"PLAN DE AUDITORÍA INTERNA A SER PRESENTADO ANTE LA SBS PARA SU AUTORIZACIÓN"

Trabajo de Investigación presentado
para optar al Grado Académico de
Magíster en Auditoría

Presentado por:

Sra. Ana Pachamango Rodríguez
Sra. Roxana Pacheco Rojas
Sr. Giomar Ruiz Tinco

Asesor: Profesor Jorge Maldonado Alarcón

2018

A mi esposo e hija, por su apoyo incondicional y por ser los motores de mi vida. A mis padres, por ser fuente de inspiración y motivación para superarme cada día más.

Ana Pachamango Rodríguez

A Dios, por guiarme y fortalecerme en cada paso que doy. A mi hija, por ser fuente de mi inspiración, crecimiento y amor. A mis padres y hermanos, por su apoyo incondicional y por ser ejemplo de integridad y perseverancia.

Roxana Pacheco Rojas

A Gaby, Antonio, Piero, Xiomy, María y Adrián, quienes son el soporte de mi crecimiento profesional y personal. Gracias por todo su apoyo, confianza, paciencia, consejos y amor hacia mí.

Giomar Ruiz Tinco

Resumen ejecutivo

El presente trabajo de investigación nació del análisis que realizamos para identificar los principales problemas que afronta una institución financiera (IF) para alinear a los objetivos estratégicos establecidos por el negocio con las actividades de auditoría especificadas en su plan anual. En la actualidad, el plan de auditoría interna de la IFes efectuado teniendo en cuenta los requerimientos regulatorios, dejando de lado la revisión de procesos clave del negocio, debido a la gran cantidad de actividades requeridas por la Superintendencia de Banca, Seguros y AFP (SBS).

A lo descrito anteriormente, se suma que las áreas de control interno en las distintas líneas de defensa generan duplicidad de revisiones de ciertos procesos. Por ello, es necesario priorizar las actividades de auditoría interna en función de los riesgos más significativos que presenta la IF, de acuerdo con la estrategia planteada para cumplir sus objetivos. En consecuencia, decidimos realizar una investigación cualitativa orientada a elaborar y documentar una propuesta de plan de auditoría interna, basada en riesgos para lograr la autorización de la SBS para la IF. La institución elegida es un banco que pertenece a un grupo español, y se encuentra facultado para captar y colocar recursos financieros y efectuar todo tipo de servicios bancarios y operaciones permitidas a la banca múltiple.

Nuestra investigación nos llevó a definir una metodología de auditoría basada en riesgos, para lo cual tuvimos que recorrer todos los procesos de la compañía, definiendo de esta manera nuestro universo auditable, para posteriormente evaluar el riesgo inherente a cada proceso, y establecer una matriz de priorización que considera la alineación de cada proceso con los objetivos estratégicos, las expectativas de la alta gerencia, la puntuación de rotación y los hallazgos significativos.

Es importante mencionar que para el desarrollo del trabajo hemos incluido el uso de un mapa de aseguramiento, para evidenciar los procesos que cuentan con un nivel de cobertura de riesgo alto por parte de otras áreas de aseguramiento, y la revisión por parte de auditoría puede implicar un reproceso y sobrecosto para la institución financiera.

Otro aspecto importante a mencionar es que para el presente trabajo se ha tomado en cuenta los recursos con los que cuenta el área de auditoría de la IF para realizar las evaluación que han sido priorizadas en la matriz mencionada anteriormente, estableciendo un cronograma de actividades como parte del plan anual de auditoría.

Las entrevistas realizadas y el análisis de las experiencias de otras instituciones financieras que cuentan con la autorización de la SBS confirman que si la IF toma en consideración la propuesta descrita en nuestra investigación, logrará contar con la autorización del ente regulador y podrá evidenciar que los riesgos estratégicos del negocio están siendo cubiertospor las evaluaciones del plan anual de auditoría interna.

Índice

Dedicatoria……..ii

Resumen ejecutivo…….…….iii

Índice de tablas……..vii

Índice de gráficos……..viii

Índice de anexos…….……ix

Introducción 1

Capítulo I. Planteamiento del problema 3

1. Antecedentes 3
2. Planteamiento del problema 4
3. Preguntas de investigación 4
4. Objetivos 5
4.1. Objetivo general 5
4.2. Objetivos específicos 5
5. Justificación 5
6. Limitaciones 5
7. Delimitaciones 6

CapítuloII. Marco teórico 7

1. Sistema financiero peruano, regulación y supervisión 7
1.1. Reglamento de auditoría interna 7
1.2. Gobierno corporativo y gestión integral de riesgos 8
2. Marco internacional para la práctica profesional 10
3. Banco Altas Cumbres 15
3.1 Descripción de la empresa 15
3.2 Grado de cumplimiento de las normas para el ejercicio profesional de la auditoría interna. 15
3.3 Nivel de coordinación de la unidad de auditoría interna con otros proveedores de aseguramiento 16
3.4 Objetivos estratégicos de la empresa 17
3.5 Cadena de valor y mapa de procesos 17
3.6 Proceso de gestión integral de riesgos 19

Capítulo III. Metodología para la elaboración de un plan de auditoría basada en riesgos 20

1. Metodología 20

1.1 Establecer el universo de auditoría 20

1.2 Evaluar el riesgo inherente en las entidades auditables 26

1.3 Identificar las unidades auditables vinculadas con elcumplimiento de los objetivos estratégicos..... 33

1.4 Ponderar las expectativas de la alta dirección..... 34

1.5 Elaboración del mapa de aseguramiento de la IF..... 44

1.6 Determinar los recursos..... 44

1.7 Elaboración del plan anual de auditoría 45

Capítulo IV. Análisis de resultados y hallazgos..... 48

1. Autorización asociada al plan 48

Conclusiones y recomendaciones 50

1. Conclusiones 50

2. Recomendaciones..... 51

Bibliografía 52

Anexos 53

Nota biográfica 67

Índice de tablas

Tabla 1. Tipos de riesgos…….…….....9

Tabla 2. Inventario de procesos …….……..…..21

Tabla 3. Inventario de sistemas ……..…….……...23

Tabla 4. Inventario de productos, servicios y canales…….……...……23

Tabla 5. Objetivos del plan estratégico……..…….…...24

Tabla 6. Requerimiento regulatorio…..…….....25

Tabla 7. Requerimiento alta dirección……...……26

Tabla 8. Factores de riesgo inherente……...…….....27

Tabla 9. Probabilidad de ocurrencia ..……...…….29

Tabla 10. Magnitud de impacto..……...……...……....30

Tabla 11. Cálculo del apetito y tolerancia……31

Tabla 12. Ponderación del riesgo inherente…….33

Tabla 13. Factores de control…….....33

Tabla 14. Vinculación a los objetivos ……...……..34

Tabla 15. Puntuación procesos críticos……....34

Tabla 16. Puntuación expectativas de la alta gerencia…….....34

Tabla 17. Puntuación según el tipo de hallazgo ……...…….....35

Tabla 18. Nivel de riesgo……..35

Tabla 19. Matriz universo de auditoria…….36

Tabla 20. Recursos……...……44

Tabla 21. Cálculos horas/hombre……...……..45

Índice de gráficos

Gráfico 1. Marco internacional para la práctica profesional……..……..……..…..….10

Gráfico 2. Marco Integral de aseguramiento y gestión de riesgos…...…..……..…...……....14

Gráfico 3. Cadena de valor ……....……18

Gráfico 4. Mapa de procesos…….…….…….....18

Gráfico 5. Líneas de defensa……..……...……...19

Gráfico 6. Metodología de PABR…….....…….20

Gráfico 7. Probabilidad por impacto ……..…...…….28

Gráfico 8. Rangos de criticidad……...…….....……..32

Gráfico 9. Actividades del plan anual de auditoria…...……...……..…...……..46

Índice de anexos

Anexo 1. Organigrama de auditoría interna del Banco Alta Cumbres…….…….……54

Anexo 2. Autoevaluación efectuada por la unidad de auditoría interna en el 2017……..….55

Anexo 3. Ponderación del riesgo inherente para el proceso de gestión de cumplimiento PLAFT…….…….……57

Anexo 4. Mapa de aseguramiento del Banco Altas Cumbres……..…… 61

Anexo 5. Puntuación de requerimientos regulatorios…….…….. 63

Anexo 6. Entrevista a expertos de auditoría interna……..64

Anexo 7. Reseña de los expertos entrevistados ……65

Anexo 8. Texto único de procedimientos administrativos……... 66

Introducción

«La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de la organización, al ayudarla a cumplir sus objetivos, aplicando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno»(IAI, 2017). En esa línea, una auditoría basada en riesgos (ABR) brindaría a accionistas, directores,gerencia general y otras partes interesadas, seguridad de que los procesos de gestión de riesgos se administran de manera efectiva conrelación al apetito de riesgo definido por la institución y, lo que no es menor, ganaría su confianza.

No son muchas las empresas del sistema financiero peruano que cuentan con la autorización de su plan de auditoría basada en riesgos (PABR) por parte de la Superintendencia de Banca, Seguros y AFP (SBS) o que cumplan con las normas internacionales para el ejercicio profesional de la auditoría interna del Instituto de Auditores Internos (IAI) para poder realizar esta gestión. Esto se debe a diferentes factores atribuibles, principalmente, a la carencia de recursos y, en menor medida, a la documentación exigida para iniciar el trámite.

En tal sentido, el presente trabajo de investigación tiene como propósito la elaboración y la documentación de la metodología del PABR para el Banco Altas Cumbres, a fin de gestionar y obtener la autorizaciónde la SBS.

El Capítulo I presenta la definición de ABR y las ventajas para las empresas de contar con una gestión de este tipo, el marco internacional para la práctica profesional de la auditoría interna del IAI y el marco regulatorio en el Perú definido por la SBS, con base en las mejores prácticas internacionales. Así mismo, en este trabajo de investigación se plantea la problemática que se busca solucionar, el objetivo principal y los objetivos específicos, la justificación, las limitaciones y las delimitaciones del mismo.

El Capítulo II describe el sistema financiero peruano y la regulación relevante emitida por la SBS relacionada con el tema de investigación, así como el marco internacional para la práctica profesional del IAI, incluyendo las guías obligatorias y las recomendadas, que servirán para desarrollar la metodología propuesta. También comprende la descripción del Banco Altas Cumbres, banco de tamaño mediano dentro del sistema financiero peruano, que tiene como principales objetivos apoyar el emprendimiento y fomentar el ahorro, principalmente en aquellos

sectores de la población descuidados por los bancos grandes, que son los quemueven la economía peruana. Asimismo, se describe la situación actual de la gestión de auditoría interna, cuyo enfoque está basado en el cumplimiento regulatorio.

En el Capítulo III se desarrolla la metodología del PABR, la cual se basa en los siete pasos siguientes: establecer el universo de auditoría, evaluar el riesgo inherente, vincular objetivos estratégicos, establecer evaluaciones, determinar recursos y obtener la aprobación del plan, el que se aplica bajo un enfoque estratégico acorde con el *core* de negocio del Banco Altas Cumbres, que va de la mano también con la auditoría del sistema de prevención del lavado de activos y del financiamiento al terrorismo, a fin de mostrar su despliegue en una actividad relevante, tanto para fines de riesgo como para el cumplimiento regulatorio. A su vez, se hace referencia a una autoevaluación realizada por el auditor interno sobre elgrado de cumplimiento de las normas internacionales para el ejercicio de la auditoría interna, según el IAI, asumiendo que ya cuenta un PABR, conbase en la metodología propuesta.

El Capítulo IV contiene el análisis de resultados y hallazgos, así como los pasos a seguir para tramitar la autorización del PABR del Banco Altas Cumbres ante la SBS.Finalmente, presentamos nuestras conclusiones y recomendaciones.

Capítulo I. Planteamiento del problema

1. Antecedentes

La auditoría basada en riesgos (ABR) es una metodología que se utiliza para dar aseguramiento independiente respecto deque los riesgos de una empresa se gestionan con base en el apetito al riesgo establecido como aceptable por el directorio.

En tal sentido, de acuerdo con el marco internacional para la práctica profesional de la auditoría interna emitido por el Instituto de Auditores Internos (IAI), el director ejecutivo de auditoría debe establecer un plan basado en los riesgos (PABR), a fin de determinar las prioridades de la actividad de auditoría interna, consistente con los objetivos clave de la empresa. El IAI es una organización fundada en 1941 en los Estados Unidos, que constituye la principal asociación profesional de magnitud internacional y detenta el liderazgo mundial en investigación, educación, guía tecnológica y certificación de auditores internos.

Las empresas del sistema financiero, en nuestro país, son reguladas y supervisadas por la Superintendencia de Banca Seguros y AFP (SBS). La SBS establece en su Reglamento de Auditoría Interna, aprobado mediante Resolución SBS N°11699-2008, que como parte del plan anual, las empresas deberán programar las actividades previstas en dicha regulación.

Asimismo, recogiendo las normas internacionales para el ejercicio profesional de la auditoría interna del IAI, la SBS señala que aquellas empresas que cuenten con prácticas sólidas de auditoría interna y un adecuado cumplimiento delos criterios previstos en la regulación, podrán solicitarsu autorización para que, en la formulación de su plan anual, se consideren solo las actividades programadas que resulten relevantes, según la propia metodología de auditoría basada en riesgos implementada por la empresa. Las solicitudes de autorización a la SBS deberán incluir la descripción del enfoque de auditoría basada en riesgos y metodología asociada. Cabe señalar que a la fecha son pocas las empresas que cuentan con la autorización de su PABR por parte de la SBS.

La Institución Financiera (IF)de esta investigación, que denominaremos Banco Altas Cumbres o IF por motivos de confidencialidad, «está formada por capitales privados bajo la denominación de sociedad anónima, que inicia operaciones a fines del año 1990 con la autorización de la SBS, y tiene como giro de negocio la intermediación financiera» (Memoria Anual 2017). A setiembre del 2017, dos de las principales empresas clasificadoras de riesgo en el Perú asignaron al Banco Altas Cumbres la categoría de riesgo A+, la máxima calificaciónexistente, que ratifica la posición

del banco dentro del grupo de los cinco mayores bancos del país, por su volumen de créditos y depósitos. Así, el Banco Altas Cumbres asume, dentro de su estrategia, el desarrollo de productos y servicios diseñados para las necesidades de sus clientes e implementa los procedimientos y herramientas de forma permanente, «es decir se necesita reforzar la gestión de riesgos a los que se encuentra expuesta debido al rápido crecimiento y expectativas del mercado y replantear la función de auditoría interna» (Memoria Anual 2017).

El presente trabajo de investigación tiene como objetivo elaborar y documentar un PABR para el Banco Altas Cumbres y cumplir con los requerimientos exigidos por el ente regulador, para poder desarrollar sus actividades de acuerdo conlos riesgos de la institución y su estrategia.

2. Planteamiento del problema

En la actualidad, el plan de auditoría interna del BancoAltas Cumbreses efectuado bajo un enfoque regulatorio, orientado en un bajo alcance a la revisión de los procesos clave del negocio, debido a la gran cantidad de actividades requeridas por la SBS.

Esta situación, genera que varios de los procesos asociados a la estrategia del negocio no estén siendo incluidos dentro de las actividades de evaluación que realiza el área de auditoría interna, debido a la sobrecarga de evaluaciones de cumplimento requeridas por la SBS para aquellas instituciones financieras que no cuentan con un PABR autorizado.

Otro punto importante se ve reflejado en la generación de sobrecostos, debido a la existencia de duplicidad de revisiones por parte de otras áreas de control.Por ello, es necesario priorizar las actividades de auditoría interna en función de los riesgos más significativos que presenta la IF, acorde con la estrategia de la misma, con la finalidad de cumplir sus objetivos. Lo indicado anteriormente genera que el Banco Altas Cumbres elabore un plan anual de auditoría basado en el cumplimiento de leyes y regulaciones, sin considerar los riesgos relevantes a su estrategia, por no contar con la autorización del ente regulador para desarrollar un PABR.

3. Preguntas de investigación

- ¿Cómo generará un plan de auditoría basado en riesgos (PABR) mayor valor para el directorio?
- ¿Cómo puede apoyar un mapa de aseguramiento al Banco Altas Cumbres en la gestión de riesgos y en la reducción de la duplicidad en la supervisión?

- ¿Cómo busca mitigar el Banco Altas Cumbres la exposición a los riesgos clave que podrían afectar el logro de sus objetivos?

4. Objetivos

4.1. Objetivo general

El propósito de este trabajo de investigación cualitativo es elaborar y documentar los requisitos para el diseño de un PABR, enfocado en los riesgos críticos del Banco Altas Cumbres, para obtener la autorización del ente regulador.

4.2. Objetivos específicos

- Evaluar oportunamente actividades alineadas con la estrategia de negocio, las cuales serán detalladas en el PABR.
- Desarrollar el mapa de aseguramiento para el Banco Altas Cumbres, identificando los riesgos significativos con cobertura de aseguramiento inadecuado o áreas con cobertura duplicada de aseguramiento.
- Preparar el PABR, utilizando el marco internacional para la práctica profesional de la auditoría interna, provista por el IAI.
- Elaborar la documentación y los protocolos básicos relacionados con eldesarrollo de un PABR para obtener la autorización de la SBS.

5. Justificación

- Actualmente el porcentaje de actividades de evaluación de cumplimiento del área de auditoría interna supera el 60%.
- Deben priorizarselas revisiones alineadas con la estrategia de la empresa (identificación de riesgos críticos).
- Hay que desarrollar una metodología de ABR alineada con la estrategia del Banco Altas Cumbres.
- Es necesario generar mayor valor al banco respecto delcumplimiento de objetivos estratégicos y no solo mitigar riesgos de sanción por parte del regulador.

6. Limitaciones

En este trabajo de investigación no vamos a utilizar el nombre real de la institución financiera y en su reemplazo se está utilizando el nombre Banco Altas Cumbres o las siglas IF. No se

presentaron limitaciones en las diversas actividades llevadas a cabo para el desarrollo del presente trabajo de investigación y se contó con la colaboración del personal y directivos de las diversas áreas del banco, así como con la opinión ylas sugerencias de funcionarios de otras entidades financieras.

7. Delimitaciones

De acuerdo con la norma 2010 Planificación del Marco Internacional para la Práctica de la Profesión de Auditoría Interna, para estructurar el universo auditable y priorizar riesgos se vincularán los riesgos críticos con objetivos específicos y procesos de negocio. Se tendrá en cuenta los riesgos internos y externos que afectan a los grupos de interés de la institución financiera.La propuesta del PABR se aplicará alineada a la estrategia de la empresa para los años 2014 – 2018.

CapítuloII. Marco teórico

1. Sistema financiero peruano, regulación y supervisión

El sistema financiero peruano es regulado y supervisado por la Superintendencia de Banca, Seguros y AFP (SBS). A través de su regulación, busca que las instituciones supervisadas tomen decisiones que les permita mantener su estabilidad y solvencia a largo plazo, y así preservar los intereses de los depositantes; por lo tanto, establece parámetros mínimos para que las empresas cuenten con sistemas que le permitan identificar, medir, controlar y monitorear sus riesgos de una manera eficiente.

Con relación a la supervisión, esta se realiza de manera directa o indirecta, apoyándose en colaboradores externos, entre los que se incluyen los auditores internos y externos, entre otros. Con base en ello, la SBS establece los requisitos y los estándares de auditoría interna y externa, en conformidad con el artículo 180° (Auditoría de las Empresas) de la Ley General del Sistema Financiero y de Seguros y Orgánica de la SBS, Ley N°26702, y modificatorias (Ley General), que establece los requisitos, los derechos, las obligaciones, las garantías, las restricciones y las demás condiciones de funcionamiento a las que se encuentran sujetas las personas jurídicas de derecho privado que operan en el sistema financiero y de seguro.

Para que las instituciones financieras cuenten con un sistema de evaluación y supervisión para la eficaz gestión de riesgos y de gobierno corporativo, la SBS dicta la normativa necesaria para su cumplimiento, entre las que se encuentran las disposiciones vigentes que señalamos a continuación, que son pertinentes al trabajo de investigación.

1.1. Reglamento de auditoría interna

«El reglamento de auditoría interna establecido por la Resolución SBS N°11699-2008, define que la auditoría basada en riesgos (ABR) consiste en un conjunto de procesos mediante los cuales la auditoría provee aseguramiento independiente al Directorio acerca de:

- Si los procesos y medidas de gestión del riesgo que se encuentran implementadas están funcionando de acuerdo a lo esperado;
- Si los procesos de gestión de riesgos son apropiados y están bien diseñados; y,
- Si las medidas de control de riesgos que la Gerencia ha implementado son adecuadas y efectivas, y reducen el riesgo al nivel de tolerancia aceptado por el Directorio.

Con relación a la ABR indica que depende del nivel de desarrollo que la propia empresa ha alcanzado en la gestión de riesgos, y el grado en que han sido definidos los objetivos por la Gerencia contra los cuales pueden medirse los riesgos asociados»(Resolución SBS N°11699-2008).

Cabe indicar que cuando la empresa cuenta con un sistema de gestión del riesgo adecuado en las áreas evaluadas, la ABR puede confiar en mayor grado en la evaluación del riesgo que la propia empresa ha realizado, y desarrollar un plan basado en riesgos (PABR) que complemente las acciones realizadas por la empresa y aumente el valor de las actividades de la auditoría interna. Cuando la empresa cuenta con un sistema de gestión del riesgo menos desarrollado, la ABR requiere descansar más en la evaluación del riesgo realizada por la propia auditoría interna.

1.2. Gobierno corporativo y gestión integral de riesgos

«El reglamento de gobierno corporativo y de la gestión integral de riesgos establecido por la Resolución SBS Nº272-2017, establece que la gestión integral de riesgos es un proceso efectuado por el directorio, la gerencia y el personal e incluye a la totalidad de la empresa, sus líneas de negocio, procesos y unidades organizativas, a través de todos sus riesgos relevantes, y este debe ser aplicado a toda la organización y a su estrategia, este proceso está diseñado para identificar potenciales eventos que pueden afectarla, gestionándolos de acuerdo a su apetito de riesgo y proveer una seguridad razonable en el logro de sus objetivos»(Resolución SBS Nº 272-2017).

El reglamento indica que las empresas deben diseñar y aplicar una gestión integral de riesgos, adecuada a su naturaleza, tamaño y a la complejidad de sus operaciones y servicios que brinda, así como al entorno que afecta a los mercados en los que opera. El ente regulador establece en dicho reglamento que las empresas bajo su supervisión deben contar con un marco de gestión de riesgos que se adapte a su organización y necesidades. Para ello, el regulador toma como referencia las prácticas internacionales detalladas en el marco internacional para gestión de riesgo (COSO), considerando los ocho componentes de este marco: i) ambiente interno, ii) establecimiento de objetivos, iii) identificación de riesgos, iv) evaluación de riesgos, v) respuesta al riesgo, vi) control, vii) información/comunicación y viii) monitoreo. Asimismo, define nueve tipos de riesgos, los cuales pueden surgir por diversas fuentes, internas o externas, a los que se encuentren expuestas las organizaciones.

Tabla 1. Tipos de riesgos

Tipo de riesgo	Concepto
Riesgo de crédito	La posibilidad de pérdidas por la incapacidad o falta de voluntad de los deudores, emisores, contrapartes o terceros obligados de cumplir sus obligaciones contractuales.
Riesgo de lavado de activos y del financiamiento del terrorismo	La posibilidad de que la empresa sea utilizada para fines de lavado de activos y de financiamiento del terrorismo. Esta definición excluye el riesgo de reputación y el operacional.
Riesgo de liquidez	La posibilidad de pérdidas por la venta anticipada o forzosa de activos a descuentos inusuales para hacer frente a obligaciones, así como por el hecho de no poder cerrar rápidamente posiciones abiertas o cubrir posiciones en la cantidad suficiente y a un precio razonable.
Riesgo de mercado	La posibilidad de pérdidas derivadas de fluctuaciones en las tasas de interés, los tipos de cambio, los precios de instrumentos de renta variable y otros precios de mercado, que incidan sobre la valuación de las posiciones en los instrumentos financieros.
Riesgo de reputación	La posibilidad de pérdidas por la disminución de la confianza en la integridad de la institución que surge cuando el buen nombre de la empresa es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una organización.
Riesgo técnico	La posibilidad de pérdidas o modificación adversa del valor de los compromisos contraídos, en virtud de los contratos de seguros, de reaseguros y de coaseguros. En el caso de los seguros de no-vida, se consideran las fluctuaciones relacionadas con la frecuencia, la severidad, y la liquidación de los siniestros. Para el caso de los seguros de vida, esto puede incluir la posibilidad de pérdidas por variaciones en el nivel, la tendencia o la volatilidad de las tasas de mortalidad, longevidad, invalidez, morbilidad, renovación o rescate de los contratos de seguros, entre otros parámetros y supuestos, así como de los gastos de ejecución de dichas obligaciones.
Riesgo de reaseguro	La posibilidad de pérdidas en caso de insuficiencia de la cobertura de reaseguro contratada por la empresa de seguros cedente, cuando las necesidades de reaseguro no fueron identificadas, determinadas o precisadas adecuadamente en los contratos; o cuando el reasegurador no se encuentra en capacidad de cumplir sus compromisos de pago, o no está dispuesto a pagarlos por discrepancias en la aplicación de las condiciones del contrato de seguro y de reaseguro; así como la demora en los pagos del reasegurador que puedan afectar los flujos de efectivo de la cedente, generando un riesgo de liquidez. En el reaseguro aceptado, comprende el riesgo derivado de la aplicación de una tarifa inadecuada por parte de la cedente y el riesgo de correr la misma suerte, por el que, como reasegurador, participará de los resultados, positivos o negativos, a los que está expuesto su cedente, en virtud del seguro directo.
Riesgo estratégico	La posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias clave de la empresa y en el proceso de generación e innovación de valor.

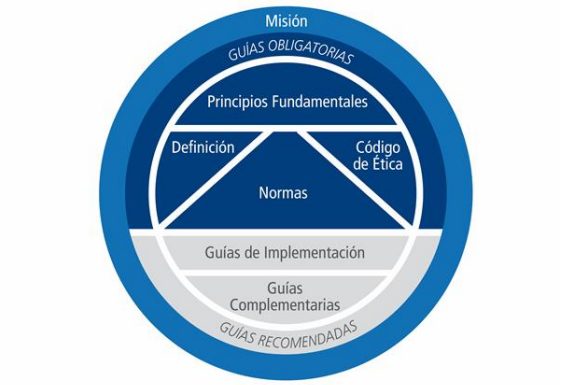
Tipo de riesgo	Concepto
Riesgo operacional	La posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

Fuente: Resolución SBS Nº272-2017.

2. Marco internacional para la práctica profesional

«El Marco Internacional para la Práctica Profesional (MIPP) de la Auditoría Interna,es el marco conceptual que organiza la guía autorizada promulgada por elInstituto de Auditores Internos» (IAI, 2017).

Gráfico 1. Marco internacional para la práctica profesional



Fuente: Marco Internacional para la Práctica Profesional de la Auditoría Interna, enero 2017.

La misión de auditoría internaes mejorar y proteger el valor de la empresa, proporcionando aseguramiento, asesoría y análisis conbase en riesgos. Describe el propósito primario de auditoría interna y es el objetivo general que engloba el MIPP. En tal sentido, alcanzar la misión es soportada por el MIPP en su conjunto.

El aumento del interés acerca de los roles y las responsabilidades de la alta dirección y el comité de auditoría ha motivado a muchas organizaciones a aumentar el énfasis en las actividades de aseguramiento. El glosario de las normas define servicios de aseguramiento como «un examen objetivo de evidencias con el propósito de proporcionar una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización»(IAI, 2017). El directorio utilizará múltiples recursos para obtener aseguramiento fiable. El aseguramiento de la alta

dirección es fundamental y debe estar complementado por el aseguramiento ofrecido por la auditoría interna y otras terceras partes. Los gestores de riesgos, los auditores internos y los profesionales del cumplimiento se preguntan: ¿Quién hace qué y por qué?. Especialmente los comités comienzan a preguntarse quién les ofrece el servicio de aseguramiento, dónde está la línea divisoria entre las funciones y si existe superposición entre ellas.

Existen tres clases principales de proveedores de servicios de aseguramiento, diferenciadas por las partes interesadas a las que sirven, por su nivel de independencia de las actividades sobre las que ofrecen aseguramiento y por la solidez del aseguramiento.

- Los que informan a la alta dirección o son parte de la dirección (aseguramiento de la dirección), en los que se incluye a quienes realizan autoevaluaciones de control, auditores de calidad, auditores medioambientales y otro personal de aseguramiento designado por la dirección.
- Los que informan al comité, incluyendo auditoria interna.
- Los que informan a las personas interesadas externas (aseguramiento de auditoría externa), papel tradicionalmente realizado por el auditor independiente.

El nivel de aseguramiento deseado, y quién debe proporcionarlo, variaría en función del riesgo.
Existen diversos proveedores de servicios de aseguramiento para una organización.

- Cargos directivos y empleados (la dirección ofrece aseguramiento en primera línea de defensa sobre los riesgos de los que es responsable).
- Alta dirección.
- Auditores externos e internos.
- Cumplimiento.
- Aseguramiento de la calidad.
- Gestión de riesgos.
- Auditores medioambientales.
- Auditores de seguridad e higiene en el lugar de trabajo.
- Auditores del desempeño del gobierno.
- Equipos de análisis de informes financieros.
- Subcomités del directorio (por ejemplo, de auditoría, de crédito o de gobierno).
- Proveedores externos de servicios de aseguramiento, incluyendo estudios y análisis especializados, entre otros.

Por lo general, la actividad de auditoría interna proporcionará aseguramiento para toda la organización, incluyendo los procesos de gestión de riesgos (tanto en sus diseños como en su efectividad operacional), la gestión de aquellos riesgos clasificados como clave (incluyendo la efectividad de los controles y otras respuestas), la verificación de la fiabilidad e idoneidad de la evaluación de riesgos e informes sobre el estado de riesgos y control. La edición de diciembre del 2016 de la revista Internal Auditor del IAI ofrece un ejemplo de cómo trazar un mapa de aseguramiento, teniendo en cuenta los siguientes campos:

Riesgo:«Al crear el mapa, los auditores internos deberían comenzar con el plan estratégico de la organización basada en sus objetivos clave. Entre los ejemplos está el lanzamiento de tres productos nuevos para filiales del 2017 o la reducción de la deserción de personal a menos de un 7 por ciento anual para el 31 de marzo de 2018. Los riesgos clave tomados del marco de ERM de la organización deberían presentar eventos que puedan evitar que se logren los objetivos cruciales. Los auditores deberían agrupar estos riesgos identificados por categoría (estratégicos, operativos, de informes y de cumplimiento) para facilitar la evaluación y las consideraciones de la respuesta»(Revista Internal Auditor, 2016).

«Para cada riesgo clave, el mapa de aseguramiento debería mencionar el propietario del riesgo que es responsable de gestionar el riesgo y realizar las actividades de aseguramiento. Debería calificar el riesgo inherente de los eventos según su impacto y probabilidad en una escala que vaya de menor (verde) a crítico (rojo). Las estrategias de mitigación están diseñadas para evitar que se produzca un evento de riesgo o para mitigar los efectos después de que se ha producido un evento. Los controles claves son aquellas respuestas que ayudan a gestionar y reducir el riesgo dentro del nivel de aceptación de riesgo. Por último, el mapa ilustra el riesgo residual después de que la dirección ha implementado actividades de respuesta al riesgo»(Revista Internal Auditor, 2016).

Aseguramiento:«La siguiente serie de columnas proporciona la cobertura de los servicios de aseguramiento por parte de las tres líneas de defensa de la organización. El nivel 1 muestra la supervisión directa de las operaciones diarias por parte de los propietarios del proceso. Por ejemplo, los directores operativos de la línea frontal supervisan los sistemas y mecanismos de supervisión y autoevaluación. El nivel 2 muestra las funciones de supervisión que respaldan a la dirección al proporcionar conocimientos para el desarrollo de políticas y la supervisión de su ejecución. El nivel 3 muestra los proveedores independientes y objetivos de aseguramiento sobre

la adecuación y eficacia general de la gestión de riesgos, el gobierno y el control interno, según lo establezcan el primer y el segundo nivel» (Revista Internal Auditor, 2016).

«La siguiente columna en el mapa, Depende de proveedores de aseguramiento, clasifica la cobertura de aseguramiento proporcionada. Algunos de los criterios son:

- Responsabilidad primaria, secundaria y terciaria.
- Contribuyente significativo, moderado, insignificante y desconocido al aseguramiento.
- Aseguramiento amplio, regular, ad hoc o sin aseguramiento proporcionado»(Revista Internal Auditor, 2016).

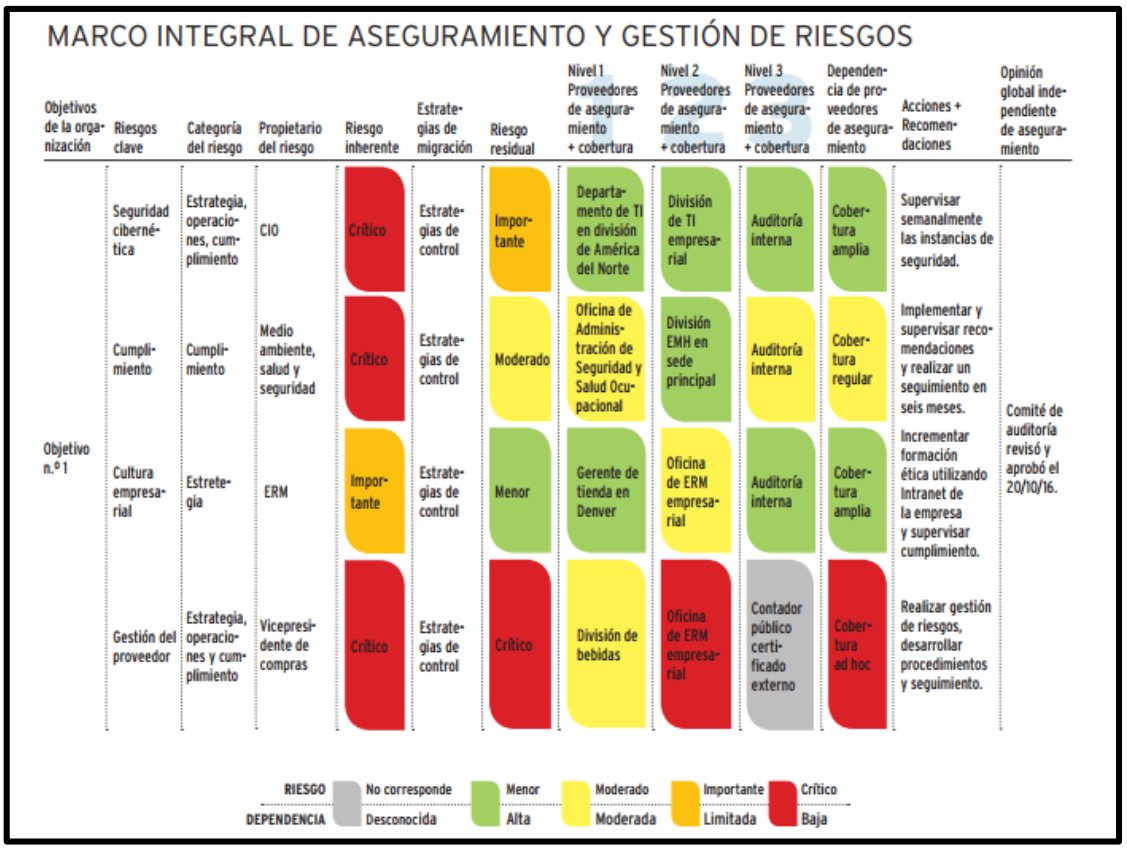
«La evaluación general de auditoría interna de la calidad y la cantidad de aseguramiento recibido se basa en criterios que incluyen conocimientos en la materia, experiencia habilidades y metodología. Por ejemplo, sin dependencia indica que no hay información disponible para evaluar la adecuación de las actividades de aseguramiento proporcionadas. Una dependencia baja implica que hay una falta de información para evaluar la adecuación de las actividades de aseguramiento. Una dependencia limitada significa solo las revisiones de la dirección de la eficacia de la gestión se han aplicado. En este caso, la organización ha tenido una evaluación independiente limitada o nula de la suficiencia del diseño del control y la eficacia operativa. Una dependencia moderada indica que las funciones de supervisión que respaldan a la dirección han evaluado consistentemente la adecuación de las actividades de aseguramiento. Una amplia dependencia indica que se han proporcionado servicios de aseguramiento independientes y objetivos para evaluar la adecuación de las actividades de aseguramiento»(Revista Internal Auditor, 2016).

«La siguiente columna detalla las acciones de subsanación para abordar las debilidades y garantizar la mejora continua del proceso de aseguramiento para alcanzar el nivel de aseguramiento deseado y anhelado. Los objetivos incluyen eliminar las brechas de aseguramiento, reducir las superposiciones de aseguramiento e incrementar la fuerza y cobertura del aseguramiento proporcionado al documentar las acciones de seguimiento como:

- Asignar propietarios del aseguramiento.
- Especificar la misión y el alcance del aseguramiento.
- Identificar la naturaleza y la frecuencia de las actividades de aseguramiento planificadas.
- Determinar el cronograma y la frecuencia de las revisiones de aseguramiento» (Revista Internal Auditor, 2016).

«En la columna final, la opinión global independiente de aseguramiento consiste en la evaluación escrita del DEA sobre la eficacia del enfoque que tiene la organización para gestionar el riesgo. Por ejemplo, “Si consideramos las actividades de aseguramiento realizadas durante el año, en nuestra opinión los sistemas de gestión de riesgos y control interno son eficaces (ineficaces) tomando en cuenta el nivel específico de aceptación de riesgos de la empresa”» (Revista Internal Auditor, 2016).

Gráfico 2. Marco integral de aseguramiento y gestión de riesgos



Fuente: Revista Internal Auditor, diciembre 2016.

Para el presente trabajo de investigación se realizará un mapa de aseguramiento del BancoAltas Cumbres, con la finalidad de alinear los esfuerzos de auditoría interna con los riesgos identificados en la organización, evitando la duplicidad de revisiones por parte de las áreas de aseguramiento.

3. Banco Altas Cumbres

3.1 Descripción de la empresa

El Banco Altas Cumbres se constituyó como una sociedad anónima de plazo indefinido, mediante escritura pública a fines de 1990, y autorizada por la SBS a principios de 1991. Esta IF, que pertenece a un grupo español, se dedica a la intermediación financiera en el sector privado para los sectores A y B (mediana empresa y banca comercial). Hacia el año 2008, después de diecisiete años de operaciones, la compañía decide diversificar su portafolio de servicios accesible a mercados de menores ingresos. Durante el 2014,el Banco Altas Cumbres afianzó su presencia en el mercado y continuó su plan de expansión con oficinas en lima y provincias, finalizando el año con 87 oficinas en todo el país. El objeto social del banco es realizar actividades de intermediación financiera, a fin de promover el desarrollo de la economía nacional. Está facultado, además, para captar y colocar recursos financieros y efectuar todo tipo de servicios bancarios y operaciones permitidas a la banca múltiple.

El banco asume, dentro de su estrategia como banco múltiple, el desarrollo de productos y servicios diseñados para las necesidades de sus clientes e implementa los procedimientos y herramientas de forma permanente. Asimismo, apoya toda esta estrategia en la fuerza de un equipo humano comprometido con los valores de la IF y que busca mantener siempre la excelencia en el servicio. El banco mantiene su objetivo de seguir mejorando sus procesos, de cara a una excelente experiencia por parte de susclientes. Por eso, se han hecho mejoras sustanciales en los procesos de originación, que son la base del negocio.

3.1.1 Estructura organizacional

La estructura organizacional del Banco Altas Cumbres está encabezada por la Junta General de Accionistas y el directorio, el cual está conformado por sietedirectores, siendo cuatro de ellos independientes. «El Comité de Auditoría, en representación del Directorio, tiene como propósito principal vigilar que los procesos contables y de reporte financiero sean apropiados, así como evaluar las actividades realizadas por los auditores internos y externos»(Memoria Anual, 2017). Cabe indicar, que la Unidad de Auditoría Interna depende funcionalmente del directorio. El organigrama de la IF está incluido en el anexo 1.

3.2 Grado de cumplimiento de las normas para el ejercicio profesional de la auditoría interna

Desde el año 2014,el banco realiza anualmente la autoevaluación de calidad de la actividad de auditoría interna para determinar los siguiente:

- Si cumple con las normas emitidas por el IAI, así como si los auditores internos aplican el código de ética del IAI.
- Si opera de forma eficaz y eficiente.
- Si agrega valor y mejora las operaciones del banco.

Si bien los resultados indican que generalmente cumple con esto, las principales observaciones refieren que el banco no dispone de una matriz de riesgos y que la actividad de auditoría interna no tiene un enfoque y metodología basada en riesgos. El resumen de la autoevaluación efectuada por la unidad de auditoría interna en el 2017 está incluida en el anexo 2.

La misión de la actividad de auditoría interna del Banco Altas Cumbres «es proveer servicios de aseguramiento y consulta independientes y objetivos, concebidos para agregar valor y mejorar las operaciones de la organización» (IAI, 2017).

El alcance del trabajo de auditoría interna es determinar si la red de la organización, relacionada con los procesos de administración de riesgo, control y gobierno corporativo, tal como están diseñados y representados por la gerencia, es adecuada y funciona para asegurar que:
- Los riesgos se identifiquen y administren de manera apropiada;
- La información financiera, administrativa y operativa sea exacta, confiable y oportuna;
- Las acciones de los empleados se desarrollen conforme a las políticas, las normas, los procedimientos, los reglamentos y las leyes aplicables;
- Los recursos se adquieran de manera económica, se utilicen en forma eficiente y se protejan adecuadamente;
- Se logren desarrollar los programas y los planes y se alcancen los objetivos;
- Se fomente la calidad y la mejora continua en el proceso de control de la organización; y
- Se reconozcan y aborden en forma adecuada las cuestiones legales o reguladoras que impacten en la organización.

3.3 Nivel de coordinación de la unidad de auditoría interna con otros proveedores de aseguramiento

La gestión integral del riesgo en el banco es una función de carácter transversal que abarca las diferentes tipologías de riesgos, como crédito, mercado y operaciones, entre otros. Interrelaciona las diferentes áreas del banco, soportada en políticas y lineamientos que permiten normar las actividades de riesgo para lograr una cartera de colocaciones e inversiones sana y rentable.

En el Banco Altas Cumbres, la gestión integral del riesgo sigue un modelo sobre la base de tres líneas de defensa independientes. Sin embargo, el correcto funcionamiento y coordinación de actividades entre auditoría interna y otras funciones de aseguramiento propicia beneficios para la institución.A la fecha solo existe, para el cumplimiento regulatorio, dicha coordinación, tanto con proveedores externos como con el regulador.

3.4 Objetivos estratégicos de la empresa

El objetivo estratégico general del Banco Altas Cumbres es desarrollar productos y servicios diseñados para las necesidades de los clientes e implementar los procedimientos y las herramientas de forma permanente. Esta estrategia se apoya en la fuerza de un equipo humano comprometido con los valores del banco, que busca mantener siempre la excelencia en el servicio.

Por su parte, sus objetivos específicos comprenden lo siguiente:

- Mayor rentabilidad.
- Obtener mayores ingresos.
- Mayor eficiencia de las operaciones.
- Generar diferencia en el mercado.
- Mejorar las capacidades del personal.

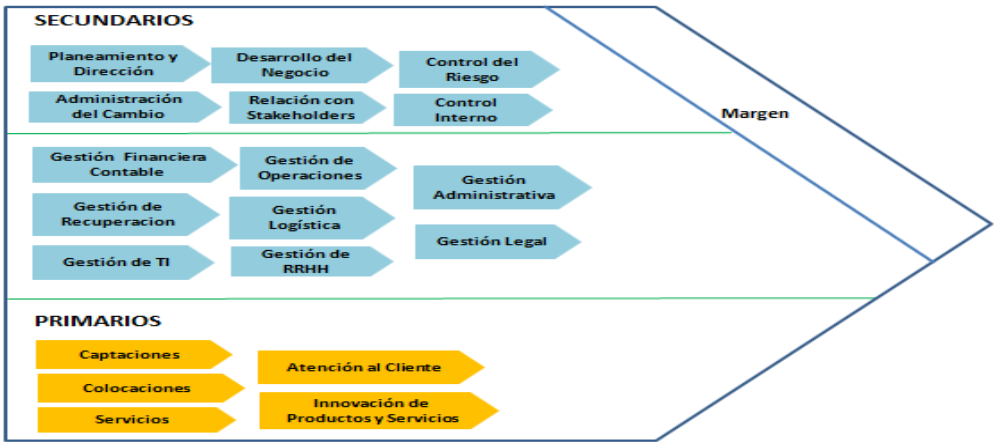
3.5 Cadena de valor y mapa de procesos

3.5.1 Cadena de valor

La cadena de valor identifica y establece la secuencia de los procesos, subprocesos y actividades que contribuyen directamente a satisfacer las necesidades y los requerimientos del cliente, y cumplir con los objetivos estratégicos de la organización.

A través de la cadena de valor, el banco crea valor para sus clientes y grupos de interés. La configuración de esta cadena de valor describe la lógica que sigue el conjunto de actividades primarias, desde el desarrollo del producto hasta la realización del servicio; así mismo, se observan los procesos de soporte, los cuales son transversales a la organización y apoyan en el cumplimiento de los objetivos estratégicos. A continuación se presentala cadena de valor para el Banco Altas Cumbres.

Gráfico 3. Cadena de valor

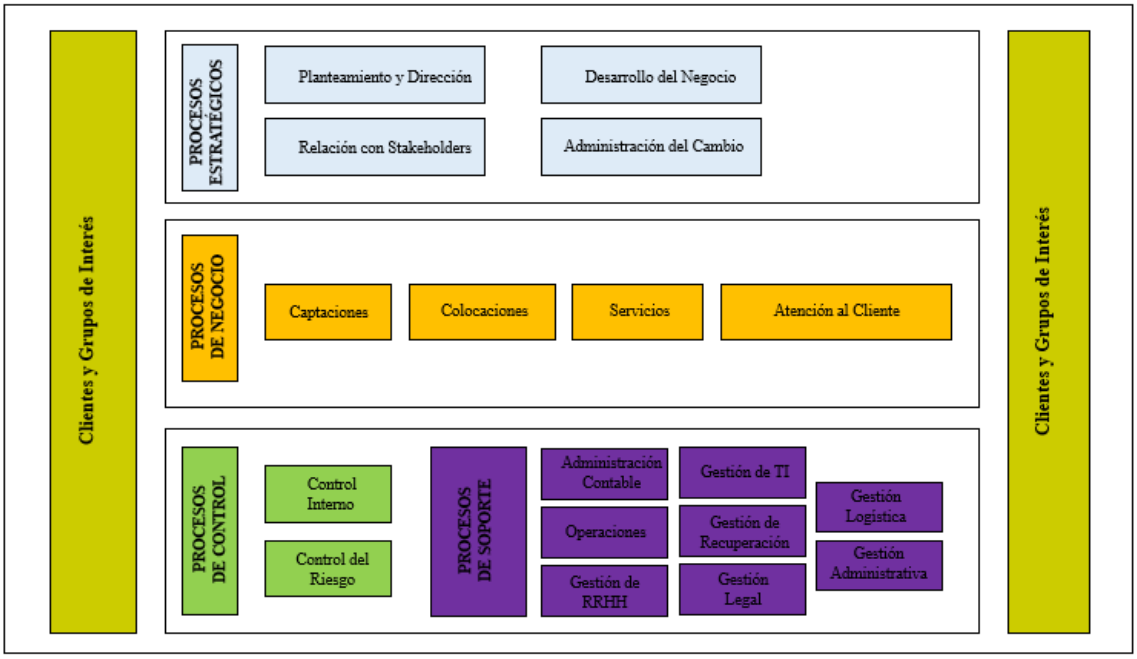


Fuente: Memoria Anual, 2017.

3.5.2 Mapa de procesos

El banco ha clasificado los procesos en cuatro grandes grupos: estratégicos, de negocios, de control y de soporte.

Gráfico 4. Mapa de procesos



Fuente:Elaboración propia, 2017.

A continuación describiremos un proceso de control fundamental para el banco.

3.6 Proceso de gestión integral de riesgos

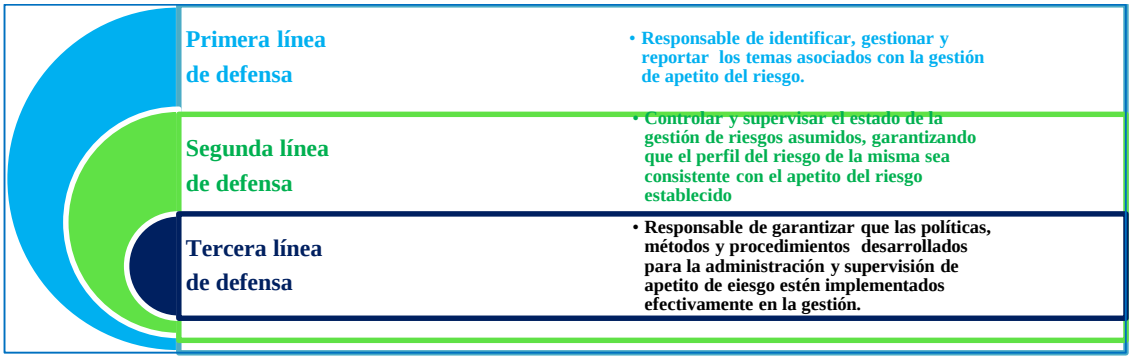
La gestión integral de riesgos del Banco Altas Cumbres es un proceso que abarca a toda la organización, interrelacionada con las diferentes vicepresidencias del banco y cuyo control puede evitar impactos negativos en los resultados y en el valor de la entidad.

«La gestión de riesgos siguiendo un modelo de gestión basado en tres líneas de defensa independientes, donde la Primera Línea es responsable de identificar, medir, evaluar, monitorizar, mitigar y reportar los riesgos en la ejecución de las operaciones bajo las directrices de la segunda línea; la Segunda Línea es la encargada del control y la vigilancia independiente del riesgo asumido por la primera como control de cumplimiento de políticas, monitoreo periódico del perfil de riesgos, control de excesos de límites y desarrollo de modelos, así mismo es la encargada de la definición del Apetito de Riesgo; y finalmente la Tercera Línea encargada de realizar la revisión independiente de los procesos para asegurar que existan funciones efectivas de gestión y control de riesgos implantadas» (Memoria Anual, 2017).

Este modelo de gestión se sustenta en los siguientes procesos clave:

- Identificación del universo de riesgos y definición del mapa de riesgos.
- Declaración del apetito al riesgo y seguimiento periódico del perfil de riesgos.
- Generación de políticas para la gestión de los riesgos.
- Autoevaluación de riesgos.
- Análisis de riesgos asociados con nuevos productos y servicios.
- Validación independiente de modelos.
- Incorporación de información y reportes de riesgos.
- Transmisión de la cultura de riesgos.

Gráfico 5. Líneas de defensa de la IF



Fuente: Memoria Anual IF, 2017.

Capítulo III. Metodología para la elaboración de un plan de auditoría basada en riesgos

1. Metodología

El plan de auditoría basada en riesgos lo elaboraremos y documentaremos siguiendo el siguiente esquema, a nivel de procesos del Banco Altas Cumbres:

Gráfico 6.Metodología de PABR

Fuente: Elaboración propia, 2017.

1.1 Establecer el universo de auditoría

El universo de auditoría está compuesto por un inventario de entidades, como procesos, sistemas, productos y servicios, entre otros, que conforman el listado de todas las auditorías que pudieran realizarse, siendo estos los componentes o las unidades auditables,que pueden representar un riesgo para el cumplimiento de los objetivos de la organización. Para determinar las unidades auditables en este trabajo se considerarán los siguientes elementos como *inputs*:

- El mapa de procesos de la IF;
- Los sistemas que soportan el procesamiento de las operaciones;
- Productos, servicios y canales de atención;
- El plan estratégico del Banco Altas Cumbres;
- Los requerimientos regulatorios; y
- Los requerimientos o sugerencias del directorio y la alta gerencia.

Cabe precisar que, según el libro The Internal Auditor’s Guide to Risk Assessment de Rick A. Wright Jr.Cia, el universo de auditoría de cada organización es único y es una compilación de muchos factores, los cuales evolucionan a lo largo de la vida de la organización y de la función de auditoría interna.

1.1.1 Mapa de procesos del Banco Altas Cumbres

Con base en el mapa de procesos del banco, se obtuvo un inventario de procesos que se detalla en la tabla 2.

Tabla 2. Inventario de procesos

No.	Macro proceso	Procesos
1	Planeamiento y dirección	Formulación y aprobación de plan estratégico, operativo y comercial
2		Formulación y aprobación del presupuesto
3		Formulación y aprobación de plan de apertura, cierre y traslado de oficinas
4		Estudios, análisis e información estratégica
5	Desarrollo del negocio	Diseño y desarrollo de productos
6		Campaña y promoción comercial
7	Gestión del cambio	Administración de proyectos de mejora de procesos
8		Administración de proyectos estratégicos
9		Gestión normativa
10	Relación stakeholders	Gestión de responsabilidad social
11		Gestión de imagen y comunicaciones
12		Administración de secretaría de directorio
13	Productos pasivos	Proceso cuentas de ahorros
14		Proceso Cuentas Corrientes
15		Proceso cuentas a plazo
16		Proceso de CTS
17	Productos activos	Préstamos comerciales
18		Préstamos hipotecarios
19		Leasing y lease back
20		Financiamiento comercio exterior
21		Préstamos convenio
22		Descuentos
23		Tarjeta de crédito
24		Factoring
25		Avance inmobiliario
26		Préstamos libre disponibilidad
27		Préstamo vehicular
28		Préstamos empleados
29		Sobregiros
30	Servicios	Recaudación
31		Corresponsalía
32		Fideicomiso
33		Administración delpPlan de cuentas

No.	Macro proceso	Procesos
34	Gestión financiera contable	Conciliación y Control
35		Elaboración de estados financieros, reportes y anexos
36	Gestión de operaciones	Administración de garantías
37		Transferencias interbancarias
38		Procesos centrales
39	Gestión de RR.HH.	Reclutamiento, selección e incorporación
40		Formación y capacitación
41		Compensación del colaborador
42	Gestión de TI	Soporte de usuarios
43		Desarrollo de aplicativos
44		Administración de infraestructura tecnológica
45	Gestión de recuperaciones	Adjudicación de bienes
46		Recuperación de créditos
47		Formulación y aprobación de castigo de créditos
48	Gestión logística	Adquisiciones y contrataciones
49		Proveedores
50	Gestión administrativa	Administración de la seguridad física
51		Seguridad y salud en el trabajo
52		Administración e infraestructura
53		Control patrimonial
54		Administración de archivo general
55	Gestión legal	Servicios contractuales
56		Administración de procesos judiciales y arbitrales
58		Transparencia de información a clientes
59		Atención de reclamos de clientes
60		Formulación, ejecución y seguimiento del cumplimiento normativo
61		Gestión de cumplimiento PLAFT
62	Gestión de administración de riesgos	Gestión de riesgo crediticio
63		Gestión de riesgo de mercado y liquidez
64		Gestión de riesgos cambiarios
65		Gestión de riesgo operacional
66		Gestión de seguridad de la información
67		Control del riesgo
68		Inspectoría

Fuente: Elaboración Propia, 2017.

1.1.2 Sistemas del Banco Altas Cumbres

El inventario de los sistemas de la IF se ha esquematizado como sigue:

Tabla 3. Inventario de sistemas

No.	Sistemas de la IF
1	Sistema AS\400
2	Sistema de operaciones en la red de oficinas
3	Swift - Transferencias interbancarias
4	Sistema de control de gastos
5	Sistema de planillas
6	Sistema de firmas y poderes
7	LBTR – Sistema para transferencias al BCRP
8	Sistema de arrendamiento financiero
9	Sistema de cajeros automáticos
10	Sistema de cajeros corresponsales
11	Seguridad en el computador central
12	Gestión de cambios en los sistemas informáticos
13	Desarrollo de aplicaciones
14	Mantenimiento de aplicaciones y control de cambios
15	Producción y operaciones de TI
16	Seguridad de información
17	Administración de accesos y perfiles lógicos
18	Infraestructura y redes de comunicación
19	Lotes contables

Fuente: Elaboración propia,2017.

1.1.3 Productos, servicios y canales de atención

Se elaboró un listado de todos los productos, servicios y canales de atención de la IF. En la siguiente tabla detallamos un ejemplo del inventario.

Tabla 4. Inventario de productos, servicios y canales

No.	Origen	Descripción
1	Productos	Proceso cuentas de ahorros
2	Productos	Proceso cuentas corrientes
3	Productos	Proceso cuentas a plazo
4	Productos	Proceso de CTS
5	Productos	Préstamos comerciales

No.	Origen	Descripción
6	Productos	Préstamos hipotecarios
7	Productos	Leasing y *lease back*
8	Productos	Financiamiento comercio exterior
9	Productos	Préstamos convenio
10	Productos	Descuentos
11	Productos	Tarjeta de crédito
12	Productos	Factoring
13	Productos	Avance inmobiliario
14	Productos	Préstamos libre disponibilidad
15	Productos	Préstamo vehicular
16	Productos	Préstamos empleados
17	Productos	Sobregiros
18	Servicios	Recaudación
19	Servicios	Corresponsalía
20	Servicios	Fideicomiso
21	Canales de atención	Red de oficinas
22	Canales de atención	Banca por internet
23	Canales de atención	Cajeros corresponsales

Fuente: Elaboración propia,2017.

1.1.4 Objetivos del plan estratégico del Banco Altas Cumbres

Se obtuvo información de los objetivos estratégicos de la IF, así como del plan de actividades que se efectuará para lograrlos. A continuación, se detalla, a manera de ejemplo, algunos de los objetivos de la IF.

Tabla 5. Objetivos del plan estratégico de la IF

Objetivo estratégico		Objetivo especifico
1	Incrementar los ingresos financieros	1.1. Reducción de costos
2		1.2. Mejorar la calidad de la cartera
3		1.3. Incrementar las captaciones y las colocaciones
4	Aumentar el número de clientes	2.1. Mejorar la calidad de servicio hacia los clientes
5		2.2. Diversificar los canales de atención
6		2.3. Incrementar la producción de la fuerza de ventas
7	Lograr niveles de excelencia en los procesos	3.1. Mejorar los modelos de riesgos
8		3.2. Incrementar el uso de herramientas tecnológicas para dar soporte a los procesos internos

Objetivo estratégico		Objetivo especifico
9		3.3. Mejorar los tiempos de respuesta a los clientes internos y externos para los diferentes productos y servicios
10	Incrementar la satisfacción del talento humano	4.1. Desarrollar el potencial del talento
11		4.2. Mejorar los beneficios de los colaboradores

Fuente: Elaboración propia,2017.

1.1.5 Requerimientos regulatorios

Las actividades regulatorias que son de requerimiento del ente de control y se detallan en la tabla siguiente.

Tabla 6. Requerimientos regulatorios

No.	Actividad requerida por la Superintendencia de Banca, Seguros y AFP
1-3	Clasificación cuatrimestral de la cartera crediticia no minorista (3 actividades)
4	Revisión anual de la clasificación de la cartera minorista
5	Riesgo cambiario crediticio
6	Riesgo de sobreendeudamiento de deudores minoristas
7	Contratos de financiamiento con garantía de cartera crediticia
8	Transferencia y adquisición de cartera crediticia
9	Riesgo de liquidez
10	Riesgo de tasa de interés
11	Administración del riesgo cambiario
12	Cartera de inversiones
13	Instrumentos financieros derivados
14	Administración del riesgo país
15	Sistema de prevención de lavado de activos
16	Reglamento de transparencia de información a clientes
17	Atención de reclamos de clientes
18	Reglamento de gestión de riesgo social y ambiental
19	Registro contable de las colocaciones, provisiones, intereses y comisiones
20	Bienes adjudicados y recuperados
21	Gestión integral de riesgos
22	Administración de los riesgos de operación y tecnológicos
23	Normas sobre vinculación y grupo económico
24	Límites legales de las empresas bancarias
25	Asignación de capital por riesgo, apalancamiento y patrimonio

No.	Actividad requerida por la Superintendencia de Banca, Seguros y AFP
26	Reglamento de cuentas corrientes
27	Evaluación de la función de cumplimiento normativo
28	Programa de aseguramiento de la calidad de la función de auditoría interna
29-31	Evaluación cuatrimestral del avance del plan 2018 de auditoría interna (3 actividades)
32	Plan de auditoría interna correspondiente al próximo año
33-36	Seguimiento trimestral de recomendaciones (4 actividades)

Fuente: Superintendencia de Banca y Seguros y AFPs.

1.1.6 Requerimientos de la alta dirección

Las expectativas obtenidas del comité de auditoría, el directorio y la alta gerencia serán documentadas.

Tabla 7. Requerimientos alta dirección

No.	Requerimiento Alta Dirección
1	Evaluación a la red de oficinas de la IF

Fuente: Elaboración propia, 2017.

1.2 Evaluar el riesgo inherente en las entidades auditables

El evaluar el riesgo en cada entidad auditable es parte fundamental del proceso de planeación de auditoría. El utilizar el enfoque basado en riesgo permite determinar la importancia de cada entidad auditable. Se debe efectuar una evaluación documentada de los riesgos inherentes que afectan a las entidades auditables. Esta evaluación permitirá conocer cómo los eventos potenciales impactan en la consecución de los objetivos dela entidad, siendo una evaluación preliminar del riesgo sin tener en cuenta las medidas de mitigación o controles. Esta actividad deberá efectuarse anualmente por el equipo de auditoría interna, evaluando desde una doble perspectiva de probabilidad de ocurrencia y la magnitud del impacto.

1.2.1 Riesgos inherentes

Las organizaciones, independientemente de su actividad económica, tamaño y estructura, se enfrentan a riesgos en todos los niveles. Los riesgos afectan la capacidad que tienen las organizaciones de competir exitosamente y alcanzar sus objetivos. La evaluación de riesgos inherentes se debe realizar con base en la situación real del negocio, eliminando el efecto de los controles.

1.2.2 Factores del riesgo inherente

Los factores de riesgo inherente que se utilizarán para la evaluación de riesgos serán los siguientes:

Tabla 8. Factores de riesgo inherente

Factor de riesgo	Definición
Crédito	Riesgo de pérdida financiera ocasionado por la incapacidad del deudor de cumplir con sus obligaciones contractuales con la IF.
Mercado y liquidez	Riesgo de pérdida ocasionado por las variaciones en los precios de mercado. Este riesgo incluye el riesgo de tasa de interés, riesgo cambiario, riesgo de liquidez de mercado y riesgo de opciones.
Operacional	
Planeación / Administración / Coordinación	Riesgo ocasionado por la falta de coordinación entre las distintas áreas de negocio para alcanzar los objetivos de la IF.
Personal	Riesgo ocasionado por la incapacidad de atraer o retener colaboradores productivos y competentes que cumplan con expectativas de desempeño y conducta.
Organización, roles y responsabilidades	Riesgo ocasionado por la falta de esfuerzo coordinado entre las distintas áreas de negocio de la IF para el logro de los objetivos.
Aplicación de procedimientos y procesamiento de transacciones	Riesgo ocasionado por la toma de decisiones inapropiadas y la incapacidad de ejecutar un procesamiento de transacciones confiables.
Contabilidad / Valuación / Reportes	Riesgo ocasionado por errores en el manejo de información contable e informes regulatorios.
Fraude	Referido a actividades fraudulentas efectuadas por colaboradores o terceros contra la IF, generando exposición a pérdidas económicas y reputacionales.
Cumplimiento	
Confidencialidad	Riesgo ocasionado por revelar información de uso privado.
Conflictos de interés	Riesgo ocasionado por una unidad de negocio o por los individuos dentro de la misma con interese diferentes a los de la IF.
Regulatorio	Riesgo que puede ocasionar multas y sanciones con impacto reputacional por incumplimiento de normas.
Reputacional	Riesgo que ocasiona impacto negativo en la IF respecto de su reputación.
Prevención de lavado de activos	Susceptibilidad a efectuar actividades de lavado de dinero y financiamiento al terrorismo.

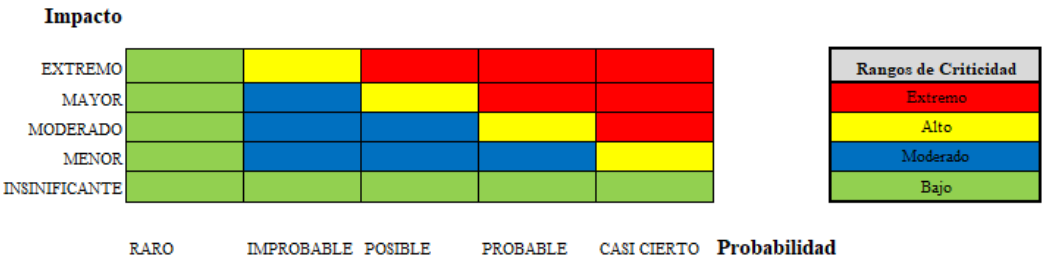
Factor de riesgo	Definición
Tecnología	Riesgo de no contar con tecnología que satisfaga las necesidades del negocio de la IF.
Infraestructura	Riesgo de que la infraestructura de la IF sea inadecuada para soportar de manera segura y oportuna el procesamiento de las aplicaciones.
Información	Riesgo de que la información utilizada en la toma de decisiones no sea confiable (que la información no sea exacta, completa, confidencial y relevante)
Sistemas/ Aplicaciones /Bases de datos / Hojas de cálculo	Riesgo de que los sistemas no proporcionen funcionalidad y confiabilidad para proporcionar adecuado soporte al negocio.
Outsourcing	Riesgo de que el proveedor de servicios no cumpla con lo contractualmente establecido.

Fuente: Elaboración propia, 2017.

1.2.3 Medición de los riesgos inherentes

El nivel de riesgo inherente se determina a través de una expresión de valores de probabilidad e impacto, dentro de un contexto determinado. Por ejemplo, cuando el impacto de un factor de riesgo es importante, pero la probabilidad de ocurrencia es mínima, entonces la dimensión del riesgo es considerada baja o moderada. Esta relación se puede expresar gráficamente de la siguiente manera:

Gráfico 7. Probabilidad por impacto



Fuente: Elaboración propia, 2017.

1.2.4 Probabilidad de ocurrencia

Para cada evento de riesgo identificado, se realiza una estimación cualitativa o cuantitativa de la tasa de ocurrencia que tendría el mismo, para materializarse. A partir de la tabla, se selecciona el valor que, a juicio experto y por historial de eventos, se aproxime al número posible de ocurrencia (en valor anualizado) y se consigna según los rangos establecidos:

- Casi cierto
- Probable
- Posible

- Improbable
- Raro

La asignación de estos valores se realiza en términos discretos; esto es, los cinco puntos son los únicos posibles. Los valores asignados han sido dados tomando en cuenta las recomendaciones de la industria financiera (Entidades locales bancarias y de seguros), las cuales incluyen como parte de su metodología de gestión de riesgos tableros de 5x5 y rangos de probabilidad similares a los propuestos en el presente trabajo de investigación, así como lo indicado en el libro "The Internal Auditor's Guide to Risk Assessment".

Tabla 9. Probabilidad de ocurrencia

Nivel	Puntos	Descripción
Casi cierto	12	▪ Eventos similares ocurren o pueden ocurrir todos los meses. ▪ Hay sustento de ocurrencia en la base de datos de eventos de pérdida (BDEP).
Probable	2	▪ Eventos similares ocurren o pueden ocurrir cada seis meses. ▪ Hay sustento en la BDEP, al menos una vez en los últimos dos años.
Posible	1	▪ Eventos similares ocurren o pueden ocurrir una vez al año. ▪ No ha ocurrido, pero es inminente si no se aplica un control.
Improbable	0.333	▪ Eventos similares ocurren o pueden ocurrir una vez cada tres años.
Raro	0.2	▪ Eventos similares ocurren o pueden o pueden ocurrir una vez cada cinco años.

Fuente: Elaboración propia, 2017.

(1) Raro: Tasa de ocurrencia anualizada igual o menor a 0.2 veces.

(2) Improbable: tasa de ocurrencia anualizada mayor que 0.2 y hasta 0.333, inclusive.

(3) Posible: tasa de ocurrencia anualizada mayor que 0.333, pero menor que 2 veces.

(4) Probable: tasa de ocurrencia anualizada mayor o igual que 2, pero menor a 12 veces.

(5) Casi cierto: tasa de ocurrencia anualizada mayor o igual que 12 veces.

1.2.5 Magnitud del impacto

Para cada evento de riesgo identificado (estratégico/de negocio, de reputación, operacional o múltiple), se debe realizar una estimación cualitativa o cuantitativa del impacto financiero que tendría, de materializarse.A partir de la siguiente tabla, se deberá determinar el nivel que, a juicio experto, y por historial de eventos previos, se aproxime más al impacto financiero esperado, según los siguientes rangos:

- Extremo
- Mayor
- Moderado

- Menor
- Insignificante

Tabla 10. Magnitud de impacto

Categoría	Intervalo(1)	Procesos(2)	Medios(3)	Personas(4)
Extremo	200% - 250% (AyT)(5)	▪ Interrupción de procesos con tiempo objetivo de recuperación (RTO) de 1 – 4 horas.	▪ Incidente mayor. ▪ La opinión pública cuestiona la credibilidad de la IF. ▪ Difusión vía medios escritos, televisivos, radiales e internet.	▪ Pérdida de 3 o más miembros de alta gerencia. ▪ Pérdida de 10 o más gerencias de negocio o soporte. ▪ Indisponibilidad de más de 50% del personal crítico.
Mayor	150% - 200% (AyT) (5)	▪ Interrupción de procesos con RTO de 4 – 24 horas.	▪ Incidente de interés. ▪ Cierto sector cuestiona la credibilidad de la IF. ▪ Difusión vía medios escritos, televisivos, radiales e internet.	▪ Pérdida de 1 o 2 miembros de alta gerencia. ▪ Pérdida de 7 a 9 gerencias de negocio o soporte. ▪ Indisponibilidad de entre 40% o 50% del personal crítico.
Moderado	100% - 150% (AyT) (5)	▪ Interrupción de procesos con RTO de 24 – 48 horas.	▪ Incidente de interés. ▪ Difusión vía medios escritos, televisivos, radiales. ▪ Alcance local o regional.	▪ Pérdida de 4 a 6 gerencias de negocio o soporte. ▪ Indisponibilidad de entre 20% y 40% del personal crítico.
Menor	50% - 100% (AyT) (5)	▪ Interrupción de procesos con RTO de 48 – 1 semana.	▪ Incidente podría ser de interés. ▪ Difusión vía medios escritos y radiales, locales o regionales.	▪ Pérdida de 2 o 3 gerencias de negocio o soporte. ▪ Indisponibilidad de entre 10 % y 20% del personal crítico.
Insignificante	0% - 50% (AyT) (5)	▪ Interrupción de procesos con RTO mayor a 1 semana.	▪ Incidente de menor interés. ▪ Posible difusión vía medios escritos locales o regionales.	▪ Pérdida de 1 gerencias de negocio o soporte. ▪ Indisponibilidad menor al 10% del personal crítico.

Fuente: Elaboración propia, 2017.

(1) Intervalo: valor monetario referencial para la presentación gráfica en el mapa de riesgos.

(2) Procesos: sujeto a la priorización de procesos críticos de continuidad del negocio.

(3) Medios: establece el cumplimiento de, al menos, 2 de los criterios por categoría.

(4) Pérdida intempestiva y por 15 días o más; ocurrencia de, al menos, uno de los criterios por categoría

(5) AyT: apetito y tolerancia, criterio que prioriza los riesgos significativos de la IF; todos aquellos riesgos que sobrepasen este nivel serán considerados de importancia y deberán contar obligatoriamente con planes de acción definidos en tiempo y costo.

La asignación de estos valores se realiza en términos discretos; esto es, los cinco puntos son los únicos posibles. Los valores asignados han sido dados tomando en cuenta las recomendaciones de la industria financiera (Entidades locales bancarias y de seguros), las cuales incluyen como parte de su metodología de gestión de riesgos tableros de 5x5 y rangos de impacto similares a los propuestos en el presente trabajo de investigación, así como lo indicado en el libro "The Internal Auditor's Guide to Risk Assessment".

Tabla 11. Cálculo del apetito y tolerancia

Criterio	Valores S/
Utilidad antes de impuestos al cierre del periodo 2017 (UAI)	125.060.000
Patrimonio al cierre del periodo 2017 (PAT)	969.552.000
Obtenemos el 5% (UAI)	6.253.000
Obtenemos el 1% (PAT)	9.695.000
Error tolerable / Hallazgo tolerable (50% del valor menor entre el 5%UAI y 1% PAT))	3.126.500
Apetito y tolerancia (50% del error tolerable)	**1.563.250**

Fuente: Elaboración propia, 2017.

El cálculo propuesto en este trabajo de investigación, ha sido elaborado tomando como referencia practicas de calculo de apetito y tolerancia en las entidades financieras locales y de acuerdo a las recomendaciones propuestas por en el libro "*The Internal Auditor's Guide to Risk Assessment"*.

1.2.6 Cálculo de probabilidad por impacto

Para evaluar los rangos de criticidad del proceso, se ponderará la cantidad de riesgos inherentes, según la siguiente metodología:

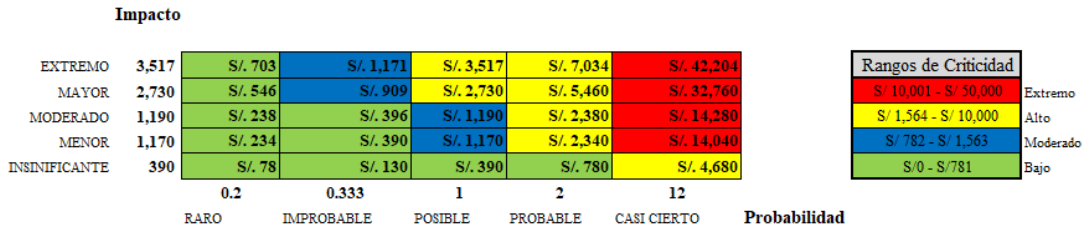
Rango de criticidad = Impacto x Probabilidad

De acuerdo conlos cinco niveles de impacto (semisuma de los valores inferiores y superiores por cada nivel) y cinco niveles de probabilidad, se define un total de cuatro niveles de criticidad, de acuerdo con elsiguiente gráfico:

- Extremo
- Alto
- Moderado
- Bajo

Gráfico 8. Rangos de criticidad

*Los valores del rango de criticidad e impacto están expresados en miles de soles (S/).



Fuente: Elaboración propia, 2017.

1.2.7 Ponderación del riesgo inherente del proceso

Para evaluar la criticidad del proceso, se ponderará la cantidad de riesgos inherentes, según la siguiente metodología:

- Si la cantidad de riesgos extremos representa un valor mayor o igual al 20% de la sumatoria total de la cantidad de riesgos, la ponderación para el proceso será extremo.
- Si la suma de riesgos extremos y altos representa un valor mayor o igual al 30% de la sumatoria total de la cantidad de riesgos, la ponderación para el proceso será alto.
- Si la suma de riesgos extremos, altos y moderados representa un valor mayor o igual al 40% de la sumatoria total de la cantidad de riesgos, la ponderación para el proceso será moderado.
- Si la cantidad de riesgos bajos representa el 61% más que la sumatoria de los riesgos extremos, altos y moderados, la ponderación para el proceso será bajo.

En la siguiente tabla, a manera de ejemplo aplicativo, detallamos la ponderación para el proceso Gestión de Cumplimiento del Sistema de Prevención de Lavado de Activos y del Financiamiento del Terrorismo (PLAFT).

Tabla 12.Ponderación del riesgo inherente

Proceso	Número de riesgos inherentes por calificación de probabilidad e impacto					Ponderación del riesgo inherente del proceso
	Extremo	Alto	Moderado	Bajo	Total	
Gestión de cumplimiento PLAFT	0	2	6	8	16	Moderado

Fuente: Elaboración propia, 2017.

1.2.8 Factores de control

Los factores de control utilizados durante la evaluación del riesgo son los siguientes:

Tabla 13. Factores de control

Factor de control	Definición
Ambiente de control	El ambiente de control es la parte central de una organización y establece el grado de influencia en la conciencia de control entre los colaboradores de esta. Influye en el establecimiento de los objetivos, la evaluación de riesgos, la estructuración y el apego a los controles.
Evaluación de riesgos	La evaluación de riesgos consiste en la identificación y el análisis de los riesgos que influyen en el logro de los objetivos de negocio y en la formulación de cómo debe administrarse el riesgo.
Actividades de control	Las actividades de control representan las políticas y los procedimientos que permiten asegurar el cumplimiento de las directivas de la gerencia y la toma de medidas necesarias para controlar los riesgos que afectan el cumplimiento de los objetivos de la IF.
Información y comunicación	La información y la comunicación representan la identificación, la recopilación y la difusión adecuada y oportuna de la información, sea interna o externa, a fin de que el personal pueda cumplir con sus responsabilidades.
Monitoreo	Evalúa la calidad de los sistemas de control en el tiempo y su capacidad para adaptarse a los cambios que puedan surgir. Esta se realiza mediante la combinación de actividades de monitoreo de los procesos o mediante evaluaciones independientes.

Fuente: Committee of Sponsoring Organizations of the Treadway Commission [COSO].

En el anexo 3 detallamos un ejemplo de la ponderación del riesgo inherente para el proceso de gestión de cumplimiento PLAFT.

1.3 Identificar las unidades auditables vinculadas con elcumplimiento de los objetivos estratégicos.

Se efectuará la identificación de aquellas unidades auditables que se encuentren directamente relacionados con elcumplimiento de los objetivos estratégicos de la organización.

Tabla 14. Vinculación con los objetivos

Objetivo estratégico		Macro - Proceso vinculado
1	Incrementar los ingresos financieros	Productos pasivos
		Productos activos
		Servicios
2	Aumentar el número de clientes	Desarrollo del negocio
3	Lograr niveles de excelencia en los procesos	Gestión del cambio
		Gestión de TI
		Gestión de administración de riesgos
4	Incrementar la satisfacción de nuestro talento humano	Gestión de recursos humanos (RR.HH.)

Fuente: Elaboración propia, 2017.

Una vez identificados, se les asignará un puntaje para su priorización, según la siguiente tabla:

Tabla 15. Puntuación de los procesos críticos

Rango	Puntuación
No contribuye al logro del objetivo	No = 0
Contribuye parcialmente al logro del objetivo	Parcial =1
Sícontribuye al logro del objetivo	Sí = 2

Fuente: Elaboración propia, 2017.

1.4 Ponderar las expectativas de la alta dirección

1.4.1 Obtener requerimientos del comité de auditoría, el directorio y la alta gerencia

Se obtendrá y documentarán las expectativas del comité de auditoría, el directorio y la alta gerencia. Aquellos requerimientos que sugieran revisar dichas autoridades recibirán un puntaje, a efectos de ser priorizados. En la siguiente tabla detallamos el puntaje.

Tabla 16. Puntuación de expectativas de la alta gerencia

Rango	Puntuación
No requerido	No = 0
Requerido	Sí = 1

Fuente: Elaboración propia, 2017.

1.4.2 Ponderar los tipos de hallazgos de aquellos procesos que han sido evaluados

Se considerará una puntuación según el tipo de hallazgo que se obtuvo en su última evaluación.

Tabla 17. Puntuación según el tipo de hallazgo

Rango	Puntuación
Hallazgo significativo	Sí = 1
Hallazgo no significativo	No = 0

Fuente: Elaboración propia, 2017.

1.4.3 Construir unplan de rotación

El plan de rotación para las revisiones que efectuará auditoría interna tendrá un puntaje asignado para ser priorizado. El puntaje estará determinado por el nivel de riesgo del proceso o actividad y por la antigüedad de la revisión.

Tabla 18. Nivel de riesgo

Nivel de riesgo	Rotación	Puntuación
Extremo	1 año	4
Alto	Hasta 2 años	3
Moderado	Hasta 3 años	2
Bajo	Hasta 4 años	1

Fuente: Elaboración propia, 2017.

Luego de aplicar la metodología descrita, se obtendrá las evaluaciones que conformarán el plan de auditoría basado en riesgo a ejecutarse en un año. En la siguiente matriz se detalla las actividades que conformarán el plan de auditoría basado en riesgos para el año 2018.

Tabla 19.Matriz del universo de la auditoría

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
1	Formulación y aprobación de plan estratégico, operativo y comercial	0	1	0	4	5	Bajo	1	0	0	0	2	0	3
2	Formulación y aprobación del presupuesto	0	1	0	4	5	Bajo	1	0	0	0	2	0	3
3	Diseño y desarrollo de productos	0	1	1	4	6	Bajo	1	2	0	0	2	0	5
4	Administración de proyectos de mejora de procesos	0	1	3	8	12	Bajo	1	2	0	0	2	0	5
5	Gestión de responsabilidad social	0	0	2	3	5	Bajo	1	0	0	0	2	0	3
6	Administración de secretaría de directorio	0	0	1	2	3	Bajo	1	0	0	0	4	0	5
7	Proceso cuentas de ahorros	0	1	4	6	11	Moderado	2	2	0	0	3	0	7
8	Proceso cuentas corrientes	1	2	1	8	12	Bajo	1	2	0	0	2	0	5
9	Proceso cuentas a plazo	0	1	0	7	8	Bajo	1	2	0	0	2	0	5
10	Proceso de CTS	0	2	1	6	9	Bajo	1	2	0	0	2	0	5

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
11	Préstamos comerciales	0	5	4	10	19	Moderado	2	2	0	0	3	0	7
12	Préstamos hipotecarios	0	4	2	12	18	Bajo	1	2	0	0	2	0	5
13	Leasing y *lease back*	4	4	4	8	20	Extremo	4	2	1	0	4	1	12
14	Financiamiento comercio exterior	1	3	5	8	17	Moderado	2	2	0	0	3	0	7
15	Préstamos convenio	0	2	5	9	16	Moderado	2	0	0	0	3	0	5
16	Descuentos	0	2	6	5	13	Moderado	2	0	0	0	3	0	5
17	Tarjeta de crédito	0	3	6	6	15	Moderado	2	0	0	0	3	0	5
18	*Factoring*	0	2	0	8	10	Bajo	1	0	0	0	2	0	3
19	Avance inmobiliario	0	2	3	4	9	Moderado	2	0	0	0	3	0	5
20	Préstamos libre disponibilidad	1	4	4	6	15	Alto	3	2	0	0	4	0	9
21	Préstamo vehicular	0	1	3	6	10	Bajo	1	0	0	0	2	0	3
22	Préstamos empleados	0	0	2	6	8	Bajo	1	0	0	0	2	0	3
23	Sobregiros	2	1	3	8	14	Moderado	2	0	0	0	3	0	5
24	Recaudación	0	2	6	8	16	Moderado	2	2	0	0	3	0	7
25	Corresponsalía	0	2	4	6	12	Moderado	2	0	0	0	3	0	5
26	Fideicomiso	0	2	2	6	10	Bajo	1	0	0	1	2	0	4
27	Administración de garantías	1	2	6	6	15	Moderado	2	2	0	0	3	0	7

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
28	Transferencias interbancarias	0	0	1	6	7	Bajo	1	0	0	0	2	0	3
29	Procesos centrales	0	0	1	7	8	Bajo	1	0	0	0	2	0	3
30	Adquisiciones y contrataciones	1	1	1	9	12	Bajo	1	2	0	0	2	0	5
31	Proveedores	0	0	2	6	8	Bajo	1	0	0	0	2	0	3
32	Conciliación y control de cuentas por cobrar, pagar y operaciones en trámite	1	1	2	6	10	Bajo	1	0	0	0	2	0	3
33	Elaboración de estados financieros, reportes y anexos	0	1	5	8	14	Moderado	2	0	0	0	3	0	5
34	Adjudicación de bienes	2	2	0	4	8	Extremo	4	0	0	1	4	1	10
35	Recuperación de créditos	1	1	0	6	8	Bajo	1	0	0	0	2	0	3
36	Formulación y aprobación de castigos y créditos	0	1	3	4	8	Moderado	2	0	0	0	3	0	5
37	Administración de la seguridad física	0	0	4	8	12	Bajo	1	0	0	0	2	0	3
38	Administración e infraestructura	0	0	2	4	6	Bajo	1	0	0	0	2	0	3
39	Control patrimonial	0	0	0	5	5	Bajo	1	0	0	0	2	0	3

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
40	Administración del archivo general	0	0	0	6	6	Bajo	1	0	0	0	2	0	3
41	Servicios contractuales	0	1	2	7	10	Bajo	1	0	0	0	2	0	3
42	Administración de procesos judiciales y arbitrales	0	1	2	6	9	Bajo	1	0	0	0	2	0	3
43	Transparencia de información a clientes	1	4	4	6	15	Alto	3	2	0	1	4	0	10
44	Atención de reclamos de clientes	1	4	4	6	15	Alto	3	0	0	1	4	0	8
45	Formulación, ejecución y seguimiento del cumplimiento normativo	0	3	4	6	13	Moderado	2	0	0	1	3	0	6
46	Gestión de cumplimiento PLAFT	2	4	5	8	19	Alto	3	1	0	1	4	0	9
47	Gestión de riesgo crediticio	1	2	4	8	15	Moderado	2	2	0	0	3	0	7
48	Gestión de riesgo de mercado y liquidez	0	1	4	6	11	Moderado	2	0	0	0	3	0	5
49	Gestión del riesgo operacional	1	4	5	8	18	Moderado	2	2	1	1	3	0	9
50	Gestión de seguridad de la información	0	1	2	6	9	Bajo	1	0	0	0	2	0	3
51	Control del riesgo	0	2	6	8	16	Moderado	2	0	0	0	3	0	5

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
52	Reclutamiento, selección e incorporación	0	1	5	8	14	Moderado	2	0	0	0	3	0	5
53	Soporte de usuarios	0	2	3	5	10	Moderado	2	0	0	0	3	0	5
54	Desarrollo de aplicativos	0	1	3	6	10	Bajo	1	0	0	0	2	0	3
55	Administración de infraestructura tecnológica	0	2	3	7	12	Moderado	2	0	0	0	3	0	5
56	Sistema AS\400: administración y seguridad	1	2	6	5	14	Moderado	2	0	0	0	3	0	5
57	Sistema de operaciones en la red de oficinas	1	3	5	7	16	Moderado	2	2	1	0	3	1	9
58	Swift - Transferencias interbancarias	1	2	6	4	13	Moderado	2	0	0	0	3	0	5
59	Sistema de control de gastos	0	6	4	4	14	Alto	3	0	0	0	4	0	7
60	Sistema de planillas	0	2	5	7	14	Moderado	2	0	0	1	3	0	6
61	Sistema de firmas y poderes	0	1	5	6	12	Moderado	2	0	0	0	3	0	5
62	Sistema de cajeros automáticos	1	2	6	8	17	Moderado	2	0	0	0	3	0	5
63	Sistema de cajeros corresponsales	1	1	1	6	9	Bajo	1	0	0	0	2	0	3

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
64	Seguridad en el computador central	1	1	1	8	11	Bajo	1	0	0	0	2	0	3
65	Gestión de cambios en los sistemas informáticos	0	1	1	8	10	Bajo	1	0	0	0	2	0	3
66	Desarrollo de aplicaciones	1	1	1	6	9	Bajo	1	0	0	0	2	0	3
67	Mantenimiento de aplicaciones y control de cambios	0	1	1	8	10	Bajo	1	0	0	0	2	0	3
68	Producción y operaciones de TI	0	1	1	8	10	Bajo	1	0	0	0	2	0	3
69	Seguridad de información	0	1	1	7	9	Bajo	1	0	0	0	2	0	3
70	Administración de accesos y perfiles lógicos	1	1	2	9	13	Bajo	1	0	0	0	2	0	3
71	Infraestructura y redes de comunicación	0	2	4	7	13	Moderado	2	0	0	0	3	0	5
72	Lotes contables	4	1	4	8	17	Extremo	4	0	0	0	4	1	9
73	Red de oficinas	4	10	3	7	24	Alto	3	0	0	0	4	0	7
74	Banca por internet	0	3	2	8	13	Bajo	1	2	0	0	2	0	5
75	Clasificación cuatrimestral de la cartera crediticia no minorista	3	2	2	9	16	Alto	3	0	0	1	4	0	8

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
76	Revisión anual de la clasificación de la cartera minorista	0	0	3	6	9	Bajo	1	0	0	1	2	0	4
77	Riesgo cambiario crediticio	0	0	3	8	11	Bajo	1	0	0	1	2	0	4
78	Riesgo de sobreendeudamiento de deudores minoristas	0	1	3	9	13	Bajo	1	0	0	1	2	0	4
79	Contratos de financiamiento con garantía de cartera crediticia	0	0	2	6	8	Bajo	1	0	0	1	2	0	4
80	Transferencia y adquisición de cartera crediticia	0	0	2	6	8	Bajo	1	0	0	1	2	0	4
81	Riesgo de liquidez	0	0	4	5	9	Moderado	2	0	0	1	3	0	6
82	Riesgo de tasa de interés	0	0	4	6	10	Bajo	1	0	0	1	2	0	4
83	Administración del riesgo cambiario	0	0	2	6	8	Bajo	1	0	0	1	2	0	4
84	Cartera de inversiones	0	1	4	5	10	Moderado	2	1	0	1	3	0	7
85	Instrumentos financieros derivados	0	1	3	8	12	Bajo	1	0	0	1	2	0	4
86	Administración del riesgo país	0	0	2	7	9	Bajo	1	0	0	1	2	0	4

	Entidad auditable	Número de riesgos inherentes por calificación de impacto y probabilidad de ocurrencia					Ponderación del riesgo inherente del proceso	Puntaje de riesgo inherente	Asociado al cumplimiento de objetivos estratégicos	Requerimientos del comité de auditoría o la dirección	Requerimientos de ley para la auditoría interna	Puntaje de rotación	Puntaje de hallazgos significativos	Suma de puntaje
		Extremo	Alto	Moderado	Bajo	Total								
87	Reglamento de gestión de riesgo social y ambiental	0	0	1	6	7	Bajo	1	0	0	1	2	0	4
88	Registro contable de colocaciones, provisiones, intereses y comisiones	0	0	5	2	7	Moderado	2	0	1	1	3	2	9
89	Gestión integral de riesgos	0	0	1	8	9	Bajo	1	0	0	1	2	0	4
90	Normas sobre vinculación y grupo económico	0	0	1	9	10	Bajo	1	0	0	1	2	0	4
91	Límites legales de las empresas bancarias	0	0	1	8	9	Bajo	1	0	0	1	2	0	4
92	Asignación de capital por riesgo, apalancamiento y patrimonio	0	1	1	10	12	Bajo	1	0	0	1	2	0	4
93	Reglamento de cuentas corrientes	0	0	2	8	10	Bajo	1	0	0	1	2	0	4

Fuente: Elaboración propia, 2017.

1.5 Elaboración del mapa de aseguramiento de la IF

De acuerdo con elmapa de procesos de la organización, se ha buscado el nivel de aseguramiento que ofrecen las distintas unidades, ya sean de la segunda o tercera línea de defensa, así como el alcance que tienen sus revisiones, para que esto pueda ser comparado con las revisiones de auditoría interna y así no duplicar esfuerzos en revisiones que cuentan con una alta cobertura de aseguramiento. Del resultado obtenido se puede observar que existe una alta cobertura de aseguramiento por parte del área de riesgo operacional, lo cual ayudará al área de auditoria a hacer revisiones con un mayor nivel de detalle y centrándose específicamente en aquellos procesos que no cuentan con aseguramiento por ninguna área adicional a auditoría. Esto lo podemos observar en mayor detalle en el anexo 4.

1.6 Determinar los recursos

De acuerdo con las actividades que se contemplarán en el plan, se debe calcular las horas/hombre disponibles para el cumplimiento del mismo. A la fecha, se cuenta con trece personas en la vicepresidencia de auditoría interna.

Tabla 20. Recursos

Tipo de auditoría	Cantidad de recursos
Auditoría de tecnologías de información	2
Auditoría de créditos	3
Auditoría de mercado y liquidez	2
Auditoría de procesos	3
Auditoría de red de oficinas	3
Total de recursos	**13**

Fuente: Elaboración propia, 2017.

El cálculo de las horas/hombre disponible para la realización de los exámenes de auditoría asciende a 22-152 horas. En la siguiente tabla se detalla los cálculos efectuados.

Tabla 21. Cálculos horas/hombre

Concepto	Número de horas	Porcentaje
Total horas / hombre año 2018 (13 auditores)	26,208	
Vacaciones del personal	-2,288	9%
Capacitación	-520	2%
Horas disponibles para el plan	23,400	100%
Reserva horas para encargos e imprevistos	-1,248	5%
Total horas para exámenes del plan	22,152	95%

Fuente: Elaboración propia, 2017.

No se consideran las horas de la vicepresidencia, ya que estas están dedicadas a labores de supervisión y dirección.El plan contempla ejecutar un total de 61 actividades, el cual soportará el proceso integral de auditoría y contribuirá a incrementar su productividad y eficiencia.El plan también considera un tiempo de reserva de horas para atender casos especiales, imprevistos, solicitudes de la dirección general corporativa, directorio y gerencia del banco y las horas de capacitación del personal de auditoría.

1.7 Elaboración del plan anual de auditoría

De acuerdo con lo planteado en nuestra metodología, procederemos a desarrollar nuestro plan de auditoría basada en riesgos, la que será presentada a la SBS para su aprobación. Dicho plan está sustentado en un enfoque integral de los riesgos a los que se encuentra expuesta la IF y, como tal, incorpora la identificación de los procesos clave, el mapa de riesgos, las evaluaciones de riesgos realizadas, la estructura tecnológica y organizativa que soporta el modelo de negocios de la IF y los requerimientos regulatorios.

En cuanto a los requerimientos regulatorios, se identificará aquellas actividades que, según la resolución SBS 11699-2008 - Reglamento de Auditoría Interna, son requeridas por el ente de control externo para ser revisadas y que serán consideradas siempre que estén dentro de nuestro enfoque metodológico presentado, lo que se detalla en el anexo 5.

En concordancia con su misión y alcance del trabajo, el accionar de auditoría interna en el horizonte de un año se ha plasmado en el plan. Asimismo, el plan establece los periodos en que se realizarán los trabajos de auditoría y los recursos que demandan su ejecución. Debemos tener en cuenta que las actividades desde la N° 38 a la N° 46 no se encuentran incluidas dentro de la matriz de priorización y, debido a su naturaleza regulatoria, están enfocadas en el monitoreo, la evaluación y la planificación del plan de auditoría y al aseguramiento de la calidad.

Gráfico 9. Actividades del plan anual de auditoria

CRONOGRAMA DE ACTIVIDADES AÑO 2018

N°	Descripción de la Actividad	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	N° de Informes
1-3	Clasificación cuatrimestral de la cartera crediticia no minorista	←	→	→	→	←	→	→	←	→	→	→		3
4	Préstamos comerciales	←	→	→	→									1
5	Préstamos hipotecarios	←	→	→	→									1
6	Leasing y *lease back*	←	→	→	→									1
7	Financiamiento comercio exterior	←	→	→	→									1
8	Tarjeta de crédito								←	→	→	→		1
9	Avance inmobiliario				←	→	→	→						1
10	Préstamos libre disponibilidad	←	→	→	→									1
11	Conciliación y control de cuentas por cobrar, pagar y operaciones en trámite								←	→	→	→		1
12	Recuperación de créditos								←	→	→	→		1
13	Formulación y aprobación de castigos y créditos	←	→	→	→									1
14	Administración del archivo general				←	→	→	→						1
15	Registro contable de las colocaciones, provisiones, intereses y comisiones				←	→	→	→						1
16	Administración de procesos judiciales y arbitrales				←	→	→	→						1
17	Gestión de riesgo crediticio								←	→	→	→		1
18	Lotes contables	←	→	→										1
19	Red de oficinas	←	→	→	→	→	→	→	→	→	→	→		1
20	Riesgo de liquidez								←	→	→	→		1
21	Cartera de inversiones				←	→	→	→						1

CRONOGRAMA DE ACTIVIDADES AÑO 2018

N°	Descripción de la Actividad	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre	N° de Informes
24	Formulación, ejecución y seguimiento del cumplimiento normativo	←	—	→										1
25	Gestión de cumplimiento PLAFT				←	—	—	→						1
26	Gestión del riesgo operacional								←	—	—	→		1
27	Gestión de seguridad de la información				←	—	—	→						1
28	Soporte de usuarios	←	—	→										1
29	Sistema AS\400: administración y seguridad				←	—	—	→						1
30	Sistema de operaciones en la red de oficinas	←	—	→										1
31	LBTR – Sistema para transferencias al BCRP									←	—	→		1
32	Seguridad en el computador central								←	—	—	→		1
33	Gestión de cambios en los sistemas informáticos	←	—	→										1
34	Administración de accesos y perfiles lógicos				←	—	—	→						1
35	Banca por internet	←	—	→										1
36	Transparencia de información a clientes				←	—	—	→						1
37	Atención de reclamos de clientes				←	—	—	→						1
38 - 41	Seguimiento trimestral de recomendaciones	←	—	→	←	—	—	→	←	—	—	→		4
42 - 44	Evaluación del plan 2018 de auditoria	←	—	→	←	—	—	→	←	—	—	→		3
45	Plan de auditoria interna correspondiente al 2019								←	—	—	→		1
46	Programa de aseguramiento de la calidad de la función de auditoria interna	←	—	—	—	—	—	—	—	—	—	→		1
														46

Fuente: Elaboración propia, 2017.

Capítulo IV. Análisis de resultados y hallazgos

Históricamente, la evaluación del riesgo de auditoría interna se ha centrado principalmente en los objetivos de cumplimiento, financieros y operativos del negocio. Los objetivos estratégicos no se consideraban tradicionalmente en las actividades de evaluación de riesgos, probablemente porque se trataba de un área considerada de gestión de nivel superior y porque no había orientación profesional sobre el tema.

Actualmente, existe una oportunidad significativa para mejorar la proposición de valor de auditoría interna con respecto de la consideración de áreas de interés estratégico. Es por ello que nuestro trabajo de investigación está tomando este enfoque, el cual apoyará al Banco Altas Cumbres a capitalizar sus prioridades bajo el esquema de riesgos de unidades auditables y factores de riesgo, desde una perspectiva de crecimiento empresarial y competitivo de largo plazo.

Debemos indicar que, como parte dellevantamiento de información, la cual se obtuvomediante la aplicación dediversas encuestas a destacados profesionales de las principales instituciones financieras del ámbito local(ver las preguntas abiertas en el anexo 6),todos llegaron a la conclusión de que noexiste una forma correcta o incorrecta para seleccionar riesgos clave;lo más importante es tener claro el alcance y el enfoque para las pruebas de aseguramiento basadas en el riesgo clave para los objetivos. Asimismo, indicaron que contar con una metodología basada en riesgos les permite definir puntos críticos, objetivos específicos de auditoria y agregar un mayor nivel de aseguramiento a las metas trazadas por la institución financiera. Sobre este último punto se nos indicó que contar con un mapa de aseguramiento brindará la posibilidad de utilizar los recursos de las distintas áreas de control interno de una manera eficiente y sin caer en reprocesos y sobrecostos.

1. Autorización asociada al plan

Las empresas que cuenten con prácticas sólidas de auditoría interna y un adecuado cumplimiento de los criterios previstos en el citado reglamento podrán solicitar autorización a la Superintendencia de Banca, Seguros y AFP (SBS) para que, en la formulación de su plan anual, se consideren solo las actividades programadas que seanrelevantes, según la propia metodología de auditoría basada en riesgos implementada en la empresa.La SBS toma en consideración lo siguiente, para efectuar la evaluación de la autorización:

- Metodología para la elaboración del plan
- Adecuada asignación de recursos
- Cumplimiento de normas internacionales (IAI)

Las entidades que tienen autorización para utilizar el plan ABR lo pueden dejar de considerar para actividades que, de otro modo, serían obligatorias.

Para solicitar la autorización delente regulador, se deberá presentar lo siguiente:

- Solicitud realizada por el auditor interno o el comité de auditoría
- Descripción del enfoque de auditoría basada en riesgos y la metodología asociada
- Relación de recursos humanos y técnicos existentes
- Autoevaluación realizada por el auditor interno sobre el grado de cumplimiento de las normas internacionales para el ejercicio de la auditoría interna.

Se incluye el Texto Único de Procedimientos Administrativos (TUPA) N° 117, autorización para presentar el plan de trabajo de auditoría basado en riesgos (PBR) aprobado por la SBS, como parte del anexo 8.

Conclusiones y recomendaciones

1. Conclusiones

- La elaboración de un PABR ayuda a fortalecer las relaciones con los *stakeholders*, proporcionando un marco de referencia mediante las evaluaciones de las diferentes actividades, las que se enfocarán en generar valor agregado para la IF y ayudar al logro de los objetivos estratégicos.
- La función de auditoría interna con el PABR busca mejorar su propuesta de valor para las partes interesadas, integrando la metodología basada en riesgo en toda la institución.
- En el caso de la IF, cuyo plan de auditoría actualmente incluye más del 60% de actividades regulatorias, con esta metodología basada en riesgos se enfocara en los procesos clave del negocio, lo cual contribuye al logro de los objetivos de la IF, asimismo se lograra un mayor nivel de aseguramiento al contar con un enfoque sistémico de los riesgos relacionados con los procesos.
- La elaboración y documentación de un PABR debe contar con el respaldo del directorio y la alta gerencia de la IF, pues de esta manera la IF podrá evaluar cíclicamente las actividades más significativas y priorizarlas, haciendo un uso más eficiente de sus recursos, y contribuir al logro de los objetivos estratégicos del negocio y, en paralelo, evaluar con menor frecuencia aquellas actividades que representen un riesgo bajo o que no hayan sufrido mayores cambios.Así, la unidad de auditoría interna reforzará su rol como socio estratégico del negocio y consolidará la confianza en la actividad que realiza de las partes interesadas.

2. Recomendaciones

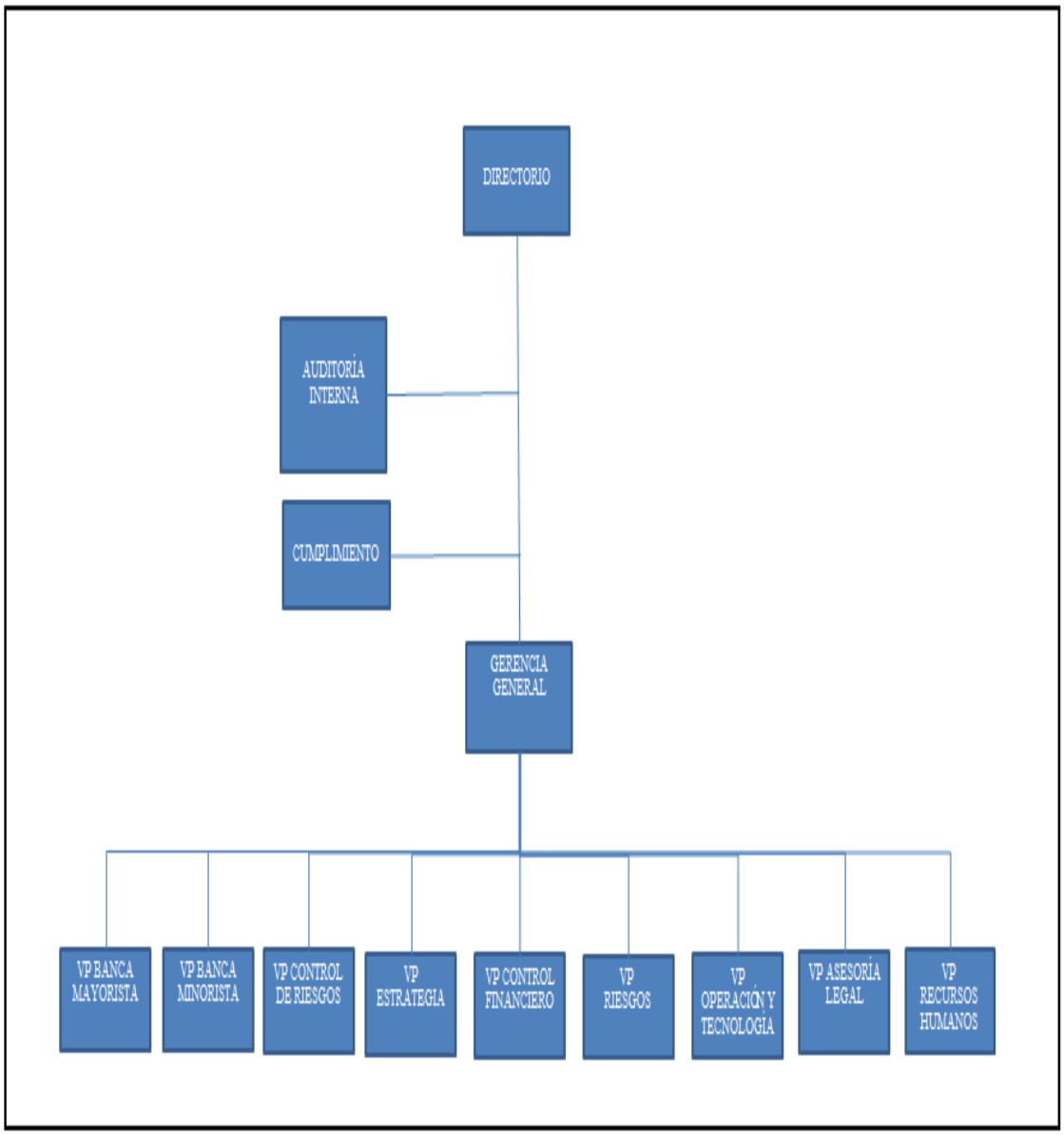
- Iniciar la implementación, la elaboración y la documentación de la metodología, según plan de auditoría basado en riesgos, de acuerdo con elmodelo propuesto, con enfoque en los riesgos clave de la IF, que agrega valor, con el respaldo del directorio y la alta gerencia.
- Elaborar el mapa de aseguramiento para el Banco Altas Cumbres, con la finalidad de determinar el nivel de aseguramiento que ofrecen las distintas unidades de la IF, así como el nivel de alcance que tienen sus revisiones, a efectos de no duplicar esfuerzos, lo cual ayudará al área de auditoría interna a centrarse específicamente en procesos críticos que no cuentan con aseguramiento de otra línea de defensa.

Bibliografía

- PwC. “Enterprise Risk Management – Integrating with Strategy and Performance”.*COSO*, 01/06/2017, Fecha de Consulta: 15/12/2017. Disponible en: < *https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf* >.
- COSO (2013). *Internal Control Integrated Framework*. USA.
- Hernández Sampieri, Fernández Collado, Baptista Lucio (2014). *Metodología de la investigación*. (McGraw-Hill / Interamericana Editores),6ta edición.
- Banco Interamericano de Finanzas (2017). “*Memoria Anual*”
- Banco Interamericano de Finanzas (2016). “*Memoria Anual*”
- Marks, Norman (2015). “El director de auditoría eficaz”. “*Internal Audit Magazine*”, Número 73, p 56-63.
- Rick A. Wright Jr. Cia.(2013) “*The Internal Auditor’s Guide to Risk Assessment*” (The IIA Research Foundation)
- Superintendencia de Banca, Seguros y AFP (2008), “*Resolución SBS N°11699-2008-Reglamento de Auditoría Interna*”. Perú.
- Superintendencia de Banca, Seguros y AFP (2008), “*Resolución SBS N° 272-2017- Reglamento de Gobierno Corporativo y de la Gestión Integral de Riesgos*”. Perú.
- The Institute of Internal Auditors (2017). “*International Professional Practices Framework (IPPF)*”. The Institute of Internal Auditors Research Foundation, Florida.
- Villanueva Chang, Juan. “Actualización COSO ERM - Gestión del Riesgo Empresarial: Alineación del Riesgo con la Estrategia y el Rendimiento”. *AUDITOOL*,Fecha de consulta: 15/12/2017. Disponible en: <*https://www.auditool.org/blog/control-interno/4340-actualizacion-coso-erm-gestion-del-riesgo-empresarial-alineacion-del-riesgo-con-la-estrategia-y-el-rendimiento>*

Anexos

Anexo 1. Organigramade auditoría interna del Banco Alta Cumbres



Fuente: Elaboración propia, 2017

Anexo 2. Autoevaluación efectuada por la unidad de auditoría interna en el 2017

Normas del IIA y directrices de ISACA		Nivel de cumplimiento
Evaluación global		CG
Normas sobre atributos		CG
1000/ISS1001	Propósito, autoridad y responsabilidad	CG
1100/ISS1003	Independencia y objetividad	CG
1200/ISS1005	Aptitud y cuidado profesional	CG
1300/ISS1001	Programa de aseguramiento y mejora de la calidad	CG
Normas sobre desempeño		CG
2000/ISS1001/ISS1002/ISS1003	Administración de la actividad de auditoría interna	CG
2100/ISS1004	Naturaleza del trabajo	CG
2200/ISS1201/ISS1202	Planificación del trabajo	CG
2300/ISS1203/ISS1204	Desempeño del trabajo	CG
2400/ISS1401	Comunicación de resultados	CG
2500/ISS1402	Seguimiento del grado de implementación de los resultados	CG
2600/ISS1402	Comunicación de la aceptación de los riesgos	CG
Código de ética		CG

CG: Cumple generalmente
CP: Cumple parcialmente
NC: No cumple
NA: No aplica

Fuente: Elaboración propia, 2017

Normas del IIA y Directrices de ISACA		Nivel de Cumplimiento		
		CG	CP	NC
Normas sobre Atributos		X		
1000/S1	**Propósito, Autoridad y Responsabilidad**	X		
1010	Reconocimiento de los elementos obligatorios en el estatuto	X		
1000/S2	**Independencia y Objetividad**	X		
1110	Independencia dentro de la organización	X		
1111	Interacción directa con el consejo	X		
1120	Objetividad individual	X		
1130	Impedimentos a la independencia u objetividad	X		
1200/S3/S4	**Aptitud y Cuidado Profesional**	X		
1210	Aptitud	X		
1220	Cuidado profesional	X		
1230	Desarrollo profesional continuo	X		
1300/S1	**Programa de Aseguramiento y Mejora de la Calidad**	X		
1310	Requisitos del programa de aseguramiento y mejora de la calidad	X		
1311	Evaluaciones internas	X		
1312	Evaluaciones externas	X		
1320	Informe del programa de aseguramiento y mejora de la calidad	X		
1321	Utilización de 'Cumple con las Normas Internacionales'	X		
1322	Declaración de incumplimiento		N/A	
Normas sobre Desempeño		X		
2000/S5/S13/S16	**Administración de la Actividad de Auditoría Interna**	X		
2010	Planificación	X		
2020	Comunicación y aprobación	X		
2030	Administración de recursos	X		
2040	Políticas y procedimientos	X		
2050	Coordinación y confianza	X		
2060	Informe a la alta dirección y al consejo	X		
2070	Proveedor de servicios externos		N/A	
2100/S10/S11/S15	**Naturaleza del Trabajo**	X		
2110	Gobierno	X		
2120	Gestión de riesgos	X		
2130	Control	X		
2200/S5/S9/S11/S12	**Planificación del Trabajo**	X		
2201	Consideraciones sobre planificación	X		
2210	Objetivos del trabajo	X		
2220	Alcance del trabajo	X		
2230	Asignación de recursos para el trabajo	X		
2240	Programa de trabajo		X	
2300/S6/S14	**Desempeño del trabajo**	X		
2310	Identificación de la información	X		
2320	Análisis y evaluación	X		
2330	Documentación de la información	X		
2340	Supervisión del trabajo		X	
2400/S7	**Comunicación de Resultados**	X		
2410	Criterios para la comunicación	X		
2420	Calidad de la comunicación	X		
2421	Errores y omisiones	X		
2430	Uso de 'Realizado de conformidad con las Normas'	X		
2431	Declaración de incumplimiento de las normas		N/A	
2440	Difusión de resultados	X		
2450	Opiniones globales	X		
2500/S8	**Seguimiento del grado de implementación de los resultados**	X		
2600/S8	**Comunicación de la Aceptación de los Riesgos**	X		
Código de Ética		X		

Fuente: Elaboración propia, 2017

Anexo 3. Ponderación del riesgo inherente para el proceso de gestión de cumplimiento PLAFT

Proceso de negocio	Objetivos del proceso	Evaluación de criticidad del proceso E, A, M, B	Riesgo inherente	Contiene riesgo de fraude S / N	Controles existentes	Eval. Ctrol E, NE, RM	Evaluación total A, M, B	Será auditado Sí / No	Objetivos de la auditoría
Ambiente de Control									
Estructura organizacional gerencia de prevención lavado de activos (GPLA)	Existencia de una adecuada estructura organizacional que permita a la GPLA cumplir con sus objetivos y desarrollar sus actividades de una manera adecuada, facilitando el flujo de la información.	B	Planificación -No exista una comunicación adecuada entre la GPLA y las diferentes áreas del banco. -Inadecuada estructura organizacional para el cumplimiento de objetivos del área.	N	- Estructura organizacional aprobada y actualizada.	E	M	S	Evaluar si la estructura organizacional de la GPLA es apropiada para cumplir con sus actividades. La estructura organizacional debe permitir la separación de las funciones y un flujo de información óptimo.
Comité de prevención de lavado de activos (CPLA)	Contar con un comité de PLA que asista al oficial de cumplimiento en el análisis de operaciones sospechosas, establecimiento de políticas y procedimientos, entre otros de acuerdo con lo establecido por el ente regulador.	M	Planificación Las decisiones tomadas por el comité que no se encuentren documentadas tienen un nivel de impacto alto. Regulatorio Incumplimiento de los requerimientos mínimos establecidos por el ente regulador para la conformación del CPLA.	N	-El CPLA se encuentra conformado por funcionarios de primer nivel de acuerdo con la estructura del banco y se reúne en la periodicidad establecida en su reglamento. -Las funciones del CPLA están formalizadas en la política interna. --Los acuerdos del comité son suscritos en actas. -La GPLA efectúa el seguimiento a los acuerdos establecidos en dicho comité.	E	M	S	Comprobar que se cuente con un CPLA que brinde apoyo al oficial de cumplimiento en temas de PLA, de acuerdo con lo establecido por el ente regulador.
Roles y responsabilidades	Asignar responsabilidades y delegación de facultades para el cumplimiento de los objetivos de la GPLA, documentados en el manual de organización y funciones (MOF).	B	Organización de roles y responsabilidades -Responsabilidades no acordes con las funciones o nivel del empleado o de acuerdo con lo establecido en la regulación. -Imposibilidad de deslindar responsabilidades al no encontrarse actualizadas o documentadas en el MOF o directivas relacionadas.		-El MOF de la GPLA vigente incluye las funciones y responsabilidades del OCC y personal relacionado con dicho proceso. -La regulación externa y la normativa del banco establecen las funciones y las responsabilidades del OCC. -El OCC ha establecido puestos para el personal de la GPLA; sus funciones son distribuidas de acuerdo con el conocimiento y la experiencia del personal.	E	M	S	-Validar que las funciones y las responsabilidades se encuentren formalizadas en el MOF. -Verificar que la descripción de puestos reflejan su posición actual. -Determinar si la asignación de responsabilidades dentro de la unidad/proceso es apropiada y revisada periódicamente por los niveles correspondientes.
Capacitación al personal (PLA)	▪ Contar con programas de capacitación anual de PLA a fin de instruir al personal del banco sobre las normas vigentes, procedimientos establecidos y tipologías de PLA detectadas. ▪ El personal de la GPLA deberá contar con capacitaciones especializadas de acuerdo con lo requerido por el ente regulador.	B	Riesgo operacional -No brindar al personal la capacitación adecuada que le permita conocer y aplicar los controles establecidos para PLA. -Que el personal no pueda identificar operaciones inusuales relacionadas con PLA o clientes de alto riesgo. Riesgo regulatorio -Incumplimiento de los requerimientos del ente regulador, al no realizar programas de capacitación sobre la materia para el personal del banco y la GPLA.	N	-Existe un programa de capacitación anual de PLAFT para el personal de soporte y capacitación especializada para el personal que tiene contacto con el público. -El personal nuevo rinde su capacitación de PLAFT durante los primeros 15 días posteriores a su ingreso. -Los programas de capacitación son revisados y actualizados anualmente por el OCC. -El OCC cuentan con certificaciones internacionales de PLAFT. -El personal de la GPLA tiene capacitaciones anuales especializadas.	E	M	S	-Comprobar que se haya desarrollado programas de capacitación anual con el fin de instruir a su personal sobre las normas vigentes en PLAFT. -Comprobar que el personal nuevo cuente con inducción dentro de los 15 días de haber ingresado al banco. -Comprobar que el personal de la GPLA haya recibido capacitación especializada en PLAFT.
Evaluación de riesgo									
Políticas y procedimientos	Las políticas y procedimientos de PLA deben estar documentados y cubrir los principales riesgos identificados.	M	Riesgo operacional -Falta de políticas y procedimientos que cubran todos los riesgos de PLA. -Que la difusión de las políticas y los procedimientos no sea efectiva.	N	-Existe un manual de PLAFT aprobado por el directorio, que incorpora los requerimientos regulatorios. -El manual de PLAFT es actualizado periódicamente por el OC y difundido al personal a través de la intranet.	E	M	S	-Comprobar que se cuente con políticas y procedimientos que mitiguen el riesgo de PLAFT y que estas se encuentren formalizadas en un manual de PLAFT de acuerdo con lo establecido por la regulación

Proceso de negocio	Objetivos del proceso	Evaluación de criticidad del proceso E, A, M, B	Riesgo inherente	Contiene riesgo de fraude S / N	Controles existentes	Eval. Ctrol E, NE, RM	Evaluación total A, M, B	Será auditado Sí / No	Objetivos de la auditoría
									y sean de conocimiento del personal del banco.
Autoevaluación de riesgos - PLA	Contar con mecanismos que permitan identificar la ocurrencia de eventos que impidan alcanzar los objetivos de la gerencia y del banco.	B	Riesgo de AML/ATF -Inadecuada identificación de riesgos propios de la gerencia de PLA que no permita la implementación de un sistema adecuado de PLA.	N	-Se han establecido procedimientos y un formato estándar para realizar una evaluación anual de los riesgos y los controles relacionados a PLA.	E	M	S	-Comprobar que se realizan autoevaluaciones de PLA y que los planes de acción se ejecutan en los plazos establecidos.
Programa anual de trabajo de PLA	-Que el OC elabore un programa anual de trabajo que establezca la metodología y actividades para las revisiones del nivel de cumplimiento del sistema de PLA.	M	Riesgo reputacional y regulatorio -No contar con una metodología que permita revisar el cumplimiento del sistema de PLA y el detalle de las actividades para su ejecución.	N	-El OC elabora un programa anual de trabajo de PLA, el cual es aprobado por el directorio antes del cierre de cada año. -En los informes regulatorios se comunica el grado de avance del programa anual de trabajo de PLA, el cual es presentado al directorio y al ente regulador.	E	M	S	-Comprobar que el OC haya preparado un programa anual de trabajo de PLA y que este defina sus actividades para asegurar su cumplimiento y avance. -Verificar que el programa sea aprobado por el directorio. -Comprobar que el programa de trabajo anual contemple planes de acción para mitigar los riesgos identificados en las autoevaluaciones de riesgos u observaciones recibidas por el regulador, auditoría externa e interna.
Identificación y evaluación de riesgo	▪ Contar con una evaluación de riesgos de PLA/FT de los negocios críticos.	M	Riesgo operativo No identificar los productos y servicios que se encuentran expuestos al riesgo de PLA, así como la probabilidad de ocurrencia del mismo.	N	-El OC realiza un mapeo de los riesgo de PLA, para identificar los riesgos sobre productos y servicios, clientes y canales en los cuales se desarrollan las actividades del banco, -Cada vez que se crea un producto o servicio en el banco, la unidad de riesgo operativo envía un análisis a la GPLA para su revisión.	E	M	S	-Comprobar que el OC haya cumplido con evaluar el perfil de riesgo de banco y si el proceso de evaluación de riesgos es adecuado.
Actividades de Control									
Clientes de alto riesgo y sujetos obligados	Asegurar que los clientes de alto riesgo sean identificados oportunamente por los funcionarios de negocio y GPLA y se requiera la aplicación de una diligencia debida mejorada para su aceptación como cliente por la gerencia. Así mismo, a los sujetos obligados se les solicita los documentos regulatorios.	A	Riesgo reputacional y de PLA: -La no identificación de clientes y mantener relaciones comerciales con ellos. - Que la relación comercial con clientes de alto riesgo no se encuentre autorizada por los niveles gerenciales correspondientes. -Que no se realice un monitoreo de las operaciones de aquellos clientes que presentan un mayor riesgo debido a la naturaleza de sus negocios.	N	-Existen políticas y procedimientos para la identificación y el tratamiento de clientes de alto riesgo. -Los funcionarios de negocios elaboran un análisis de riesgo del cliente que mantiene negocios de alto riesgo. -La aceptación del cliente de alto riesgo está a cargo del nivel gerencial de la banca correspondiente. -Los clientes de alto riesgo se encuentran marcados en el sistema del banco para la generación de un perfil específico y generación de alertas mensuales. -Anualmente, el OC actualiza los parámetros del perfil de los clientes de alto riesgo en el sistema del banco. -La GPLA cuenta con bases de clientes de alto riesgo identificados, a fin de hacer seguimiento a la evaluación de alto riesgo preparada por el funcionario de negocios.	E	A	S	▪ Verificar que se cumple con las políticas y los procedimientos establecidos para la identificación, la evaluación de clientes alto riesgo y el monitoreo de sus operaciones.

Proceso de negocio	Objetivos del proceso	Evaluación de criticidad del proceso E, A, M, B	Riesgo inherente	Contiene riesgo de fraude S / N	Controles existentes	Eval. Ctrol E, NE, RM	Evaluación total A, M, B	Será auditado Sí / No	Objetivos de la auditoría
Clientes PEP	-Asegurar que los clientes PEP sean identificados oportunamente por los funcionarios de negocios y GPLA y se aplique o se requiera la aplicación de una diligencia debida mejorada o reforzada para su aceptación como cliente por la gerencia.	A	<u>Riesgo reputacional y de PLA:</u> -La no identificación de clientes PEP al inicio de la relación comercial y aplicación de diligencias más rigurosas y mantener relaciones comerciales con ellos. -Que la relación comercial con los PEP no se encuentre autorizada por los niveles gerenciales correspondientes. -Que no se realice un seguimiento de las operaciones de aquellos clientes que presentan un mayor riesgo debido a la naturaleza de sus cargos públicos.	N	-Existen políticas y procedimientos para la identificación y tratamiento de clientes PEP. -La base de PEP es actualizada por la GPLA con base en los nuevos nombramientos de funcionarios públicos emitidos en las normas legales, verificando en el sistema del banco si estos son clientes y mantienen productos con el banco. -A los clientes PEP identificados se les solicita declaración de origen de fondos. -Los funcionarios de negocios elaboran un documento de conocimiento de cliente PEP, el cual es firmado por un primer nivel gerencial comercial, en señal de aceptación como cliente. -La GPLA mantiene un control de los documentos de clientes PEP remitidos por los funcionarios de negocios. -Los clientes PEP se encuentran marcados en el sistema del banco y se le asigna un perfil más restrictivo.	RM	A	S	▪ Comprobar que se cumple con las políticas y procedimientos establecidos para la identificación, la evaluación y el tratamiento de clientes PEP, así como para el monitoreo de sus operaciones.
Filtro con bases negativas	Contar con bases de datos (listas negativas) que permitan identificar clientes que están siendo investigados por delitos de PLA o estén vinculados con personas inmersas.	M	<u>Riesgo reputacional</u> Mantener relaciones con clientes que estén incluidos en las listas negativas. <u>Riesgo PLA</u> No identificar a personas que estén vinculadas al lavado de activos previo al inicio de la relación comercial.	N	-La base de clientes nuevos es cruzada con las listas negativas; las coincidencias son analizadas e informadas a los niveles y entes correspondientes.	E	M	S	Comprobar que se cuenta con políticas y procedimientos para filtrar a los clientes del banco versus listas negativas y, por las coincidencias, aplicar la debida diligencia mejorada.
Registro de operaciones	▪ Mantener un registro de operaciones realizadas por los clientes de acuerdo con lo establecido por el ente regulador.	M	<u>Riesgo regulatorio</u> -No contar con los registros de operaciones. -Que los ROU y ROA no contengan la información mínima requerida por el regulador.	N	-Se cuentan con Registro de Operaciones físicos y virtuales. -La GPLA mantiene acceso a los sistemas del banco para visualizar el Registro de Operaciones. -La GPLA realiza de manera bimensual una revisión aleatoria para asegurar el correcto llenado de los ROU y ROA. -La GPLA realiza un monitoreo de las operaciones acumuladas en el mes. -El registro es guardado por un periodo de 10 años.	E	M	S	-Comprobar que la GPLA efectué la revisión trimestral del correcto llenado de los ROU y ROA por el personal de oficina, así como su adecuado archivo, conservación y disponibilidad.
Análisis de operaciones inusuales	▪ Identificación y evaluación de las operaciones inusuales de los clientes que excedan el perfil asignado.	B	<u>Riesgo de LA</u> -Inadecuada identificación de operaciones inusuales que pueden resultar posiblemente sospechosas. -No contar con la suficiente información o documentación que evidencia el análisis realizado. <u>Riesgo regulatorio</u> Sanciones del ente regulador por incumplimiento	N	-El sistema del banco establece perfiles a los clientes según el segmento al que pertenece y el tipo de personería, emitiendo alertas a clientes que exceden el perfil asignado. -Las alertas son evaluadas por la GPLA y en caso sea necesario son remitidas a los funcionarios de negocio para su calificación, según la política de conocimiento del cliente. -Se realiza un seguimiento de las alertas enviadas a los funcionarios de negocios y las que son informadas como inusuales son analizadas por la GPLA. -El análisis realizado es documentado en el sistema y se decide si el caso es cerrado, elevado al CPLA o rechazado. -En caso los funcionarios de negocio no remitan la información requerida por la GPLA, dichos incumplimientos son comunicados a las gerencias respectivas.	E	M	S	-Comprobar que el proceso de identificación de operaciones relevantes, inusuales sean efectivos y quede documentada la labor de seguimiento y el análisis realizado por la GPLA.

Proceso de negocio	Objetivos del proceso	Evaluación de criticidad del proceso E, A, M, B	Riesgo inherente	Contiene riesgo de fraude S / N	Controles existentes	Eval. Ctrol E, NE, RM	Evaluación total A, M, B	Será auditado Sí / No	Objetivos de la auditoría
Información y comunicación									
Reporte de transacciones sospechosas	Cumplir con reportar al ente de control las operaciones inusuales consideradas como sospechosas en un plazo no mayor a los 30 días de haberlas identificado, de acuerdo con lo establecido por el regulador, dejando evidencia del análisis y la evaluación realizada por el OC.	B	Riesgo regulatorio No reportar oportunamente las operaciones sospechosas puede derivar en sanciones por parte de los entes reguladores. Riesgo reputacional Procesos judiciales contra los representantes y funcionarios del banco por no comunicar oportunamente las operaciones sospechosas.	N	-Existen procedimientos y mecanismos a través de los cuales el OC evalúa y analiza las operaciones presuntamente sospechosas, las cuales son informadas al comité PLA para su evaluación y, de ser el caso, reportarlas a la UIF. -El análisis realizado por el OC para la determinación de una operación sospechosa es documentado y custodiado por el OC.	E	M	S	-Comprobar que el análisis de las operaciones sospechosas por el OC sea documentado y reportado a la UIF en forma oportuna y de acuerdo con lo establecido por la regulación.
Monitoreo									
Supervisión de actividades	-Garantizar que las actividades clave del proceso se ejecutan correctamente por el personal de la GPLA.	B	Riesgo de PLA No identificar deficiencias en los controles incrementa el riesgo de lavado de activos.	N	-El OC supervisa el cumplimiento del sistema de PLAFT de acuerdo con elprograma anual. -El OC mantiene una supervisión constante de las labores realizadas por el personal de la GPLA y monitorea que los funcionarios de negocio realicen la calificación de las operaciones inusuales.	E	M	S	-Comprobar si durante el desarrollo de las operaciones se realizan actividades regulares de supervisión, a fin de identificar el adecuado funcionamiento del control interno.
Monitoreo de acuerdos del comité de PLA	-Garantizar el cumplimiento de los acuerdos tomados por el comité de PLA	B	Riesgo regulatorio Sanciones del ente regulador por incumplimiento de la legislación vigente de lavado de activos.	N	-La GPLA realiza un seguimiento del cumplimiento de los acuerdos de comité.	E	M	S	-Comprobar que se dé cumplimiento a los acuerdos tomados en el comité de PLA.

Fuente: Elaboración propia, 2017

Anexo 4. Mapa de aseguramiento del Banco Altas Cumbres

Macroprocesos	Proceso	Riesgo inherente	Riesgo residual	Alcance	Proveedor de aseguramiento	Cobertura de aseguramiento
Productos activos	Préstamos hipotecarios	Extremo	Medio	- Verificación del seguimiento de la vigencia de los seguros de desgravamen, lo cual podría perjudicar la recuperación del crédito. - Verificación de los pagos de las pólizas externas (endosadas) del bien o desgravamen.	- Riesgo operacional	Medio
	Tarjeta de crédito	Alto	Medio	- Validación de fraudes internos por emisiones en tarjetas de crédito sin propuesta de crédito (persona natural y persona jurídica). - Validación de fraudes externos por disposición en efectivo por ventanilla de clientes foráneos con órdenes de pago (*voucher*), consignadas inadecuadamente.	- Riesgo operacional	Medio
	Factoring	Alto	Medio	- Validación de supervisión en la recepción de facturas o letras en descuento y que estas no se encuentren inhabilitadas o sean de diferente moneda para ejecutarlas judicialmente ante el no pago de obligaciones del cliente. - Revisión de los pagarés desembolsados, así como también la revisión de los cronogramas de pagos. - Revisión del ambiente de custodia de los títulos valor. - Revisión de las entregas de aviso de vencimiento de letra por vencer.	- Riesgo operacional	Medio

Macroprocesos	Proceso	Riesgo inherente	Riesgo residual	Alcance	Proveedor de aseguramiento	Cobertura de aseguramiento
Gestión de recursos humanos	Reclutamiento, selección e incorporación	Medio	Bajo	- Validación de requisitos para la selección del personal (domiciliarias, crediticias, laborales, penales, judiciales, policiales, SBS). - Validación de requisitos en sus datos académicos. Nota: incluye fallas en los proveedores de servicios.	- Riesgo operacional	Alta
	Formación y capacitación	Medio	Bajo	-Validación de capacitaciones al personal de caja (JOS y RCS) relacionados con las transacciones en ventanilla. - Validación del número de asistentes exigidos por el regulador a las capacitaciones dictadas por la IF.	- Riesgo operacional	Alta
	Compensación del colaborador	Medio	Bajo	- Seguimiento a la cantidad de horas prestadas por el proveedor. - Registro de todos los documentos inherentes a la relación laboral (RIT, código de conducta, ficha de datos). - Cambios en la legislación laboral referidas a la jornada de trabajo y a la protección al trabajador (personas con discapacidad, contratos con extranjeros).	- Riesgo operacional	Alta
Gestión de tecnología de información	Soporte de usuarios	Medio	Bajo	- Auditoría aplicativos - licenciamiento de software - Análisis y aprehensión de los aplicativos.	- Seguridad de la información - Auditoría de TI	Alta
	Desarrollo de aplicativos	Medio	Bajo	- Identificar los procedimientos de carga que se realizan por medio de *interface* o *batch* a los sistemas de información y validar por medio de una muestra a uno de los procedimientos de *interface*, la integridad y confiabilidad de la información.	- Seguridad de la información - Auditoría de TI	Alta
	Administración de infraestructura tecnológica	Medio	Bajo	- Para el proceso de administración de la infraestructura de TI de la unidad de tecnología e informática se revisará lo relacionado con el proceso COBIT versión 4.1 lo siguiente: determinar la dirección tecnológica, en lo relacionado con el plan de infraestructura tecnológica, proceso de monitoreo de la infraestructura de TI;la continuidad del negocio y la seguridad no serán exhaustivas en esta auditoría, por tratarse de temas independientes que requieren ser tratados de manera exclusiva en una auditoría.	- Seguridad de la información - Auditoria de TI	Alta
Gestión de recuperaciones	Adjudicación de bienes	Alto	Bajo	- Validación de la documentación de las prendas a ejecutar. - Validación que los bienes a adjudicar de la IF estén sujetos a robos y no estén asegurados.	- Riesgo operacional	Alta

Fuente: Elaboración propia, 2017

Anexo 5. Puntuación de requerimientos regulatorios

No.	Actividad
1-3	Clasificación cuatrimestral de la cartera crediticia no minorista (3 actividades)
4	Revisión anual de la clasificación de la cartera minorista
5	Riesgo cambiario crediticio
6	Riesgo de sobreendeudamiento de deudores minoristas
7	Contratos de financiamiento con garantía de cartera crediticia
8	Transferencia y adquisición de cartera crediticia
9	Riesgo de liquidez
10	Riesgo de tasa de interés
11	Administración del riesgo cambiario
12	Cartera de inversiones
13	Instrumentos financieros derivados
14	Administración del riesgo país
15	Sistema de prevención de lavado de activos
16	Reglamento de transparencia de información a clientes
17	Atención de reclamos de clientes
18	Reglamento de gestión de riesgo social y ambiental
19	Registro contable de las colocaciones, provisiones, intereses y comisiones
20	bienes adjudicados y recuperados
21	Gestión integral de riesgos
22	Administración de los riesgos de operación y tecnológicos
23	Normas sobre vinculación y grupo económico
24	Límites legales de las empresas bancarias
25	Asignación de capital por riesgo, apalancamiento y patrimonio
26	Reglamento de cuentas corrientes
27	Evaluación de la función de cumplimiento normativo
28	Programa de aseguramiento de la calidad de la función de auditoría interna
29-31	Evaluación cuatrimestral del avance del plan 2018 de auditoría interna (3 actividades)
32	Plan de auditoría interna correspondiente al próximo año
33-36	Seguimiento trimestral de recomendaciones (4 actividades)

Fuente: Elaboración propia, 2017

Anexo 6. Entrevista a expertos de auditoría interna

Entrevistas abiertas a expertos sobre plan anual de auditoría interna

1. ¿Considera Ud. que el plan anual de auditoría debe elaborarse con un enfoque basado en riesgos? Explique porqué.

   Sí, los planes de auditoria de las empresas del sistema financiero deben ser elaborados bajo unenfoque de riesgos que les permita evaluar de una manera más eficiente y con un enfoque integral los procesos de la empresa, identificando procesos críticos, riesgos asociados y sistemas de control, de tal manera que estos sean evaluados y se pueda generar valor a la organización.

2. ¿Considera que la gestión de auditoría en el sistema financiero peruano ya se encuentra alineado conlos parámetros de una auditoría basada en riesgos?

   Sí, la mayoría de las empresas privadas del sistema financiero ya incorpora los riesgos como buena práctica y como parte de su evaluación para un mejor resultado de sus objetivos.

3. ¿Cuál considera que es el impacto del cambio de una auditoría de cumplimiento a una auditoría basada en riesgo?

   El impacto es sustancial, teniendo en cuenta que la auditoría basada en riesgos ve a la empresa en su conjunto, bajo un enfoque integral. Es así como se identifican los procesos clave materiales para la empresa y se debe asegurar que los riesgos estén siendo identificados y los sistemas de control que presenten seanadecuados, en comparación con la auditoria de cumplimiento, la cual solo evalúa el cumplimiento de determinada normatividad específica, sin considerar el enfoque integral antes mencionado.

4. ¿Cuál es su apreciación respecto de la metodología presentada?

   La metodología presentada bajo el enfoque basado en riesgos va a generar mucho valor al ser implementada en la organización.Esto debido a que para su elaboración se ha considerado aspectos relevantes de toda la organización,identificando los lineamientos adecuados para priorizar las actividades que serán evaluadas en el plan anual de auditoria y que estas sean lasde importancia alta para la empresa, las cuales generarán valor para el cumplimiento de los objetivos organizacionales.

Anexo 7. Reseña de los expertos entrevistados

Ricardo Izaguirre – Auditor general

Ejecutivo con 35 años de experiencia en auditoría en el sistema financiero. Actualmente es Auditor General de Banco Interamericano de Finanzas S.A.A. Fue auditor delBanco Internacional del Perú SAA.Contador Público, graduado en la Universidad Inca Garcilaso de la Vega, con estudios de Economía en la Pontificia Universidad Católica del Perú.

Guillermo Zegarra – Auditor general Pacífico Seguros

Ejecutivo con 25 años de experiencia laboral nacional e internacional en el sector bancario y de seguros.Posee un MBA otorgado por la Pontificia Universidad Católica del Perú - Escuela de Negocios CENTRUM Católica. Es el actual presidente de ISACA Perú y se viene desempeñando como Gerente de Auditoría en Pacífico Seguros.Contador Público, graduado en la Universidad San Martin de Porres.

Anexo 8. Texto único de procedimientos administrativos

TEXTO ÚNICO DE PROCEDIMIENTOS ADMINISTRATIVOS - TUPA												
N° de orden	DENOMINACIÓN DEL PROCEDIMIENTO	REQUISITOS		DERECHO DE TRAMITACIÓN (*)		CALIFICACIÓN			PLAZO PARA RESOLVER (en días hábiles)	INICIO DEL PROCEDIMIENTO	AUTORIDAD COMPETENTE PARA RESOLVER	INSTANCIAS DE RESOLUCIÓN DE RECURSOS	
		Número y Denominación	Formulario / código / Ubicación	(en % UIT)	(en S/.)	Auto-mático	Evaluación Previa					RECONSI-DERACIÓN	APELACIÓN
							Posi-tivo	Nega tivo					
117	**Autorización para presentar el Plan de Trabajo de Auditoría basado en riesgos (PBR)** Tercera Disposición Final del Reglamento de Auditoría Interna aprobado por Resolución SBS N° 11699 -2008.	Las empresas que cuenten con prácticas sólidas de auditoría interna y un adecuado cumplimiento de los criterios previstos en el citado reglamento podrán solicitar autorización a la Superintendencia para que en la formulación de su plan anual se consideren sólo las actividades previstas en el anexo "Actividades Programadas" que resulten relevantes según la propia metodología de auditoría basada en riesgos implementada por la empresa, salvo los aspectos contemplados en el artículo 19° del Reglamento. Para ello, las empresas deberán presentar las solicitudes de autorización, cuando menos 60 días calendarios antes de la presentación de su plan anual, para lo cual deben adjuntar la documentación siguiente: a) Solicitud realizada por el auditor interno o comité de auditoría b) Descripción del enfoque de auditoría basada en riesgos y metodología asociada. c) Relación de recursos humanos y técnicos existentes, así como políticas relacionadas de contratación. d) Autoevaluación realizada por el auditor interno sobre el grado de cumplimiento de las "Normas Internacionales para el Ejercicio de la Auditoría Interna" según el Instituto de Auditores Internos (IIA), y las medidas que tomará con relación a los casos en que existiera una desviación importante.						X	30 (Treinta días calendario)	Mesa de Partes de la SBS Av. 2 de Mayo 1511 San Isidro	Superintendente Adjunto de Banca y Microfinanzas/ Superintendente Adjunto de Seguros/ Superintendente Adjunto de Adminis-tradoras Privadas de Fondos de Pensiones	Recursos de Reconsideración conforme al procedimiento Nº 72	Recursos de Apelación conforme al procedimiento Nº 72
Notas para el ciudadano:													
Modificacion aprobada por Res. SBS N° 5829-2014 del 05 de setiembre del 2014.													

Fuente: portal web www.sbs.gob.pe

Nota biográfica

Ana Pachamango Rodríguez

Nació en Trujillo en 1977. Es titulada en ingeniería de computación y sistemas por la Universidad Privada Antenor Orrego y cuenta con cursos de especialización en social CRM en ESAN y gestión de proyectos en CENTRUM Católica. Con doce años de experiencia como gestora de proyectos en el rubro de banca y finanzas, actualmente es especialista de tecnología de información en Scotiabank Perú.

Roxana Pacheco Rojas

Nació en Lima en 1979.Es titulada enadministración de empresas porla Universidad San Martín de Porres y cuenta con especializaciones en control interno y gestión de riesgo en la Universidad de Lima.Tiene diez años de experiencia en auditoría interna y se ha desempeñado en empresas del rubro. Actualmente es auditora *senior* en el Banco Interamericano de Finanzas.

Giomar Ruiz Tinco

Nació en Lima en 1988.Es ingeniero informático por la Pontificia Universidad Católica del Perú y cuenta con una especialización en ley de protección de datos personales, por la Pontificia Universidad Católica del Perú, y una especialización en finanzas por la Universidad Nacional de Ingeniería. Cuenta con siete años de experiencia en gestión de riesgos, habiendo participado en la creación de dos compañías de seguros en el Perú, Crecer Seguros (Grupo Pichincha) y Coface Seguro de Crédito Perú, desempeñándose como gerente de riesgos en esta última empresa. Actualmente lidera el área de seguridad de la información en la red de clínicas SANNA.