o reputacional a la que una entidad bancaria se encuentra expuesta como consecuencia de no cumplir con las normas, regulaciones, procedimientos exigidos por las entidades supervisadas aplicables a esta. Asimismo, precisa que el incumplimiento del código de ética y conducta aplicable a con sus actividades puede conllevar posibles riesgos operativos, regulatorios (sanciones) y/o reputacionales causando una impresión contraria a las expectativas de crecimiento para la compañía. Busca como objetivo principal incentivar la implementación de un procedimiento metodológico que califique los riesgos para priorizar diversos factores que puedan perjudicar el tipo

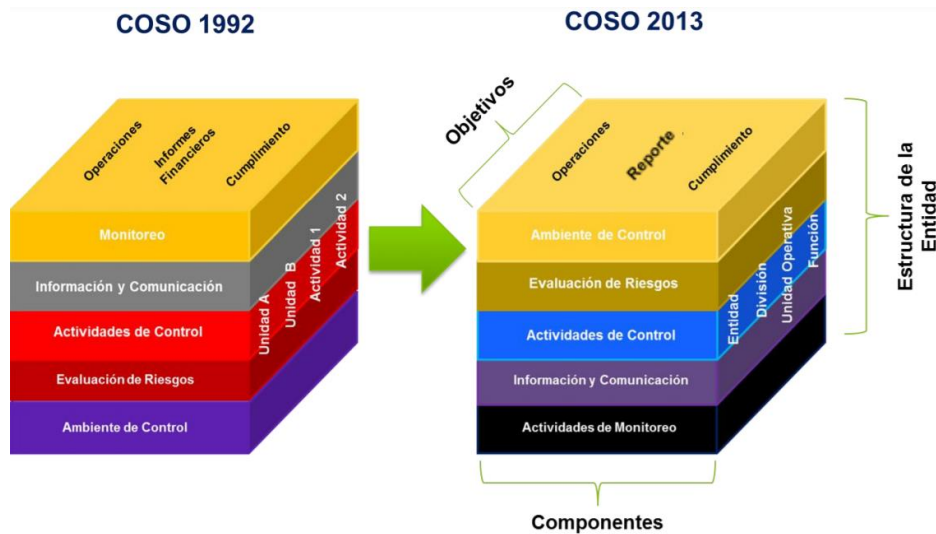
de negocio de la organización, la reputación o los distintos escenarios financieros por no contar con el nivel necesario por las regulaciones, las políticas y los modelos internos.

El cumplimiento normativo tiene como función considerar la valoración y la supervisión del cumplimiento de aquellas regulaciones externas e internas que tienen un impacto directo en las actividades de la compañía supervisada, teniendo como prioridad identificar y comunicar oportunamente a las áreas responsables de estas compañías, con el fin que tomen las medidas oportunas y necesarias para asegurar el cumplimiento a dichas disposiciones. Superintendencia de Banca, Seguros y AFP (SBS) 2017. Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos. Cumplimiento Normativo.

Las empresas supervisadas por la SBS deben establecer la manera más oportuna y eficiente de realizar la aplicación de cumplimiento normativo en función a las necesidades de su compañía, consiguiendo que dicha aplicación contemple los medios necesarios para desarrollar una exitosa gestión. Esto no obliga a las empresas a formar un área únicamente para realizar dichas funciones, pero sí requiere la existencia y la asignación de un Oficial de Cumplimiento Normativo (OCN), el cual deberá ser aprobado por el directorio de la compañía, contando con un rango gerencial. El OCN dependerá del directorio para la toma de decisiones y le reportará de manera directa. (SBS, 2017).

2.1.3.2 Control interno. El Marco Integrado de Control Interno se desarrolló en 1992, convirtiéndose en un marco líder desde la planeación hasta su implementación. Sin embargo, como resultado de los cambios que fueron sufriendo las distintas industrias, en mayo de 2013, se presenta una versión actualizada la cual tenía como objetivo principal que las compañías implementen y conversen de forma efectiva y eficiente los mecanismos de control interno que les permita realizar aportes en el proceso de implementación al cumplimiento de los principios de la compañía, los cambios constantes, la reducción de los riesgos a un grado aceptable, y base para la toma de decisiones y un buen gobierno corporativo. COSO. (2013). Control Interno – Marco Integrado. Resumen Ejecutivo.

Figura 5
Coso 1992 vs 2013



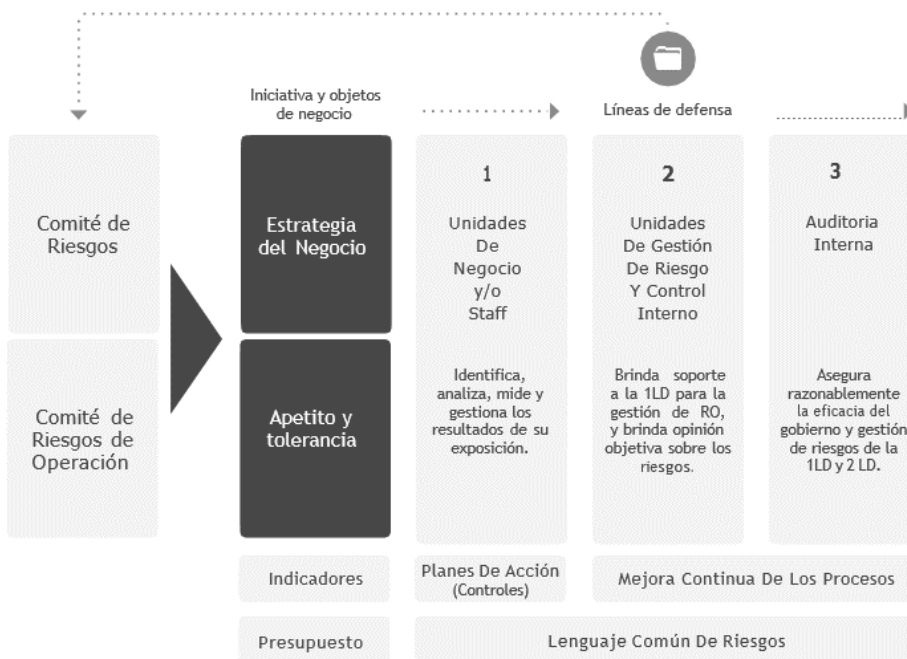
Nota. Galaz, Yamasaki, & Ruiz Urquiza (2015).

Este diseño presentado por COSO se ha establecido para asegurar y enfocar el avance del control interno y del gobierno corporativo, así como para mejorar el control de los recursos públicos o privados en cualquier tipo de empresa respondiendo a la presión pública, como resultado de los distintos problemas financieros e ilegales presentados. Un sistema efectivo de control interno es planteado con la finalidad de suministrar un nivel de seguridad razonable en relación con la eficacia y la eficiencia de las operaciones, requiere principalmente la toma de decisiones, la confiabilidad de la información financiera, y el cumplimiento de las regulaciones aplicables. Este diseño ha sido ideado para que pueda ser implementado en distintas empresas y sus respectivas áreas, está compuesto por 5 componentes, los cuales están relacionados y permiten tener un conocimiento del control, valoración del riesgo, sistemas de información y comunicación, y una adecuada supervisión del sistema implementado. COSO. (2013).

Las líneas de defensa están diseñadas para ser flexibles, donde cada compañía tiene la posibilidad de adecuar el modelo más adecuado para su sector financiero, volumen, operaciones y enfoque hacia la gestión de riesgos.

Figura 6

Funciones y línea de defensa para la evaluación del riesgo de operación



Nota. Maximizing value from your lines of defense – Ernst & Young (s.f.)

Las actividades de control se ven reflejadas a través de los procedimientos y políticas internas que buscan asegurar que se implementen todas aquellas acciones que permitan mitigar los potenciales riesgos en la compañía. Parte de los beneficios de implementar actividades de control es la adecuación y cumplimiento con los principios 10, 11 y 12 del Marco Integrado de Control Interno COSO (2013):

- Principio 10: busca que la compañía diseñe e implemente acciones de control que permitan mitigar los riesgos hasta lograr la consecución de las metas.
- Principio 11: busca que la compañía diseñe e implemente acciones de control a nivel de entidad respecto al desarrollo tecnológico para conseguir los objetivos.
- Principio 12: la empresa despliega las políticas que contienen los procedimientos y las actividades de control para lograr estas.

2.1.3.3 Riesgo. Son los posibles escenarios y eventos asociados, estos pueden ser internos y externos, que pueden ocasionar acciones negativas que atenten contra los objetivos y/o metas planificadas por la empresa, pudiendo ocasionar pérdidas económicas.

Como se puede visualizar en la figura 7, un riesgo se identifica con la selección de su origen, el evento y su consecuencia, como se describe a continuación:

- Origen:** es un grupo de factores que dan origen al riesgo operacional y es la causa o razón que podría originar que la acción (riesgo identificado) se materialice ocasionando pérdidas financieras para la compañía.

- b) **Evento:** es un grupo de sucesos que ocurren durante el mismo periodo de tiempo, originados por la misma causa. Estos pueden ser internos o externos a la Compañía.
- c) **Consecuencia:** es la posibilidad de pérdida o materialización del evento, pudiendo producir un impacto financiero, por riesgo operativo y/o legal.

Figura 7

Método para la identificación de un riesgo



Nota. Manual de riesgos de Operación del Banco XYZ

2.1.3.4 Medición de los riesgos. Rodríguez, Piñeiro y de Llano (2013) en la medición de los riesgos considera dos factores: (a) impacto, y (b) tasa de ocurrencia. Ambos dan como resultado la criticidad del riesgo.

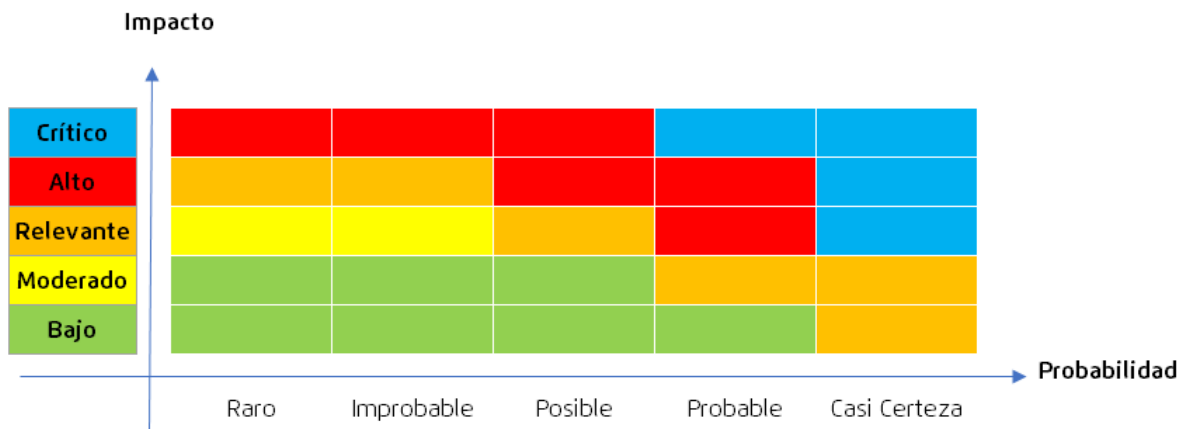
- a) **Impacto:** es el importe estimado de pérdida económica al materializarse el riesgo. Se puede medir a través de la revisión de la historia de eventos o incidentes que estén relacionados con el riesgo identificado para determinar el impacto materializado del evento o nivel de exposición asumido en el incidente. También se puede medir a través del juicio experto, se debe consultar el importe mínimo y máximo de impacto de materializarse el riesgo. La determinación del impacto legal o regulatorio también es considerada un método donde se debe determinar si existe la posibilidad de que la compañía tenga pérdidas económicas como resultado del deficiente desarrollo en acuerdos contractuales, incumplimiento no intencional de las normas, factores externos, tales como cambios regulatorios, entre otros. Una vez determinado el impacto económico estimado de pérdida, se deberá ubicar el impacto dentro del rango que corresponda en la escala de impactos de evaluación.
- b) **Tasa de ocurrencia:** es el número estimado de veces que un riesgo puede materializarse en un año. Se puede medir a través de la revisión de la historia de eventos que estén relacionados con el riesgo identificado para determinar la frecuencia con que ocurren dichos eventos. El juicio experto, es otro método de medición, se debe consultar al experto

las veces que, de acuerdo con su experiencia, se materializan los riesgos a través de eventos de pérdida y/o incidentes y así poder determinar la frecuencia estimada.

La criticidad es la multiplicación de los valores de impacto y de la tasa de ocurrencia da por resultado el nivel o grado de criticidad del riesgo, conocido como riesgo residual. Los valores resultantes son: bajo, moderado, relevante, alto o crítico. Esta medición puede esquematizar en un mapa semántico como se puede observar en la figura 8, construido con la combinación de un gráfico basado en el valor del impacto de cada riesgo por el número de veces al que la compañía está expuesta a que suceda el riesgo. Neil (2012).

Figura 8

Mapa semántico de probabilidad / impacto



Nota. Elaboración propia con información extraída de Neil (2012), Mapa de Riesgos.

2.1.3.5 Evaluación. El directorio de la empresa supervisada tiene el deber de aprobar las políticas y procedimientos internos, los cuales deben contener como mínimo los principales procesos que permitirán identificar, prevenir y/o mitigar algún potencial riesgo de incumplimiento normativo en todos los rangos de la empresa. Asimismo, serán los responsables de aprobar el programa anual de cumplimiento antes del 31 de diciembre de cada año. Dicho programa tiene el deber de contemplar dentro de sus funciones las actividades relacionadas a lo siguiente: a) elaborar informes que contengan la autoevaluación del correcto cumplimiento de las regulaciones externas, así como de las normas internas relacionadas a aquellas que tienen impacto directo en la empresa, conforme al procedimiento establecido por ella. b) considerar el inicio y término de las actividades programadas, así como el involucramiento de las áreas relacionadas y los entregables por cada actividad propuesta. (SBS, 2017).

2.2 Descripción de las acciones, metodologías y procedimientos

2.2.1 Mapeo regulatorio, priorización y evaluación

Consistió en identificar las obligaciones normativas que impactan a la empresa de estudio permitiendo elaborar una matriz de impacto. En esta etapa del procedimiento, con el fin de obtener

el score inicial de la regulación y/o proceso, se evaluó la criticidad de las regulaciones de acuerdo con la exposición en la empresa de estudio aplicando el *Compliance Risk Assessment* (CRA).

El desarrollo de la matriz de impacto consistió en la identificación de riesgos (posibles eventos y escenarios asociados a los riesgos internos y externos de la empresa de estudio), determinación del impacto legal o regulatorio (posibilidad de ocurrencia de pérdidas financieras para la empresa de estudio) y determinación de la tasa de ocurrencia (número de veces que el riesgo puede materializarse en un año.)

Dicha matriz de impacto permitió elaborar la propuesta y el cronograma de trabajo del periodo 2020 que fue aprobado por el OCN. La propuesta indicada fue elaborada a través de la priorización de las regulaciones y/o procesos, que consistió en la selección de normas que serían evaluadas para la identificación de riesgos de cumplimiento, considerando, ordenar de mayor a menor score y seleccionar las normas con score igual a: relevante, alto o crítico.

Las evaluaciones desarrolladas permitieron identificar las obligaciones normativas de cumplimiento y el impacto que afecta directamente a las operaciones del negocio, productos y/o servicios de la empresa de estudio. Además, se identificaron los riesgos de cumplimiento normativo, la gravedad de sus consecuencias, la probabilidad de que el incumplimiento se materialice y los controles existentes para mitigarlos. Con la finalidad de vigilar y asegurar el rendimiento óptimo de cumplimiento, se realizó un seguimiento continuo y oportuno a fin de asegurar el cierre del riesgo identificado.

2.2.2 Metodología del estudio

La metodología empleada para el desarrollo del presente trabajo de suficiencia profesional ha sido de tipo descriptiva, que está orientada en la recopilación de información que faculta revisar las obligaciones normativas de la regulación, la misma que puede tener un alcance transversal a diferentes procesos de la empresa de estudio, y los procedimientos de verificación del debido cumplimiento de la norma priorizada, según el alcance establecido.

También se ha desarrollado una metodología cualitativa, teniendo como objeto la descripción de los lineamientos y metodologías que han permitido prevenir, identificar y mitigar los posibles incumplimientos normativos.

La entrevista y la encuesta de satisfacción fueron consideradas para la elaboración del presente trabajo de suficiencia profesional, aplicadas al Oficial de Cumplimiento Normativo, Gerente de Control de Cumplimiento y Sub Gerente de Supervisión de Cumplimiento, permitiendo identificar las deficiencias de la empresa de estudio, principalmente en las políticas internas y procedimientos que tienen la finalidad de asegurar el cumplimiento continuo a las regulaciones internas y externas que afectan a esta.

2.2.3 Entrevista de investigación

La entrevista contribuyó para el desarrollo de este estudio, permitiendo la recopilación de información fundamental. Se realizaron entrevistas al Oficial de Cumplimiento Normativo, Gerente de Control de Cumplimiento y Sub Gerente de Supervisión de Cumplimiento de la empresa de estudio, con la finalidad de entender y conocer a detalle los mecanismos, funciones y procedimientos que se ejecutan. Se desarrolló un modelo de entrevista libre, logrando obtener respuestas con más información que permitieron identificar y valorar las deficiencias del procedimiento de evaluación de regulaciones internas y externas de la empresa de estudio.



Capítulo 3 Aporte y desarrollo de experiencias

2.1 Aportes

Para lograr la aplicación del *Compliance Risk Assessment* (CRA) con el fin de identificar y/o mitigar riesgos de cumplimiento normativo y reputacionales al que potencialmente se expone la empresa de estudio, para lo cual se realizaron los siguientes aportes:

2.1.1 Mapeo regulatorio

Considerando los resultados de la metodología de investigación del presente trabajo, se elaboró el mapeo regulatorio, en esta etapa del procedimiento, se registraron en el inventario de regulaciones, a todas aquellas normas que impactan a la empresa de estudio emitidas por parte del regulador con 2 años de antigüedad, debido a que las regulaciones emitidas en el año corriente cuentan con un tratamiento diferente.

2.1.2 Desarrollo de la matriz impacto

Para la elaboración y desarrollo de la matriz de impacto, se procedió con la identificación de riesgos (internos y externos) y el origen que causa cada uno de ellos para considerar los factores que pueden materializar las pérdidas financieras para la empresa de estudio. Como se puede visualizar en la tabla 1, los riesgos fueron clasificados según el tipo de origen.

Tabla 1

Tipos de origen de riesgo

Tipo de origen de riesgo	Descripción
Personas	Las personas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, fraude, corrupción, apropiación de información sensible, entre otros.
Procesos internos	La empresa debe gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.
Tecnología de información	La empresa debe gestionar los riesgos asociados a la tecnología de información, relacionados a falta de confidencialidad, falta de integridad, entre otros.
Eventos externos	La empresa debe gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a cambios regulatorios, conducta indebida con terceros, problemas políticos o de gobierno.
Relaciones con terceros	Asociados por la interacción con personas ajenas a la institución: funcionarios públicos, proveedores, clientes, contrapartes, entre otros.

Nota. Manual de Gestión de Riesgos Operativos del Banco XYZ

Para la evaluación de las regulaciones se establecieron los criterios para el cálculo de la probabilidad, el cual se determinó en función de 4 factores a los que se les asignó un valor. Estos valores se promedian y el resultado se traduce en las categorías de la tabla 2. Asimismo, se

establecieron los criterios para el cálculo del impacto, el cual se determinó en función de 5 factores a los que se les asignó un valor como se observa en la tabla 2.

Tabla 2

Criterios para el cálculo de probabilidad e impacto

<p>CÁLCULO DE PROBABILIDAD: Se determina en función de los 4 <u>Criterios de Probabilidad</u> (Frecuencia, Conocimiento, Antecedentes y Exposición) a los que se les asigna un valor, estos valores se <u>promedian</u> y el resultado se traduce en las siguientes categorías de medición de probabilidad</p>		<p>CÁLCULO DE IMPACTO: Se determina en función de los 5 <u>Criterios de Impacto</u> (Sanción, Confianza, Reputación, Importancia para la autoridad y Beneficio) a los que se les asigna un valor, estos valores se <u>promedian</u> el resultado se traduce en las siguientes categorías de medición de impacto.</p>	
CASI CIERTA	4,0 - 5,0	BAJO	0 - 0,9
PROBABLE	3,0 - 3,9	MODERADO	1,0 - 1,9
POSIBLE	2,0 - 2,9	RELEVANTE	2,0 - 2,9
IMPROBABLE	1,0 - 1,9	ALTO	3,0 - 3,9
RARO	0 - 0,9	CRÍTICO	4,0 - 5,0

Nota. Procedimiento de Normas Existentes del Banco XYZ

Adicionalmente, se determinó la valoración del control relacionado a cada regulación a través de los procedimientos y políticas internas que conllevan a avalar que se lleven a cabo los procedimientos para mitigar los riesgos con mayor impacto.

Tabla 3

Valoración de nivel de control

Control	Concepto	Valor
Deficiente	No hay controles	1
Regular	Controles no documentados	2
Más que regular	Controles parcialmente documentados	3
Bueno	Controles documentados	4
Óptimo	Controles probados	5

Nota. Procedimiento de Normas Existentes del Banco XYZ

Finalmente, se determinó el cálculo del riesgo residual, el cual se obtuvo de la multiplicación de los valores de impacto y probabilidad menos el nivel de controles actuales dando por resultado el grado de criticidad del riesgo, conocido como riesgo residual. Los valores resultantes fueron: bajo, moderado, relevante, alto o crítico.

Tabla 4*Cálculo del riesgo residual*

CÁLCULO DEL RIESGO RESIDUAL	VALOR	RIESGO RESIDUAL
CÁLCULO DEL RIESGO RESIDUAL	8,0 - 25,0	CRÍTICO
	6,0 - 7,99	ALTO
	4,0 - 5,99	RELEVANTE
	0,2 - 3,99	MODERADO
	0,2 - 1,99	BAJO

Nota. Procedimiento de Normas Existentes del Banco XYZ

2.1.3 Evaluación

En lo que respecta a las evaluaciones, se formalizaron los procedimientos internos los cuales contienen como mínimo los principales procesos que permiten identificar, prevenir y/o mitigar algún potencial riesgo de incumplimiento normativo en todos los rangos de la empresa teniendo en cuenta lo solicitado por la SBS. Asimismo, con el fin de contar con las evidencias de dichas evaluaciones se acordó elaborar un informe como entregable de la evaluación realizada, asegurando el correcto cumplimiento de las regulaciones externas, así como de las normas internas relacionadas a aquellas que tienen impacto directo en el proceso evaluado.

Asimismo, teniendo en cuenta las necesidades del OCN de realizar más evaluaciones en el periodo, se elaboró y desarrolló una propuesta con un procedimiento de evaluación alternativo fomentando la evaluación descentralizada, donde los dueños del proceso a través de la metodología brindada logren identificarse con el riesgo al que están expuestos frente a un marco regulatorio asociado a su proceso.

Con relación al párrafo anterior, se logró demostrar que el nuevo procedimiento permite una reducción del 50% de horas incurridas en el desarrollo de la evaluación de la regulación frente al procedimiento tradicional. Adicionalmente, a través de una encuesta de satisfacción a los dueños del proceso del marco regulatorio evaluado se pudo concluir que este procedimiento es más flexible y permite un mayor involucramiento y participación de estos.

2.2 Desarrollo de experiencias

El autor del presente trabajo, a través de su experiencia profesional, ha logrado desarrollar los aportes descritos en párrafos anteriores, los cuales han sido reconocidos por el Oficial de Cumplimiento Normativo, Gerente de Control de Cumplimiento y Sub Gerente de Supervisión de Cumplimiento, quienes son sus supervisores directos permitiéndole asumir nuevos retos dentro de la empresa de estudio.

Las enseñanzas y experiencias adquiridas a lo largo de la vida universitaria y profesional del autor han tenido una gran contribución para el desarrollo del presente trabajo. Asimismo, con la finalidad de afianzar sus conocimientos, implementar mejoras en los procesos y mitigando riesgos regulatorios y reputacionales ha continuado ampliando sus conocimientos en compliance, control interno y control de gestión.



Conclusiones

Se logró demostrar que la aplicación del *Compliance Risk Assessment* (CRA) permite un adecuado sistema de control interno y de gestión de riesgos, permitiendo contar con controles efectivos, los cuales han sido diseñados para el cumplimiento del Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos (Resolución SBS N°272-2017).

Esta aplicación supone nuevos esfuerzos en las entidades supervisadas por la SBS, tanto por la implementación de nuevos procedimientos como en el número de evaluaciones de regulaciones, debido a que en distintas situaciones las herramientas utilizadas presentan debilidades que no comprometen el ambiente de control y que deben ser corregidas y/o reforzadas.

En particular, el CRA aplicado en la empresa de estudio nos ha permitido verificar que se han implementado procedimientos adecuados que permiten asegurar la correcta verificación del debido cumplimiento de la norma evaluada, según el alcance establecido. Esta implica una revisión de las obligaciones normativas de la norma, la misma que puede tener un alcance transversal a diferentes procesos de la empresa.





Recomendaciones

Establecer una frecuencia de revisión a la matriz de regulaciones con el objetivo de reevaluar todos los criterios de selección: impacto, frecuencia y evaluación del control. Ello permitirá garantizar una adecuada selección de las normas a evaluar.

Evaluar si los criterios incluidos en el cálculo del impacto y la frecuencia de los riesgos preliminares, que son seleccionados a juicio del analista deben tener el mismo peso que aquellos criterios seleccionados en base a información disponible después de la evaluación.

Considerar dentro de la matriz de regulaciones los resultados de las normas evaluadas para llevar un control de estas, lo cual permitirá garantizar una adecuada selección de las normas a evaluar.

Capacitar a los colaboradores que forman parte del Área de Gestión de Cumplimiento con la nueva metodología, con la finalidad de lograr una correcta aplicación del *Compliance Risk Assessment* (CRA) y se pueda replicar en las empresas del mismo grupo de la empresa de estudio.





Lista de referencias

- Cárdenas-Cuba, J. M. (2019). El compliance o debida diligencia entendidas como la satisfacción del criterio de idoneidad como requisito adicional para la deducción de los atributos fiscales de costo y/o gasto en la determinación del impuesto a la renta. [tesis de maestría, Universidad de Lima]. Repositorio Institucional ULima. https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/10648/Cardenas_Cuba_Juan_Manuel.pdf?sequence=1&isAllowed=y
- COSO (2013). Control Interno – Marco Integrado. Resumen Ejecutivo. https://auditoresinternos.es/uploads/media_items/coso-resumen-ejecutivo.original.pdf
- Ernst and Young (2013). Maximizing value from your lines of defense – Ernst & Young. <https://www.iia.nl/SiteFiles/EY-Maximizing-value-from-your-lines-of-defense.pdf>
- Galaz, Yamasaki, & Ruiz Urquiza, S. (2015). Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno. <https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf>
- ISO 37001 (2016). Sistemas de gestión antisoborno. <https://www.iso.org/obp/ui#iso:std:iso:37001:ed-1:v1:es>
- Nancy Yong. (2021). ¿Qué entendemos por Compliance? 13/05/2021, de Gestión. <https://gestion.pe/blog/brujula-de-gestion-empresarial/2021/05/que-entendemos-por-compliance.html/?ref=gesr>
- Neil, M. (2012): Using “Risk Maps” to visually model & communicate risk. www.agenarisk.com
- Proética. (s.f.) Perú mejora dos puntos en evaluación mundial sobre percepción de la corrupción de transparencia internacional. <https://www.proetica.org.pe/contenido/peru-mejora-dos-puntos-en-evaluacion-mundial-sobre-percepcion-de-la-corrupcion-de-transparencia-internacional/>
- Proética. (s.f.) La tolerancia a la corrupción, grande y pequeña, se mantiene extendida según la última encuesta nacional sobre corrupción de Proética. <https://www.proetica.org.pe/contenido/xi-encuesta-nacional-sobre-percepciones-de-la-corrupcion-en-el-peru-2019/>
- Rodríguez, Piñeiro y de Llano (2013). Mapa de Riesgos Identificación y Gestión de Riesgos. <https://dialnet.unirioja.es/servlet/articulo?codigo=4744304>
- Sanclémente-Arciniegas, J. (2020). Compliance, empresas y corrupción: una mirada internacional. Derecho PUCP, (85), 9-40. <https://doi.org/10.18800/derechopucp.202002.001>
- Superintendencia de Banca, Seguros y AFP (SBS) (2017). Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos. Cumplimiento Normativo. https://www.sbs.gob.pe/Portals/0/jer/Auto_Nuevas_Empresas/Normas_Comunes/5.%20Reg.%20de%20Gobierno%20Corporativo_Res.%20SBS%20N%C2%B0%20272-2017.pdf

Talavera Díaz, R. M. (2020). Necesidad de implementar programas de cumplimiento normativo en empresas públicas del sector financiero frente a actos de corrupción. Análisis en el marco de la ley N° 30424. [tesis de maestría, Pontificia Universidad Católica Del Perú]. Repositorio Institucional de la PUCP. [http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/16154/TALAVERA_D%
c3%8dAZ_NECESIDAD_DE_IMPLMENTAR_PROGRAMAS_DE_CUMPLIMIENTO_NORMATIVO_
EN_EMPRESAS_PUBLICAS.pdf?sequence=1&isAllowed=y](http://tesis.pucp.edu.pe/repositorio/bitstream/handle/20.500.12404/16154/TALAVERA_D%c3%8dAZ_NECESIDAD_DE_IMPLMENTAR_PROGRAMAS_DE_CUMPLIMIENTO_NORMATIVO_EN_EMPRESAS_PUBLICAS.pdf?sequence=1&isAllowed=y)

