



**“IMPLEMENTACIÓN DE UN PROGRAMA CRÍTICO
ANTIFRAUDE EN LA COMPAÑÍA RIMAC INTERNACIONAL”**

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

Presentado por

Margiori Natalia Massenza Dolci Bonilla
Shirley Ledda Villacorta Aristondo

Asesor: José Díaz Ismodes
[0000-0001-9216-4974](tel:0000-0001-9216-4974)

Lima, Febrero 2012

Agradecimiento

Este trabajo es el resultado de un esfuerzo en el que participaron muchas personas que nos apoyaron leyendo, opinando, guiando, dando ánimo y acompañándonos en los momentos de crisis y en los de tranquilidad.

Un especial agradecimiento al Sr. Óscar Caipo Guerrero por brindarnos la oportunidad de contar con una plataforma profesional tan valiosa como es la Maestría en Auditoría, experiencia que nos permitió re-definir nuestro concepto de la profesión y potenciar nuestro rol como auditores internos.

Así mismo, dedicamos este trabajo a nuestra querida Abigail Ibañez, que nos centró, enfocó y apoyó en el inicio de este proceso; mil gracias Abi.

Finalmente, agradecemos a Dios y a la Divina Providencia por permitirnos crecer en lo personal y lo profesional a través de este proyecto.

Resumen Ejecutivo

El objetivo principal de esta tesis es exponer el valor y los beneficios que la implementación de un Programa Crítico Antifraude (PCA) aportará a la Compañía Peruana de Seguros Rímac Internacional en los ámbitos de gobierno corporativo, control interno, gestión de riesgos y monitoreo continuo; así como su contribución al fortalecimiento de los procesos de negocio.

El trabajo de investigación explicará los componentes necesarios para la implementación del Programa Crítico Antifraude como una herramienta estratégica para la prevención, identificación y detección de riesgos de fraudes; y evidenciará sus beneficios mediante un análisis de costos-beneficio respecto a la prevención de ocurrencia del fraude y el ahorro de costos. Este programa además sustenta su continuidad, basado en un análisis de riesgos y actividades de monitoreo.

Consideramos que la motivación de este estudio va encaminada no sólo a la implementación de un esquema antifraude para la empresa Rímac Internacional, sino que, además, será un programa de referencia para las empresas del mercado asegurador peruano.

ÍNDICE

Agradecimiento.....	II
Resumen Ejecutivo.....	IV
 CAPÍTULO I INTRODUCCIÓN.....	 2
 CAPÍTULO II MARCO TEÓRICO.....	 4
2.1 Definiciones Generales.....	4
2.1.1 Definición del fraude.....	4
2.1.1.1 Definición del fraude ocupacional.....	5
2.1.1.2 Definición del fraude en el mercado asegurador.....	6
2.1.2 Móviles para la comisión del fraude.....	7
2.1.2.1 El Triángulo del Fraude.....	7
FIGURA 2.1.....	9
2.1.2.2 El Diamante del Fraude.....	9
2.1.3 Clasificación del Fraude.....	10
2.1.3.1 Fraude Interno.....	10
FIGURA 2.2.....	10
TABLA 2.1.....	12
2.1.3.2 Fraude Externo.....	12
2.2 Marco de Referencia para la Gestión del Riesgo de Fraude.....	13
2.2.1 Gobierno del Riesgo de Fraude.....	13
2.2.1.1 Roles y Responsabilidades.....	14
2.2.1.2 Elementos clave para un efectivo Programa Crítico Antifraude.....	16
2.2.2 Evaluación del Riesgo del Fraude.....	19
2.2.3 Prevención del Fraude.....	19
TABLA 2.2.....	20
2.2.4 Detección del Fraude.....	20
2.2.5 Investigación del Fraude y Acciones Correctivas.....	21

2.3	Herramientas	22
2.3.1	Esquemas de Reporte	22
2.3.2	Herramientas para el análisis de información	23
2.4	El costo del fraude	23
TABLA 2.4		24
2.5	Programa Crítico Antifraude	25

CAPÍTULO III ANÁLISIS DE LA GESTIÓN DEL RIESGO DE FRAUDE EN SUDAMÉRICA Y EL SECTOR ASEGURADOR PERUANO26

3.1	Gestión del Fraude en Sudamérica	26
TABLA 3.1		27
3.2	Gestión del fraude en seguros	28
3.3	Gestión del riesgo de fraude en el sector asegurador peruano	29
TABLA 3.2		29
3.3.1	Prevención de Lavado de Activos	30
3.3.2	Principios de Buen Gobierno Corporativo	30

CAPÍTULO IV DIAGNÓSTICO DE LA GESTIÓN DEL FRAUDE EN RÍMAC INTERNACIONAL COMPAÑÍA DE SEGUROS Y REASEGUROS30

4.1	Descripción de la compañía:.....	31
4.1.1	Organización Interna:.....	31
FIGURA 4.1		31
4.1.2	Gobierno Corporativo.....	31
4.1.3	Marco Normativo.....	31
4.1.4	Control Interno	32
TABLA 4.2		32
4.2	Gestión del Fraude en Rímac Internacional:.....	33
4.2.1	La Gestión del fraude desde la perspectiva de cumplimiento regulatorio	33

4.2.2	Actividades de supervisión para la gestión del fraude	34
	TABLA 4.3	34
4.3	Principales tipos y modalidades de fraude.....	35
4.3.1	Tipificación.....	35
4.3.1.1	Por procedencia del fraude.....	36
4.3.1.2	Por tipo de dolo.....	36
4.3.1.3	Inherentes a las actividades de seguros.....	37
4.4	Análisis de Brechas para la implementación de un Programa Crítico Antifraude en Rímac Internacional	37
4.4.1	Análisis del Gobierno sobre la Gestión del Fraude	38
	TABLA 4.4	38
4.4.1.1	Roles y Responsabilidades.....	38
4.4.1.2	Elementos Claves.....	39
4.4.2	Evaluación del Riesgo de Fraude	39
	TABLA 4.5	39
4.4.3	Prevención del Fraude.....	40
4.4.4	Detección del Fraude:.....	41
4.4.5	Investigación del Fraude y Acciones Correctivas.....	42
CAPÍTULO V PROPUESTA DE PROGRAMA CRÍTICO ANTIFRAUDE		
EN LA COMPAÑÍA RÍMAC INTERNACIONAL.....		
5.1	Nombre, descripción y objetivos del Programa Crítico Antifraude	43
5.2	Alcance del Programa.....	44
5.3	Beneficios propuestos de la implementación:.....	44
5.4	Al Gobierno Corporativo	44
5.4.1	Al Control Interno.....	44
5.4.2	La Gestión de Riesgos.....	45
5.4.3	Las actividades de monitoreo continuo y supervisión	45
5.5	Diseño del Programa	45

CAPÍTULO VI ANÁLISIS COSTO BENEFICIO DE LA IMPLEMENTACIÓN DEL PROGRAMA CRÍTICO ANTIFRAUDE.....	47
6.1 Recuperación de la Inversión:	48
6.2 Trascendencia de la implementación del Programa Crítico Antifraude en Rímac Internacional:.....	48
Conclusiones y Recomendaciones.....	50
BIBLIOGRAFÍA.....	51
ANEXO I – Glosario de Términos del Sector Asegurador	58
ANEXO II – Matriz de Decisión sobre el Fraude.....	61
ANEXO III – Proceso de Investigación para el Fraude	62
ANEXO IV – Principios de Bueno Gobierno Corporativo en el Perú	63
ANEXO V – Mapa de madurez para la evaluación de componentes del PCA	68
ANEXO VI – Nivel de Madurez respecto a los Elementos Clave del PCA	70
ANEXO VII – Análisis de Brecha respecto a los Roles y Responsabilidades sobre la Gestión del Fraude	74
ANEXO VIII – Análisis de Brecha respecto al cumplimiento de los Elementos Claves para la implementación de un efectivo Programa Antifraude	77
ANEXO IX - Análisis de Brecha respecto al cumplimiento de los Elementos Claves para la implementación de un efectivo Programa Antifraude	81
ANEXO X Análisis de Brecha – Controles Preventivos	83
ANEXO XI – Evaluación del Riesgo de Fraude al Proceso de Gestión de TI y Seguridad de la Información.....	85
ANEXO XII Cronograma – Definición de Planes de Acción	88
ANEXO XIII - Encuesta sobre el Valor de la Implementación de un PCA	90
ANEXO XIV Tabulación de Encuestas sobre el Valor de la Implementación de un PCA	
91	
ANEXO XV Matriz de Evaluación de Riesgos	93
NOTA BIOGRÁFICA	95

CAPÍTULO I INTRODUCCIÓN

Históricamente y a nivel mundial, la comisión de fraude genera la caída de importantes organizaciones, pérdidas masivas de inversión, costos legales, costos sociales y erosiona la confianza en los mercados de capitales. Y el mercado de seguros no es ajeno a estos hechos.

En el mercado asegurador, el fraude puede ser cometido en diferentes puntos de la operación: por los solicitantes de seguros, a través de las pólizas y mediante esquemas de colusión con los peritos o corredores, entre otros. Los agentes de seguros y empleados de la empresa también pueden cometer fraude; sin embargo, con el desarrollo de las operaciones y avances tecnológicos, los esquemas de fraude van evolucionando, tornándose cada vez más complejos.

En Latinoamérica, la lucha contra el fraude en las empresas de seguro se viene enfocando principalmente en prevenir los casos provenientes del ramo vehicular; no obstante, existen otros ramos donde los casos de fraude son recurrentes y en los cuales aún no se toman mayores medidas para prevenir o detectar dichos eventos.

En el caso peruano, la prevención antifraude tiene principalmente base regulatoria a través de la resolución N° 838-2008: “Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo”, emitida por la Superintendencia de Banca y Seguros (SBS). Si bien dicha resolución brinda un marco regulatorio para la identificación de operaciones asociadas a este delito, el contenido se centra en sólo uno de los diversos esquemas de defraudación a los que se enfrentan las compañías de seguro.

En tal sentido, este trabajo propone el presente documento que contiene prácticas sugeridas para el desarrollo de un Programa Crítico Antifraude para el sector de

seguros en el Perú, aplicando dichas prácticas a la Compañía Peruana de Seguros Rímac Internacional.

El PCA sugerido se plantea como una herramienta estratégica para la investigación preventiva y oportuna de fraudes, y evidenciará sus beneficios respecto a la reducción del impacto resultante de los fraudes y el ahorro de costos.

La investigación se desarrollará con base en los siguientes objetivos:

1. Definir el fraude en el seguro con el fin de comprender no solo reclamaciones fraudulentas y testimonios falsos en la aplicación de seguros, sino también, el hurto y la malversación de los activos de los asegurados o de la compañía.
2. Recomendar el proceso, procedimientos, criterios y políticas así como las actividades de control más efectivas para prevenir el fraude en las operaciones, que debe aplicar la auditoría integral para que sea una herramienta efectiva contra el fraude.
3. Medir el impacto económico de la aplicación del programa crítico antifraude en la empresa Rímac Seguros.
4. Establecer la trascendencia de la implementación del programa crítico antifraude.

CAPÍTULO II MARCO TEÓRICO

El capítulo recoge las definiciones de fraude y mejores prácticas definidas para la adecuada administración, prevención, detección y respuesta al riesgo de fraude, que servirán de fundamento para el desarrollo del presente trabajo de investigación.

2.1 Definiciones Generales

Lograr un entendimiento claro sobre qué es el fraude, su naturaleza e impacto en las organizaciones, es un punto importante para la construcción de cualquier iniciativa antifraude que busque posicionarse como una herramienta estratégica.

2.1.1 Definición del fraude

El concepto de fraude presenta definiciones de acuerdo al contexto en el que este se comete (fraude médico, fraude financiero, fraude de seguros), de acuerdo con el entorno desde el cual se analiza (desde el punto de vista del derecho civil, del derecho penal), por tipología (fraude ocupacional), y así sucesivamente. Para efectos de la investigación consideramos el uso de tres conceptos: el fraude en su sentido más general, el fraude ocupacional y su definición en el mercado de seguros, los cuales describimos a continuación.

Para entender cómo se explica el fraude, en su sentido más general, recogimos dos definiciones: «Acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete » (Real Academia Española 2001)¹. Y la que propone Albrecht en su libro *The Nature of Fraud*: «...un término genérico, e incluye todos los múltiples medios que el ingenio humano puede concebir, y que son realizados por un individuo, para obtener ventaja sobre otro a través de falsas representaciones... este incluye la

¹ *Diccionario de la lengua española - Vigésima segunda edición*. Consulta: 23 de junio de 2011

< <http://lema.rae.es/drae/?val=fraude> >

sorpresa, el engaño, la astucia y maneras injustas a través de las cuales otro es engañado» (Albrecht et al. y Zimbelman 2011:6).

Ambos conceptos nos permiten situar al fraude como un acto de engaño intencional; es decir, no es un acto forzado, ni tampoco se comete por error.

2.1.1.1 Definición del fraude ocupacional

Para el concepto de fraude ocupacional, tomamos como referencia las definiciones brindadas por las siguientes organizaciones:

ACFE (Asociación de Examinadores de Fraudes Certificados) con sede en Texas, Estados Unidos: « El uso de una ocupación para el enriquecimiento personal a través del mal uso o apropiación deliberada de los recursos o activos de la organización » (ACFE 2008:6).

El Instituto Americano de Contadores Públicos (AICPA - American Institute of Certified Public Accountants) con sede en Washington DC, Estados Unidos: «...dos tipos de fraude: inexactitudes generadas por informes financieros fraudulentos (distorsión de los estados contables de una organización como consecuencia de “dibujar los números”) e inexactitudes generadas por la malversación de activos (robo o uso indebido de los bienes de una organización) » (Vona L 2006:7).

El Instituto de Auditores Internos (IIA – The Institute of Internal Auditors) con sede en Florida, Estados Unidos: «Todo acto ilegal caracterizado por engaño, ocultación o abuso de confianza. Son actos que no dependen de amenazas, de violencia ni de fuerza física. Los fraudes son cometidos por personas y organizaciones para obtener dinero, bienes o servicios, para evitar el pago o la pérdida de servicios, o para obtener una ventaja personal o comercial. » (The Institute of Internal Auditors 2011:2).

Con base a las descripciones citadas en los párrafos anteriores y en complemento a la definición general del fraude analizada en el apartado 2.1.1, podemos concluir que

el efecto del fraude en las organizaciones es de naturaleza económica y comprende los recursos y bienes de las compañías, por lo que su materialización constituye un riesgo para la empresa. Así, el impacto de la comisión del riesgo de fraude puede generar contingencias financieras (pérdida de inversiones, fraude financiero), reputacionales (confianza de los mercados de capitales), laborales o regulatorias (sanciones de entidades gubernamentales) y legales (responsabilidades penales o civiles); las cuales, de suceder, pueden llegar a paralizar el ciclo de vida de la empresa. Esta visión será clave para la implementación de cualquier iniciativa de prevención contra el fraude.

Para fines de la investigación, y en síntesis de los conceptos revisados, el fraude ocupacional lo interpretamos como <<la utilización del tiempo ocupacional para enriquecimiento personal a través del deliberado derroche o abuso de los recursos o activos de la organización>> (Colegio de Contadores Públicos de México 2005: 3)

2.1.1.2 Definición del fraude en el mercado asegurador

El Instituto de Información de Seguros (III - Insurance Information Institute), define al fraude en el mercado de seguros como: «un engaño deliberado perpetrado en contra o por una compañía o agente de seguros con el fin de obtener beneficios económicos. El fraude puede ser cometido en diferentes puntos de la operación de seguro por los solicitantes de seguros, pólizas, reclamantes de terceros o profesionales que prestan servicios a los demandantes. Los agentes de seguros y empleados de la empresa también pueden cometer fraude de seguros» (III 2011).

De esta definición podemos identificar que el fraude en seguros no sólo comprende la tipología de fraude ocupacional, desarrollado en el apartado 2.1.1.1 del presente capítulo; sino que además puede ser ejecutado por personas ajenas a la organización. Siendo este último escenario el tipo más común de fraude en el mercado de seguros, donde se usan elementos de engaño para obtener más coberturas sobre hechos reales, se tergiversan hechos en las solicitudes de seguro, se presentan reclamos por lesiones o daños que nunca ocurrieron, entre otros. (Insurance Information Institute

2011: 30).² Esta característica hace del mercado asegurador un entorno complejo respecto a los puntos de atención que deben cubrir las compañías para luchar contra el fraude.

Por otro lado, el efecto del fraude en seguros no sólo repercute en la compañía, sino que, además, tiene un impacto económico en la comunidad. Cada vez que se comete un fraude los elementos que terminan siendo afectados en las compañías de seguros son los resultados técnicos, el costo de las primas y el monto asegurado (cobertura) del producto. Como consecuencia, son los asegurados los que terminan pagando un valor más alto en las primas por la comisión de estos delitos debido a que el costo del fraude termina dispersándose en los costos a los que la compañía de seguros debe incurrir al momento de ofertar una póliza y asegurarse de que estará en la capacidad de cubrir el monto asegurado.

2.1.2 Móviles para la comisión del fraude.

Los factores que motivan la comisión del fraude son descritos a través de dos teorías que son aplicables a cualquier contexto de negocios y, por ende, al entorno de seguros: El Triángulo del Fraude y el Diamante del Fraude. Ambas teorías requieren ser utilizadas en los procesos de investigación del fraude debido a que permiten a las compañías identificar los móviles que facilitaron el dolo. A continuación trataremos cada una de ellas con el objetivo de seleccionar el marco conceptual a ser aplicado en la implementación del Plan Crítico Antifraude:

2.1.2.1 El Triángulo del Fraude

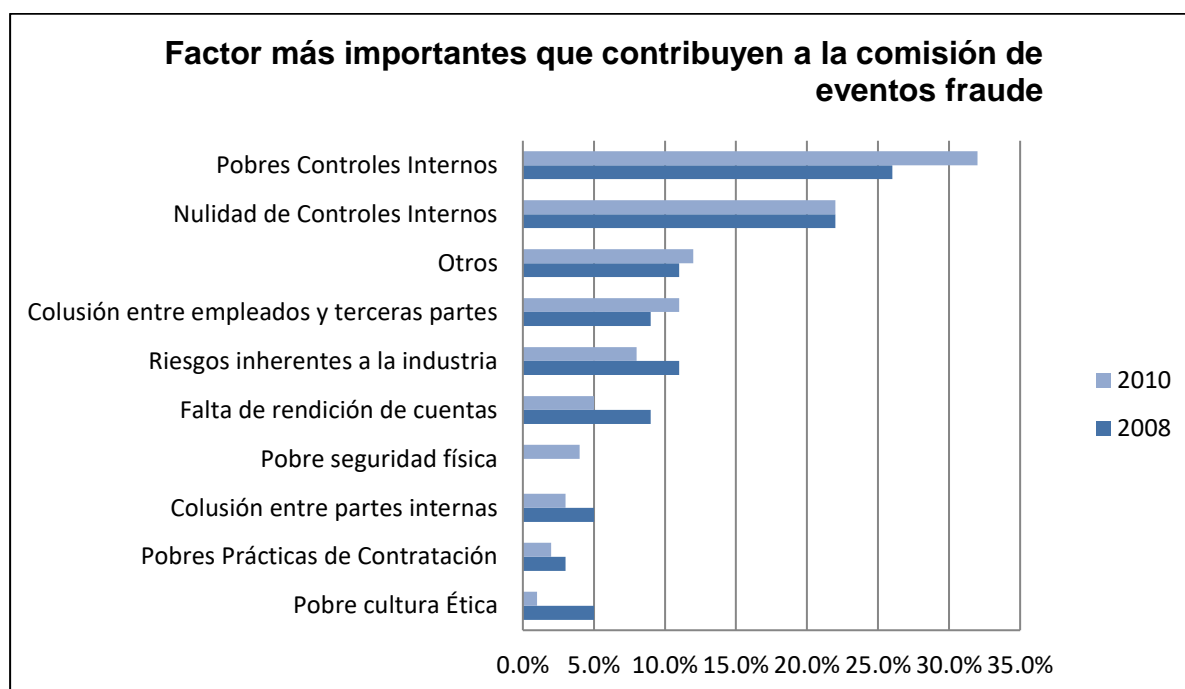
² En esta definición se citan términos inherentes al sector de seguros como pólizas, reclamantes, coberturas, los cuales se encuentran descritos en el ANEXO I.

La teoría nace a finales de 1940, como resultado de una investigación realizada por Donald R. Cressey que buscaba identificar porqué se cometían fraudes. La investigación dio como resultado que tres factores se presentaban constantemente: la oportunidad para realizar el dolo, la presión o motivación del defraudador y la racionalización o justificación para su comisión. A continuación describiremos cada uno de los factores:

- a) **Presión:** Se presenta en el perpetrador como la razón por la cual requiere cometer el dolo: satisfacer necesidades financieras personales, cumplir objetivos para lograr un mejor posicionamiento (por ejemplo: programa de incentivos), hasta por esconder las malas noticias de los inversionistas y el mercado de capitales. (Center for Audit Quality 2010:3)

- b) **Oportunidad:** El fraude es realizado la mayoría de las veces cuando se presentan debilidades de control y monitoreo. El perpetrador del fraude se basa en esta debilidad y asume que no será descubierto. Entre los factores de debilidad más conocidos se encuentran la ausencia o pobre existencia de una cultura de conocimiento o educación respecto al fraude, debilidades de control con terceros, y así sucesivamente. (Center for Audit Quality 2010: 4). La siguiente figura muestra factores que fueron identificados en el 2010 por la consultora KPMG como elementos que incentivan la comisión del fraude:

FIGURA 2.1



Fuente: Encuesta de Fraude y Conducta inapropiada KPMG 2010: 18

c) **Racionalización o la justificación de la actividad:** esta arista puede estar sujeta al nivel de ética personal del perpetrador, ética de la cultura organizacional, la necesidad del perpetrador de ganar reconocimiento por la comisión del fraude o cuando descubre que las reglas del negocio lo permiten.

2.1.2.2 El Diamante del Fraude

En el 2004, David T. Wolfe y Dana R. Hermanson proponen un cuarto elemento al Triángulo del Fraude: la Capacidad del defraudador. La capacidad se define como los rasgos y habilidades necesarias para que la persona adecuada lleve a cabo el fraude, ya que, sin esto, no podría materializarse. (Wolfe T. David y Dana R. Hermanson: 2004). De esta manera, aún si se presentaran los factores de oportunidad, la racionalización y presión que describe el triángulo del fraude, si el defraudador no tiene la capacidad, el fraude no se comete.

Ambas teorías, desde nuestra opinión son aplicables al contexto empresarial; sin embargo, consideramos que el factor de capacidad puede ser o bien trasladable a terceros bajo el esquema de colusión, o bien se entiende como un factor inherente a los trabajadores; por lo que a efectos del trabajo propuesto, utilizaremos la teoría del triángulo del fraude.

2.1.3 Clasificación del Fraude

En el apartado 2.1.1.2, mencionamos que el fraude en seguros no sólo comprende la tipología de fraude ocupacional (fraude interno), sino que además comprende fraudes cometidos por terceros, ajenos a la organización (fraude externo). Explicaremos a continuación ambas clasificaciones:

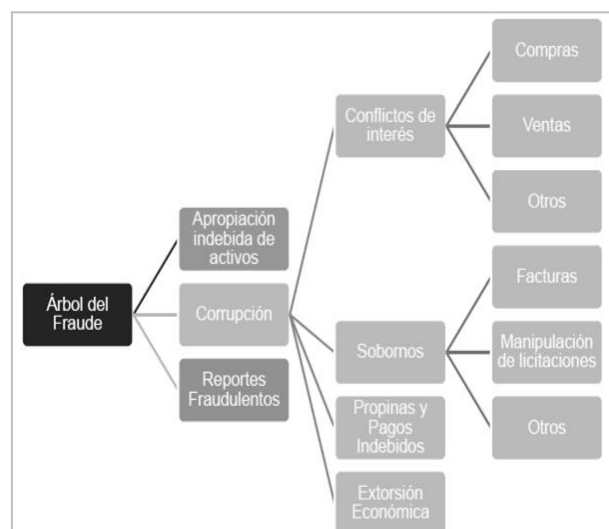
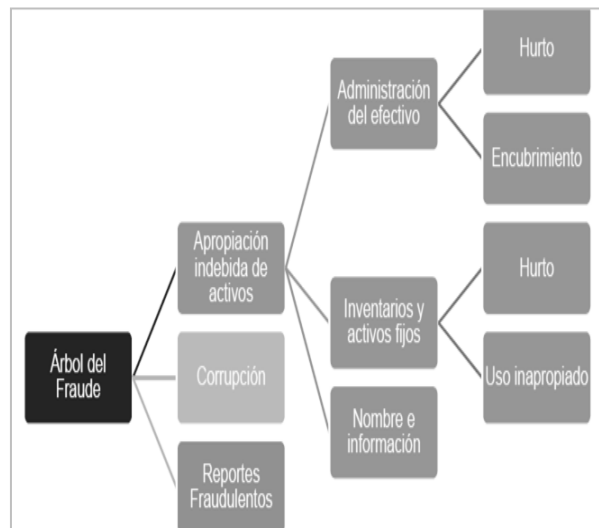
2.1.3.1 Fraude Interno

La Asociación de Examinadores Certificados de Fraude es la entidad responsable de categorizar los esquemas asociados al fraude ocupacional desde 1996 con base en el esquema denominado “Sistema de Clasificación de Abuso y Fraude Ocupacional” o “Árbol de Fraude”. A continuación mostramos las cincuenta y tres modalidades a las que toda organización puede estar afectada:

FIGURA 2.2

SISTEMA DE CLASIFICACIÓN DE ABUSO Y FRAUDE OCUPACIONAL





Fuente: ACFE - Report to the Nations on Occupational Fraud and Abuse 2010

De estos tipos de fraude, las investigaciones del 2010 y del 2012 realizadas por la ACFE identifican como los esquemas más utilizados para defraudar a las compañías de seguro la Corrupción y los de facturación, tal como se muestra en la siguiente tabla:

TABLA 2.1

Esquemas de Fraude Ocupacional en el Sector Seguros		
Número de Casos por esquema de fraude	Report to the Nations 2012	Report to the Nations 2010
Corrupción	21	30
Facturación	24	19
Fraguado de Cheques	13	15
Robo de dinero	12	13
No Financiero	6	9
Dinero en mano	3	9
Hurto	5	8
Desembolso de gastos	7	7
Planilla	3	6
Fraude en Estados Financieros	2	3
Registro de desembolsos	0	3

Fuentes: ACFE - Report to the Nations on Occupational Fraud and Abuse 2010 y 2012

2.1.3.2 Fraude Externo

En esta clasificación se encuentran los fraudes cometidos por asegurados, terceras partes reclamantes, intermediarios, profesionales que brindan servicios relacionados a reclamos, liquidadores o ajustadores. Y estos, a su vez, se pueden clasificar por los tipos de ramos de seguro en los que se presentan. No es la intención del presente documento citar todos los tipos existentes porque estos pueden variar por país y por empresa. Lo primordial sobre las diversas tipologías existentes es que las compañías de seguro tengan claramente identificadas cuáles son las modalidades a las cuales sus productos o ramos están afectados, información sobre la cual deberán realizar un análisis de riesgos y controles con el objetivo de reducir o evitar la comisión de dichos tipos de defraudación. En la presente investigación el apartado 4.3 “Principales tipos y modalidades de fraude” del capítulo V describe la tipología de fraudes relevantes para la Compañía de Seguros Rímac Internacional.

2.2 Marco de Referencia para la Gestión del Riesgo de Fraude

En el apartado 2.1.1 describimos la naturaleza del fraude en seguros y concluimos, en base a las definiciones presentadas, por qué el fraude representa para las organizaciones un riesgo. En el presente apartado describiremos las prácticas que serán utilizadas para la construcción del Programa Crítico Antifraude propuesto para Rímac Internacional.

Para la adecuada gestión del riesgo de fraude, el Instituto de Auditores Internos, el Instituto Americano de Contadores Públicos Certificados y la Asociación de Examinadores certificados del Fraude sugieren la implementación de los siguientes principios:

Principio 1: Definir el gobierno de la gestión del fraude.

Principio 2: Evaluación del Riesgo de fraude.

Principio 3: Definir procesos y técnicas de prevención del fraude.

Principio 4: Definir procesos y técnicas de detección del fraude.

Principio 5: Definir procesos y técnicas de investigación y respuesta al fraude.

(The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 6). A continuación describiremos cada uno de ellos:

2.2.1 Gobierno del Riesgo de Fraude

Ante la detección de un alerta de fraude, las compañías podrían presentar dificultades para determinar quién o quiénes son responsables de las acciones a seguir. Dicha situación puede agravar el impacto del fraude debido a la ejecución de acciones no oportunas o procedimientos no adecuados.

En este contexto, el Instituto de Auditores Internos, el Instituto Americano de Contadores Públicos Certificados y la Asociación de Examinadores Certificados de Fraude recomiendan que para ayudar a la organización a contar con un efectivo

programa de gestión de riesgos de fraude, es importante comprender las funciones y responsabilidades que el personal, en todos los niveles de la organización, tiene con respecto a la gestión del riesgo de fraude (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

A continuación presentamos los roles clave que debe considerar una organización en la implementación de un programa de gestión de riesgos de fraude:

2.2.1.1 Roles y Responsabilidades

2.2.1.1.1 **El Rol del Directorio:** los directores deben garantizar que se cuente con un esquema de gobierno apropiado. Esto abarca todos los aspectos del gobierno del Directorio, incluyendo la presencia de miembros independientes que ejercen el control sobre la información que se presenta en las reuniones, las agendas, el acceso de las gerencias y asesores externos, así como sobre los roles responsables de tomar decisiones en la compañía. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

2.2.1.1.2 **El Rol del Comité de Auditoría:** el Comité de Auditoría debe estar compuesto por consejeros independientes y debe tener al menos un experto en finanzas, preferentemente con formación contable. Deberá reunirse con una frecuencia determinada, para periodos suficientemente largos, y con la preparación adecuada para evaluar de manera apropiada los eventos de fraude y responder a los mismos con los protocolos formales definidos, lo cual puede implicar reemplazar los controles internos existentes en la organización. En tal sentido, es clave que el Comité de Auditoría reciba informes periódicos sobre el estado de los eventos de fraude reportados o presuntos fraudes (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

2.2.1.1.3 **El Rol de la Gerencia:** la gerencia tiene la responsabilidad de efectuar el diseño e implementación de un programa de gestión de riesgo de fraude, incluyendo:

- a) El establecimiento de directivas al resto de la organización. La gerencia requiere crear una cultura a través de acciones y frases que contengan un mensaje claro y que incluyan que el fraude no es tolerable, que los eventos de fraude son tratados con rapidez y decisión y que los denunciantes no sufrirán represalias.
- b) La implementación de controles internos adecuados, incluyendo la documentación de políticas y procedimientos de gestión de riesgos de fraude, alineados con la evaluación de los riesgos de fraude de la compañía.
- c) La comunicación al Directorio de las acciones que serán llevadas a cabo para administrar los riesgos de fraude y el reporte de la efectividad del programa de gestión de riesgos de fraude.

(The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

2.2.1.1.4 **El Rol del Personal:** todo el personal de la organización, incluida la gerencia, debe:

- Poseer un entendimiento general del fraude en la organización.
- Entender y asumir el rol que les corresponde en el marco de control interno: comprender que en algunas ocasiones el incumplimiento de controles internos podría estar creando oportunidades para que suceda un fraude.
- Leer y entender las políticas y procedimientos (por ejemplo, la política contra el fraude, el código de conducta, y la política de los denunciantes), así como otras políticas y procedimientos operacionales, tales como manuales de compras, de reclutamiento y selección, entre otros.

(The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

2.2.1.1.5 **Rol del Auditor Interno:** El estándar de Auditoría de la PCAOB (Public Company Accounting Oversight Board) cita que: "El auditor debe evaluar todos los controles destinados específicamente a hacer frente a los riesgos de fraude que tienen al menos una probabilidad razonablemente posible de tener un efecto significativo sobre los estados financieros de la empresa." (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 12).

Una vez establecidos los roles descritos, es importante que la organización tenga claramente definidos cuáles son las relaciones de interacción entre dichos roles. Para poder visualizar cuál es el grado de responsabilidad de cada uno de estos roles respecto al fraude, el Instituto de Auditores Internos, el Instituto Americano de Contadores Públicos Certificados y la Asociación de Examinadores Certificados de Fraude nos sugiere utilizar la Matriz de Decisiones del Fraude. (Ver [ANEXO II](#)).

2.2.1.2 Elementos clave para un efectivo Programa Crítico Antifraude

El Instituto de Auditores Internos, el Instituto Americano de Contadores Públicos Certificados y la Asociación de Examinadores Certificados de Fraude recomiendan que los siguientes elementos se encuentren definidos en un Programa Crítico Antifraude:

- i. **Compromiso:** El Consejo y la Alta Dirección deben comunicar su compromiso con la gestión del riesgo de fraude. Un método sería integrar este compromiso en los valores de la organización o en los principios y código de conducta. Otro método consiste en la emisión de un documento breve (por ejemplo, carta) a disposición de todos los empleados, proveedores y clientes. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 16)
- ii. **Conciencia del Fraude:** Un programa de concienciación en curso es un factor clave, así como un control preventivo eficaz. Los programas de prevención y concienciación sobre esquemas de fraude y mala conducta se deben desarrollar a

través de evaluaciones periódicas, capacitación y comunicación frecuente. El uso de un Programa Crítico Antifraude ayudará a la organización en la sensibilización sobre el fraude. Al diseñar programas de sensibilización sobre el fraude, la gerencia debe considerar la frecuencia de asistencia, la duración, la permeabilidad cultural, la orientación sobre la manera de resolver los dilemas éticos y los métodos de entrega. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 16).

iii. **Proceso de Confirmación:** una organización debe determinar si existen cuestiones legales involucradas con el tener un proceso de confirmación, que es el requisito para los directores, empleados y contratistas a reconocer que han leído, entendido y están de acuerdo con el código de conducta, con la política de control del fraude, y cualquier otra documentación que soporte la gestión de riesgos de fraude en la compañía. Existe el riesgo de fraude en el que la organización no cuenta con un proceso de confirmación. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 16).

iv. **Conflicto de Interés:** la compañía debe implementar un proceso que delimite las consideraciones de conflicto de interés tanto para los directores, como para los empleados y los contratistas a nivel interno, describiendo la responsabilidad que tienen cada uno de ellos de revelar los conflictos potenciales o reales de interés. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 17).

v. **Evaluación del Riesgo de Fraude:** una evaluación de riesgo de fraude debe ser realizada de forma sistemática y recurrente, involucrar al personal, considerar los regímenes pertinentes contra el fraude y los escenarios y la asignación de los esquemas de fraude, así como los controles de mitigación. El Sistema de Control Interno de una organización debe estar diseñado para hacer frente a los riesgos inherentes de los negocios. Los riesgos del negocio son identificados en el protocolo de la empresa de evaluación de riesgos. Para esta tarea se puede hacer uso del marco de control interno COSO. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 18).

vi. **Los procedimientos de información y protección de denunciantes:** la documentación no sólo debe articular una organización con tolerancia cero para el fraude, sino que también debe establecer la expectativa de que toda sospecha de fraude debe ser reportada de inmediato y proporcionar los medios para hacerlo. Los canales para reportar cualquier sospecha de problemas de fraude deben ser claramente definidos y comunicados. Teniendo en cuenta que las personas son el mejor activo de una organización para prevenir, detectar y disuadir el fraude, una organización debe considerar el difundir de qué recursos dispone el individuo para reportar tales. Para fomentar la denuncia oportuna de cuestiones de sospecha, la organización debe comunicar el grado de protección otorgado. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 18).

vii. **Proceso de Investigación:** las organizaciones deben exigir que se dé un proceso de investigación ante la comisión del fraude. Una vez que un problema se informó, un proceso de investigación debe ejecutarse. El Directorio y la Gerencia deben tener un protocolo documentado para este proceso, incluida la consideración de quiénes deben llevar a cabo la investigación - ya sea personal interno o la contratación de expertos en este campo - las reglas de evidencia, cadenas de custodia, mecanismos de información a los encargados del gobierno, los requisitos reglamentarios, y acciones legales. Las organizaciones también deben considerar la posibilidad de exigir a todos los empleados, como condición de empleo, que cooperen plenamente con una investigación sobre cualquier presunto fraude o sospecha. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 16).

viii. **Acciones Correctivas:** como un elemento de disuasión, las políticas deben reflejar las consecuencias y los procesos para los que cometen o toleran la actividad fraudulenta. Estas consecuencias pueden incluir la terminación del empleo o de un contrato y presentación de informes a las autoridades legales y reglamentarias. La organización debe articular que tiene el derecho de iniciar acciones civiles o penales contra cualquier persona que comete el fraude. (The Institute of Internal Auditors, The

American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 19).

ix. **Proceso de Evaluación y Mejora:** Se debe contar con documentación que indique si la gerencia evaluará periódicamente la efectividad del Programa de Gestión de Riesgos de Fraude y también el cómo se espera que esta evaluación se lleve a cabo. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 19).

x. **Monitoreo Continuo:** El Programa Crítico Antifraude, incluidos los documentos relacionados, deben ser revisados con base en las necesidades cambiantes de la organización. La documentación sobre la gestión del riesgo de fraude debe ser actualizada en forma continua para reflejar las condiciones actuales y reflejar el compromiso continuo de la organización sobre el mismo. (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 16)

2.2.2 Evaluación del Riesgo del Fraude

El riesgo del fraude se define como: «la probabilidad de que ocurra un fraude y las consecuencias potenciales para la organización cuando ocurra.» (The Institute of Internal Auditors 2008); sin embargo, la probabilidad de su comisión dependerá de si la organización cuenta con actividades para prevenirlo. La construcción de esta evaluación se realiza en cinco fases:

Fase 1: identificar los factores relevantes de riesgo de fraude.

Fase 2: identificar esquemas de fraude y priorizarlos con base en los riesgos.

Fase 3: comparar los controles existentes respecto a los esquemas de fraude.

Fase 4: probar la efectividad de controles para la prevención y detección del fraude.

Fase 5: documentar y reportar la evaluación de riesgos de fraude.

2.2.3 Prevención del Fraude

La prevención del fraude involucra acciones que disminuirán y limitarán su comisión, para lo cual se debe establecer primordialmente una fuerte cultura ética y establecer un adecuado mensaje respecto a la importancia del fraude para la organización. A continuación, citaremos elementos de prevención y detección desde la perspectiva del modelo COSO (Committee of Sponsoring Organizations of the Treadway Commission):

TABLA 2.2
Controles Preventivos de Fraude

Dimensiones de COSO	Control Preventivo
Entorno de Control	<ul style="list-style-type: none"> • Código de Conducta • Política de Ética o Fraude. • Programas de Línea de Reporte Directo. • Prácticas y guías de contratación y promoción. • Revisión del tópico de fraude por comités
Evaluación de Riesgo	Realizar evaluaciones de riesgo de manera periódica.
Actividades de Control Antifraude	Políticas y procedimientos del negocio, incluyendo los límites de funciones y la segregación de funciones.
Información y Comunicación	Promover la importancia de los programas de gestión de riesgo de fraude y la posición de la organización respecto al riesgo de fraude tanto interna como externamente a través de: <ol style="list-style-type: none"> a) Programas de entrenamiento, y procedimientos. b) Procesos de certificación o afirmación para confirmar que los empleados han leído y entendido las políticas corporativas.
Monitoreo	Realizar evaluaciones periódicas de controles antifraude: <ul style="list-style-type: none"> · A través de revisiones de auditores internos. · Implementando tecnología para asegurar el monitoreo continuo y actividades de detección.

Fuente: The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA) y Association of Certified Fraud Examiners (ACFE) 2010:79

2.2.4 Detección del Fraude

Los mecanismos implementados por la organización para la detección del fraude deben estar basados en herramientas y controles que provean alertas o evidencias para una detección oportuna del dolo. Motivo por el cual, los métodos requieren ser flexibles, adaptables en el tiempo, y estar alineados con los riesgos/objetivos del negocio.

Sin embargo, notamos en el estudio efectuado por la ACFE al 2010 que aproximadamente el 50% de los casos de fraude en Latinoamérica y el Caribe fueron detectados a través de soplos (43.2%) o por accidente (10.8%), tal como se muestra en la siguiente tabla:

TABLA 2.3

Métodos de Detección de Fraude Ocupacional en Latinoamérica y el Caribe a diciembre 2011	
	Porcentaje
Soplo	43.20%
Revisión Gerencial	10.80%
Auditoría Interna	13.50%
Por Accidente	10.80%
Reconciliación Contable	8.10%
Examinación de Documentos	5.40%
Auditoría Externa	0%
Notificado por la Policía	2.70%
Vigilancia Monitoreo	0%
Confesión	2.70%
Otros	0%
Controles de Tecnología de la Información	2.70%

Fuentes: ACFE - Report to the Nations on Occupational Fraud and Abuse 2012

2.2.5 Investigación del Fraude y Acciones Correctivas

Al ser identificado el fraude, se deben seguir procesos estandarizados de comunicación y reporte del mismo ante las entidades de la organización definidas con la finalidad de que se proceda a realizar una investigación coordinada que permita establecer acciones correctivas de manera oportuna, entre las cuales, se debe

considerar la modificación de controles internos que no son eficaces en la detección del fraude, la sanción correspondiente al personal que comete fraude y el diseño de una estrategia de comunicación del mismo por parte de la gerencia, entre otros.

Respecto a la conducción del proceso de investigación Ernst&Young muestra un modelo adaptado del marco de referencia a GRC – Governance Risk & Compliance, del Group Open Compliance and Ethic Group (OCEG), para realizar investigaciones de fraude. Dicho modelo secciona en cinco fases la investigación: Captura. Filtro, Planeación e Investigación y Resolución (Ernst&Young 2010). VER [ANEXO III](#).

Hay que tener en cuenta que las investigaciones de fraude tienen como objetivo formular un reporte con evidencias del hecho para luego ser evaluadas por la entidad o persona asignada en el ámbito judicial o legal. Finalmente, se debe tomar en consideración que las primeras cuarenta y ocho horas de la investigación del fraude son determinantes debido a que en este lapso de tiempo la empresa debe haber analizado si inicia o no una investigación de fraude, si va a involucrar a personal especializado, si debe brindar una respuesta a grupos de interés públicos y debe haber activado los procedimientos para proteger las evidencias probatorias y conservar su validez legal.

2.3 Herramientas

El presente apartado recoge las prácticas de referencia que existen sobre los esquemas de reporte de fraude, que se sitúan en el frente de detección; y el uso de herramientas informáticas, que se sitúa en el frente de prevención.

2.3.1 Esquemas de Reporte

Las alertas o "Banderas rojas" (deviene del término en inglés *Red Flag*), representan las comunicaciones o eventos con información de posibles eventos de fraudes. La importancia de una adecuada administración de alertas para las empresas radica en que estas son la base sobre la cual se pueden iniciar o no procesos de investigación.

Ernst&Young sugiere que «las compañías deben brindar canales eficientes para hacer que esta información fluya a los niveles apropiados oportunamente» y que deben «...actuar con debida diligencia respecto a la información recibida, lo que incluye una validación inicial para identificar si existen elementos suficientes para que los niveles apropiados decidan si deben iniciar o no una investigación» (Ernst&Young 2010 – Sesión 6: 2)

2.3.2 Herramientas para el análisis de información

La tecnología de análisis de datos permite identificar qué tan bien están funcionando los controles internos y qué transacciones pueden estar siendo afectadas por actividades fraudulentas. (ACL Services Ltd 2010: 4)

Para habilitar el uso de herramientas de análisis de datos la organización debe identificar: las áreas en las que ocurre el fraude, qué actividades fraudulentas podrían interpretarse en el análisis de datos y qué fuentes de información se requiere analizar para evaluar posibles indicadores de fraude. En el mercado existen diversas herramientas para la implementación de estrategias de antifraude tales como: Herramientas de Análisis de Datos para Auditoría como ACL e IDEA, herramientas de Minería de Datos, herramientas Estadísticas, como el software IBM SPSS Predictive Claims de IBM y soluciones de Análisis de Fraude, como las plataformas Fraud Analytics Suite de Computer Science Corporation o Fraud Insurance Manager de FICO, entre otros.

Para efectos de la investigación sugerimos el uso de la herramienta ACL, considerando que Rímac Internacional cuenta al 2012 con licencias para el uso de esta aplicación.

2.4 El costo del fraude

El costo del fraude considera dos frentes: la valorización del costo total del dolo para la empresa, incluyendo los fraudes no reportados y reportados; y, por otro lado, la valorización del costo de la investigación. (Deloitte Touche Tohmatsu 2008)

En relación al primer frente, la Asociación de Examinadores de Fraude Certificados (ACFE), en su encuesta 2010 expone que el verdadero valor del costo total del fraude para una empresa es incalculable. (ACFE Report to the Nations on Occupational Fraud and Abuse 2010:8). Esta condición respecto al costo se debe a la naturaleza oculta para la comisión del mismo, motivo por el cual muchos de los fraudes realizados no son revelados.

El segundo frente, tradicionalmente, calcula el costo del fraude considerando el valor del activo fraguado y el valor de los costos operacionales, legales o judiciales en los que incurre la empresa durante la fase de investigación. Sin embargo, el costo de la comisión de un delito de fraude también implica otros factores de costo (ver TABLA 2.4) que de no ser tomados en cuenta afectarían la estimación del costo total del fraude que sí es investigado:

TABLA 2.4

Costo Total de Investigar un Fraude		
Costo Fijo	Costo Variable	Costo Indirecto
Costos de Investigación (horas hombres incurridos)	Contingencias laborales.	Recuperar los procesos del negocio (reingeniería o rediseño).
Costo activo fraguado o pérdida.	Contingencias legales. Contingencias regulatorias.	Costo de la pérdida de confianza de clientes y empleados.

Fuente: elaboración propia

Para efectos de la investigación, a continuación citaremos algunas estadísticas que servirán de base en el capítulo V para sustentar el cálculo esperado de ahorro que conlleva la implementación de un Programa Crítico Antifraude (PCA):

- En promedio, el costo total del fraude representa aproximadamente el 5% de sus ingresos totales anuales (ACFE Report to the Nations on Occupational Fraud and Abuse 2012:4)
- Una organización puede gastar aproximadamente el 8% del monto perdido en la ejecución de la investigación, y un promedio de 95 horas laborales investigando los eventos de fraude significativos. (Fraud and Misconduct Survey 2010 – KPMG 2010: 15).

2.5 Programa Crítico Antifraude

Como revisamos a lo largo del apartado 2.2 “Marco de Referencia para la Gestión del Riesgo de Fraude”, para que una organización cuente con una adecuada gestión del riesgo de fraude, los cinco principios descritos deben ser implementados. Adicionalmente a dichos principios y basándonos en lo descrito en el apartado 2.3 “Herramientas”, la gestión antifraude debe soportarse en esquemas de reporte y herramientas informáticas que permitan implementar técnicas de monitoreo continuo. Para unificar estas prácticas las compañías plasman sus estrategias de lucha contra el fraude en lo que se denomina Programa Antifraude (PA). Tomando en cuenta el enfoque estratégico que tiene para la empresa la adecuada administración del riesgo de fraude, estimamos que la mejor denominación de una solución antifraude debe titularse “Programa Crítico Antifraude”.

CAPÍTULO III ANÁLISIS DE LA GESTIÓN DEL RIESGO DE FRAUDE EN SUDAMÉRICA Y EL SECTOR ASEGURADOR PERUANO

El presente capítulo recoge estadísticas sobre el grado de adhesión y uso de las prácticas antifraudes descritas en el capítulo anterior en Sudamérica. Asimismo, se describen las iniciativas de lucha contra el fraude que se están llevando en la región. Para luego describir el estado de la gestión del fraude en el mercado asegurador peruano donde se desarrolla Rímac Internacional.

3.1 Gestión del Fraude en Sudamérica

La información recogida para analizar el entorno de eventos de fraude en la región se basa en encuestas de carácter público obtenidas en el proceso de investigación a través de la Internet y presentan las siguientes características:

- a) Son realizadas principalmente por las cuatro compañías líderes en servicios de consultoría y auditoría (Ernst&Young, PricewaterhouseCoopers, Deloitte & Touche y KPMG). (Ver tabla 3.1)
- b) Tienen carácter global y son desarrolladas tomando información de ciertos países, sea que la encuesta presente resultados de carácter internacional o para la región latinoamericana. (Ver tabla 3.1).
- c) Las encuestas globales que incluyen información de Latinoamérica se encuentran limitadas a ciertos países de dicha región. Por ejemplo, la 11va encuesta anual sobre el fraude realizada por Ernst&Young tomó para los indicadores en Latinoamérica solo a Brasil y México. (Ver tabla 3.1).

Asimismo, identificamos que los artículos periodísticos o de opinión disponibles en la Internet que desarrollan la temática del fraude en Sudamérica, refieren principalmente las fuentes descritas en los puntos (a), (b) y (c).

TABLA 3.1

Encuestas sobre la Comisión del Fraude en Latinoamérica		
Estudio / Informe / Encuesta	Alcance	Periodo
Report to the Nations on occupational fraud and abuse. Global Survey. Asociación de Examinadores de Fraude Certificados (ACFE).	Información provista por los miembros certificados como Examinadores de Fraude por la ACFE	2010 y 2012
Informe KPMG- El fraude Corporativo en Latinoamérica	Argentina, Brasil, Chile, Colombia, México y Uruguay	2008-2011
Encuesta Nacional de Fraude de Ernst & Young	Argentina	2007
11th Global Fraud Survey – Driving ethical growth, new markets, new challenges	Brasil y México	2009 - 2010
Encuesta Global sobre delitos económicos 2009, Suplemento América Latina	Argentina, Brasil, Chile y México.	2009

Fuente: elaboración propia

Tal como se aprecia en el cuadro anterior, el estudio más idóneo para efectos de la investigación es el realizado por la consultora KPMG debido a que incluye a la mayor cantidad de países de la región. En el siguiente apartado analizaremos las estadísticas recogidas. Del estudio realizado por KPMG los siguientes indicadores nos llevan a concluir que un promedio significativo de empresas latinoamericanas han dejado de lado el uso de herramientas para la detección, identificación y prevención del fraude, lo que ha generado una subida vertiginosa de eventos de fraude:

- a) «En promedio, sólo un 35% de las empresas latinoamericanas cuenta con un programa de prevención de fraudes». (KPMG El Fraude Corporativo en Latinoamérica 2010: 5).
- b) «..la mayor parte de los fraudes cometidos en compañías que operan en Latinoamérica no son detectados por medio de los controles internos de las organizaciones» (KPMG El Fraude Corporativo en Latinoamérica 2010: 7)

- c) Existe «poca efectividad de los sistemas de control interno que en general tienen las empresas que operan en Latinoamérica». (KPMG El Fraude Corporativo en Latinoamérica 2010: 8).
- d) Los fraudes que se cometieron en contra de empresas se descubrieron hasta seis meses después de ocurridos, a pesar de que en la mitad de los casos se tuvieron señales claras de que alguna irregularidad estaba sucediendo. (KPMG El Fraude Corporativo en Latinoamérica 2010: 8)
- e) «La malversación de activos ha sido y sigue siendo el tipo de fraude más frecuente». (KPMG El Fraude Corporativo en Latinoamérica 2010: 11). Recordemos que la malversación de activos implica falsificación de cheques, robo de mercadería, robo de efectivo y pagos fraudulentos.
- f) El fraude en los estados financieros «representa un problema cada vez más perjudicial para empresas que operan en Latinoamérica. En general, este tipo de fraude alcanza el 15% del total de fraudes cometidos en la región, pero representa más del 60% de los costos totales provocados por los delitos de fraude». (KPMG El Fraude Corporativo en Latinoamérica 2010: 11)
- g) «El 60% de los fraudes cometidos, ha sido perpetrado por empleados de la propia compañía». (KPMG El Fraude Corporativo en Latinoamérica 2010: 13).

3.2 Gestión del fraude en seguros

En Latinoamérica, para tener una referencia sobre el estado de la gestión de riesgo de fraude, identificamos que las iniciativas antifraude sobre el sector de seguros se ha reforzado principalmente en cuatro países: Chile, Argentina, Uruguay y Colombia. Sin embargo, dichos se han basado en los seguros del ramo automotriz.

En el caso argentino y chileno las asociaciones CESVI –Argentina y CESVI Chile, buscan reforzar la cultura antifraude en la región. CESVI Argentina, institución que opera desde el 2002, es un referente en dicho país. Actualmente organiza Seminarios Latinoamericanos de Seguros y Reaseguros y entre sus aportes más importantes se encuentra la gestión del software SOFIA (MAPFRE 2006:25). SOFIA, conocido también como Sistema Integrado fue creado en el 2001 y contiene en sus bases los

datos de información de más del 70% del mercado asegurador argentino respecto al ramo automotor. En el caso de CESVI AGENCIA CHILE, la institución opera desde agosto 2008 y al igual que CESVI Argentina cuenta con el software SOFIA. (CESVI s.f.)

En el caso colombiano, se cuenta con la organización INIF (Instituto Nacional de Investigación y Prevención del Fraude). (MAPFRE 2010:21).

3.3 Gestión del riesgo de fraude en el sector asegurador peruano

El mercado de seguros peruano, al segundo trimestre del 2011 está conformado por 14 empresas. De estas, cuatro están dedicadas a ramos generales y de vida, cinco exclusivamente a ramos generales, y cinco exclusivamente a ramos de vida, tal como se describe en el siguiente cuadro (Superintendencia de Banca y Seguros AFP 2011).

TABLA 3.2
Empresas de Seguros en el Perú al 30 de junio 2011

Ramos Generales y de Vida	Ramos Generales	Ramos de Vida
ACE	El Pacífico Peruano Suiza	El Pacífico Vida
Cardif	La Positiva	Invita
Interseguro	Mapfre Perú	La Positiva Vida
Rímac	Secrex	Mapfre Perú Vida
	Insur	Protecta

Fuente: Superintendencia de Banca y Seguros AFP

Tal como mencionamos al inicio del apartado 3.1, no identificamos en la bibliografía revisada información pública sobre el grado de adherencia o uso de prácticas antifraude en el Perú o en el mercado asegurador del país. Considerando esta limitación, tomamos como iniciativas principales los marcos legales y regulatorios vigentes que tratan sobre la prevención de lavado de activos, y las prácticas de control Interno contenidas en el marco del “Buen Gobierno Corporativo” impulsado por la Bolsa de Valores de Lima, los cuales desarrollaremos a continuación:

3.3.1 Prevención de Lavado de Activos

En el Perú rige desde el 26 de junio del 2002 la Ley Penal contra el lavado de activos (N° 27765), la misma que extiende el lavado de activos a otros delitos como fuentes generadoras de ganancias ilegales. En el caso de las empresas privadas de banca y seguros supervisadas por la SBS, el cumplimiento de esta ley está a cargo del oficial de cumplimiento. La actualización más reciente de esta ley se dio el 27 de mayo de 2011. (Superintendencia de Banca y Seguros y AFP del Perú 2011).

3.3.2 Principios de Buen Gobierno Corporativo

Los Principios de Buen Gobierno Corporativo que rigen en el Perú son 26. Dichos principios se crearon con el propósito de ser una guía para las empresas y para servir como un marco referencial para los diferentes grupos de interés. (Superintendencia del Mercado de Valores 2011). Ver [ANEXO IV](#).

En síntesis, «el gobierno corporativo explica las reglas y los procedimientos para tomar decisiones en asuntos como el trato equitativo de los accionistas, el manejo de conflictos de interés, la estructura de capital, los esquemas de remuneración e incentivos de la administración, las adquisiciones de control, la revelación de información y la influencia de inversionistas institucionales, entre otros, que afectan el proceso a través del cual las rentas de la sociedad son distribuidas. » (Superintendencia del Mercado de Valores 2011).

CAPÍTULO IV DIAGNÓSTICO DE LA GESTIÓN DEL FRAUDE EN RÍMAC INTERNACIONAL COMPAÑÍA DE SEGUROS Y REASEGUROS

El presente capítulo describe la organización y gestión actual del riesgo de fraude en la Compañía Rímac Internacional.

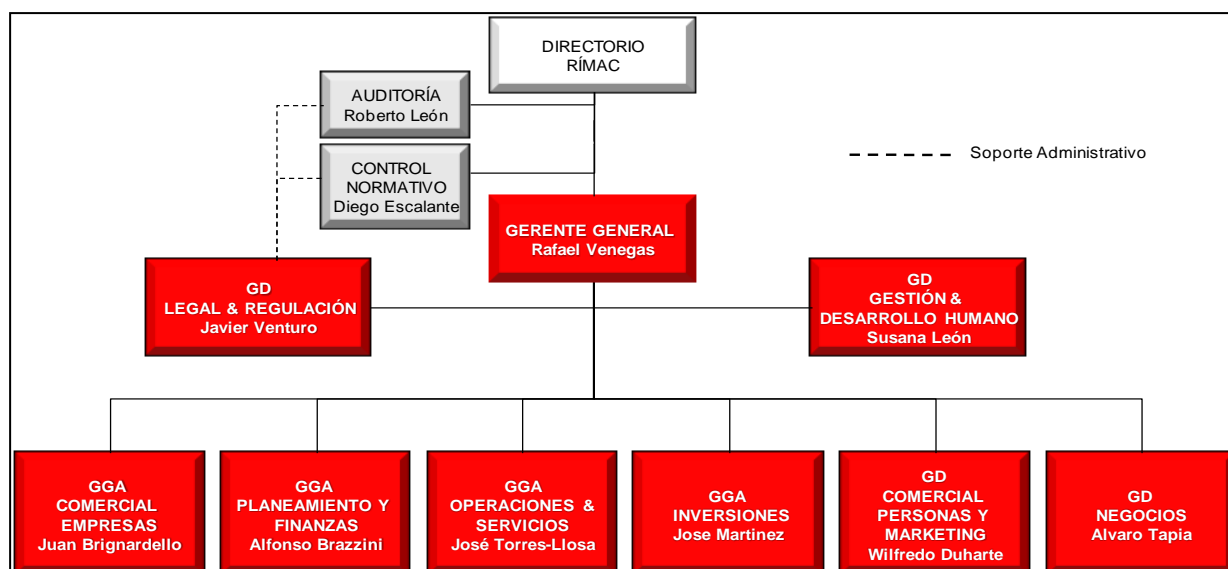
4.1 Descripción de la compañía:

Rímac Internacional Compañía de Seguros y Reaseguros, que denominamos en el presente documento como Rímac Internacional, es una compañía de seguros peruana con más de 114 años de experiencia en el mercado de seguros y es líder en el sector.

4.1.1 Organización Interna:

Rímac Internacional está conformada por las siguientes unidades:

FIGURA 4.1
ORGANIGRAMA DE RÍMAC INTERNACIONAL



Fuente: Rímac Internacional - Gestión y Desarrollo Humano - agosto 2011.

4.1.2 Gobierno Corporativo

La compañía considera dentro de la gestión de su Directorio las prácticas de Buen Gobierno Corporativo aplicables al Perú. (VER [ANEXO IV](#)). Además, cabe mencionar que el Directorio, como principal órgano de gobierno, dirige la estrategia corporativa.

4.1.3 Marco Normativo

Las operaciones de Rímac Internacional están reguladas por la Constitución Política del Perú, el Código Civil Peruano, la Ley General de Sociedades, el Código de Comercio y la Ley de Títulos y Valores, la Ley General del Sistema Financiero y el Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP (Ley 26702).

4.1.4 Control Interno

Rímac Internacional cuenta con un sistema de control interno, definido como el conjunto de políticas, procedimientos y técnicas de control establecidas. En complemento, el Sistema de Gobierno Corporativo de Rímac Internacional contempla la existencia de los siguientes comités especiales del Directorio:

TABLA 4.1

Comités Especiales del Directorio de Rímac Internacional	
Comité	Función
Auditoría	Tiene como función principal evaluar el diseño, alcance y funcionamiento del control interno de la empresa, así como evaluar el cumplimiento de las disposiciones legales e internas de la compañía.
Riesgos	Tienen la responsabilidad de identificar y evaluar los riesgos asociados a diversos procesos de la compañía.
Riesgos de Inversión	Tienen la responsabilidad de identificar y evaluar los riesgos de inversión de la compañía.

Fuente: elaboración propia

La organización también cuenta con los siguientes comités para evaluar las desviaciones de cumplimiento de los lineamientos establecidos:

TABLA 4.2

Comités Internos de Control de Rímac Internacional	
Comité	Función
Comité de Alta Dirección (CAD)	Toma decisiones sobre la administración y gestión de la empresa, sobre los controles internos y los controles normativos; de acuerdo con los estatutos, lineamientos estratégicos y objetivos estratégicos.

Comités Internos de Control de Rímac Internacional	
Comité	Función
Ética	Encargado de vigilar el adecuado cumplimiento del código de ética y estándares de conducta de la compañía.
Incidencias	Órgano de apoyo del Comité de Ética que tiene como función principal investigar, analizar y presentar informes y conclusiones sobre las denuncias presentadas por los colaboradores o terceros.
Prevención de lavado de activos	Evaluar, en apoyo al oficial de cumplimiento, si una operación puede ser considerada sospechosa de lavado de activos y del financiamiento del terrorismo y la puesta en práctica del Sistema de Prevención.

Fuente: elaboración propia

4.2 Gestión del Fraude en Rímac Internacional:

Rímac Internacional ha desarrollado diversas herramientas orientadas a prever la situación de fraude y que forman parte de la regulación de la empresa:

4.2.1 La Gestión del fraude desde la perspectiva de cumplimiento regulatorio

a) Manual de Inducción: el documento fomenta la cultura ética y legal en todos los colaboradores al momento de su ingreso a la compañía. Este manual contiene el Código de Ética y Conducta, el Reglamento Interno del Trabajo y el Manual de Lavado de Activos, entre otra información vital para la relación con la empresa. Esta información está a disposición de los proveedores y clientes ya que se ha establecido un acceso web en el portal de la compañía que cualquier persona puede consultar.

b) Supervisión permanente: Auditoría Interna y la Unidad de Riesgos monitorean los diversos procesos de negocio y operativos de la compañía. Estas áreas analizan y evalúan las desviaciones en los procedimientos establecidos así como los diversos riesgos a los cuales los procesos podrían estar expuestos, incluyendo el riesgo moral de los empleados y fraudes. Los informes de ambas áreas son presentados de manera mensual ante el Comité de Gerencia y de manera trimestral ante el Directorio (Comité de Auditoría y Comité de Riesgos – ver tabla 4.1).

c) Comité de Incidentes: investiga, analiza y presenta informes de los casos de irregularidades ocurridas, tales como fraudes o conductas éticas inapropiadas, tanto internas como externas. Si bien no existe indicador alguno relacionado con la conducta ética, la Alta Dirección revisa y aprueba los planes de acción o medidas correctivas correspondientes.

d) Comité de Ética: Se encarga de vigilar el adecuado cumplimiento del Código de Ética y los estándares de conducta de la compañía.

e) Comité de Lavado de Activos: tiene como función principal analizar y evaluar, en apoyo al Oficial de Cumplimiento, si una operación puede ser considerada sospechosa de lavado de activos y del financiamiento del terrorismo.

4.2.2 Actividades de supervisión para la gestión del fraude

Rímac Internacional fomenta y gestiona la cultura ética y legal a través de los mecanismos descritos en la tabla mostrada a continuación:

TABLA 4.3

Mecanismos de Supervisión de la Cultura Ética y Legal en Rímac Internacional			
Mecanismo	Descripción	Mecanismo de comunicación	Participación de la Alta Dirección
Valores corporativos	El valor sinceridad incluye la honestidad y transparencia como componentes primordiales.	<ul style="list-style-type: none"> * Manual y Taller de Inducción para nuevos colaboradores * Protector de pantalla y murales * Revista interna * Actividades de celebración 	*Aprobación de los valores corporativos y participación en las actividades de celebración.

Mecanismos de Supervisión de la Cultura Ética y Legal en Rímac Internacional			
Mecanismo	Descripción	Mecanismo de comunicación	Participación de la Alta Dirección
Código de Ética y Estándares de Conducta	Compromiso de la empresa y sus colaboradores con altos principios de ética personal y profesional.	* Entrega del Código a todos los colaboradores. * Charla en Taller de Inducción. * Correo electrónico especial para reclamos y denuncias	* Aprobación del Código * Participación en Comité de Ética y Comité de Incidencias
Manual para Prevención de Lavado de Activos	Marco general de procedimientos y actividades para prevenir el lavado de activos.	* Entrega del manual a todos los colaboradores y publicación vía Web. * Correo electrónico de reporte. * Capacitación anual. * Charla en talleres de inducción	* Aprobación del Manual y Plan Anual de Trabajo. * Participación en el Comité para Prevención de Lavado de Activos
Reglamento Interno de Trabajo (RIT)	Establece los derechos y obligaciones de los colaboradores.	Entrega de RIT	Aprobación de RIT
Sistema de Control Interno	Evaluar el diseño y funcionamiento, así como el cumplimiento de las disposiciones legales e internas de la compañía	Explicado en punto P.1.b.1	Participación en Comité de Auditoría

Fuente: elaboración propia

4.3 Principales tipos y modalidades de fraude

Considerando la experiencia proveniente de los incidentes de fraude ocurridos en Rímac Internacional, la organización cuenta con tres tipologías que describiremos a continuación:

4.3.1 Tipificación

A continuación describiremos la tipología utilizada por Rímac Internacional:

4.3.1.1 Por procedencia del fraude

1. **Fraude Interno:** pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicado, al menos, un miembro de la empresa.
2. **Fraude externo:** pérdidas derivadas de dolos cometidos por parte de un tercero.

4.3.1.2 Por tipo de dolo

1. **Malversación de activos o apropiación indebida de recursos.-** Esta clasificación comprende, pero no se limita a:

- Hurto en sus distintas clasificaciones y formas.
- Apropiación física de bienes, sin la respectiva autorización.
- Apropiación de dinero, títulos representativos de valor o similares. Desfalcos.
- En general, toda apropiación, desviación o uso de los bienes de propiedad o bajo responsabilidad de la entidad para ser destinados a fines diferentes de aquellos para los cuales hayan sido específicamente adquiridos o recibidos.

2. **Corrupción.-** Tales como:

- Aceptación de un beneficio personal o para terceros como forma de influenciar una decisión administrativa.
- Cualquier pago hecho a un empleado de parte de un proveedor/corredor a cambio de un tratamiento favorable a este último.

- Sobornos a funcionarios públicos o privados por realizar una determinada acción u omitir una actuación.

3. Manipulación, falsificación o alteración de información financiera, de registros o documentos.- Dicha manipulación comprende, pero no se limita a:

- Alterar el registro de ingresos, para disminuir los resultados de un período.
- Alterar o registrar un egreso, en fecha diferente al de su causación, con el propósito de mejorar los resultados de un período.
- El traslado periódico de obligaciones reales o ficticias, de un acreedor o deudor a otro, real o ficticio, con el propósito de falsear la realidad de los saldos de cuentas por cobrar, cuentas por pagar u otros activos o pasivos.
- En general, toda manipulación contable de la realidad financiera de la entidad.

4.3.1.3 Inherentes a las actividades de seguros

- 1) Multiplicación de seguros en la contratación de la póliza: de forma premeditada, una persona asegura su vehículo con varios seguros, para reclamar a las respectivas aseguradoras un mismo siniestro.
- 2) Ocultar o falsear datos en la solicitud de seguro.
- 3) Contratación de pólizas sin interés asegurable (seguros de vida): el contratante de la póliza asegura a tercero sin vínculo evidente (interés asegurable) con la finalidad de solicitar la anulación del seguro luego de pagada la póliza con la finalidad de obtener la devolución de lo pagado lavando activos.
- 4) Falsificación de documentos: falsificación de firmas de clientes en solicitudes con el objetivo de cumplir cuotas de ventas.
- 5) Falsificación de siniestros: Tales como, simulación de robo, atenciones médicas falsas, muerte simulada.

4.4 Análisis de Brechas para la implementación de un Programa Crítico Antifraude en Rímac Internacional

El siguiente análisis ha sido realizado contrastando el apartado 2.2 "Marco de Referencia para la Gestión del Riesgo de Fraude" en el capítulo II y la situación actual de Rímac Internacional sobre la gestión del riesgo de fraude en el apartado 4.2 "Gestión del Fraude en Rímac Internacional" del presente capítulo.

4.4.1 Análisis del Gobierno sobre la Gestión del Fraude

Para calificar el cumplimiento de las prácticas sobre Gobierno para la Gestión del Fraude se utilizará el siguiente criterio de valoración:

TABLA 4.4

Calificación sobre el Grado de Cumplimiento				
No Cumple	Cumple algunas pautas	Cumple Parcialmente	Cumple casi en su totalidad	Cumple Integralmente
0%	25%	50%	75%	100%

Fuente: elaboración propia

Para el contraste tomamos en consideración las prácticas sugeridas sobre la definición de Roles y Responsabilidades (apartado 2.2.1.1 del capítulo II) y las prácticas respecto a los elementos claves para un efectivo Programa Crítico Antifraude (apartado 2.2.1.2 del capítulo II).

4.4.1.1 Roles y Responsabilidades

Como resultado, concluimos que Rímac Internacional cumple íntegramente con uno de los cinco roles y parcialmente con tres de ellos, lo que en promedio se traduce en un cumplimiento al 65%. Ver [ANEXO VII](#) – "Análisis de Brecha Respecto a los Roles y Responsabilidades sobre la Gestión del Fraude".

Del análisis realizado, se identificaron las siguientes brechas:

- Necesidad de incrementar el número de miembros independientes en el Directorio.
- Implementar un programa integral para la gestión y evaluación del riesgo de fraude.

- Se requiere desarrollar un documento que consolide las políticas y el compromiso de la empresa respecto a la lucha contra el fraude.
- Se necesita implementar programas de capacitación.
- Implementar una metodología para la investigación preventiva y detectiva por parte de Auditoría Interna sobre posibles eventos de fraude

4.4.1.2 Elementos Claves

Como resultado, concluimos que Rímac Internacional cumple íntegramente con tres de los elementos y parcialmente con siete de ellos, cumpliendo en promedio con el 62% de estos. Ver [ANEXO VII](#) – “Análisis de Brecha respecto al cumplimiento de los Elementos Claves para la implementación de un efectivo Programa Antifraude”.

4.4.2 Evaluación del Riesgo de Fraude

Con la finalidad de determinar el grado de implementación de las fases requeridas para contar con un adecuado marco para la Evaluación de Riesgos de Fraude se utilizará el siguiente criterio de valoración:

TABLA 4.5

Calificación sobre el Grado de Cumplimiento				
No Cumple	Cumple algunas pautas	Cumple Parcialmente	Cumple casi en su totalidad	Cumple Integralmente
2	4	6	8	10

Fuente: elaboración propia

Tomando como referencia la información descrita en el apartado 4.2 del presente capítulo respecto a la Gestión del Fraude en Rímac Internacional y las prácticas sugeridas en el apartado 2.2.2 “Evaluación del Riesgo de Fraude” del capítulo II, se obtuvo como resultado que los marcos de evaluación para los Riesgos de Fraude

Ocupacional y Riesgo de Fraude Externo cumplen hasta un 48% las prácticas sugeridas.

TABLA 4.6

Calificación sobre la Gestión del Fraude						
Fases para la Evaluación del Riesgo de Fraude	Fase 1	Fase 2	Fase 3	Fase 4	Fase 5	Calificación Final
Riesgo de Lavado de Activos (Peso 40% - Carácter Regulatorio)	8	8	8	8	8	8
Riesgo de Fraude Ocupacional (Peso 30%)	4	4	6	6	4	4.8
Riesgo de Fraude Externo (Peso 30%)	4	4	6	6	4	4.8
Calificación sobre las Fases	5.6	5.6	6.8	6.8	5.6	6.08

Fuente: elaboración propia - Ver detalle en [ANEXO IX](#).

Con el análisis realizado se identificaron las siguientes brechas:

- Se requiere implementar programas de sensibilización sobre el fraude.
- Se requiere elaborar un programa de capacitación electrónica sobre entendimiento del Código de Ética que incluya test (examen).
- Se requiere actualizar y mejorar la versión actual del Código de Ética, a fin de que incluya el procedimiento que deben seguir los proveedores, corredores y clientes para informar a la compañía acerca posibles casos de conflicto de interés.
- No se han establecido criterios marco homogéneos para establecer el objetivo de la evaluación del riesgo de fraude de manera preventiva (Tipificación según la Asociación de Examinadores de Fraude / Por tipo de delito).
- No se cuenta con documentación formal sobre el procedimiento seguido para la investigación análisis y conclusiones de los casos de irregularidades detectadas.
- No se cuenta con indicadores de comportamiento ético.
- No se cuenta con un esquema estructurado de procedimientos para la evaluación continua ni para la detección oportuna de potenciales fraudes.

4.4.3 Prevención del Fraude

Tomando como referencia las prácticas sugeridas en el apartado 2.2.3 “Prevención del Fraude -Capítulo II- realizamos el análisis de brechas entre los controles preventivos de fraude existentes en Rímac Internacional y los sugeridos sobre la base de las dimensiones del modelo COSO. Como resultado, identificamos que la empresa cumple con un 63% de las prácticas sugeridas. Ver [ANEXO X](#) “Análisis de Brecha – Controles Preventivos”. Del análisis realizado, se identificaron las siguientes brechas:

- No se cuenta con una Política Antifraude.
- La validación de antecedentes penales y policiales no es obligatoria al momento del proceso de selección, salvo en puestos claves de la organización.
- No se cuenta con actividades de monitoreo continuo.

Asimismo, se identificaron brechas detectadas en la evaluación realizada de los apartados 4.4.2 y 4.4.1 del presente capítulo.

4.4.4 Detección del Fraude:

Rímac Internacional cuenta con los siguientes métodos para la detección de fraude:

- a) Denuncia vía correo electrónico.
- b) Revisiones de Auditoría: Interna, Externa, Regulatoria y Corporativa.
- c) Denuncia vía comunicación a Auditoría Interna.
- d) Controles de TI.
- e) Controles para la prevención del fraude por Lavado de Activos y Financiamiento del Terrorismo.

Consideramos necesario que Rímac Internacional refuerce sus mecanismos de reporte de fraude incorporando un marco para la captura, análisis y categorización de alertas de fraude. Asimismo, se requiere reforzar el esquema de reporte vigente (correo electrónico) e incorporar otros métodos como líneas anónimas. Finalmente, consideramos relevante que la compañía adopte prácticas de monitoreo continuo. Considerando estas brechas, identificamos un grado de cumplimiento del 65%.

4.4.5 Investigación del Fraude y Acciones Correctivas

De la información contenida en el apartado 4.2 Gestión del Fraude en Rímac Internacional del presente capítulo, las actividades de investigación son realizadas de manera reactiva. Como resultado, presenta un cumplimiento del 50%.

Finalmente, del análisis efectuado se infiere que Rímac Internacional requiere cerrar las brechas identificadas para la implementación total de un programa crítico antifraude efectivo.

CAPÍTULO V PROPUESTA DE PROGRAMA CRÍTICO ANTIFRAUDE EN LA COMPAÑÍA RÍMAC INTERNACIONAL

El presente capítulo desarrolla la propuesta de implementación de un Programa Crítico Antifraude (PCA) para Rímac Internacional. El PCA pretende ser una plataforma estratégica para la gestión del fraude, alineada con las mejores prácticas descritas en el capítulo II y cubriendo así los frentes de prevención, detección y respuesta al riesgo de fraude.

El PCA propuesto busca ser una solución que funcione de manera integral, alineada con los objetivos estratégicos de la empresa y sobre la cual se puedan incorporar todos los procesos críticos de la compañía. Para fines demostrativos de la presente tesis, la propuesta describirá, a manera de ejemplo, la incorporación del Proceso de Gestión de Seguridad de la Información al PCA. La selección de este proceso se basa en el alto grado de madurez que presenta, considerando los siguientes aspectos:

- a) Desde el 2009 la compañía cuenta con un Sistema para la Gestión de la Seguridad de la Información (SGSI), diseñado por la consultora PriceWaterHouseCoopers alineado con la normativa ISO 27001 “Gestión de la Seguridad”.
- b) El SGSI se encuentra alineado con el marco normativo exigido por la Superintendencia de Banca y Seguros Peruana bajo la circular G140-2009 y es evaluado anualmente tanto por la unidad de Auditoría Interna de Rímac Internacional, como por Auditoría Corporativa, Auditoría Externa, así como por la Superintendencia de Banca y Seguros Peruana.
- c) La compañía cuenta con una Política de Seguridad de la Información, sobre la cual se ha desarrollado un marco normativo para los aspectos operativos y de procedimiento. El marco normativo está compuesto por directivas, procedimientos, instructivos y formatos.

Finalmente, el PCA propuesto incorpora una etapa denominada “Implementación de Planes de Acción”. Dicha etapa propone la implementación de Planes de Acción en respuesta a las brechas identificadas en el apartado 4.4 “Análisis de Brechas respecto a los elementos claves para la implementación de un Programa Crítico Antifraude” en el capítulo IV.

5.1 Nombre, descripción y objetivos del Programa Crítico Antifraude

Nombre: Programa Crítico Antifraude o “PCA”. Ver capítulo IV.

Descripción: El PCA propuesto es una plataforma que incluye elementos para la prevención, detección y respuesta al riesgo de fraude.

Objetivos: La finalidad de toda compañía al poner en marcha un Programa Crítico Antifraude, es asegurar el valor de sus operaciones.

Para lograr dicha meta, el PCA propuesto para Rímac Internacional tiene como objetivo:

- a. Afianzar la cultura antifraude para prevenir y detectar oportunamente los riesgos de fraude inherentes a los procesos y los relacionados con el sector.
- b. Definir roles, responsabilidades y participación de todo el personal respecto al fraude.
- c. Consolidar el compromiso de prevenir, detectar y luchar contra el fraude, frente a los órganos de control y supervisión gubernamentales del Perú.
- d. Contar con recursos adecuados y orientados a la detección, prevención y respuesta al fraude.
- e. Fortalecer la efectividad y eficiencia de las investigaciones de fraude, contando con procedimientos que aseguren la calidad, conducción y oportunidad de las mismas.

5.2 Alcance del Programa

El PCA comprende la implementación de los cinco principios descritos en el apartado 2.2 “Marco de Referencia para la Gestión del Riesgo de Fraude”.

5.3 Beneficios propuestos de la implementación:

A continuación citaremos los beneficios esperados por la implementación de un frente integral antifraude:

5.4 Al Gobierno Corporativo

Ser una solución que refuerce el compromiso de la Alta Gerencia y del Directorio respecto a la gestión del riesgo de fraude.

5.4.1 Al Control Interno

Incorporar al Sistema de Control en curso, controles antifraude que reforzarán las actividades de control existentes.

5.4.2 La Gestión de Riesgos

Brindar una plataforma que permita a la compañía mantener de manera vigente la evaluación y valorización de los riesgos de fraude, impactando directamente y de forma positiva en el componente de control interno de riesgos de la compañía.

5.4.3 Las actividades de monitoreo continuo y supervisión

Reforzar la calidad y la efectividad de los programas y controles antifraude.

5.5 Diseño del Programa

El diseño propuesto se basa en la implementación de las siguientes actividades:

1. **PRINCIPIO 1 Definición del Gobierno para la Gestión del Fraude:**

Considerando que la compañía ya cuenta con un marco normativo donde se han definido roles y funciones sobre el control interno (apartado 4.1 "Descripción de la Compañía" - capítulo IV); los aspectos que se encuentran pendientes de implementar para contar con un adecuado entorno de gobierno para la Gestión de Fraude, son:

- a) Incrementar el número de directores independientes en el Directorio.
- b) Elaborar una Directiva, así como una Política respecto al Fraude. Dicho documento debe incluir la definición de roles, responsabilidades, la metodología para la evaluación de riesgos de fraude, los lineamientos de denuncia y protección del denunciante, así como el proceso de investigación.
- c) Definir estrategias de comunicación y difusión sobre el compromiso de la compañía respecto a la lucha contra el fraude interno.
- d) Definir e implementar programas de capacitación respecto al fraude ocupacional y de seguros.

2. **PRINCIPIO 2 Evaluación de Riesgos de Fraude:** una vez definidos los roles y funciones que soportarán el sistema del Programa Crítico Antifraude, la compañía deberá seleccionar un proceso sobre el cual iniciar la gestión del riesgo de fraude.

En este caso, realizaremos una simulación de Evaluación del Riesgo de Fraude aplicado al ámbito de la Gestión de la Seguridad de Tecnología de la Información en Rímac Internacional tomando como referencia los riesgos de fraude en tecnología descritos por IIA (Institute of Internal Auditors) en el Global Technology Audit Guide para la Prevención y Detección del Fraude en un Mundo Automatizado. Para la evaluación del proceso seleccionado, nos entrevistamos con el Gerente de Tecnología (Sr. Martin Kerrigan) para realizar la Evaluación de Riesgos de Fraude. Dicha evaluación ha sido documentada tomando la matriz de evaluación de riesgos propuesta por la ACFE (The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiner 2010: 55).

Como resultado de la evaluación realizada en la tabla 5.1, identificamos que se requiere implementar las siguientes acciones para consolidar los frentes de prevención y detección sobre el proceso de Gestión de la Seguridad de la Información. Dichas acciones están relacionadas a la aplicación de los Principios tres, cuatro y cinco.

3. PRINCIPIO 3 Prevención del Fraude:

- Implementar líneas anónimas para el reporte de posibles eventos de fraude. Este plan de acción servirá para todos los procesos que se implementen en el PCA.
- Elaborar y difundir los siguientes lineamientos: Política Antifraude. (Propuesta en el PRINCIPIO1), Política de Seguridad de la Información a proveedores y el Código de Ética y Conducta a Proveedores

4. PRINCIPIO 4 Detección del Fraude:

- Implementar un sistema para la captura, evaluación y categorización de alertas de fraude. Este plan de acción servirá para todos los procesos que se implementen en el PCA.

- Implementar actividades de monitoreo continuo a través de herramientas de explotación de información. Dicha tareas pueden ser llevadas a cabo por el área de Auditoría Interna a través de la herramienta ACL.

5. PRINCIPIO 5 Investigación y Respuesta al Fraude:

- Implementar protocolos para la conducción de investigaciones de fraude.
- Elaborar protocolos de respuesta y comunicación frente hechos de fraude que deban ser reportados a entes reguladores locales, internacionales y a otros grupos de interés.

Para la implementación exitosa de estas prácticas es importante resaltar la necesidad de un alto grado de compromiso por parte de la Alta Gerencia y en especial del personal que se asigne para liderar el despliegue de las actividades.

CAPÍTULO VI ANÁLISIS COSTO BENEFICIO DE LA IMPLEMENTACIÓN DEL PROGRAMA CRÍTICO ANTIFRAUDE.

Con la finalidad de dimensionar el costo y el tiempo que llevaría a la compañía definir los componentes de alto nivel (Gobierno), así como la definición de una estrategia para la implementación del Programa Crítico Antifraude, determinamos un cronograma aproximado de cuatro meses. Ver [ANEXO XII](#) – Cronograma Definición de Planes de Acción.

En base al cronograma propuesto, solicitamos a dos compañías consultoras con sede en Lima, Perú, una cotización tentativa. Como resultado, ambas cotizaciones se valorizaron en un promedio de \$83 mil dólares americanos.

6.1 Recuperación de la Inversión:

Considerando los montos defraudados reportados durante los últimos cinco años (2005 – 2010), los cuales superan en promedio un millón y medio de soles, la inversión calculada debe ser medida con respecto a los fraudes que el PCA ayudará a prevenir a la compañía.

6.2 Trascendencia de la implementación del Programa Crítico Antifraude en Rímac Internacional:

Para medir la trascendencia, elaboramos una encuesta del tipo cualitativo ([Ver ANEXO XIII](#)). Dicha encuesta fue aplicada a los siguientes colaboradores de Rímac Internacional:

Sr. Mario Potestá	Gerente de la División Transformación y Tecnología
Sr. Manuel de la Flor	Oficial de cumplimiento
Sra. Jessica Zuñiga	Jefe de Auditoría Interna
Sr. Akio Murakami	Gerente del Área de Soporte de Negocios
Sr. Martin Kerrigan	Gerente de Tecnología

El detalle de las mismas se encuentra en ANEXO XIV del presente documento.

A continuación presentamos los resultados de las encuestas realizadas:

1. En promedio el 60% de los encuestados consideran que la compañía Rímac Internacional requiere reforzar o implementar mecanismos para la prevención y detección de riesgos de
2. El 75% de encuestados considera que un Esquema de Monitoreo Continuo sobre transacciones susceptibles de fraude ayudaría a la detección oportuna de fraudes.
3. El 40% de los encuestados consideran que la implementación de mecanismos de cómputo forense significaría un esfuerzo altamente complejo,

Por otro lado, de la encuesta efectuada identificamos que el 100% de los encuestados coincidieron en:

- a) Que un esquema de monitoreo continuo en procesos y transacciones críticas ayudaría a la detección oportuna de posibles eventos de fraude.
- b) La implementación de un PCA reforzaría el cumplimiento de sus funciones, bajo un entorno de control adecuado.
- c) La implementación de un PCA promovería la interacción necesaria para la creación de una cultura de prevención y detección del fraude.
- d) Reforzaría la posición de cumplimiento de la empresa frente a los entes reguladores.
- e) La implementación de un PCA impactaría positivamente en la eficiencia de los procesos.
- f) La implementación de un PCA aportaría valor al enfoque estratégico actual.

Conclusiones y Recomendaciones

Si bien se observa que Rímac Internacional cuenta con mecanismos articulados para la gestión del riesgo de fraude tal como se ha observado a lo largo de la investigación, la compañía no cuenta con un Programa Integral para la Gestión y Evaluación del Riesgo de Fraude. Resulta necesario que Rímac Internacional refuerce sus mecanismos actuales para la gestión del fraude dentro de esquemas integrales, incorporando un marco homogéneo para la captura, análisis y categorización de alertas de fraude, así como para el proceso de investigación y de monitoreo continuo del riesgo.

Finalmente, consideramos que la aplicación de un Programa Crítico Antifraude es el modelo de control completo para la gestión del riesgo de fraude y recomendamos su aplicación como la solución integral para prevenir y detectar oportunamente los riesgos de fraude inherentes a los procesos, así como para el tratamiento de los eventos ocurridos. Este esquema no solo reforzará el compromiso de la Alta Gerencia y del Directorio frente a la gestión del riesgo de fraude sino que, además, permitirá asegurar el valor de las operaciones de la empresa en términos económicos, operativos y de imagen corporativa frente a reguladores, clientes o grupos de interés.

BIBLIOGRAFÍA

ACL Services Ltd

2010 «Fraud Detection Using Data Analytics in the Insurance Industry» [9]. s.l.
 Consulta: 12 de Julio de 2011.
 <http://www.acl.com/pdfs/DP_Fraud_detection_INSURANCE.pdf>

Albrecht et al. Y Zimbelman

2011 «The Nature of Fraud». *Fraud Examination*. 4ta ed. Mason: South-Western Cengage Learning, pp 6. Fecha de consulta: 17/04/2011.
 <http://books.google.com.pe/books?id=SBzJYBs-FPIC&printsec=frontcover&dq=Fraud+definition+Albrecht&source=bl&ots=30IVQvb3pb&sig=y0IWLqB7ET2VSP9cAdFEtpY4BE&hl=es&sa=X&ei=VwogUPvRHe_6AGBp4CQCw&ved=0CDEQ6EwAA#v=onepage&q=Fraud%20definition%20Albrecht&f=false>

Asociación de Examinadores de Fraudes Certificados (ACFE)

2012 «Report to the Nations on Occupational Fraud and Abuse». 2012. Fecha de consulta: 3 de agosto 2012.
 <http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rtnn/2012-report-to-nations.pdf>.

2010 «Report to the Nations on Occupational Fraud and Abuse». 2010. Fecha de consulta: 12 de julio 2011.
 <http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/rtnn-2010.pdf>

2008 «Report to the Nations on Occupational Fraud & Abuse». 2010. Fecha de consulta: 03 de junio 2011.
 <http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/2008-rtnn.pdf>

Baldillo A. Jorge

s.f. «Auditoría Forense - Fundamentos» En: The Institute of Internal Auditors. 2011.
Fecha de consulta: 05 de abril de 2011.
< <http://www.theiia.org/chapters/pubdocs/70766573/Auditoria.pdf>>.

Bell, Eric

2009 « Internal Control Checklist: 5 Anti-Fraud Strategies to Deter, Prevent, and Detect Fraud» En: Corporate Compliance Insights. 2010. Fecha de consulta: 27 de marzo de 2011. < <http://www.corporatecomplianceinsights.com/2010/internal-control-checklist-deter-prevent-detect-fraud/>>

Bishop, Toby J.F y Frank E. HYDOSKI

2010 “*Capacidad de recuperación empresarial: administración del creciente riesgo de fraude y corrupción*”. En: MANTILLA, Samuel Alberto (trad.). *Administración del creciente riesgo de fraude y corrupción*. Colombia: ECOE Ediciones.

Center for Audit Quality

2010 «Deterring and Detecting Financial Reporting Fraud» En: Center for Audit Quality. 2011. Fecha de consulta: 13 de febrero 2011 pp. 3-5.
<<http://www.thecaq.org/Anti-FraudInitiative/CAQAnti-FraudReport.pdf>>.

CESVI

2011 «Cultura Antifraude. Una iniciativa de CESVI Argentina». s.l. Fecha de consulta: 17 de mayo de 2011.
<<http://www.culturaantifraude.com/evento.html>>
s.f. «Software» s.l. Fecha de consulta: 17 de mayo de 2011.
<<http://www.cesvi.cl/software.htm>>

Colegio de Contadores Públicos de México

2005 «Consideraciones sobre fraude». [10]. México: Colegio de Contadores Públicos de México. Consulta: 13 de junio 2011.

<<http://www.ccpm.org.mx/avisos/boletines/boletinindependiente8.pdf>>

Corner J. Michael

1987 “*El fraude en la empresa. Manual para su detección*”. 2da Edición. España: Ediciones Deusto, S.A, pp. 41-4x

Deloitte Touche Tohmatsu

2008 «Programas & Controles Antifraude» [34]. Colombia: DeloitteTouche Tohmatsu. Consulta: 15 de mayo 2011.

<<http://webserver3.deloitte.com.co/A%20WEB%20Recursos/Rec%20Auditoria/2.%20Fraude/Programas%20y%20Controles%20Antifraude.pdf>>

2010 «The cost of fraud»[7]. s.l. DeloitteTouche Tohmatsu. Consulta: 15 de mayo 2011.

<http://www.deloitte.com/view/en_US/us/Services/Financial-Advisory-Services/Forensic-Center/0570e7560aaa7210VgnVCM200000bb42f00aRCRD.htm>

Ernst & Young Global Limited (EYG)

2010 «Driving ethical growth – new markets, new challenges. 11th Global Fraud Survey » En: Ernst&Young. 2011. Fecha de consulta: 6 de febrero 2011.

<<http://www.ey.com/au/GL/en/Services/Assurance/Fraud-Investigation---Dispute-Services/11th-Global-Fraud-Survey---Driving-ethical-growth---new-markets--new-challenges>>.

2011 «Driving ethical growth – new markets, new challenges. 11th Global Fraud Survey » En: *Ernst&Young*. 2011. Fecha de consulta: 6 de febrero de 2011.

<<http://www.ey.com/GL/en/Services/Assurance/Fraud-Investigation---Dispute->

Services/11th-Global-Fraud-Survey---Driving-ethical-growth---new-markets--
new-challenges

2011 «Sesión 6: Auditoría Forense Maestría en Auditoría – Universidad del Pacífico»
En: *Ernst&Young*. 2011. Consulta: agosto 2011.

KPMG

2010 «Fraud and Misconduct Survey 2010»[48] Australia: KPMG. 2010. Fecha de
Consulta: 7 de junio de 2011. [48]

<<https://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Documents/Fraud-and-Misconduct-Survey-2010.pdf>>

2010 «El Fraude Corporativo en Latinoamérica 2008-2010» [18] Argentina: KPMG.
2010. Fecha de Consulta: 7 de junio de 2011. [48]

< http://www.kpmg.com.ar/fraude/PDF/El_Fraude_Corporativo.pdf >

Lawrence G. Michael y Joseph T. Wells

2004 «Basic Legal Concepts. Beware insufficient knowledge of the law» En: Journal
of Accountancy. 2011. Fecha de consulta: 05 de abril de 2011. <
<http://www.journalofaccountancy.com/Issues/2004/Oct/BasicLegalConcepts.htm>
>.

MAPFRE

2010 «MAPFRE Informe Anual 2010» En: Mapfre Colombia. Fecha de consulta: 30 de
agosto de 2011. pp 21.

<http://www.mapfre.com.co/es/c/document_library/get_file?uuid=6374bed3-1ecc-42f7-ab45-7851bf1d6928&groupId=18>

2006 «El Seguro de Automóviles en Iberoamérica» En: Fundación Mapfre. 2006.
Fecha de Consulta: 18 de agosto de 2011. pp 24-25

<<http://www.mapfre.com/ccm/content/documentos/fundacion/cs-seguro/libros/el-seguro-de-automoviles-en-iberoamerica-101.pdf>>

PricewaterhouseCoopers LLP

2010 «Face to Face. Fraudulent relationships in general insurance» En: PricewaterhouseCoopers. 2011. Fecha de consulta: 6 de febrero de 2011. <http://www.pwc.com/jm/en/research-publications/series_on_fraud.jhtml>.

Pomerrantz, Glenn y Timothy L. MOHR

s.f «Opportunity in a Downturn: The Value of an Anti-Fraud Program». En: BDO Consulting. Fecha de consulta: 25/02/2011. <<http://www.bdoconsulting.com/news/docs/Corporate_Governance_Advisor_Article_-_12.18.08.pdf>>

Government Printing Office

2002 «Public Law 107- 204 – Sarbanes- Oxley Act of 2002». En: *U.S. Government Printing Office / Keeping America Informed*. Fecha de consulta: 25/02/2011. <<http://www.gpo.gov/fdsys/pkg/PLAW.107publ204/content-detail.htm>>

Superintendencia de Banca y Seguros y AFP del Perú

2011 «Empresas de Seguros» En: Perú. Fecha de Consulta: 17 de julio de 2011. <http://www.sbs.gob.pe/0/modulos/JER/JER_Interna.aspx?ARE=0&PFL=1&JER=293>

2011 «Prevención de Lavado de Activos» En: Perú. Fecha de Consulta: 17 de julio de 2011 <http://www.sbs.gob.pe/0/home_lavado_activos.aspx>

2009 «Circular N° G-140-2009 Gestión de la Seguridad de la Información». Archivo de Acrobat Reader. Lima, 2009, pp.1-9.

2008 «Resolución N° 838-2008 Normas Complementarias para la Prevención del Lavado de Activos y del Financiamiento del Terrorismo». Archivo de Acrobat Reader. Lima, 2008, pp.1-9.

2008 «Resolución N° 37-2008 Reglamento de la Gestión Integral de Riegos». Archivo de Acrobat Reader. Lima, 2008, pp.1-13.

VONA, Leonard W.

2006 «Fraud Definitions».[9] Siena: Marina Kinner. Consulta: 16 de junio de 2011.

<<http://www.fraudauditing.net/FraudDefinitions.pdf>>

The Institute of Internal Auditors (IIA)

2011 «Conducting Fraud Risk Assessments» [16]. En: *Institute of Internal Auditors San Jose Chapter*. Fecha de consulta: 14/08/2011. Febrero del 2011.

<http://www.theiia.org/chapters/pubdocs/79/Conducting_a_Fraud_Risk_Assessment.pdf >

2009 «Global Technology Audit Guide – Fraud Prevention and Detection in an Automated World». En: *The IIA Research Foundation Bookstore*. Fecha de consulta: 14/08/2011. Diciembre de 2009.

<<http://www.theiia.org/bookstore/product/global-technology-audit-guide-gtag-13-fraud-prevention-and-detection-in-an-automated-world-download-pdf-1464.cfm>>

The Institute of Internal Auditors (IIA), The American Institute of Certified Public Accountants (AICPA) y Association of Certified Fraud Examiners (ACFE)

2010 «Managing the Business Risk of Fraud: A Practical Guide». Consulta: 2 de mayo de 2011< http://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf>

The Insurance Information Institute

2011«Fraud» New York. 2011. Consulta: 28 de abril de 2011.

<http://www.iii.org/facts_statistics/fraud.html>

Wells T. Joseph

2001 «Why Employees Commit Fraud» En: Association of Certified Fraud Examiners. 2011. Fecha de consulta: 27 de marzo de 2011.

< <http://www.acfe.com/resources/view.asp?ArticleID=41>>

Wolfe T. David y Dana R. Hermanson

2004 «The Fraud Diamond: Considering the Four Elements of Fraud» En: *The CPA Journal*. 2009. Fecha de consulta: 27 de marzo de 2011.
<<http://www.nysscpa.org/cpajournal/2004/1204/essentials/p38.htm>>

ANEXO I – Glosario de Términos del Sector Asegurador

Asegurado: En sentido estricto, es la persona que en sí misma o en sus bienes o intereses económicos está expuesta al riesgo.

Asegurador: Nombre que se da a la entidad de seguros que mediante la formalización de un contrato de seguro, asume las consecuencias dañosas producidas por la realización del evento cuyo riesgo es objeto de cobertura

Beneficiario: Persona designada en la póliza por el asegurado o contratante como titular de los derechos indemnizatorios que en dicho documento se establece.

Cobertura: Compromiso aceptado por un asegurador en virtud del cual se hace cargo, hasta el límite estipulado, de las consecuencias económicas derivadas de un siniestro.

Comisión: Sistema de retribución económica de las funciones de producción de los agentes, consistente en una parte proporcional de las primas conseguidas por estos en su labor comercial directa o a través de su intervención o colaboración.

Contratante: Persona que suscribe con una entidad aseguradora una póliza de seguro. Generalmente, su personalidad coincide con la del asegurado.

Contrato de seguro: Documento escrito con una entidad de seguros en el que se establecen las normas que han de regular la relación contractual de aseguramiento entre ambas partes (asegurador y asegurado), especificándose sus derechos y obligaciones respectivos. Este contrato se caracteriza por ser fundamentalmente consensual, bilateral, aleatorio, oneroso, de adhesión y por estar basado en la buena fe.

Dolo: Sinónimo de mala fe.

Duración del seguro: Plazo durante el cual tiene vigencia las garantías de un contrato de seguro. Este plazo comienza con la fecha de efecto inicial de la póliza y finaliza con el vencimiento de esta, que suele ser un año.

Fraude en el seguro: En general, situación que se produce cuando el propio asegurado ha procurado intencionalmente la ocurrencia del siniestro o exagerado sus consecuencias con ánimo de conseguir un enriquecimiento injusto a través de la

indemnización que espera lograr del asegurador. En sentido amplio, una actuación fraudulenta es aquella que se realiza en contra del principio de buena fe.

Garantía: Compromiso aceptado por un asegurador en virtud del cual se hace cargo, hasta el límite estipulado, de las consecuencias económicas derivadas de un siniestro.

Gastos: Conjunto de desembolsos que debe realizar una entidad a consecuencia directa o indirecta del ejercicio de sus actividades empresariales. En una entidad de seguros, son los derivados de la práctica de la actividad aseguradora.

Incapacidad: En el seguro de Accidentes, se denomina así a la imposibilidad de una persona para el desarrollo de sus funciones normales.

Indemnización: En el seguro de Accidentes, se denomina así a la imposibilidad de una persona para el desarrollo de sus funciones normales.

Indemnización: Importe que está obligado a pagar contractualmente la empresa aseguradora en caso de producirse un siniestro. Es por ello, la contraprestación que corresponde al asegurador frente a la obligación de pago de prima que tiene el asegurado.

Interés asegurable: Requisito que debe concurrir en quien desee la cobertura de determinado riesgo, reflejado en su deseo sincero de que el siniestro no se produzca, ya que a consecuencia de él originará un perjuicio a su patrimonio.

Notificación del siniestro: Comunicación al asegurador que efectúa el asegurado para darle cuenta de la ocurrencia de un siniestro. Es una de las obligaciones principales del asegurado, en caso de siniestro, cuyo incumplimiento (dentro de un plazo determinado en las condiciones generales de las pólizas) puede dar lugar a la pérdida de la indemnización debida por el asegurador.

Objeto del seguro: Es la compensación del perjuicio económico experimentado por un patrimonio a consecuencia de un siniestro. También es el bien material afecto al riesgo sobre el cual gira la función indemnizatoria.

Obligaciones del asegurador: Se refieren principalmente al pago de la indemnización acordada en póliza, una vez producido el siniestro.

Pago de primas: Es una de las obligaciones esenciales del asegurado, hasta el punto de que mientras no se cumpla no tomará efecto el contrato.

Póliza: Documento que instrumenta el contrato de seguro, en el que se reflejan las normas que de forma general, particular o especial regulan las relaciones contractuales convenidas entre el asegurador y el asegurado. En tanto haya sido emitido y aceptado por ambas partes se puede decir que han nacido los derechos y obligaciones que del mismo se derivan. Pese al tratamiento unitario que la legislación concede a la póliza de seguro, en la práctica es frecuente distinguir partes diferenciadas de ella, cuya denominación está íntimamente ligada a su contenido. En este sentido, puede hablarse de condiciones generales, condiciones particulares y condiciones especiales.

Prima: Aportación económica que ha de satisfacer el contratante o asegurado a la aseguradora en concepto de contraprestación por la cobertura de riesgo que esta le ofrece.

Ramo: Modalidad o conjunto de modalidades de seguro relativas a riesgos de características o naturaleza semejantes. En este sentido se habla de Ramo de Automóviles, Ramo de Incendios, entre otros.

Reclamación: En general, es una solicitud planteada a una persona para la satisfacción de un derecho; en la terminología aseguradora, esta palabra se utiliza frecuentemente para referirse a la demanda de indemnización.

Riesgo: En la terminología aseguradora, se emplea este concepto para expresar indistintamente dos ideas diferentes; de un lado, riesgo como objeto asegurado; de otro riesgo como posible acontecimiento, cuya aparición real o existencia se previene y garantiza en la póliza.

Seguro: Es una actividad económico-financiera que presta el servicio de transformación de los riesgos de diversa naturaleza a que están sometidos los patrimonios, en un gasto periódico presupuestable, que puede ser soportado fácilmente por cada unidad patrimonial.

Siniestro: Es la manifestación concreta del riesgo asegurado, que produce unos daños garantizados en la póliza hasta determinada cuantía

Fuente: Asociación Peruana de Empresas de Seguro. Consultada el 20 de mayo de 2011. <<http://www.apeseg.org.pe/j.html>>

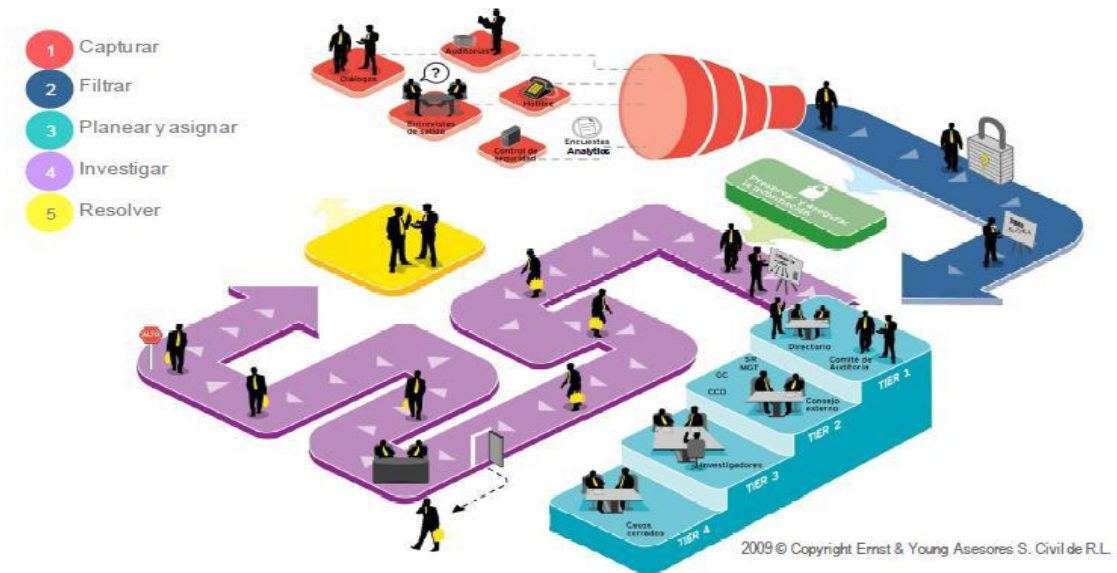
ANEXO II – Matriz de Decisión sobre el Fraude

Acción Requerida	Unidad de Investigación	Auditoría Interna	Contabilidad Financiera	Gerencia General	Gerencias de Línea	Gerencia de Riesgo	Relaciones Públicas	Relaciones con Empleados	Legal
1 Controles para la prevención del Fraude	RS	RS	RS	RP	RC	RS	RS	RS	RS
2 Reporte de Incidentes	RP	RS	RS	RS	RS	RS	RS	RS	RS
3 Investigación del Fraude	RP	RS					RS	RS	RS
4 Cumplimiento Regulatorio	RP								RS
5 Recuperación de Montos Defraudados	RP								
6 Recomendaciones para la prevención de Fraudes	RC	RC	RS	RS	RS	RS	RS	RS	RS
7 Revisión de Controles Internos		RP							
8 Manejar casos sensitivos	RP	RS		RS		RS		RS	RS
9 Publicidad / Comunicados de Prensa	RS	RS					RP		
10 Litigios Civiles	RS	RS							RP
11 Acciones Correctivas / Recomendaciones para prevenir ocurrencias	RC	RC		RS	RC	RS			RS
12 Monitoreo para asegurar la recuperación	RS		RP						
13 Auditoría Proactiva sobre el Fraude	RS	RP							
14 Entrenamiento Antifraude	RP	RS			RS		RS		
15 Análisis de Riesgo	RS	RS				RP			
16 Análisis de Casos	RP	RS							
17 Línea de Reporte de Fraudes	RP	RS							
18 Línea Ética	RS	RS							RP
RP Responsabilidad Primaria									
RS Responsabilidad Secundaria									
RC Responsabilidad Compartida									

Fuente: Ernst & Young

ANEXO III – Proceso de Investigación para el Fraude

ERNST&YOUNG 2010



Fuente: Ernst & Young

ANEXO IV – Principios de Bueno Gobierno Corporativo en el Perú

LOS DERECHOS DE LOS ACCIONISTAS

1. No se debe incorporar en la agenda asuntos genéricos, debiéndose precisar los puntos a tratar de modo que se discuta cada tema por separado, facilitando su análisis y evitando la resolución conjunta de temas respecto de los cuales se puede tener una opinión diferente.
2. El lugar de celebración de las Juntas Generales se debe fijar de modo que se facilite la asistencia de los accionistas a las mismas.
3. Los accionistas deben contar con la oportunidad de introducir puntos a debatir, dentro de un límite razonable, en la agenda de las Juntas Generales.
Los temas que se introduzcan en la agenda deben ser de interés social y propio de la competencia legal o estatutaria de la Junta. El Directorio no debe denegar esta clase de solicitudes sin comunicar al accionista un motivo razonable. El estatuto no debe imponer límites a la facultad que todo accionista con derecho a participar en las Juntas Generales pueda hacerse representar por la persona que designe.
4. Es recomendable que la sociedad emisora de acciones de inversión u otros valores accionarios sin derecho a voto, ofrezca a sus tenedores la oportunidad de canjearlos por acciones ordinarias con derecho a voto o que prevean esta posibilidad al momento de su emisión.

TRATAMIENTO EQUITATIVO DE LOS ACCIONISTAS

5. Se debe elegir un número suficiente de directores capaces de ejercer un juicio independiente, en asuntos donde haya potencialmente conflictos de intereses, pudiéndose, para tal efecto, tomar en consideración la participación de los accionistas carentes de control.

6. Los directores independientes son aquellos seleccionados por su prestigio profesional y que no se encuentran vinculados con la administración de la sociedad ni con los accionistas principales de la misma.

COMUNICACIÓN Y TRANSPARENCIA INFORMATIVA

7. Si bien, por lo general las auditorías externas están enfocadas a dictaminar información financiera, estas también pueden referirse a dictámenes o informes especializados en los siguientes aspectos: peritajes contables, auditorías operativas, auditorías de sistemas, evaluación de proyectos, evaluación o implantación de sistemas de costos, auditoría tributaria, tasaciones para ajustes de activos, evaluación de cartera, inventarios, u otros servicios especiales.
Es recomendable que estas asesorías sean realizadas por auditores distintos o, en caso las realicen los mismos auditores, ello no afecte la independencia de su opinión. La sociedad debe revelar todas las auditorías e informes especializados que realice el auditor. Se debe informar respecto a todos los servicios que la sociedad auditora o auditor presta a la sociedad, especificándose el porcentaje que representa cada uno, y su participación en los ingresos de la sociedad auditora o auditor.
8. La atención de los pedidos particulares de información solicitados por los accionistas, los inversionistas en general o los grupos de interés relacionados con la sociedad, debe hacerse a través de una instancia o personal responsable designado al efecto.
9. Los casos de duda sobre el carácter confidencial de la información solicitada por los accionistas o por los grupos de interés relacionados con la sociedad deben ser resueltos. Los criterios deben ser adoptados por el Directorio y ratificados por la Junta General, así como incluidos en el estatuto o reglamento interno de la sociedad. En todo caso la revelación de información no debe poner en peligro la posición competitiva de la empresa ni ser susceptible de afectar el normal desarrollo de las actividades de la misma.

10. La sociedad debe contar con Auditoría Interna. El auditor interno, en el ejercicio de sus funciones, debe guardar relación de independencia profesional respecto de la sociedad que lo contrata. Debe actuar observando los mismos principios de diligencia, lealtad y reserva que se exigen al Directorio y a la Gerencia.

LAS RESPONSABILIDADES DEL DIRECTORIO.

11. El Directorio debe realizar ciertas funciones claves, a saber: evaluar, aprobar y dirigir la estrategia corporativa; establecer los objetivos y metas así como los planes de acción principales, la política de seguimiento, control y manejo de riesgos, los presupuestos anuales y los planes de negocios; controlar la implementación de los mismos y supervisar los principales gastos, inversiones, adquisiciones y enajenaciones.
12. Seleccionar, controlar y, cuando se haga necesario, sustituir a los ejecutivos principales, así como fijar su retribución.
13. Evaluar la remuneración de los ejecutivos principales y de los miembros del Directorio, asegurándose que el procedimiento para elegir a los directores sea formal y transparente.
14. Realizar el seguimiento y control de los posibles conflictos de intereses entre la administración, los miembros del Directorio y los accionistas, incluidos el uso fraudulento de activos corporativos y el abuso en transacciones entre partes interesadas.
15. Velar por la integridad de los sistemas de contabilidad y de los estados financieros de la sociedad, incluida una auditoría independiente, y la existencia de los debidos sistemas de control, en particular, control de riesgos financieros y no financieros y cumplimiento de la ley.
16. Supervisar la efectividad de las prácticas de gobierno de acuerdo con las cuales opera, realizando cambios a medida que se hagan necesarios.
17. Supervisar la política de información.
18. El Directorio podrá conformar órganos especiales de acuerdo a las necesidades y dimensión de la sociedad, en especial aquella que asuma la función de auditoría.

Asimismo, estos órganos especiales podrán referirse, entre otras, a las funciones de nombramiento, retribución, control y planeamiento. Estos órganos especiales se constituirán al interior del Directorio como mecanismos de apoyo y deberán estar compuestos preferentemente por directores independientes, a fin de tomar decisiones imparciales en cuestiones donde puedan surgir conflictos de intereses.

19. El número de miembros del Directorio de una sociedad debe asegurar pluralidad de opiniones al interior del mismo, de modo que las decisiones que en él se adopten sean consecuencia de una apropiada deliberación, observando siempre los mejores intereses de la empresa y de los accionistas.
20. La información referida a los asuntos a tratar en cada sesión, debe encontrarse a disposición de los directores con una anticipación que les permita su revisión, salvo que se traten de asuntos estratégicos que demanden confidencialidad, en cuyo caso será necesario establecer los mecanismos que permita a los directores evaluar adecuadamente dichos asuntos.
21. Siguiendo políticas claramente establecidas y definidas, el Directorio decide la contratación de los servicios de asesoría especializada que requiera la sociedad para la toma de decisiones.
22. Los nuevos directores deben ser instruidos sobre sus facultades y responsabilidades, así como sobre las características y estructura organizativa de la sociedad.
23. Se debe establecer los procedimientos que el Directorio sigue en la elección de uno o más reemplazantes, si no hubiera directores suplentes y se produjese la vacancia de uno o más directores, a fin de completar su número por el período que aún resta, cuando no exista disposición de un tratamiento distinto en el estatuto.
24. Las funciones del Presidente del Directorio, Presidente Ejecutivo de ser el caso, así como del Gerente General deben estar claramente delimitadas en el estatuto o en el reglamento interno de la sociedad con el fin de evitar duplicidad de funciones y posibles conflictos.
25. La estructura orgánica de la sociedad debe evitar la concentración de funciones, atribuciones y responsabilidades en las personas del Presidente del Directorio, del

Presidente Ejecutivo, de ser el caso, del Gerente General y de otros funcionarios con cargos gerenciales.

26. Es recomendable que la Gerencia reciba, al menos, parte de su retribución en función a los resultados de la empresa, de manera que se asegure el cumplimiento de su objetivo de maximizar el valor de la empresa a favor de los accionistas.

Fuente: Bolsa de Valores de Lima [http:// www.bvl.com.pe/descarga/26_principios.pdf](http://www.bvl.com.pe/descarga/26_principios.pdf).
Consultada el 15 de agosto de 2011

ANEXO V – Mapa de madurez para la evaluación de componentes del PCA

Nivel de Madurez	Descripción
0 – No existente	No hay reconocimiento de la necesidad del control del riesgo de fraude. El control no es parte de la cultura o misión de la organización. Existe un alto riesgo por las deficiencias de control e incidentes.
1 – Inicial / Reactivo	Hay algún reconocimiento de la necesidad de control de riesgo de fraude. El acercamiento al riesgo de fraude y los requerimientos de control se efectúa cuando se producen incidentes, de manera desorganizada, sin comunicación ni monitoreo. Los trabajadores desconocen sus responsabilidades en la identificación del riesgo de fraude.
2 – Repetible pero Intuitivo	Se realizan investigaciones de hechos o incidentes, de manera puntual sin tener un proceso para ello ni instancias encargadas. No se cuenta con un detalle o historia de casos presentados; no se analizan las causas/motivos. Los trabajadores pueden no conocer sus responsabilidades respecto a las acciones sobre la identificación de hechos irregulares o conductas no éticas.
3 – Definido	Se cuenta con un proceso para la investigación de hechos o incidentes pero no se ha documentado. El riesgo de fraude no es evaluado de manera específica. Existe un detalle o historia de casos presentados; sin embargo, la evaluación de las causas motivos no está documentada. Existen procedimientos específicos de información y comunicación de hechos irregulares no documentados. Se analizan datos de manera puntual por caso y con alcances limitados Trabajadores son conscientes de sus responsabilidades respecto del riesgo de fraude. No se cuentan con indicadores de cumplimiento ético.
4 – Gerenciado y Medido	Se cuenta con un proceso para la investigación de hechos o incidentes y está documentado. El riesgo de fraude es evaluado de manera específica. Existe un detalle o historia de casos presentados y se realiza la evaluación de las causas y motivos registrados. Se definen acciones para prevenir situaciones de fraude basándose en la historia analizada. Análisis de datos de manera periódica (pruebas de detección); data limitada. Se cuentan con indicadores de cumplimiento ético en base a irregularidades presentadas.
5 – Optimizado	La evaluación del riesgo de fraude considera criterios o escenarios específicos. Se cuenta con un esquema estructurado de procedimientos de evaluación continua para detección oportuna de desviaciones por potenciales fraudes de manera preventiva. Análisis de datos de manera automatizada y continua; definición de scripts. Se cuentan con indicadores de cumplimiento ético.

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO VI – Nivel de Madurez respecto a los Elementos Clave del PCA

Nivel de Madurez /Elemento Clave	1	2	3	4	5	6	7	8	9	10
1 – Inicial / Reactivo	Existencia de Código de Conducta. No integración de valores	Sin cumplimiento.	Firma de documento de recepción del Código de Ética, sin asegurar el entendimiento.	Se describe de manera genérica en Código de Ética. No describe situaciones que pueden representar conflicto de interés.	No existe monitoreo de riesgos	No existen canales definidos; el reporte del hecho ocurrido; este se reporta al superior o no se reportan.	Procesos de investigación no tienen un esquema definido; se analizan los casos ocurridos de manera independiente y desarticulada.	No se señalan las consecuencias y procesos para los actos fraudulentos; se ejecutan de manera puntual para cada caso.	Proceso de evaluación es realizado cuando ocurren los casos. No se cuenta con Políticas de gestión del riesgo de Fraude	No se realizan análisis de datos o se realizan de manera posterior al hecho.
2 – Repetible pero Intuitivo	Existencia de Código de Conducta.	Programa de concienciación básico (cartilla)	Firma de documento de recepción del Código de Ética, sin asegurar el entendimiento.	Proceso básico para informar posibles conflictos de interés de empleados mínimo. No hay descripción clara de situaciones que pueden representar conflicto de interés	Incipiente gestión de riesgos. Existencia de controles en los procesos; sin un marco de control definido. No evaluación del riesgo de fraude de manera específica	No se tiene un canal formalmente definido, sin embargo se cuenta con un procedimiento informal para reportar fraudes al superior inmediato (escalamiento).	Procesos de investigación no tienen un esquema definido, pero se cuentan con algunos procedimientos y responsabilidades no definidos formalmente, que intervienen en este proceso.	No se cuentan con procedimientos formalmente definidos pero se realizan acciones concretas para cada caso en particular, tomando como referencia la historia de casos.	No se cuenta con Políticas de gestión del riesgo de Fraude pero se mantiene historia de evaluación de los casos ocurridos.	Análisis de datos asociados a casos ocurridos durante el proceso de investigación (no periódico), de manera manual y con alcances limitados

Nivel de Madurez /Elemento Clave	1	2	3	4	5	6	7	8	9	10
3 – Definido	<p>Código de Conducta:</p> <p>Establece expresamente compromiso de la empresa y sus colaboradores con altos principios de ética personal y profesional.</p> <p>Define situaciones que representan incumplimientos éticos.</p> <p>Solo ámbito de colaboradores.</p>	<p>Comités de riesgo / fraude (incidentes) para analizar y presentar informes y conclusiones de los casos de irregularidades.</p> <p>Establecimiento de Manual de prevención / Procedimientos de Lavado de Activos</p>	<p>Firma de documento de recepción del Código de Ética / Manual de Lavado, sin asegurar el entendimiento.</p> <p>Firmas de acuerdos de confidencialidad.</p>	<p>Se describen en las situaciones que pueden sugerir conflictos de interés.</p> <p>Se indica el proceso para revelación de conflictos de interés básico (ámbito de empleados mínimo)</p>	<p>Marco de control interno definido.</p> <p>Se analizan los riesgos de fraude de manera puntual; según la ocurrencia de eventos</p>	<p>No se tiene un canal formalmente definido, sin embargo se cuenta con un procedimiento informal para reportar a áreas de control los hechos irregulares o sospechados de fraudes.</p>	<p>Se cuenta con un proceso de inicio de investigación así como las áreas responsables en su realización, pero no se encuentra documentado.</p>	<p>Tanto las políticas como el Código de Conducta y otros documentos establecidos en las sanciones y acciones de parte de la empresa frente a actos no éticos.</p>	<p>Se cuenta con políticas y definiciones referidas a evaluación del riesgo de fraude como parte de la gestión del Riesgo Operacional.</p>	<p>Análisis de datos asociados a casos ocurridos durante el proceso de investigación y de manera posterior aunque no de manera continuas; alcances limitados.</p>

Nivel de Madurez /Elemento Clave	1	2	3	4	5	6	7	8	9	10
4 – Gerenciado y Medido	Código debe señalar ciertos procedimientos y vías de reporte para denunciar incumplimientos éticos por cada situación definida.	Comités de riesgo / fraude (incidentes) para analizar y presentar informes y conclusiones de los casos de irregularidades. Presentación de casos ocurridos a la Alta Dirección / Directorio. Comités de Lavado de Activos. Programas de Capacitación en riesgos de fraude, lavado de activos (anuales).	Pruebas de Control sobre conocimiento del Código de Ética / Manual de Prevención de Lavado de Activos incluidas en las capacitaciones (test).	Se describen en las situaciones que pueden sugerir conflictos de interés (ámbito de empleados y terceros involucrados). Se indica el proceso para revelación de conflictos de interés según los diversos actores (ámbito de empleados y terceros involucrados)	Análisis de los riesgos de fraude de manera periódica. Establecimiento de escenarios y Revisión de casos históricos para determinación de causas comunes y definición de acciones correctivas / Controles.	Definición formal de canal para reporte de hechos irregulares o sospechosa de fraude. Indicación en el Código de Ética y/o Manual de Prevención de Lavado de Activos de canales establecidos.	Proceso de investigación formalmente establecido y documentado como parte de la normativa de la empresa.	Tanto las políticas como el Código de Conducta y otros documentos establecidos en las sanciones y acciones de parte de la empresa frente a actos no éticos.	Se cuenta con una gestión definida para la evaluación del riesgo de fraude; se cuentan con políticas y lineamientos formales de cómo realizar la evaluación.	Definición de bases de datos a analizar (pruebas de detección). Análisis de datos de manera periódica pero no continuada;
5 - Optimizado	Ámbito de aplicación	Campañas periódicas	Indicador % de personas	Proceso de tratamiento	Procedimientos sistemáticos	Establecimiento de línea	Proceso considera los	Tanto las políticas	Se incluye análisis	Análisis de datos

Nivel de Madurez /Elemento Clave	1	2	3	4	5	6	7	8	9	10
	n del Código de Ética abarque a clientes, proveedores y terceros interesados.	s vía Intranet / correos generales acerca de	capacidades. Medición del conocimiento de documentos de acuerdo a notas obtenidas en test.	nto de conflictos de interés a nivel de Directorio.	cos para análisis e identificación del riesgo de fraude (monitoreo continuo)	directa para denunciantes. Campañas de refuerzo sobre las líneas establecidas para reporte de hechos o sospechas de fraude.	pasos para iniciar las investigaciones, las reglas de evidencia, cadenas de custodia, mecanismos de información a los encargados del gobierno, los requisitos reglamentarios, y acciones legales.	como el Código de Conducta y otros documentos establecidos en las sanciones y acciones de parte de la empresa frente a actos no éticos.	de datos de manera continua y los resultados son comunicados periódicamente en instancias definidas (Comité de Ética)	de manera continua y automatizada. Definición de Scripts para cada data.

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO VII – Análisis de Brecha respecto a los Roles y Responsabilidades sobre la
Gestión del Fraude

Práctica Sugerida	Contraste			Aspecto por Implementar / Sugerido
	Fuente	Hallazgo	Calificación	
2.2.1.1.1 El Rol del Directorio - Capítulo II "Marco Teórico"	<p>Memoria Anual 2010</p> <p>Evaluación de Auditoría Interna al 2010 sobre el cumplimiento de los 26 Principios de Buen Gobierno Corporativo.</p> <p>Manual del Directorio</p>	<p>El Directorio de Rímac Internacional sólo cuenta con un director independiente, de los nueve miembros que lo conforman.</p> <p>El Manual del Directorio cita las responsabilidades del mismo sobre la evaluación, responsabilidad y aprobación de las acciones a tomar sobre la compañía.</p>	50%	Incrementar el número de miembros independientes en el Directorio.
2.2.1.1.2 El Rol del Comité de Auditoría - Capítulo II "Marco Teórico"	Lista de Comités activos a junio 2011	Rímac Internacional cuenta con un Comité de Auditoría. Dicho directorio recibe informe periódicos sobre el estado de los eventos de fraude reportados o presuntos fraudes	100%	-

Práctica Sugerida	Contraste			Aspecto por Implementar / Sugerido
	Fuente	Hallazgo	Calificación	
2.2.1.1.3 El Rol de la Gerencia - Capítulo II "Marco Teórico"	Manual de Organización y Funciones de Rímac Internacional. Evaluaciones de Auditoría Interna, Externa y Regulatoria al 2010.	La Gerencia General de Rímac Internacional vela por el cumplimiento y operación de un adecuado control interno, el cumplimiento regulatorio respecto a la prevención del lavado de activos, la existencia de valores y ética, así como con actividades de monitoreo y supervisión realizadas por los auditores internos y externos. No obstante, identificamos que la compañía aún no ha contemplado el diseño de un programa integral para la gestión del riesgo de fraude. Adicionalmente, distinguimos que no se ha desarrollado un documento que consolide las políticas y el compromiso de la empresa respecto a la lucha contra el fraude a todos los niveles de la operación de la compañía	50%	Implementar un programa integral para la gestión y evaluación del riesgo de fraude. Desarrollar un documento que consolide las políticas y el compromiso de la empresa respecto a la lucha contra el fraude
2.2.1.1.4 El Rol del Personal - Capítulo II "Marco Teórico"	Cursos de Capacitación sobre Prevención de Lavado de Activos y Actividades de Financiamiento del Terrorismo. Código de Ética y Conducta	La compañía cuenta con programas de entrenamiento para todo el personal respecto al riesgo de fraude por Lavado de Activos y Financiamiento del Terrorismos. Dicho se realiza una vez al año como mínimo. Respecto a la prevención de fraudes internos o externos, la compañía difunde en el personal la responsabilidad de preservar conductas éticas y de comportamiento a través del Código de Ética y Conducta. A pesar de la existencia de estos elementos, notamos que la compañía no cuenta con programas de capacitación enfocados en la lucha contra el fraude.	50%	Implementar programas de capacitación enfocados en la lucha contra el fraude.
2.2.1.1.4 El Rol del Auditor Interno - Capítulo II "Marco Teórico"	Plan Anual de Auditoría Interna 2010	El departamento de Auditoría Interna, a través del Plan Anual de Auditoría Interna evalúa los riesgos de fraude inherentes a los procesos evaluados, de acuerdo a lo establecido en su Estatuto. Pero identificamos que el monitoreo de transacciones susceptibles a fraude no se realiza en base a una metodología, sino que se realiza en base a las alertas o avisos anónimos recibidos, solicitudes internas o sobre operaciones que probablemente pueden presentar eventos de dolo.	75%	Implementar una metodología para la investigación preventiva y detectiva por parte de Auditoría Interna sobre posibles eventos de fraude.
Resultados			65%	

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

**ANEXO VIII – Análisis de Brecha respecto al cumplimiento de los Elementos Claves
para la implementación de un efectivo Programa Antifraude**

Elemento Clave	Aspecto implementado	% Cumplimiento Actual	Aspecto por implementar
Compromiso	<ul style="list-style-type: none"> Aprobación del nuevo Código de Ética y Estándares de Conducta; establece el compromiso de la empresa y sus colaboradores con altos principios de ética personal y profesional. 	100%	
Conciencia del Fraude	<ul style="list-style-type: none"> Comité de Incidentes cuya función principal es investigar, analizar y presentar informes y conclusiones de los casos. Se formaliza la creación del Comité de Ética, No se han diseñado aun programas de sensibilización sobre el fraude para los empleados y Alta Gerencia. 	50%	<p>Programas de sensibilización sobre el fraude:</p> <ul style="list-style-type: none"> Talleres de entendimiento y sensibilización sobre riesgos de fraude con gerencias de división. Talleres de mapeo e identificación de riesgo de fraude del proceso seleccionado en conjunto con la Unidad de Riesgos y la Gerencia dueña del proceso, la matriz de riesgos existentes incluyendo los riesgos de fraude.
Proceso de Confirmación	<ul style="list-style-type: none"> Firma de constancias de recepción del Código de Ética y Estándares de Conducta. No existe procedimiento para asegurar lectura y entendimiento del código. Si existe un procedimiento de constancias y confirmación de entendimiento del Manual de Prevención de Lavado de Activos y Financiamiento del Terrorismo 	50%	<ul style="list-style-type: none"> Elaborar programa de capacitación electrónica sobre entendimiento del Código de Ética que incluya test (examen). De carácter obligatorio. Establecer la periodicidad mínima (anual)
Conflicto de Interés	<ul style="list-style-type: none"> El Código de Ética y Estándares de Conducta establece la definición, situaciones que representan conflicto de interés y el procedimiento a seguir para revelar dichas situaciones. 	50%	<ul style="list-style-type: none"> Actualización y mejora de la versión actual del Código de Ética, a fin de que incluya el procedimiento que deben seguir los proveedores, corredores y clientes para informar a la

Elemento Clave	Aspecto implementado	% Cumplimiento Actual	Aspecto por implementar
	<ul style="list-style-type: none"> Solo abarca al ámbito de los empleados no contemplando un proceso interno para terceros. 		<p>compañía acerca de los casos de sospecha de conflicto de interés</p> <ul style="list-style-type: none"> Definir el canal de reporte. Aprobación de la nueva versión por el Directorio.
Evaluación del Riesgo de Fraude	<ul style="list-style-type: none"> La Auditoría Interna analiza y evalúa las desviaciones en los procedimientos establecidos. Unidad de Riesgos se encarga de monitorear los diversos riesgos incluyendo el riesgo de fraude No existe una evaluación específica y única del riesgo de fraude que considere criterios o escenarios específicos. 	40%	<ul style="list-style-type: none"> Establecer criterios marco homogéneos para la establecer el objetivo de la evaluación del riesgo de fraude de manera preventiva (Tipificación según la Asociación de examinadores de Fraude / Por tipo de delito) Incluir los tipos de fraude preestablecidos para Rímac Internacional dentro de los criterios marco: (tipificación interna para Fraude en Seguros capítulo 4.3.1) Mapear los controles antifraude en el árbol del fraude para el proceso seleccionado: <ul style="list-style-type: none"> a) clasificar y verificar el diseño de los controles antifraude actuales b) identificar los controles antifraude que no están implementados, y que se requieren poner en marcha. Definir la actividad de monitoreo para el proceso seleccionado. Realización de informe o reporte de la evaluación realizada: Procedimientos efectuados, resultados, Conclusiones, medidas de control
Procedimientos de información y protección de denunciantes	<ul style="list-style-type: none"> El Código de Ética y Estándares de Conducta exhorta a sus colaboradores a comunicar cualquier infracción. 	100%	

Elemento Clave	Aspecto implementado	% Cumplimiento Actual	Aspecto por implementar
	<ul style="list-style-type: none"> · Correo específico para la recepción de denuncias. · Se indica la protección del anonimato del denunciante si así lo requiere. 		
Proceso de Investigación	<ul style="list-style-type: none"> · La función de investigación, análisis y conclusiones de los casos de irregularidades y fraudes se encuentra establecida en el Reglamento del Comité de Ética, pero no existe un procedimiento formalmente establecido de este proceso. 	40%	<ul style="list-style-type: none"> · Documentar formalmente en procedimiento interno el proceso seguido para la investigación análisis y conclusiones de los casos de irregularidades detectadas. Incluir en el documento vía de reporte. · Actualizar el Reglamento del Comité de Ética con el fin de que se haga referencia al proceso documentado. · Aprobación de dichos procedimientos por el Directorio.
Acciones Correctivas	<ul style="list-style-type: none"> · El Código de Ética y Estándares de Conducta señala de manera expresa las amonestaciones o sanciones. La compañía no se reserva el derecho de iniciar acciones civiles o penales contra cualquier persona que comete el fraude. 	100%	
Proceso de Evaluación y Mejora	<ul style="list-style-type: none"> · No se cuenta con indicadores de comportamiento ético · Se cuenta con un indicador de incidentes y fraudes ocurridos. 	50%	<ul style="list-style-type: none"> · Definir indicador de % máximo de desviaciones obtenidas por proceso evaluado. ·
Monitoreo Continuo	<ul style="list-style-type: none"> · Se cuenta procesos de investigación, análisis y conclusiones de los casos de irregularidades. · No se cuenta con un esquema estructurado de procedimientos de evaluación continua para detección oportuna de desviaciones por potenciales fraudes de manera preventiva 	40%	<ul style="list-style-type: none"> · Identificación de controles existentes y deseados. · Seleccionar aquellos controles antifraude automatizables que serán implementados en el sistema de monitoreo preventivo antifraude utilizando la herramienta ACL (definición de scripts).

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO IX - Análisis de Brecha respecto al cumplimiento de los Elementos Claves para la implementación de un efectivo Programa Antifraude

Fases para la Evaluación del Riesgo de Fraude	Riesgo de Fraude respecto a la Prevención y Lavado de Activos (PLAFT) (Peso 40% - Carácter Regulatorio)		Riesgo de Fraude Ocupacional (Peso 30%)		Riesgo de Fraude Externo (Peso 30%)		Valor Final
	Valor de cumplimiento	Análisis	Valor de cumplimiento	Análisis	Valor de cumplimiento	Análisis	
Fase 1: Identificar los factores relevantes del riesgo de fraude	8	Prácticas Existentes: La compañía cuenta por requerimiento regulatorio con un frente dedicado a la detección, prevención, evaluación y respuesta sobre los riesgos de Fraude relacionados al PLAFT, función que es realizada por el Oficial de Cumplimiento. Estas actividades además se ven reforzadas por las sinergias existentes con la Unidad de Investigación Financiera del Gobierno Peruano y la Superintendencia de Banca y Seguros y AFP del Perú	4	Prácticas Existentes: Las fases sugeridas son realizadas sólo durante las investigaciones de fraudes reportados, los exámenes de Auditoría o durante las actividades de monitoreo manual realizado por Auditoría sobre transacciones sensibles a riesgos de fraude. Brechas: * No se cuenta con matrices donde se identifiquen los riesgos	4	Prácticas Existentes: Las fases sugeridas son realizadas sólo durante las investigaciones de fraudes reportados. Brechas: * No se cuenta con matrices donde se identifiquen los riesgos de fraude externos a los que puede estar asociado la compañía.	5.6
Fase 2: Identificar los esquemas potenciales de fraude y priorizar los basados en riesgos.	8		4		4		5.6
Fase 3: Comparar los controles existentes respecto a la prevención y detección del fraude	8		6		6		6.8
Fase 4: Probar la efectividad de controles respecto a la prevención y detección del fraude	8		6		6		6.8

Fases para la Evaluación del Riesgo de Fraude	Riesgo de Fraude respecto a la Prevención y Lavado de Activos (PLAFT) (Peso 40% - Carácter Regulatorio)		Riesgo de Fraude Ocupacional (Peso 30%)		Riesgo de Fraude Externo (Peso 30%)		Valor Final
	Valor de cumplimiento	Análisis	Valor de cumplimiento	Análisis	Valor de cumplimiento	Análisis	
Fase 5: Documentar y reportar la evaluación de riesgos de fraude	8	<p>Brechas:</p> <p>* El esquema de reporte se basa en comunicación vía correo electrónico.</p> <p>* El registro de alertas de fraude se realiza de manera manual y no se cuenta con un esquema de categorización.</p>	4	de fraude ocupacional que pueden estar asociados a los procesos críticos de la compañía.	4		5.6
Resultado							6.08
1 es el valor más bajo de cumplimiento, siendo 10 el más alto.							

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO X Análisis de Brecha – Controles Preventivos

Dimensiones de COSO	Control Preventivo	Análisis	Valor de Cumplimiento
Entorno de Control	Código de Conducta	La compañía cuenta con un código de conducta el cual es difundido a todos los colaboradores y se encuentra aprobado por el Directorio.	10
	Política de Ética o Fraude	No se cuenta con dicho control.	2
	Programas de Línea de Reporte Directo.	Se utiliza el correo electrónico como único medio de reporte.	2
	Prácticas y guías de contratación y promoción.	Si bien se cuenta con un proceso definido para la contratación de personal, la validación de antecedentes penales y policiales no es obligatoria al momento del proceso de selección salvo en puesto claves de la organización. Esta medida se toma en amparo de la Ley publicada por el Gobierno Peruano.	6
	Revisión del tópico de fraude por comités	Se cumple.	10
Evaluación de Riesgo	Realizar evaluaciones de riesgo de fraude manera periódica.	Ver apartado 4.4.2 - Evaluación del Riesgo de Fraude.	6
Actividades de Control	Políticas y procedimientos del negocio, incluyendo los límites de funciones y la segregación de funciones.	Se cumple. La compañía cuenta con manuales que describen los roles y funciones de los colaboradores por área. El cumplimiento de los mismos es evaluado durante las evaluaciones de Auditoría Interna.	8
Información y Comunicación	Promover la importancia de los programas de gestión de riesgo de fraude y la posición de la organización respecto al riesgo de fraude tanto interna como externamente a través de:	Ver apartado 4.4.2 - Evaluación del Riesgo de Fraude.	6

Dimensiones de COSO	Control Preventivo	Análisis	Valor de Cumplimiento
	a) Programas de entrenamiento, y procedimientos.	Ver apartado 4.4.2 - Evaluación del Riesgo de Fraude.	6
	b) Procesos de certificación o afirmación para confirmar que los empleados han leído y entendido las políticas corporativas.	Ver apartado 4.4.2 - Evaluación del Riesgo de Fraude.	10
Monitoreo	Realizar evaluaciones periódicas de controles antifraude: · A través de revisiones de auditores internos.	Ver apartado 4.4.2 - Evaluación del Riesgo de Fraude.	8
	· Implementando tecnología para asegurar el monitoreo continuo y actividades de detección.	No se cuenta con actividades de monitoreo continuo.	2
Resultado			6.33
1 es el valor más bajo de cumplimiento, siendo 10 el más alto.			

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO XI – Evaluación del Riesgo de Fraude al Proceso de Gestión de TI y Seguridad de la Información.

Esquema de Riesgo de Fraude	Probabilidad (*1)	Impacto	Responsable	Control Antifraude existente	Evaluación de la efectividad del control	Riesgo Residual	Control de Respuesta al Riesgo
Falta de controles físicos sobre dispositivos de TI, pueden derivar en cambios, destrucción o uso inadecuado para fines personales.	40%	3	Gerente de Producción (Sr. Ronald Mejía) - RM	<ul style="list-style-type: none"> Dispositivos críticos de tecnología se encuentran en el Centro de Datos. Acceso al centro de datos se encuentra restringido al personal autorizado. Políticas y Procedimientos Documentados. Se mantiene un registro de visitas. Se realiza un inventario anual de los dispositivos de tecnología. 	Evaluación de Auditoría (Interna, Externa, Corporativa y Regulatoria)	Bajo.	Evaluación periódica por parte de Auditoría Interna
Acceso mediante colusión o robo de credenciales de acceso al sistema para efectuar robo, mal uso de información confidencial o realizar transacciones fraudulentas.	40%	4	Jefatura de Seguridad de la Información (Srta. Johanna Cuba) - JC Gerencia de Tecnología (Sr. Martin Kerrigan) - MK	<ul style="list-style-type: none"> Gestión de cuentas de usuarios y perfiles para identificar a los dueños de transacciones. Aplicación de políticas y estándares de seguridad sobre aplicativos principales de la empresa. Segregación de funciones. Evaluaciones periódicas para realizar análisis preventivos de las vulnerabilidades de intrusión internas y externas a la red. 	Evaluación de Auditoría (Interna, Externa, Corporativa y Regulatoria)	Bajo.	Evaluación periódica por parte de Auditoría Interna

Esquema de Riesgo de Fraude	Probabilidad (*1)	Impacto	Responsable	Control Antifraude existente	Evaluación de la efectividad del control	Riesgo Residual	Control de Respuesta al Riesgo
				<ul style="list-style-type: none"> • Servidor Antivirus. 			
Cambios a programas para realizar transacciones fraudulentas	20%	4	JC MK	<ul style="list-style-type: none"> • Procedimientos para la Gestión de Cambios a programas que incluyen controles de aprobación. • Segregación de funciones y ambientes lógicos. • Acceso Restringido al área de producción. • Acceso restringido al código fuente de los programas. • Procedimientos normados para el desarrollo de programas y proyectos. 	Evaluación de Auditoría (Interna, Externa, Corporativa y Regulatoria)	Bajo.	Evaluación periódica por parte de Auditoría Interna
Actividades Fraudulentas por parte de proveedores de tecnología	20%	4	JC MK	<ul style="list-style-type: none"> • Cláusulas de confidencialidad, acceso a Auditorías, no divulgación, entre otros. • Segregación de funciones. • Controles de acceso. • Evaluación trimestral del proveedor. • Metodología para la selección y contratación de proveedores. 	Evaluación de Auditoría (Interna, Externa, Corporativa y Regulatoria)	Bajo.	Evaluación periódica por parte de Auditoría Interna
Conflicto de intereses con	20%	4	JC MK	Segregación de Funciones.	Evaluación de Auditoría (Interna,	Alto.	Se requiere implementar una línea

Esquema de Riesgo de Fraude	Probabilidad (*1)	Impacto	Responsable	Control Antifraude existente	Evaluación de la efectividad del control	Riesgo Residual	Control de Respuesta al Riesgo
proveedores y terceros				Difusión de la Política de Seguridad de la Información. Código de Ética. Monitoreo periódico sobre proveedores aprobados. Revisión de antecedentes.	Externa, Corporativa y Regulatoria)		de reporte anónima. Se requiere comunicar a los proveedores los lineamientos sobre la gestión del fraude.
<p>(1) = Remota (20%), Poco probable (40%), Razonablemente Probable (60%), Altamente Probable (80%), Probable (99%).</p> <p>(2) = Bajo (1), Moderado (2), Relevante (3), Alto (4), Crítico (5). Ver ANEXO XIV Matriz de Evaluación de Riesgos</p>							

Fuente: Elaboración propia sobre la base de la información proporcionada por la Gerencia de Tecnología de Rímac Internacional.

ANEXO XII Cronograma – Definición de Planes de Acción

Plan de Trabajo		S1	S2	S3
No	Actividades			
Fase 1: DEFINICIÓN - Definición del Marco Normativo del Programa Anti-Fraude				
1	Definición del Objetivo de la Política Anti-Fraude			
2	Definición del Alcance de la Política Anti-Fraude			
3	Definición de Roles y Responsabilidades			
3.1	Directorio			
3.2	Comité			
3.3	Oficial de Cumplimiento			
3.4	Gerencia			
3.5	Empleados			
3.6	Sociedades de Auditoría			
3.7	Seguridad de la Información			
4	Definición de Señales de Alerta sobre Procesos de Tecnología			
4.1	Proceso de Gestión de Accesos			
4.2	Proceso de Gestión de Cambios a Programas			
4.3	Proceso de Gestión de Activos de Información			
4.4	Proceso de Gestión de la Seguridad Física y del Entorno			
5	Definición de Actividades de Evaluación e Identificación de Riesgos de Fraude			
5.1	Definición de Factores de Riesgo de Fraude			
5.2	Definición de la Evaluación de Escenarios de Fraude			
5.3	Definición de la Valorización de la Probabilidad de Ocurrencia y el Impacto en la Organización			
6	Definición del Monitoreo de Materialización de Riesgo y Efectividad de Controles			
6.1	Definición de Actividades de Monitoreo Continuo			
6.2	Definición de las Actividades de Monitoreo de Auditoría			
7	Definición del Proceso de Investigación del Fraude			
8	Definición de Procedimientos para la Gestión de Denuncias			
8.1	Definición del Esquema de Comunicación de Denuncias			
8.2	Procedimiento de Atención y Valorización de Denuncias			
8.3	Procedimiento Legal por Incumplir o Tolerar el Fraude			
9	Definición de la Sensibilización al Riesgo de Fraude			
9.1	Definición de Pacto de Transparencia			
9.2	Definición de Mecanismos de Divulgación del Programas			
9.3	Definición de Comunicaciones de Interes Público			
9.4	Definición de Capacitaciones Específicas			

Fuente: elaboración propia

Plan de Trabajo		Semanas												
No	Actividades	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
Fase 1: DEFINICIÓN - Definición del Marco Normativo del Programa Anti-Fraude														
1	Definición del Objetivo de la Política Anti-Fraude													
2	Definición del Alcance de la Política Anti-Fraude													
3	Definición de Roles y Responsabilidades													
3.1	Directorio													
3.2	Comité													
3.3	Oficial de Cumplimiento													
3.4	Gerencia													
3.5	Empleados													
3.6	Sociedades de Auditoría													
3.7	Seguridad de la Información													
4	Definición de Señales de Alerta sobre Procesos de Tecnología													
4.1	Proceso de Gestión de Accesos													
4.2	Proceso de Gestión de Cambios a Programas													
4.3	Proceso de Gestión de Activos de Información													
4.4	Proceso de Gestión de la Seguridad Física y del Entorno													
5	Definición de Actividades de Evaluación e Identificación de Riesgos de Fraude													
5.1	Definición de Factores de Riesgo de Fraude													
5.2	Definición de la Evaluación de Escenarios de Fraude													
5.3	Definición de la Valorización de la Probabilidad de Ocurrencia y el Impacto en la Organización													
6	Definición del Monitoreo de Materialización de Riesgo y Efectividad de Controles													
6.1	Definición de Actividades de Monitoreo Continuo													
6.2	Definición de las Actividades de Monitoreo de Auditoría													
7	Definición del Proceso de Investigación del Fraude													
8	Definición de Procedimientos para la Gestión de Denuncias													
8.1	Definición del Esquema de Comunicación de Denuncias													
8.2	Procedimiento de Atención y Valorización de Denuncias													
8.3	Procedimiento Legal por Incumplir o Tolerar el Fraude													
9	Definición de la Sensibilización al Riesgo de Fraude													
9.1	Definición de Pacto de Transparencia													
9.2	Definición de Mecanismos de Divulgación del Programas													
9.3	Definición de Comunicaciones de Interés Público													
9.4	Definición de Capacitaciones Específicas													

Fuente: elaboración propia

ANEXO XIII - Encuesta sobre el Valor de la Implementación de un PCA

1. ¿La empresa cuenta con mecanismos estructurados que permiten identificar situaciones de riesgo de delitos y fraude de manera oportuna?
2. ¿Se aplican políticas de supervisión y vigilancia para minimizar las posibilidades de fraude?
3. ¿Se llevan a cabo diagnósticos de amenazas que el entorno ofrece para cometer delitos y fraude (Gestión del riesgo de fraude)?
4. ¿Considera que un esquema de monitoreo continuo en procesos y transacciones críticas ayudaría a la detección oportuna de posibles eventos de fraude? Explicar brevemente.
5. ¿Qué tan complejo considera la implementación de mecanismos de computo forense como parte de un Programa Antifraude frente a la actual arquitectura tecnológica de la empresa?
6. ¿Ayudaría desde el punto de vista de aseguramiento de sus funciones el contar con un Programa Antifraude? ¿Cómo?
7. ¿Considera que la implementación de un Programa Antifraude promovería la interacción necesaria para la creación de una cultura de prevención y detección del fraude?
8. ¿Cómo considera que posicionaría a la empresa el contar con un Programa Antifraude frente al regulador?
9. ¿Considera que la creación / implementación de un Programa Antifraude en la empresa puede incidir en la mejora de la eficiencia de los procesos? Explicar brevemente.
10. ¿Considera que la creación / implementación de un Programa Antifraude aportaría valor al enfoque estratégico actual?

Fuente: elaboración propia

ANEXO XIV Tabulación de Encuestas sobre el Valor de la Implementación de un
PCA

control/
costoscontrol/
costos

imagen

imagen

costos

DIMENSIONES DE TRASCENDENCIA

DIMENSIONES COSO	EC		AC		ER		MC		MC		EC / AC		IC		IC		AC		CONCLUSION	
	1		2		3		4		5		6		7		8		9		10	
Gerencia División Transformación y Tecnología	PARCIAL	50%	SI	100%	PARCIAL	50%	SI	100%	MEDIO	50%	SI	100%	SI	100%	SI	100%	SI	100%	SI	100%
Oficial de cumplimiento	SI	100%	SI	100%	PARCIAL	50%	SI	100%	ALTO	100%	SI	100%	SI	100%	SI	100%	SI	100%	SI	100%
Jefe de Auditoría Interna	PARCIAL	50%	SI	100%	PARCIAL	50%	SI	100%	ALTO	100%	SI	100%	SI	100%	SI	100%	SI	100%	SI	100%
Gerencia de Soporte de Negocios	NO	0%	NO	0%	NO	0%	SI	100%	MEDIO	50%	SI	100%	SI	100%	SI	100%	SI	100%	SI	100%
Gerencia de Tecnología	SI	100%	SI	100%	PARCIAL	50%	SI	100%	MEDIO	50%	SI	100%	SI	100%	SI	100%	SI	100%	SI	100%
Resultados promedio	60%		80%		40%		100%		70%		100%		100%		100%		100%		100%	

Fuente: elaboración propia

DIMENSIONES COSO

EC ENTORNO DE CONTROL

EV EVALUACIÓN DE RIESGOS

AC ACTIVIDADES DE CONTROL

IC INFORMACIÓN Y COMUNICACIÓN

M MONITOREO

Metodología de Valoración

SÍ	100%
PARCIAL	50%
NO	0%

ALTO	100%
MEDIO	50%
BAJO	0%

ANEXO XV Matriz de Evaluación de Riesgos

Modelo de Administración de Riesgos Operacionales																							
Inventario de riesgos por División de Negocios																							
Proceso										Responsables													
MAPA DE RIESGOS - SEGURIDAD DE LA INFORMACION										Contenido		Revisión		Aprobación									
										S. Villacorta M. Dolci M. Kerigan		S. Villacorta M. Dolci M. Kerigan		M. Kerigan M. Potesta									
Objetivos del Area:																							
Objetivo 1		Establecer controles de seguridad física para el equipamiento tecnológico ubicado en el centro de datos de Rimac																					
Objetivo 2		Establecer controles de acceso sobre activos de información																					
Objetivo 3		Cumplimiento del marco normativo del SGSI establecido por la Superintendencia de Banca y Seguros																					
Corr.	Obj.	Descripción del Riesgo	Tipo de Riesgo	i#	p#	ixp	I	P	Riesgo	Potenc.	Status	Control	Efe	Control	Efect.	Control	Efect.	Efect.	Riesgo	SCORE			
												1	1	Status	2	2	Status	3	3	Total	Resid.		
1	1,3	Falta de controles físicos sobre dispositivos de TI, pueden derivar en cambios, destrucción o uso inadecuado para fines personales.	Riesgo de Fraude / Apropiación indebida de activos	3	40%	1.2	M	B	M	Exist.	Dispositivos críticos de tecnología se encuentran en el Centro de Datos.	A	Exist.	Acceso al centro de datos se encuentra restringido al personal autorizado. Políticas y Procedimientos Documentados. Se mantiene un registro de visitas.	M	Exist.	Se realiza un inventario anual de los dispositivos de tecnología.	B	A	B	0.1944		
2	2,3	Acceso mediante colusión o robo de credenciales de acceso al sistema para efectuar robo, mal uso de información confidencial o realizar transacciones fraudulentas.	Riesgo de Fraude / Apropiación indebida de activos	4	40%	1.6	A	B	A	Exist.	Gestión de cuentas de usuarios y perfiles para identificar a los dueños de transacciones.	M	Exist.	Aplicación de políticas y estándares de seguridad sobre aplicativos core de la empresa. Segregación de funciones.	A	Exist.	Evaluaciones periódicas para realizar análisis preventivos de las vulnerabilidades de intrusión internas y externas a la red. Servidor Antivirus.	M	A	B	0.1728		

Corr.	Obj.	Descripción del Riesgo	Tipo de Riesgo	i#	p#	ixp	I	P	Riesgo	Control		Efect.	Control		Efect.	Control		Efect.	Efect.	Riesgo	SCORE	
							Potenc.	Status	1	1	Status	2	2	Status	3	3	Total	Resid.				
3	2,3	Cambios a programas para realizar transacciones fraudulentas	Riesgo de Fraude / Uso inapropiado	4	20%	0.8	A	B	A	Exist.	Gestión de Cambios a programas que incluyen controles de aprobación. Procedimientos normados para el desarrollo de programas	A	Exist.	Segregación de funciones y ambientes lógicos. Acceso Restringido al área de producción.	A	Exist.	Acceso restringido al código fuente de los programas.	A	A	B	0.0216	
4	1,2,3	Actividades Fraudulentas por parte de proveedores de tecnología	Riesgo de Fraude / Corrupción	4	20%	0.8	A	B	A	Exist.	Clausulas de confidencialidad, acceso a auditorías, no divulgación, entre otros.	M	Exist.	Segregación de funciones. Controles de acceso.	A	Exist.	Evaluación trimestral del proveedor. Metodología para la selección y contratación de proveedores.	M	A	B	0.0864	
5	2,3	Conflicto de intereses con proveedores y terceros relacionados	Riesgo de Fraude / Corrupción, conflicto de interes	4	40%	1.6	A	B	A	Exist.	Segregación de Funciones.	M	Exist.	Difusión de la Política de Seguridad de la Información. Código de Ética.	M	Exist.	Monitoreo periódico sobre proveedores aprobados. Revisión de antecedentes.	M	M	A	0.3456	
							Riesgo inicial (potencial)			6											Score residual	0.8208
																	Disminución	86%				

Fuente: elaboración propia

NOTA BIOGRÁFICA

Shirley Ledda Villacorta Aristondo

Ejecutiva de Auditoría, Máster en Auditoría de la Universidad del Pacífico e Ingeniero de Sistemas de la Universidad de Lima. Desempeña actualmente el cargo de Subgerente Adjunto de Auditoría de Procesos y TI en el Banco de Crédito del Perú, institución líder de los principales servicios financieros del sistema financiero peruano, perteneciente al holding CREDICORP y que forma parte del grupo económico líder del país. Con más de cinco años de experiencia en la profesión de auditoría interna, es responsable de entregar y garantizar el valor de los procesos y productos estratégicos evaluados. En su trayectoria profesional, ha brindado servicios a empresas reguladas por la Superintendencia de Banca, Seguros y AFP del Perú, reguladas por la Securities and Exchange Commission de los Estados Unidos, empresas de telecomunicaciones nacionales e internacionales, así como a empresas comerciales

Margiori Natalia Dolci Bonilla

Ejecutiva sénior, Magister en Auditoría, con 16 años de experiencia en auditoría auditoría financiera y operativa en empresas de banca y en seguros. Desempeña actualmente el cargo de Gerente de Gestión Administrativa y Relaciones Laborales en la compañía Rímac Internacional Cía. de Seguros y Reaseguros, primera empresa aseguradora del mercado peruano, perteneciente a uno de los grupos económicos más importantes del país. Actualmente es responsable de Gestionar los procesos administrativos, legales-laborales, mantener el control financiero y la gestión de indicadores de la División de Gestión y Desarrollo Humano bajo el principio de eficiencia, dentro del marco de la legislación laboral vigente y normativas definidas por los entes reguladores. Desempeñó el cargo de Auditor General de Rímac Internacional durante cuatro años y medio, tiempo en el que fue responsable de evaluar el adecuado funcionamiento de control interno de la compañía, vigilar la adecuada gestión del riesgo de la compañía así como el adecuado cumplimiento de

las regulaciones vigentes emitidas por los diferentes organismos de control.