UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE CIENCIAS

TÍTULO DEL REPORTE

ADMINISTRACIÓN DEL RIESGO OPERATIVO Y CONTROL INTERNO A TRAVÉS DE LOS MODELOS DE PROCESOS, RIESGOS Y CONTROL.

QUE PARA OBTENER EL TÍTULO DE:

ACTUARIA

P R E S E N T A :

MACRINA IVETH ZAMORA ENSASTEGUI

TUTOR

ACT. OSCAR ARANDA MARTÍNEZ

2007

FACULTAD DE CIENCIAS
UNAM

1. Datos del alumno
Zamora
Ensastegui
Macrina Iveth
15570118
Universidad Nacional Autónoma de México
Facultad de Ciencias
Actuaría
090262597

2. Datos del tutor
Actuario
Oscar
Aranda
Martínez

3. Datos del sinodal 1
Actuario
Ricardo
Villegas
Azcorra

4. Datos del sinodal 2
Actuario
Ricardo Humberto
Sevilla
Aguilar

5. Datos del sinodal 3
Actuario
Francisco Javier
Palacios
Roji

6. Datos del sinodal 4
Actuario
José Guadalupe
Vázquez
Vázquez

7. Datos del trabajo escrito
Administración del riesgo operativo y control interno a través de los modelos de procesos, riesgos y control.
59 p.
2009

GRACIAS DIOS, POR LA VIDA, POR LAS EXPERIENCIAS, CONOCIMIENTO Y DONES RECIBIDOS, POR LOS MAESTROS, LOS COMPAÑEROS Y AMIGOS DE ESTUDIO Y DE VIDA QUE PUSISTE EN MI CAMINO, CADA MOMENTO LO LLEVO GRABADO EN MI MEMORIA Y EN MI CORAZÓN.

Este trabajo representa el término de un ciclo en mi vida, lo dedico con mucho cariño a mi familia.

Mis padres:

- Maximiliano Zamora Casillas
- Micaela Ensastegui Ramírez

Mis hermanos:

- Horacio Israel Zamora Ensastegui
- Maximiliano Zamora Ensastegui

Mis hijos:

- Javier Martínez Zamora
- A ti bebé que estas en mi vientre.

- Padre te agradezco todo lo que me has dado, tus actos de amor e incluso tus regaños; se que para ti era importante que yo concluyera por eso te dedico este trabajo con mucho cariño y respeto.

- Madre, gracias por tu apoyo incondicional, por tu amor, tu comprensión y por estar conmigo cuando mas te he necesitado.

- Horacio gracias hermano por tu ejemplo de fortaleza, templanza y por todo el apoyo que siempre me has brindado.

- Max gracias hermano por tu calidad humana, por tu capacidad de escuchar, comprender y por tu disposición para un recto modo de proceder.

- Javier eres un regalo de Dios, gracias por el amor incondicional que despiertas en mi, por el amor que recibo de ti, eres tan calido y limpio de espíritu, me das esperanza, fortaleza y representas una hermosa responsabilidad que me ayuda a crecer.

- Para ti bebé que estas en mi vientre eres otro hermoso regalo de Dios, representas crecimiento en mi vida, esperanza y amor.

Este trabajo también quiero dedicarlo a alguien muy especial:

- Norma, se que estas en el cielo, recibe mi dedicatoria, admiración, amor y respeto, te agradezco los momento felices y tristes que pasamos juntas estos años de Universidad, eres una amiga incondicional y una compañera de vida, una hermana, te hablo así por que siempre vas ha estar viva en mi memoria y en mi corazón, como tu decías cuando seamos viejitas y platiquemos nuestras anécdotas nos vamos a reír y ha divertir mucho...

Índice

INTRODUCCIÓN

El interés por implementar la Administración del riesgo Operativo en la Compañía, surgió por el requerimiento regulatorio que la Comisión Nacional de Seguros y Fianzas (CNSF) estableció en su Circular S-11.6 emitida el 5 de octubre del 2000, en la cual da a conocer los lineamientos de carácter prudencial en materia de Administración Integral de Riesgos, estableciendo las bases para identificar, medir, monitorear, limitar, controlar y divulgar los riesgos de mercado, crédito, liquidez, operativo y legal. Derivado de este requerimiento surge el interés y posteriormente la necesidad de evaluar los riesgos operativos, ya que la gestión de este riesgo esta relacionada con la administración del sistema de control interno en la Organización.

Para la evaluación del riesgo operativo y control interno no existen métodos específicos, esto incrementó la complejidad para su evaluación, en los últimos 4 años se han planteado en la Compañía diferentes alternativas de gestión y administración de este riesgo, considerando el nivel de control y sistematización de los procesos, así como del alcance, visión y nivel de importancia o prioridad que en ese momento la Compañía le quería dar a su gestión, sin embargo dadas las características del riesgo, su importancia, el nivel de impacto financiero que puede representar y el entorno globalizado cada vez mas competido en el que se desenvuelve la Compañía, se ha requerido adoptar formas serias para su evaluación, que permitan conocer, gestionar y mejorar su nivel de respuesta al riesgo.

Los modelos aquí propuestos recogen la propia experiencia, las prácticas observadas en otras Compañías, los lineamientos establecidos por estándares Internacionales y el entorno regulador, así como la filosofía del Marco integrado sobre Administración de Riesgos Corporativos, emitido por el Comité of Sponsiring Organizations of the Treadway Commission (COSO).

Son tres modelos que se desarrollan para la administración de riesgos operacionales y el control interno; el modelo de procesos, de riesgos y de controles. Se construyen los modelos considerando que la Organización tiene un nivel básico en sus procesos, es decir no tienen documentados todos sus procesos, el personal no cuenta con una cultura de riesgo y control, no se cuentan con mapas de riesgo, no se tienen registros de pérdidas por riesgos operacionales, no existen indicadores de riesgo o de seguimiento de la eficiencia de los procesos etc.

A continuación se describe el objetivo general de los modelos antes mencionados, los cuales se van aplicando por etapas y se complementan.

- Modelo de Procesos:

Realiza la identificación clasificación y el mapa de los procesos, estableciendo algunos criterios para definir prioridades para su análisis.

- Modelo de Riesgos:

Identifica, evalua y clasifica los riesgos, así mismo genera mapas de riesgo para su administración.

- Modelo de Controles:

Mide la eficiencia del control en los procesos, en cuanto a su diseño y funcionamiento.

Con la utilización de los tres modelos se pretende administrar los riesgos operativos e identificar las debilidades de control, para disminuir el nivel de exposición al riesgo y en algunos casos el nivel de pérdidas por este cocepto.

1.-Visión general del proyecto.

1.1 Objetivo del proyecto.

Apoyar la generación de valor en la Compañía, estableciendo estrategias y metodologías que permitan administrar de manera más consciente sus riesgos operacionales, aplicando recursos eficaz y eficientemente, para encontrar un equilibrio entre las metas de crecimiento, rentabilidad y los riesgos asociados, a fin de lograr los resultados esperados.

1.2 Objetivos específicos

- Promover una **cultura de riesgo y control interno** Institucional.
- Apoyar la consecución de sus objetivos estratégicos, operativos, de reporte y de cumplimiento con las leyes aplicables.
- Promover una mayor confianza entre Consejo de Administración, Accionistas, la alta Dirección y Autoridades.
- Adaptarse a un entorno normativo cada vez más exigente.

1.3 Puntos relevantes

Todas las Compañías se enfrentan a la ausencia de certeza, el reto para estas en la Administración de Riesgos es determinar cuánta incertidumbre se puede aceptar, mientras se esfuerzan en incrementar el valor para sus grupos de interés.

La administración de riesgos, permite a la Dirección tratar eficazmente la incertidumbre, la cual implica riesgos y oportunidades y posee el potencial de erosionar o aumentar el valor en las entidades.

La administración de riesgos parte del principio de que las entidades existen con el fin último de generar valor para sus grupos de interés, para el logro de este fin, a continuación se mencionan algunos puntos relevantes:

El proyecto involucra a todos los niveles de la organización.

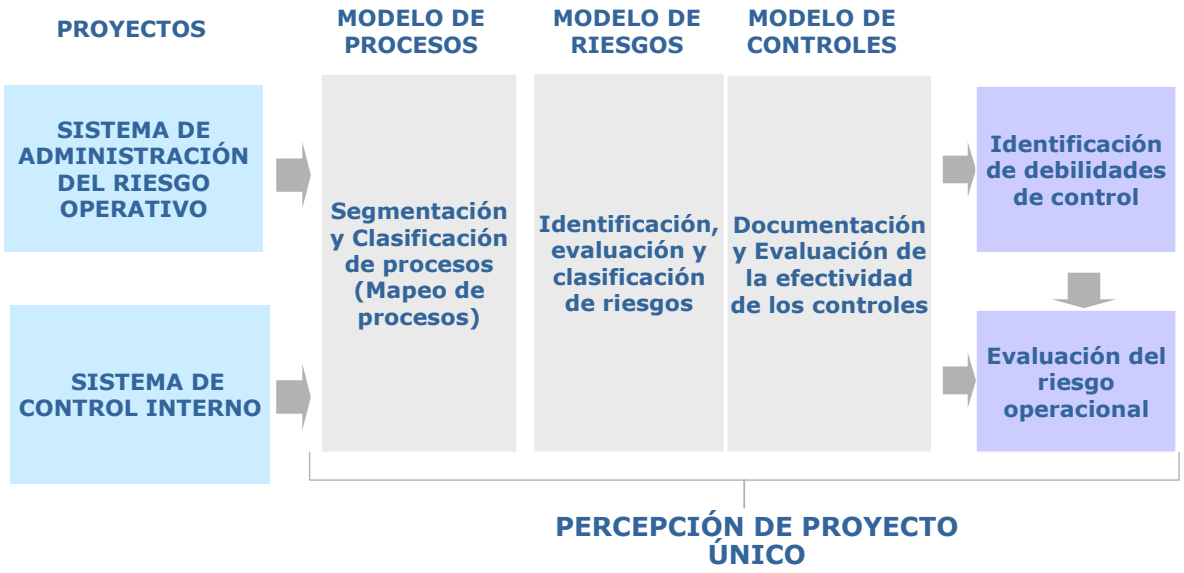
- Está orientado al logro de objetivos.
- Alinea la estrategia y el riesgo.
- Está diseñado para identificar eventos (riesgos y oportunidades) que puedan afectar a la organización.
  - Aprovecha las oportunidades.
  - Identifica y gestiona la diversidad de riesgos.
- Mejora las decisiones de respuesta a los riesgos.
- Reduce pérdidas operativas cuantificables o no.
- Optimiza la aplicación de recursos.

1.4 Alcance.

En un proyecto Institucional, participa toda la entidad y en todos los niveles de la organización.

1.5 Esquema del modelo para la gestión del Riesgo Operativo y Control Interno

El presente modelo une dos proyectos que son complementarios, el Sistema de Control Interno y el Sistema de Administración de Riesgo Operativo.



Para los dos proyectos se han diseñado estos 3 modelos, los cuales se van aplicando por etapas y se complementan.

1.6 Fases del proyecto

A continuación se presenta un desglose de las diferentes etapas en que se desarrollará el modelo antes mencionado.

Diagnóstico del ambiente interno.	Mapeo y clasificación de procesos.	Identificación, evaluación y clasificación del riesgo.	Identificación y documentación de controles.	Implementación de pruebas, para validar el diseño y aplicación de los controles.	Establecimiento de planes de acción, generación de reportes y seguimiento.
FASE 1	**FASE 2**	**FASE 3**	**FASE 4**	**FASE 5**	**FASE 6**

La visión de este proyecto a mediano plazo es la creación de un sistema que permita optimizar la evaluación de los riesgos y los controles. En un primer ejercicio los modelos se aplicarán en forma manual, con formatos que contienen los campos y los parámetros que capturan la información requerida para la alimentación de un sistema.

2.- Modelo de procesos.

2.1 Concepto preeliminares.

2.1.1 Definición de proceso.

Tradicionalmente los procesos se definen como una serie de actividades concatenadas y sistemáticas que se realizan para transformar insumos en productos o servicios. Su aspecto clave es la secuencia.

Los insumos pueden considerarse con las causas ó condiciones y los productos y/o servicios como los "resultados" o efectos.

2.1.2 Elementos del proceso.

A continuación se explica el desglose de los elementos del proceso.

Recursos Humanos: Es la parte del proceso en donde intervienen el factor humano, así que los puntos críticos son:

- **Adecuada selección y reclutamiento del personal:** el riesgo reside en que el participante no cuente con un perfil adecuado para la labor o las funciones que va ha desempeñar desde el momento de contratación.

- **Capacitación:** La capacitación debe ser continua y especifica para cubrir las necesidades del puesto o para el desarrollo de otras habilidades que contribuyan al mejor desempeño o superación del personal de la Institución.

- **Cultura y valores de la Empresa**: Es fundamental crear una identidad al momento de pertenecer a un grupo el cual se va ha distinguir por la cultura de valores y principio con que se maneje la empresa.

Estructura del Proceso: Se refiere a la forma en que esta conformado el proceso desde el diseño, los controles, el grado de sistematización y como estén divididas y asignadas las funciones que forman parte del proceso.

- **Procedimiento:** Se refiere al número de pasos a seguir para llevar a cabo una función, Es la descripción de cómo realizar las actividades por parte de un colaborador o grupo de colaboradores para la realización de la parte de un proceso.

- **Políticas:** Son lineamientos generales que regulan el actuar de las personas durante su desempeño en los procesos de la organización, tienen por objeto orientar la acción y proporcionan guías para la toma de decisiones.

- **Nivel de automatización:** Esta parte se refiere al grado de sistematización de los procesos, procedimientos, funciones o actividades a desarrollar, así como al manejo adecuado de información y para hacer más eficiente la operación. El riesgo esta en función del grado de sistematización de los procesos, entre más manuales sean estos, están sujetos a un mayor riesgo por error humano.

- **Asignación de funciones:** Se divide el proceso por procedimientos, actividades o funciones para asignar la responsabilidad de su ejecución al personal con las habilidades y conocimiento adecuados.

Controles: El control tiene como finalidad cerciorarse de que los hechos vayan de acuerdo con los planes establecidos, es la regulación de las actividades, de conformidad con un plan creado para alcanzar los objetivos. El control se enfoca a establecer una relación de la ejecución con la planeación, con el propósito de verificar el logro de los objetivos proyectados, aplicando recursos de:

- Medición: Para controlar es imprescindible medir y dimensionar los resultados, para lo cual se requieren **Indicadores,** que son índices de seguimiento, construidos a partir de variables extraídas de los procesos y cuyo comportamiento esta relacionado con el nivel de riesgo asumido. Estas variables mesurables, observables en los procesos, aportan información acerca del nivel de exposición al riesgo.

- Detección de desviaciones, como forma de identificar y localizar las diferencias que se presentan entre ejecución y planeación.

- Medidas Correctivas sobre las desviaciones detectadas, como la aportación fundamental para el logro de los objetivos planeados.

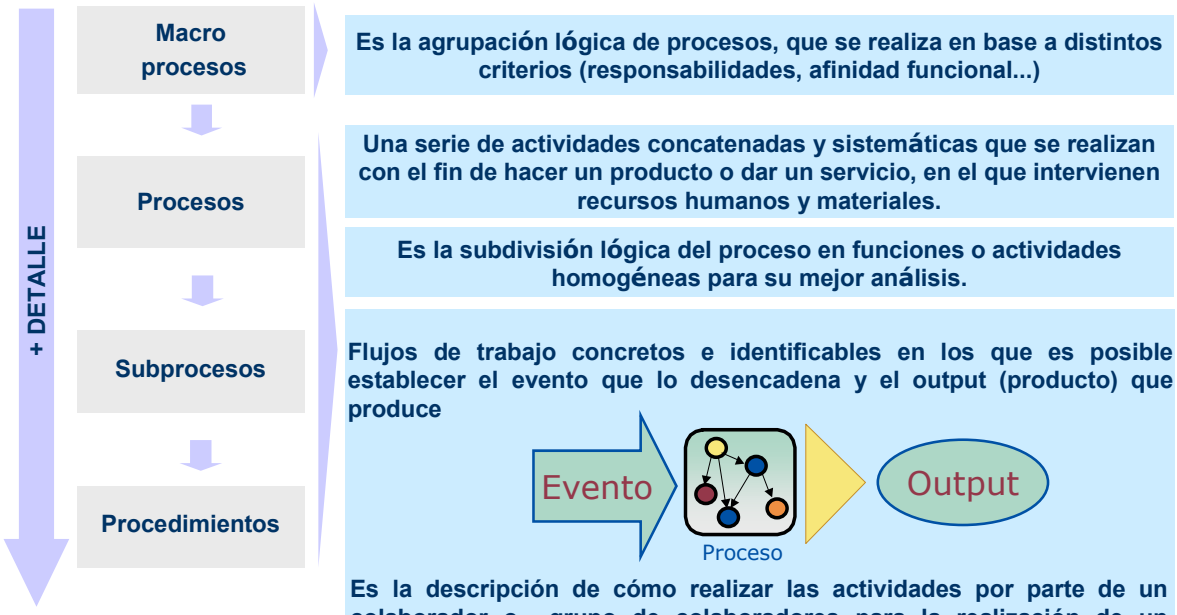
- Medidas preventivas, enfoque de los controles a prevenir irregularidades o errores.

2.1.3 Características del proceso

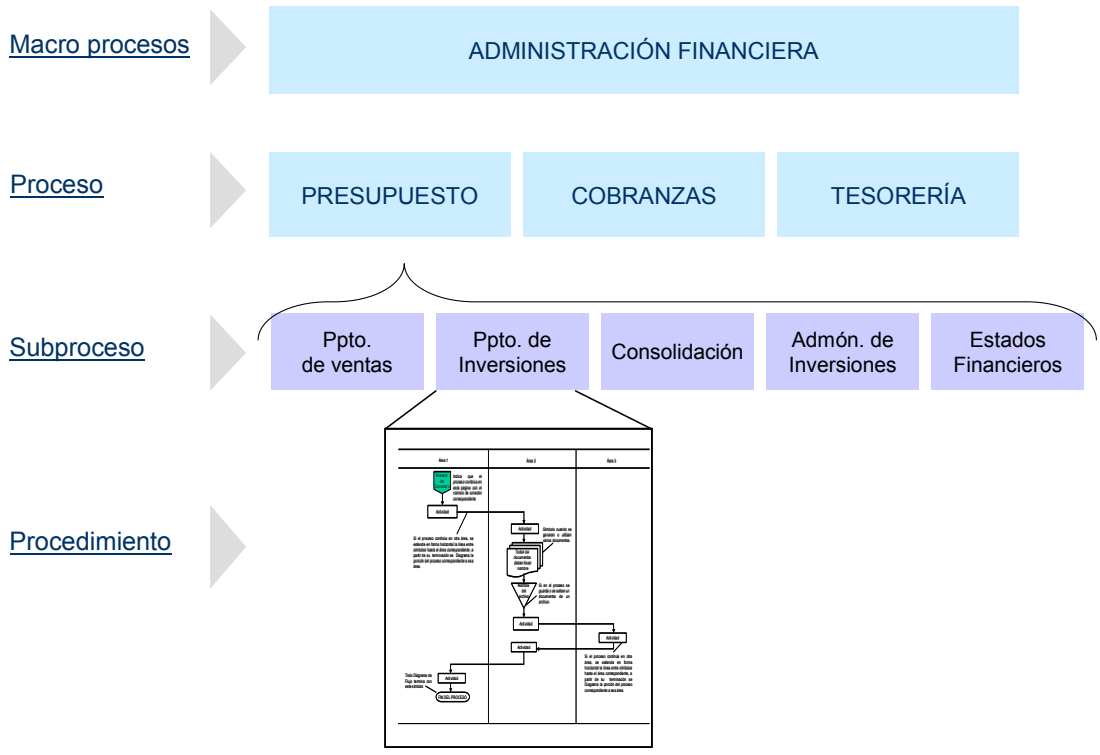
- Es repetitivo.
- Esta delimitado.
- Cuenta con proveedores y clientes.
- Esta conformado por diferentes actividades.
- Se integra por fases secuenciales.
- Tiene entrada y salida.
- Tienen secuencia lógica y enlazan la cadena “cliente-proveedor”
- Tienen una misión y se dirigen hacia el logro de objetivos de la organización.
- Transforma insumos.
- Es susceptible de ser medido bajo el establecimiento de ciertos parámetros.

2.2 Descripción del modelo de procesos

El modelo de procesos consiste en identificar sus diferentes niveles, con el objeto de facilitar su análisis, como se observa en el siguiente esquema.



A continuación se muestra un ejemplo cada uno de estos niveles:



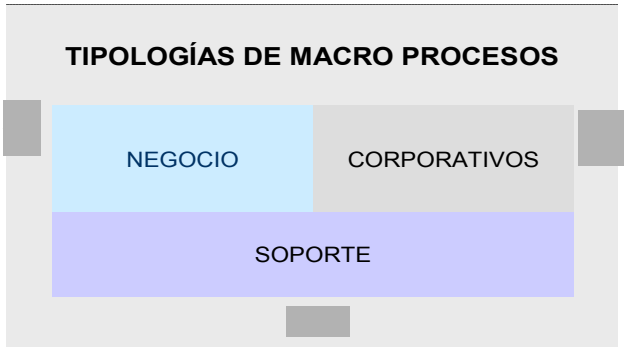
2.2.1 Definición de tipologías de macro procesos.

Es necesario hacer una identificación de los diferentes tipos de macro procesos, ya que para cada uno de estos se requiere un enfoque diferente de análisis. A continuación se definen los macro procesos de:

Negocio: Se centran en la actividad principal del negocio, como es la captación y fidelización de clientes mediante el asesoramiento y la distribución de productos y servicios.

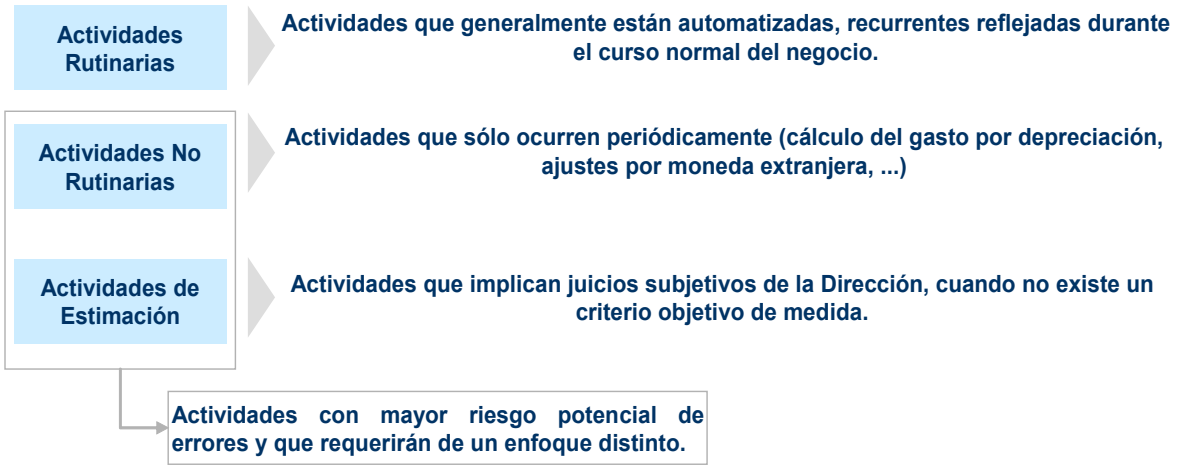
Corporativos: Garantizan el cumplimiento de las obligaciones legales y normativa interna, toma de decisiones sobre planificación y control a nivel corporativo, así como el desarrollo de actividades corporativas que no prestan un soporte específico a los negocios.

De soporte: Se desarrollan para asegurar la dotación de los recursos precisos (humanos, materiales, inmuebles, informáticos) para el correcto desarrollo de la actividad del Grupo.



2.2.2 Algunos criterios a considerar.

No toda la operación tiene la misma relevancia, por tanto recomienda clasificar la operación de una entidad de la siguiente forma:



¿Es necesario identificar todos los procesos del área?

Sí, de manera genérica es importante tener identificadas y clasificadas las actividades, rutinarias, automatizadas o manuales, las actividades que sólo ocurren periódicamente y las actividades que impliquen juicios subjetivos de la dirección o gerencia.

¿Qué procesos se deben analizar a profundidad?

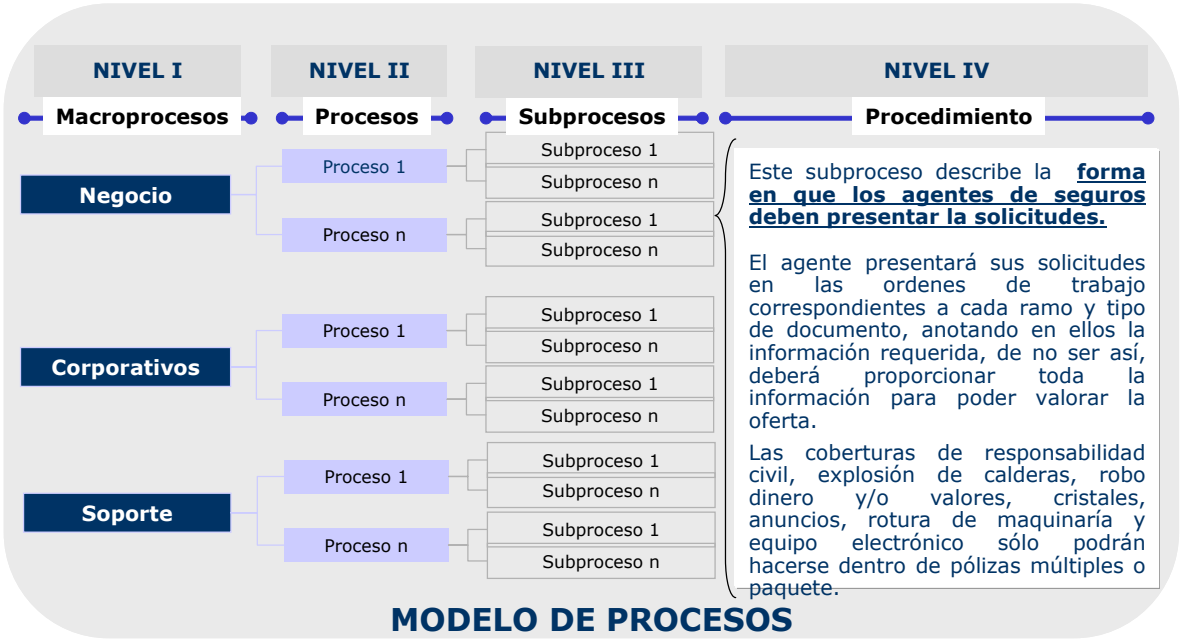
Los procesos en los que se va a profundizar más en su análisis, van a ir en función a su nivel de relevancia, el cual va a estar determinado considerando las siguientes variables:

a) Mayor importe de operaciones o recursos que maneja, (Importancia relativa que tienen el valor de las operaciones en los estados financieros).
b) Mayor volumen de operaciones.
c) Grado de importancia de la operación de acuerdo a la misión de la Compañía.

¿Es necesario documentar todos los procesos del área?

No, de manera prioritaria solo se documentarán aquellos que por su grado de impacto e importancia tienen mayor relevancia en la operación de la Compañía.

Para ejemplificar lo antes visto, se documentan los procesos en un esquema de cuatro niveles, desde grandes ciclos operativos hasta la desagregación de las tareas.



MODELO DE PROCESOS

2.2.3 Ejemplo: Desglose de los macro procesos en sus diferentes niveles.

A continuación se presenta un ejemplo del desglose de los Macro procesos como un conjunto de actividades secuenciales en el tiempo, con un inicio y un fin. El criterio general ha sido tener en cuenta el ciclo de vida de un producto (desde la perspectiva del cliente); no obstante, en determinados casos, se han desagregado los subprocesos en función de la naturaleza de los riesgos a los que esta sometido.

MACROPROCESOS CORPORATIVOS		
MACROPROCESOS	**PROCESO**	**SUBPROCESO**
Fiscal	Cumplimiento regulatorio Contingencias fiscales	
Jurídico	Gestión de contratos	Resguardo de contratos Revisión de contratos
	Gestión legal	Legislación aseguradora Reclamación de terceros
Planeación	Estrategias de negocio	Objetivos anuales Proyectos estratégicos
	Presupuesto	Definición Implementación

MACROPROCESOS NEGOCIO		
MACRO PROCESOS	**PROCESO**	**SUBPROCESO**
Desarrollo de productos	Diseño de productos	Análisis y diseño técnico o actuarial Diseño legal o contractual
	Implementación de producto	Cumplimiento regulatorio Marketing
Actividades comerciales	Agentes	Comisiones, bonificaciones e incentivos Captación y capacitación de agentes
	Gestión administrativa de ventas	Ventas foráneo Ventas local Administración de agentes y venta Atención a clientes
Suscripción de riesgo	Análisis y selección de riesgos	Selección y suscripción Reaseguro
	Procedimientos administrativos	Contratación Emisión Gestión administrativa
Siniestros	Gestión administrativa de siniestros	Control de costos Legal y recuperaciones Valuación Salvamentos Pérdidas totales
	Atención de siniestros	Asistencia telefónica (Castel) Siniestros locales Siniestros foráneos Diversos Mesa de control
Proveedores	Selección y reclutamiento	Análisis y selección Contratación
	Evaluación Gestión y administración	Seguimiento de servicio Control de costos

MACROPROCESOS DE SOPORTE		
MACROPROCESOS	**PROCESO**	**SUBPROCESO**
Recursos humanos	Gestión RH Gestión administrativa Servicios generales	
Gestión administrativa	Tesorería	Inversiones Procesos administrativos
	Contabilidad Información financiera	
	Operación administrativa	Caja Cobranza Cuentas por pagar
Infraestructura tecnológica	Desarrollo y mantenimientos	Planes de continuidad de sistemas Arquitectura de sistemas Hardware, Software
	Operación	Soporte usuarios Explotación de datos Explotación de sistema Sistemas de seguridad informática
	Comunicaciones	Redes Telefonía y otros

2.2.4 Definición de entidad y sector.

Los conceptos definidos a continuación van a servir para ubicar, identificar y clasificar los diferentes procesos, riesgos y controles, por región o unidad de negocio y por actividad, a fin facilitar su administración y construcción de un sistema informático, para la explotación de información que apoye la toma de decisiones.

Entidad:

Se identifican las distintas unidades de negocio que realizan las actividades de la Institución, para el logro de sus objetivos.

Ejemplo: Oficina Matriz, Sucursal Tijuana, Mexicali, Chihuahua, Torreón etc., Oficina La paz, Colima entre otras.

Sector:

Se define el sector, a través de las segmentaciones que se realizan en una entidad en función de diferencias significativas en la gestión de cada uno de los procesos de negocio definidos, puede ser por tipo de operación, por ramo o por proceso, lo que implica que los riesgos detectados en cada uno de los sectores puedan tener una importancia y probabilidad de ocurrencia diferentes entre sí.

En este ejemplo se identifican los sectores de acuerdo al ramo.

Vida	Individual
	Grupo
	Colectivo
	Accidentes personales
Daños	Automóviles y camiones
	Múltiple familiar y empresarial
	Marítimo y trasportes
	Equipo electrónico
Agropecuario	Agrícola
	Animal
Salud	Cuidado y mantenimiento de la salud
	Hospitalización
	Maternidad
	Auxiliares de diagnóstico en la consulta externa
	Medicamentos en la consulta externa
	Servicios odontológicos
	Beneficios adicionales

3.- Modelo de riesgos.

3.1 Antecedentes y conceptos generales.

3.1.1 Definición de riesgo

El riesgo es cualquier factor que puede tener un impacto negativo en el logro de los objetivos.

Características del riesgo.	Elementos del riesgo.	Conductas frente al riesgo.
♦ Posible	♦ Magnitud	♦ Indiferencia
♦ Incierto	♦ Probabilidad o frecuencia	♦ Negligencia
♦ Aleatorio	♦ Variación	♦ Asumirlo (Aceptar el riesgo sin hacer nada)
♦ Impacto negativo	♦ Amenazas	♦ Gestionarlo (eliminarlo minimizarlo o Transferirlo)
♦ Fortuito	♦ Vulnerabilidad	

A continuación se definen las características y elementos del riesgo.

Posible: La posibilidad es la facultad estado potencial y/u ocasión para que se presente el hecho, no tiene ponderación existe o no existe, vale o no vale cero.

Incierto**:** No saber si puede suceder o no el riesgo, no se sabe en que magnitud puede impactar.

Aleatorio: Tener la certeza de que puede suceder el riesgo.

Impacto negativo: Siempre el impacto de la materialización del riesgo tiene un efecto negativo, cuantificable o no, puede ir en función del porcentaje de la pérdida sufrida con relación al volumen de operaciones o capital, en los casos no cuantificables pueden tener impacto en, la credibilidad, la reputación, la confianza, etc.

Fortuito: Que sucede de improvisto.

Magnitud: Se le denomina también severidad y la medida correspondiente al grado de gravedad económica que puede presentar la realización del riesgo.

Probabilidad o frecuencia: Cuando existe la posibilidad, la probabilidad es la verosimilitud o calidad de razón por la cual se cree que ocurrirá el hecho, la probabilidad siempre es ponderable y su valor esta entre uno y cero. Una vez determinada la magnitud de un riesgo, éste debe ser ponderado por una medición de la frecuencia o “probabilidad” con la cual se presenta.

Variación: Es la forma en la cual se presentan los riesgos, en su magnitud y en su frecuencia con relación al tiempo.

Amenazas: Escenario intencional o no intencional (evento climático, terremoto, inundación) que puede dañar un activo. Normalmente externa (no controlables), pero puede haber internas (empleados descontentos, sindicatos). Independiente al impacto y ocurrencia.

Vulnerabilidad: Tiene que ver con las características intrínsecas del activo que lo hacen más susceptible a sufrir daños o pérdidas con respecto a las amenazas, a eventos fortuitos. Se mantienen invariables para cada activo, independiente al impacto y ocurrencia.

Estos conceptos son los que definen al riesgo en general, sin embargo existen diferentes tipos de riesgo con características particulares que pueden impactar a una Organización. La CNSF ocupada en difundir e impulsar una cultura de administración de riesgos financieros, emite la circular S-11.6, en donde establece lineamientos de carácter prudencial en materia de administración integral de riesgos, los cuales deben ser implementados por las Compañías Aseguradoras, a efectos de poder administrar los riesgos que a continuación se describen:

Riesgo de mercado: Es la pérdida potencial por cambios en los factores de riesgo que inciden sobre la valuación de las posiciones, tales como tasas de interés, tipos de cambio e índices de precios, entre otros.

Riesgo de liquidez: Es la pérdida potencial por la venta anticipada o forzosa de activos a descuentos inusuales para hacer frente a sus obligaciones, o bien, por el hecho de que una posición no pueda ser oportunamente cubierta mediante el establecimiento de una posición contraria equivalente.

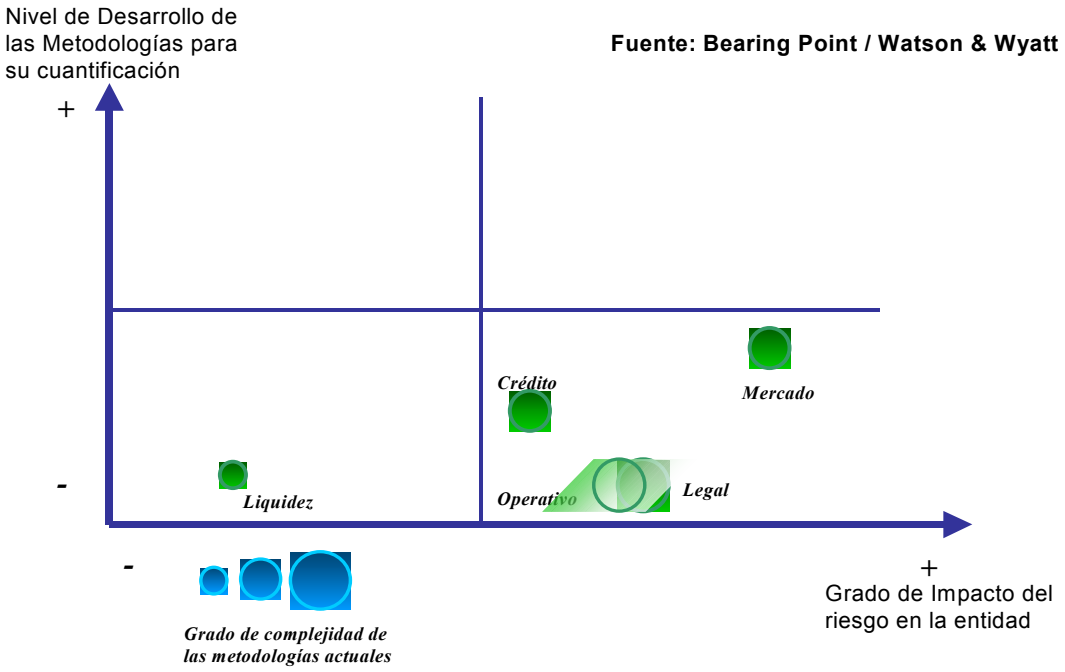
Riesgo de crédito: Es la pérdida potencial por la falta de pago de un acreditado o contraparte en las operaciones que efectúan esas instituciones.

Riesgo legal: Es la pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que esas instituciones llevan a cabo.

Riesgo operativo: Es la pérdida potencial por fallas o deficiencias en los sistemas de información, en los controles internos o por errores en el procesamiento de las operaciones.

Administración integral de riesgos: Es el conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgo a que se encuentran expuestas las Instituciones.

Los requerimientos regulatorios han sido la razón principal que ha motivado a las Compañías Aseguradoras a gestionar de manera más metódica y sistemática sus riesgos. Cada riesgo tiene diferente nivel de impacto económico o pérdida financiera, así como diferente nivel de desarrollo y complejidad en cuanto a su metodología para su cuantificación. A continuación se presenta un esquema con los cinco tipos de riesgo que regula la CNSF, con la descripción de las variables antes mencionadas.



Se observa que el riesgo de mercado es el que mayor grado de impacto tiene en las entidades, así como mayor nivel de desarrollo de la metodología para su cuantificación y con un grado de complejidad medio, después de este en cuanto a nivel de impacto se encuentra el riesgo legal y operativo que muestran el mayor grado de complejidad y menor desarrollo en cuanto a las metodologías para su cuantificación. Cabe mencionar que este estudio fue realizado con Instituciones norteamericanas en donde el riesgo legal tiene una relevancia mayor que el riesgo operativo.

El concepto de riesgo operativo es muy amplio y en la metodología aplicada a este proyecto el riego legal es solo un área de gestión del riesgo operativo.

3.1.2 Impacto e importancia del riesgo operativo

El análisis del riesgo operativo ha sido muy limitado, debido a su diversidad y complejidad para gestionarlo, monitorearlo y cuantificarlo, los modelos para medirlos y controlarlos está en sus primeras etapas, en buena medida esto se debe a que no existe una definición estándar de este riesgo, ni suficiente información que permita estimar con un nivel de confianza definido a cuanto podrían ascender las pérdidas en el caso de presentarse eventos operativos adversos, como: fraudes, abusos por información privilegiada, fallas en los sistemas de cómputo, falta de control en la operación, inversión en instrumentos no autorizados, entre otros.

Sin embargo el entorno de las organizaciones siempre cambiante, en un mundo globalizado y altamente competitivo nos obliga a mejorar nuestro desempeño y la seria gestión del riesgo

operativo sé ha tornado en una necesidad relevante para las empresas, independientemente de hacer los esfuerzos mínimos para dar cumplimiento a los requerimientos regulatorios.

3.1.3 Definición del riesgo operativo

Existen varias definiciones del Riesgo operativo que tienen cierta ambigüedad con respecto al alcance y forma de interpretarlo, a continuación se describen algunas de estas:

- **Comisión Nacional de Seguros y Fianzas Circular S-11.6:**

"Riesgo Operativo, es la pérdida potencial por fallas o deficiencias en los sistemas de información, en los controles internos o por errores en el procesamiento de las operaciones".

- **Comité de Basilea:**

"Riesgo operativo es el que proviene de la falta de información en los sistemas o en los controles internos y que pueden provocar una pérdida inesperada. Este riesgo se asocia con errores humanos, fallas de sistemas e inadecuados sistemas y controles".

- **Chase Manhattan Bank:**

"El riesgo de pérdidas debido a errores de los empleados, deficiencias organizacionales, fraudes, fallas en los sistemas, inadecuada performance por proveedores y eventos similares".

- **Canadian Imperial Bank of commerce:**

"El riesgo operacional es el que esta asignado a todos los riesgos que no son directamente atribuibles a las categorías de riesgo crediticio y riesgo de mercado".

- **Barclays:**

"El riesgo causado por fallas en los procesos operacionales o sistemas que lo soportan. Esto incluye errores, omisiones, caídas en los sistemas, desastres naturales y actividades fraudulentas que causan impactos en términos de disponibilidad del servicio, pérdidas financieras, incremento de costos, pérdida de reputación o imposibilidad de realizar las ganancias planeadas".

- **Lloys TSB:**

"La exposición a daños financieros o de otra índole que aparecen debido a eventos no previstos o fallas en los sistemas o procesos operacionales de grupo".

- **Laycock :**

"El riesgo operativo es el potencial negativo en el estado de resultados o en flujo de efectivo de una entidad debido a los efectos atribuibles a usuarios (internos y externos), controles y sistemas no definidos de una manera adecuada, fallas de control o sucesos poco manejables".

Existen autores que señalan que los riesgos operativos también pueden provenir de clientes y proveedores de la entidad, así como de sistemas poco claros o de situaciones de difícil manejo.

En una acepción universalmente aceptada del Riesgo Operativo es: *cualquier cosa que pueda impedir que una organización cumpla con sus objetivos de negocio. Son todos los riesgos que no se relacionan con riesgo crediticio y riesgo de mercado. Es el riesgo directo o indirecto de pérdidas*

resultantes de un inadecuado o fallido proceso interno, personal o sistemas o por eventos internos. Es el riesgo de pérdidas a través del procesamiento de transacciones.

3.1.4 Características del riesgo operativo.

- Está inmerso en todos los procesos de la empresa.
- Puede ser aleatorio en función de la frecuencia y lugar de ocurrencia (puede presentar en cualquier lugar y momento).
- Sus causas y consecuencias son de toda índole (heterogéneo).
- Necesariamente a menor riesgo o exposición, mayor utilidad o resultados constantes.
- Tiene un impacto económico cuantificable o no.
- Puede ser no intencional o doloso.

No intencional.	**Doloso.**
❖ Falta de capacitación	❖ Intencional
❖ Procedimientos no definidos	❖ Malversación de información
❖ Falta de políticas	❖ Fraude, robo
❖ Sobrecarga de trabajo	❖ Abuso de confianza
❖ Falta de planeación	❖ Actividades no autorizadas
❖ Falta de organización	❖ Incumplimiento de políticas y normas
❖ Descuido	❖ Incumplimiento de contratos
❖ Desconocimiento del alcance de las funciones	❖ Prácticas comerciales impropias

3.1.5 Gestión tradicional del riesgo operativo.

Se cometen diariamente errores y fallas en toda organización, algunas por descuido o falta de capacitación, cuyo impacto generalmente no es relevante, otros más serios y en algunos casos muy graves. Los riesgos operativos han existido siempre, se han gestionado con un enfoque básico de controles internos como a continuación se señala:

- ♦ Se apoya en la confianza y competencia de los empleados.
- ♦ Cada área de negocio gestiona su riesgo operacional, estableciendo los controles y medidas que estima oportunos.
- ♦ El área de Auditoría realiza inspecciones periódicas de los procesos y da seguimiento a la atención de sus hallazgos.

Algunas de las debilidades que se pueden identificar en la gestión tradicional del riesgo operativo son las que a continuación mencionamos:

- ♦ La carencia de un enfoque global y de un marco de referencia institucional para la gestión del riesgo operativo.

- Visión parcial del riesgo operacional, se adoptan algunas medidas para mitigarlo sin una visión o plan general para su control.

- Indiferencia frente al riesgo, por la falta de una cultura Institucional para generar una conciencia de la importancia de identificar los riesgos y falta de conocimiento para identificar y evaluar los riesgos.

- La carencia habitual del registro ordenado, sistemático y habitual de las incidencias operativas

- No se dispone de datos históricos fiables acerca de eventos ocurridos, ni de sistemas de información de riesgos operacionales para su análisis y cuantificación.

- No se establecen asociaciones entre factores de riesgo e indicadores de seguimiento, por lo que no se puede cuantificar los niveles de exposición.

La consideración del riesgo operativo ha sido un tema fuertemente rezagado en la presentación de servicios en general, dada la complejidad de su diversidad y gestión, el "sentido común" no basta para gestionarlo, es preciso acudir a formas serias para su identificación, evaluación, transferencia, mitigación, seguimiento y registro.

La exposición al riesgo que asumen las Compañías es de diferente naturaleza, en algunos casos esta dispuesta a asumir para crear ventajas competitivas, como es el caso del riesgo de mercado en la compra de un instrumento financiero en el cual hay una relación entre el riesgo y rendimiento, normalmente se cumple que a mayor riesgo mayor rendimiento, a diferencia de este riesgo el Riesgo Operativo, es un riesgo que a menor exposición se pude generar mayor utilidad, el riesgo de mercado es impredecible y no está dentro del control de la Compañía, el control del riesgo operativo depende en gran medida de que la Compañía establezca los controles internos adecuados, así como parámetros y metodologías bien definidos para su cuantificación.

3.2 Descripción del modelo de riesgos.

3.2.1 Objetivo.

Identificar, analizar, evaluar, documentar y clasificar los riesgos en los procesos, así como generar mapas de riesgos para apoyar la toma de decisiones de la alta Dirección.

Las cinco etapas que componen el modelo de riesgos son:

I. Definición de las categorías de riesgos
II. Identificación de riesgos
III. Documentación del riesgo
IV. Evaluación del riesgo
V. Clasificación de riesgos

3.2.2 Definición de las categorías de riesgos.

En esta etapa se definen las áreas de riesgo, las categorías y subcategorías con las que se van a clasificar los riesgos identificados, a fin de facilitar el análisis de información de manera práctica y tratando de considerar los aspectos de mayor relevancia en la operación del negocio.

Las categorizaciones de los riesgos las podemos identificar de acuerdo a lo siguiente:

Eventos de pérdida	Factores de riesgo	Tipos de pérdida
¿Qué sucedió?	¿Por qué ocurrió?	¿Cuánto costo?
Eventos	Causas	Consecuencias

Eventos de pérdida:

Los eventos de pérdida son los acontecimientos prácticos, llevados a la acción responden a la pregunta, ¿qué sucedió?

Factor de Riesgo:

Es cualquier acontecimiento que constituya en sí mismo una fuente elemental y homogénea (causal) de riesgo operacional. Ejemplo:

Fraude es una categoría de riesgo, las diferentes modalidades de fraude son los factores de riesgo: robo, atraco, falsificación, suplantación de personalidad etc.

Si alguna de estas modalidades fuera desglosada en más variantes homogéneas, seria éstas las que deberían considerarse como factores de riesgo.

Tipos de pérdida:

Son las consecuencias de haber materializado un evento de riesgo, que normalmente tienen un impacto económico cuantificable o no.

3.2.2.1 Ejemplo de clasificación de categorías de riesgos.

Área de riesgo	Categoría de riesgo	Subcategoría de riesgo
Organización	Gobierno y estructura Cultura Comunicación Gestión de proyectos Administración de políticas	
Personal	Selección y contratación Incompetencia Capacitación y desarrollo Conflicto de Intereses Administración de recursos humanos	
Procesos y políticas	Administración de procesos	Diseño Aplicación
	Administración de políticas	Diseño Aplicación
	Gestión	Documentación Supervisión Control
	Fraude	Interno Externo
Sistemas	Arquitectura de sistemas inadecuada Fallos en la implantación de sistemas Fallos de hardware	

	Fallos de Software Fallos en las Comunicaciones y redes Ausencia o deficiencia de planes de continuidad Deficiencias en los sistemas de seguridad	
Prácticas comerciales	Administración Agentes Administración Clientes Política Comercial Prácticas inadecuadas de negocio Productos defectuosos	
Legal	Contingencias fiscales y legales Gestión contratos Legislación aseguradora Gestión legal	
Externos	Eventos de caso fortuito o fuerza mayor Regulación Proveedores Robo o asalto	
	Mercado	Imagen y marca Competencia sector

Definición de las áreas de riesgos.

Organización: Riesgos resultantes de temas tales como cambios en la administración, gestión de proyectos, cultura corporativa y comunicación, responsabilidades, asignación y plantación de la continuidad del negocio.

Personal: Pérdidas asociadas de la falla de empleados, empleadores, de la violación intencional de políticas internas, manejo de conflicto de intereses, incompetencia falta de capacitación y desarrollo.

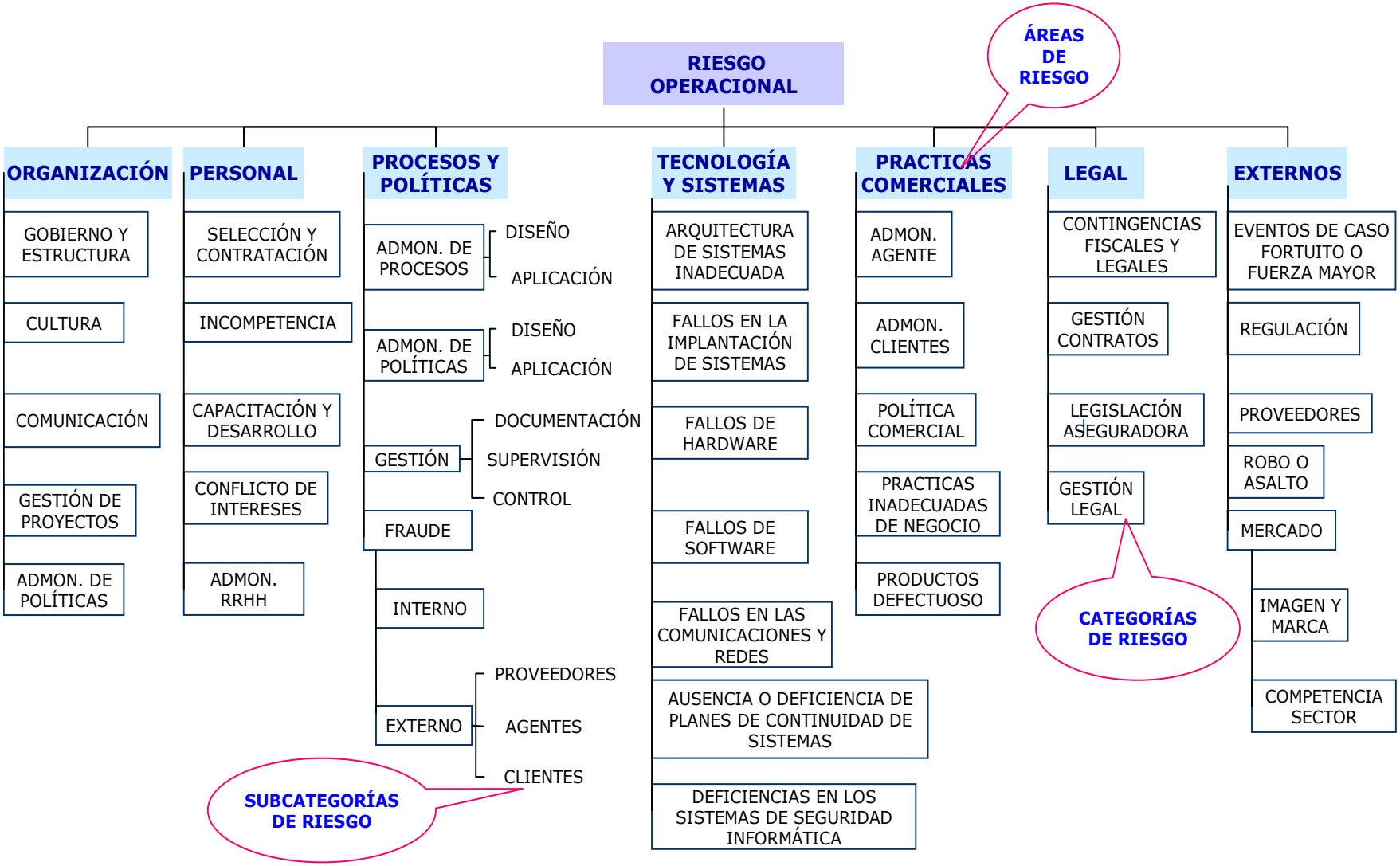
Procesos y políticas: Pérdidas debidas a deficiencias en los procesos actuales, o a la ausencia de estos, así como incumplimiento de políticas internas o de regulación externa, pudiendo ser resultado de error humano o falla en el seguimiento de un proceso existente.

Legal: Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones.

Sistemas: Riesgo ocasionado por deficiencias en el diseño o implantación de sistemas de información, problemas o demoras generados en la ejecución de procesos automáticos concretos, deficiente funcionamiento de los sistemas de procesamiento, de las tecnologías tales como redes o telecomunicaciones, pérdidas de información en los dispositivos de respaldo, o aplicaciones y desarrollos por no responder a las especificaciones del usuario, carencias en la seguridad de los edificios de proceso de datos y en la seguridad de la infraestructura tecnológica.

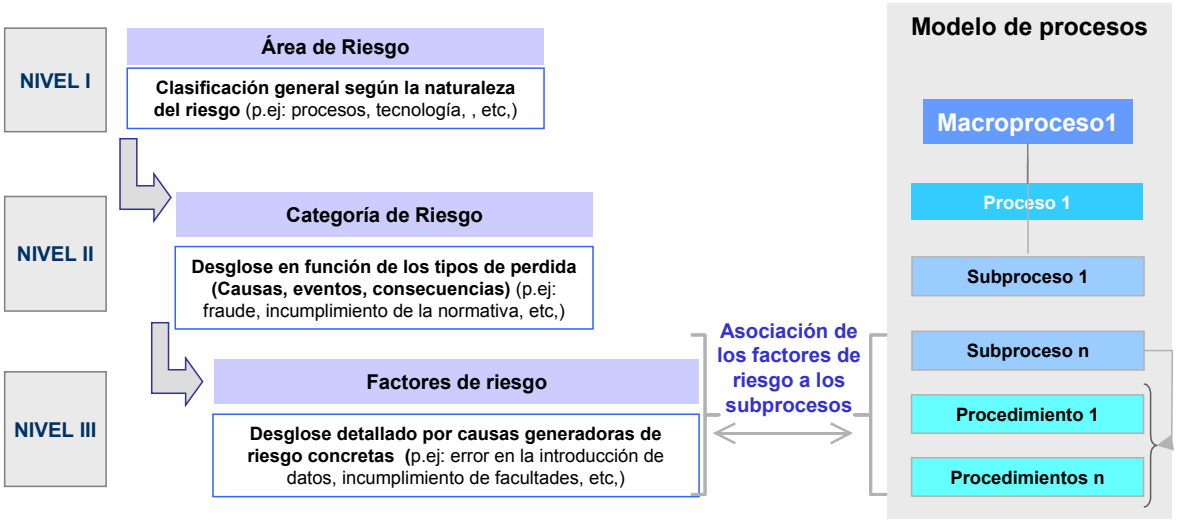
Prácticas comerciales: Riesgos por expectativas frustradas de clientes resultantes de malas prácticas y/o deficiencias en la venta de productos y prestación de servicios (Información facilitada acerca de condiciones económicas, financieras u otros costos, riesgos inherentes a la operación) y multas, sanciones e indemnizaciones como consecuencia de incorrectas prácticas comerciales.

Externos: Pérdidas resultantes de fuerzas naturales o humanas, o de la acción directa de terceros.


RIESGO OPERACIONAL
ÁREAS DE RIESGO
ORGANIZACIÓN
GOBIERNO Y ESTRUCTURA
CULTURA
COMUNICACIÓN
GESTIÓN DE PROYECTOS
ADMON. DE POLÍTICAS
PERSONAL
SELECCIÓN Y CONTRATACIÓN
INCOMPETENCIA
CAPACITACIÓN Y DESARROLLO
CONFLICTO DE INTERESES
ADMON. RRHH
PROCESOS Y POLÍTICAS
ADMON. DE PROCESOS
DISEÑO
APLICACIÓN
ADMON. DE POLÍTICAS
DISEÑO
APLICACIÓN
GESTIÓN
DOCUMENTACIÓN
SUPERVISIÓN
CONTROL
FRAUDE
INTERNO
EXTERNO
PROVEEDORES
AGENTES
CLIENTES
SUBCATEGORÍAS DE RIESGO
TECNOLOGÍA Y SISTEMAS
ARQUITECTURA DE SISTEMAS INADECUADA
FALLOS EN LA IMPLANTACIÓN DE SISTEMAS
FALLOS DE HARDWARE
FALLOS DE SOFTWARE
FALLOS EN LAS COMUNICACIONES Y REDES
AUSENCIA O DEFICIENCIA DE PLANES DE CONTINUIDAD DE SISTEMAS
DEFICIENCIAS EN LOS SISTEMAS DE SEGURIDAD INFORMÁTICA
PRACTICAS COMERCIALES
ADMON. AGENTE
ADMON. CLIENTES
POLÍTICA COMERCIAL
PRACTICAS INADECUADAS DE NEGOCIO
PRODUCTOS DEFECTUOSO
LEGAL
CONTINGENCIAS FISCALES Y LEGALES
GESTIÓN CONTRATOS
LEGISLACIÓN ASEGURADORA
GESTIÓN LEGAL
CATEGORÍAS DE RIESGO
EXTERNOS
EVENTOS DE CASO FORTUITO O FUERZA MAYOR
REGULACIÓN
PROVEEDORES
ROBO O ASALTO
MERCADO
IMAGEN Y MARCA
COMPETENCIA SECTOR

3.2.2.2 Asociación de los factores de riesgo a los procesos.

Se ha identificado y clasificado las áreas de riesgo y un listado de tipos de pérdidas que pueden influir directa o indirectamente en los procesos, los cuales se han asociado a la operación descrita en la etapa anterior.



3.2.3 Identificación de riesgos

No existe forma única para la identificación de riesgos, sin embargo resulta muy útil hacer un análisis retrospectivo y prospectivo.

Eventos ocurridos en el pasado (análisis retrospectivo)

- ❖Análisis de información estadística.
- ❖Observaciones
- ❖Quejas, Inconformidades.
- ❖Denuncias
- ❖Revisiones de Control.
- ❖Otros hechos irregulares.
- ❖Otras fuentes.

Los siguientes cuestionamientos pueden ayudar a su identificación.

- ¿Qué sucedió?
- ¿Qué originó el evento?
- ¿Cuánto costo o cual fue el impacto o la consecuencia?

Eventos que puden suceder (análisis prospectivo)

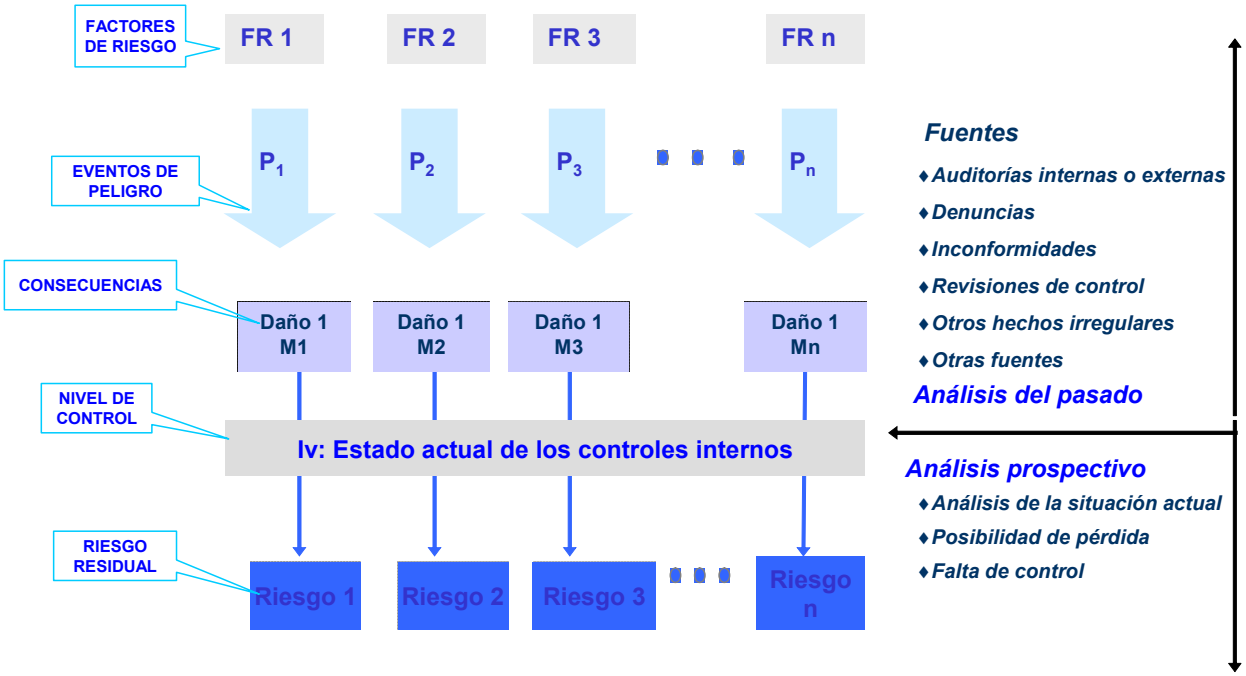
- ❖ Este análisis básicamente se sustenta en el conocimiento y visión de los responsables del proceso, analizando e identificando los posibles riesgos y faltas de control interno que puedan llevar a la materialización del riesgo.

De acuerdo a la situación actual se formulan los siguientes cuestionamientos para identificar los posibles riesgos.

- ¿Existe algún problema en mi proceso actual?

- ¿Falta definir algún procedimiento, política, implantar algún control, capacitar al personal, o alguna otra variable que afecte el desarrollo del proceso?
- ¿De no definir e implementar el control que sucedería?

3.2.3.1 Esquema para la identificación de riesgos.



3.2.4 Documentación de riesgos.

Partimos de la clasificación de los procesos por nivel de relevancia, considerando que las actividades periódicas, así como las que implican juicios subjetivos, tienen mayor riesgo y requieren un análisis más detallado.

Este formato muestra todos los elementos que debe contener la documentación de los riesgos.

ENTIDAD ----------		ÁREA DE RIESGO ----------	
SECTOR ----------		CATEGORÍA DE RIESGO ----------	
MACRO PROCESO ----------		SUBCATEGORÍA DE RIESGO ----------	
PROCESO ----------		ÁREAS/DPT AFECTADOS ----------	
SUBPROCESO ----------			

	EVENTOS	CAUSAS	CONSECUENCIAS
Subproceso	Evento de pérdida	factor de riesgo	Consecuencia o Impacto
	¿Qué sucedió? ¿Qué podría suceder?	¿Por qué ocurrió? ¿Por qué podría ocurrir?	¿Cuánto impacto? ¿Cuánto podría impactar?

A continuación se describen los elementos que se muestran en le formato de documentación.

Entidad*:* Se identifican las distintas unidades de negocio (Oficinas y Sucursales) que realizan las actividades de la institución para el logro de sus objetivos.

Sector*:* Se define el sector, a través de las segmentaciones que se realizan en una entidad en función de diferencias significativas en la gestión de cada uno de los procesos de negocio definidos, puede ser por tipo de operación, por ramo o por proceso, lo que implica que los riesgos detectados en cada uno de los sectores puedan tener una importancia y probabilidad de ocurrencia diferentes entre sí. El sector es la clasificación de las actividades de la Institución.

Macro procesos: Es la agrupación lógica de procesos, que se realiza en base a distintos criterios (responsabilidades, afinidad funcional...)

Procesos: Flujo de transacciones de información básicos, relevantes y diferenciados para la gestión de la entidad aseguradora susceptible de análisis.

Subprocesos: Desglose de un proceso de negocio que facilita su análisis y la gestión del riesgo.

Áreas de riesgo: Agrupación de tipos de riesgos relacionados entre ellos, para una simplificación en la muestra de resultados.

Categoría de riesgo*:* Es el desglose por área de riesgo de los tipos de pérdida clasificados de manera homogénea, para facilitar su análisis y la generación de mapas de riesgo.

Factor de riesgo: Es cualquier acontecimiento que constituya en sí mismo una fuente elemental y homogénea (causal) de riesgo operacional.

3.2.4.1 Ejemplo de documentación de riesgos análisis retrospectivo

ENTIDAD	**Matriz**	**ÁREA DE RIESGO**	**Procesos y Políticas**
SECTOR	**Autos**	**CATEGORÍA DE RIESGO**	**Fraude**
MACRO PROCESO	**Siniestros**	**SUBCATEGORÍA DE RIESGO**	**Externo**
PROCESO	**Atención a clientes**	**ÁREAS/DPT AFECTADOS**	**Siniestros, P. Totales**
SUBPROCESO	**Pago y liquidación**		

	EVENTOS ¿Qué sucedió?	**CAUSAS** ¿Por qué ocurrió?	**CONSECUENCIAS** ¿Cuánto impacto?
Procedimiento	**Evento de pérdida**	**factor de riesgo**	**Consecuencia o Impacto**
Indemnización de siniestros autos, pérdidas totales por robo.	Asegurar una unidad automotriz inexistente para cometer fraude, declarándola extraviada por robo. Presentación de documentación de propiedad falsa.	Por falta de capacitación el personal de siniestros no detectó la documentación falsa y tampoco solicitó una investigación sobre la misma. El agente de seguros no realizó la inspección física de la unidad asegurada.	La Compañía sufrió una pérdida de $300 mil por pagar una indemnización improcedente y totalmente fraudolenta.

3.2.5 Evaluación de riesgos

3.2.5.1 Factores a valorar.

La evaluación de un riesgo se realiza tomando en consideración lo siguiente:

- ***Impacto o magnitud***

¿Qué efecto económico tendría si se realiza el riesgo?

Se le denomina también severidad y es la medida correspondiente al grado de gravedad económica que puede representar la realización del riesgo.

Los valores que se utilizan para su evaluación son: Alto (4), Medio (2), Bajo (1)

- ***Probabilidad***

¿Qué posibilidad existe de que aparezca el riesgo?

Posibilidad de que un determinado riesgo pueda ocurrir o suceder durante el desarrollo de la ejecución de la operación.

Los valores que se utilizan para su evaluación son: Alto (3), Medio (2), Bajo (1)

- ***Nivel de control***

¿Qué tan efectivos son los controles implantados en el proceso para controlar el riesgo?

Valoración de la calidad y eficiencia de los controles implantados en el proceso para la disminución del riesgo.

Los valores que se utilizan para su evaluación son: Excelente (0.1), Bueno (0.2), Regular (0.5), Malo (0.8), Deficientes (1)

Definición conceptual del nivel de control

- *Excelente:* Su diseño se encuentra bien definido, se aplican al pie de la letra y evitan prácticamente la incidencia del peligro analizado.
- *Bueno:* Su diseño y aplicación es adecuado, pero generalmente necesitarán actuar conjuntamente con otros controles para mitigar el riesgo, además de que pueden tener mejoras.
- *Regular:* Son medianamente adecuados y requieren una revisión más detallada para implementar mejoras para su diseño y aplicación.
- *Malo:* Existen pero son muy deficientes y requieren una renovación exhaustiva.
- *Deficientes:* Son inexistentes o hay pocos controles internos y son inadecuados.

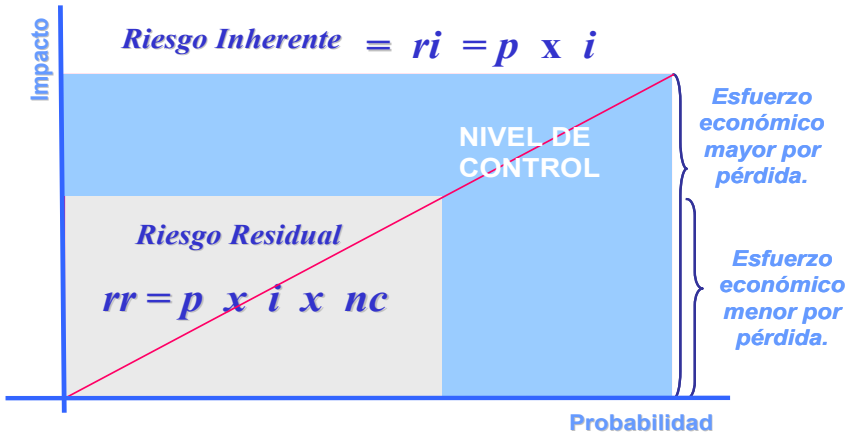
3.2.5.2 Valoración del riesgo operacional.

Los riesgos operacionales se evaluaran con dos enfoques, considerando su riesgo inherente y residual del proceso, los cuales a continuación se definen:

Riesgo Inherente: Representa el riesgo natural en que incurre la unidad de negocios por el simple hecho de llevar a cabo las operaciones, considera la posibilidad de que puedan ocurrir errores importantes en el proceso de las operaciones que impacten a los resultados.

La probabilidad de que ocurran errores importantes es mayor cuando la función está sujeta a un mayor grado de juicio gerencial.

Riesgo Residual: Es el riesgo sobrante después de haber aplicado controles al proceso, aunque los controles sean muy eficientes y el riesgo se considere mitigado, normalmente existe un riesgo residual.



Matemáticamente se define al **riesgo inherente** como: $r_i : p \ x \ i$

Donde:

r_i = Riesgo inherente

p = probabilidad de ocurrencia del peligro

i = Impacto ó severidad económica

y al **riesgo residual**: $r_r : p \ x \ i \ x \ n_c$

Donde:

r_r = Riesgo residual

n_c = Nivel de control

3.2.5.3 Criterios para evaluar el nivel de impacto.

Para analizar el nivel impacto en el proceso es necesario considerar los siguientes puntos:

- El impacto individual y global de acuerdo con el volumen de operaciones.
- Impacto consecuencial en otros procesos.

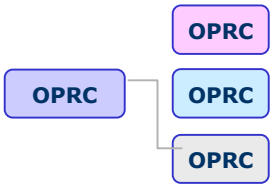
Operación independiente entre sí.

La operación puede tener un impacto económico global muy elevado por su volumen de operaciones, sin embargo, al ser independiente una operación de otra su importe individual no es significativo y si la probabilidad de que se generalice el error a toda la operación es baja, su impacto económico generalizado resulta ser no significativo.

OPRC 1 OPRC 2 OPRC 3 OPRC n

Operación no independiente entre sí.

Independientemente del impacto individual de la operación, es importante analizar si el proceso incide directamente o puede llegar afectar otras operaciones, en estos casos la posibilidad de que el riesgo sea extensible es elevada y por consecuencia el impacto económico lo será, dependiendo del volumen de procesos que afecte y del impacto que estos representen.

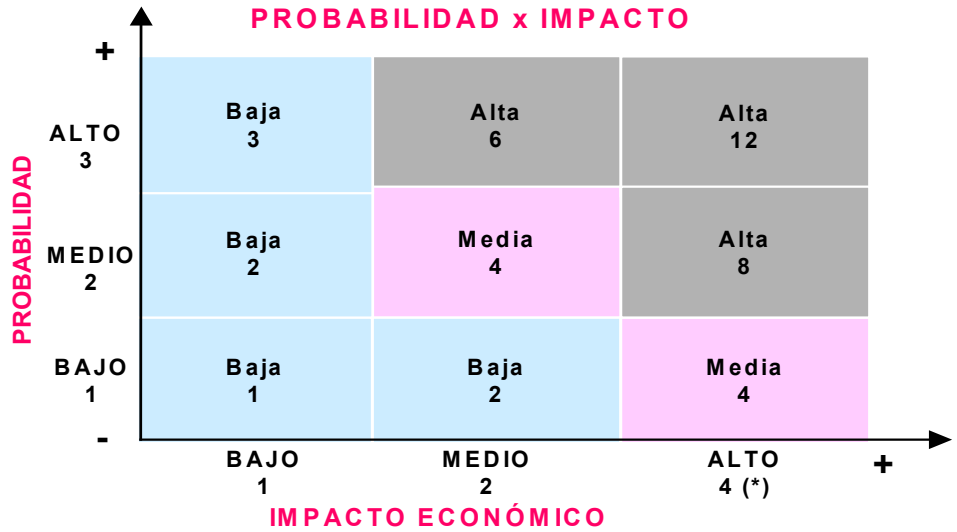


3.2.6 Clasificación de riesgos.

Todos los riesgos tienen impacto directo o indirecto en los procesos de la Organización, sin embargo no todos tienen la misma relevancia, es importante focalizar los esfuerzos en aquellas operaciones que tienen mayores riesgos inherentes y limitar el alcance del trabajo sobre los procesos relevantes en los que se realizará la identificación, documentación y pruebas de controles.

3.2.6.1 Interpretación de la evaluación del riesgo inherente.

No todos los riesgos identificados tienen la misma relevancia, por lo que para poder realizar su clasificación se evaluará su riesgo inherente.

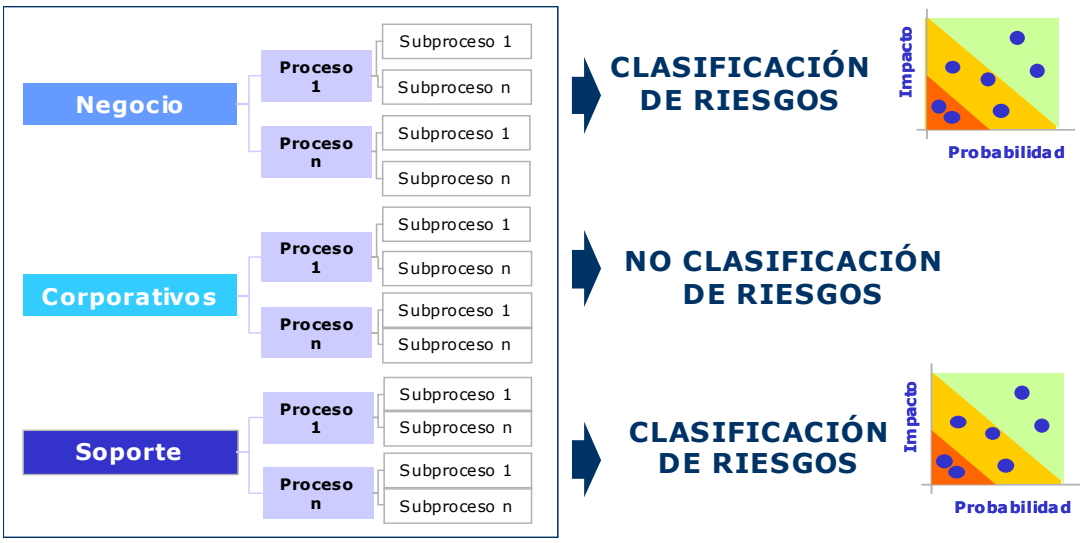


Se ha definido con Efecto Alto, exclusivamente, aquellos riesgos asociados a procesos que tengan un alto impacto económico (El impacto económico es la variable con mayor peso).

Los riesgos clasificados como alto y medio impacto, se documentarán y evaluarán sus controles asociados.

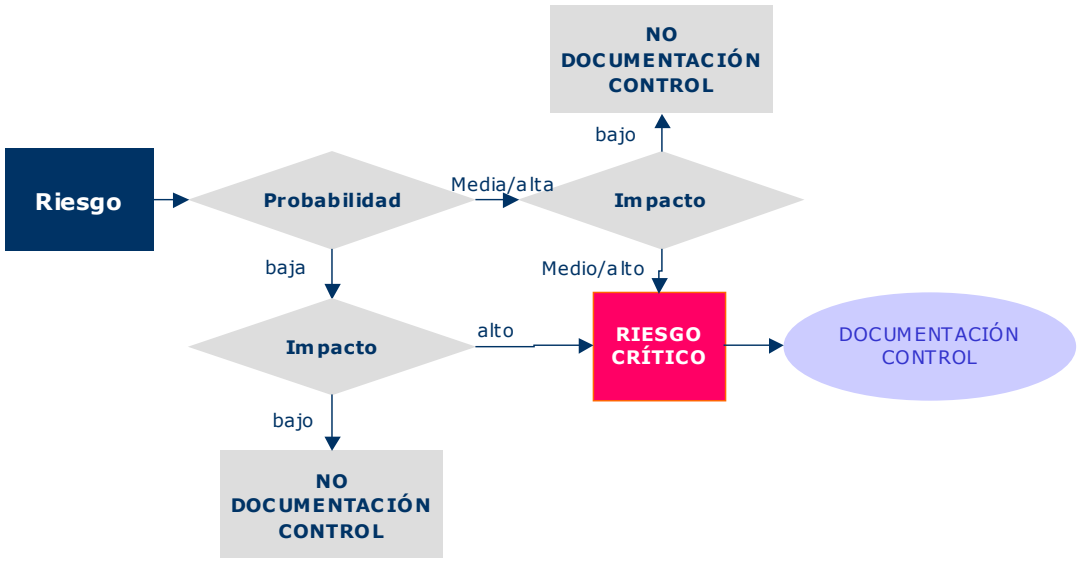
3.2.6.2 Criterios de evaluación

En los procesos corporativos no se clasifica el riesgo, para el tratamiento de estos se da mayor relevancia y un mayor alcance de las pruebas a realizar.



Es muy importante identificar y cerciorarse que no exista ningún riesgo que pudiese tener relevancia y que no haya sido seleccionado. Las Direcciones deberán validar si por razones o circunstancias particulares del área pueden existir riesgos críticos adicionales que haya que incluir.

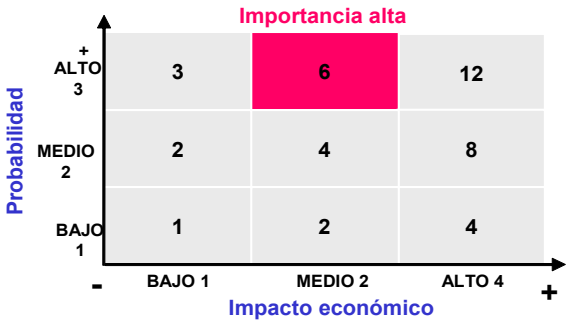
3.2.6.3 Esquema metodológico de clasificación del riesgo.



3.2.6.4 Ejemplo de evaluación del riesgo.

Entidad	**Oficina Matriz**	**Área de riesgo**	**Procesos y Políticas**
Sector	**Autos**	**Categoría de riesgo**	**Fraude**
Macro proceso	**Siniestros**	**Subcategoría de riesgo**	**Externo**
Proceso	**Indemnizaciones**	**Áreas/dpt afectados**	**Siniestros, P. Totales**
Subproceso	**Pérdida total por robo**		

Evento de pérdida	Factor de riesgo	Consecuencia o Impacto	Probabilidad	Impacto	Nivel de Control	RI	RR
Pagar una indemnización improcedente y fraudolenta. Falsificación de documentos.	Falta de definición de procedimiento y falta de capacitación al personal que ejerce la función.	La Compañía sufrió 11 fraudes por la suma total de $3,500 miles durante el año de 2005.	Medio	Alto	Regular	Alto	Alto



4.-Modelo de controles.

4.1 Antecedentes y definiciones

4.1.1 Definición de control interno.

Proceso efectuado por el consejo de administración, la dirección y demás personal en una entidad, diseñado para facilitar una seguridad razonable respecto a la consecución de objetivos en las siguientes categorías:

Operativos	• Efectividad y eficiencia en las operaciones.
Normativos	• Cumplimiento de leyes y regulaciones aplicables.
Reporte financiero	• Confiabilidad de los reportes financieros.

4.1.2 Evolución de los modelos de control interno.

Los modelos de control interno no han seguido siempre el mismo esquema, sino que han ido evolucionando con el paso del tiempo, especialmente en los últimos años.

A nivel internacional, el entorno regulatorio está acelerando la evolución hacia modelos avanzados de control interno.

Evolución de los modelos de control interno

	Nivel básico	Nivel intermedio	Nivel avanzado
Conocimiento	▪ Los controles, políticas y procedimientos no están claramente identificados.	▪ Los controles, políticas y procedimientos están identificados pero no están documentados.	▪ Los controles, políticas y procedimientos están documentados, permitiendo identificar oportunidades de mejora de forma continua.
Responsabilidad	▪ La organización desconoce con claridad sus responsabilidades en materia de control.	▪ La organización es consciente de sus responsabilidades en materia de control.	▪ La responsabilidad del control interno está asignada de forma explícita, distribuyéndose “en cadena” y comprometiendo a toda la organización.
Supervisión	▪ La evaluación de la efectividad de los controles se restringe a la labor de Auditoría Interna.	▪ Algunas áreas de negocio y soporte evalúan sus controles internos.	▪ Todas las áreas de negocio y soporte evalúan sus controles internos coordinadas por unidades corporativas especialistas.
Estructura y organización	▪ No existen unidades especializadas en la gestión de riesgos y de coordinación del control interno.	▪ Existen unidades de gestión de riesgos corporativas.	▪ Existen unidades con visión global del riesgo y del control interno, así como Órganos de Gobierno orientados al control.

4.2 Descripción del modelo de controles.

4.2.1 Objetivo

El presente modelo valida dos aspectos el diseño y funcionamiento de controles, a través de su identificación, documentación y realización de pruebas.

Las cuatro etapas que componen el modelo de controles son las siguientes:

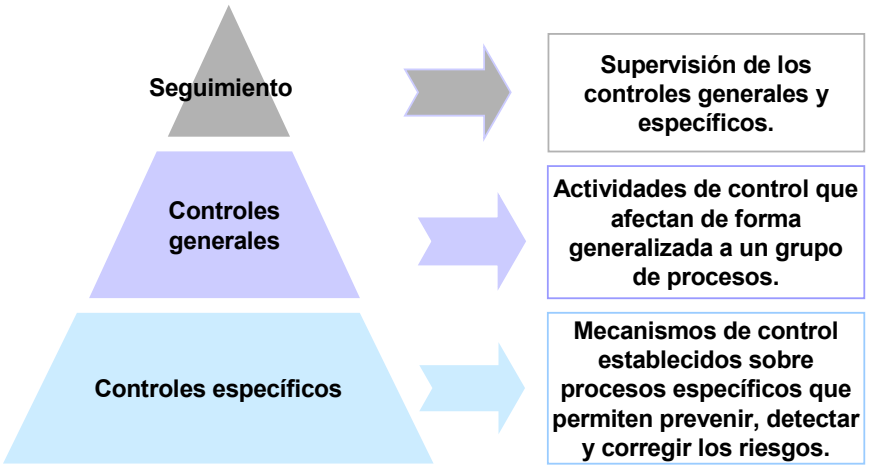
I. Estructura de controles
II. Identificación de controles
III. Documentación de controles
IV. Evaluación de controles

4.2.2 Estructura de controles.

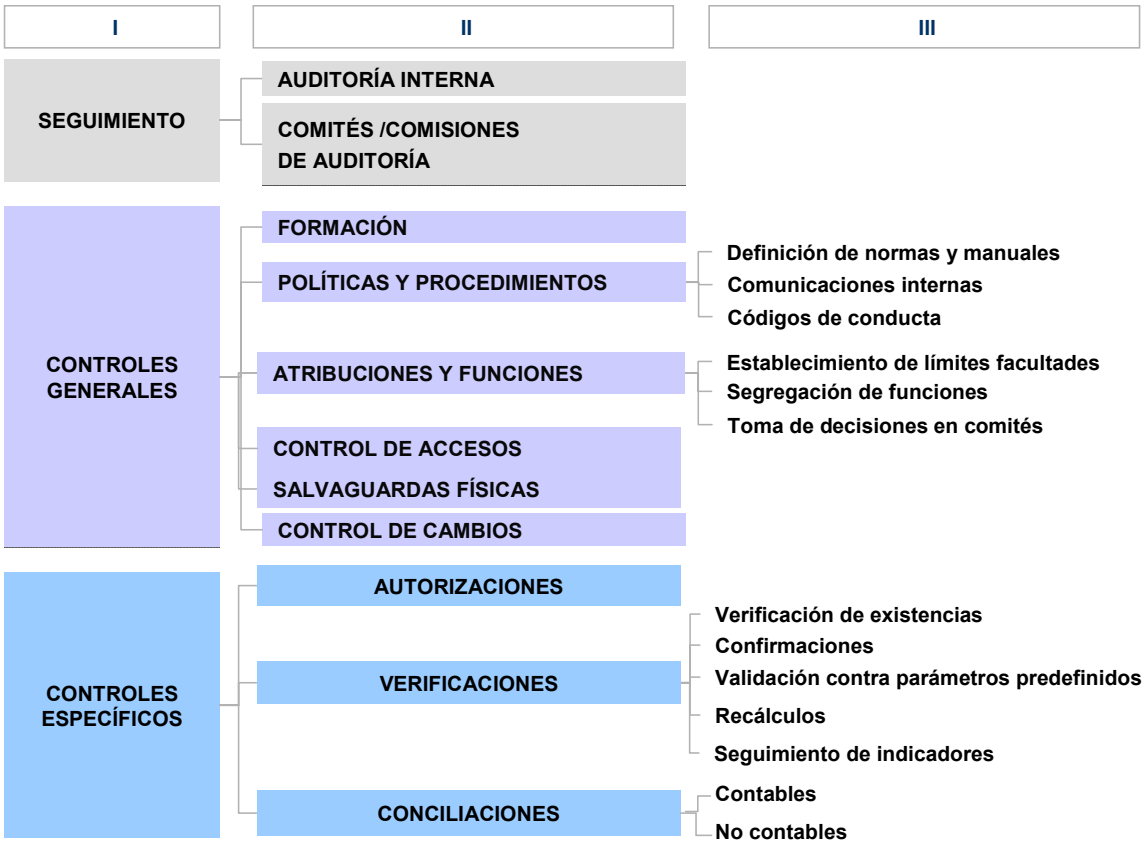
La definición de la siguiente estructura de controles permitirá facilitar la identificación y documentación de actividades de control y homogeneizar el tratamiento de tareas similares en sucursales u oficinas distintas.

Definición de Control

Cualquier actividad, tarea o procedimiento que permite gestionar, reducir y/o mitigar el riesgo al cual está expuesta la entidad.



En el siguiente esquema podemos observar el desglose de los controles de seguimiento, generales y específicos, con los que se va a analizar el proceso.



4.2.2.1 Definición de los tipos de control.

1.- CONTROLES DE SEGUIMIENTO

1.1 Auditoría Interna.

Definición: Análisis independiente dentro de la organización para examinar y evaluar sus actividades y procedimientos de control realizando un servicio de apoyo a la organización. Se suele realizar, ya sea obteniendo evidencia directa de la operación de los controles de riesgos específicos o probando los resultados del proceso de control.

Tipología: Suelen ser controles detectivos, normalmente de baja frecuencia. Encaminados a identificar errores una vez que se han producido.

Ejemplo: Revisiones por Auditoría Interna de los expedientes de siniestros atendidos y pagados por la red de sucursales, para verificar que contienen todos los requerimientos mínimos definidos por la normativa interna y los organismos reguladores.

1.2 Comités/Comisiones

Definición: Supervisión y verificación del grado de aplicación y cumplimiento de políticas, procedimientos, normativas contables, legales, interna/externa...

Se caracterizan por estar formados por más de 1 miembro y por tomar decisiones de forma conjunta, con lo que se reduce el riesgo y los potenciales errores de las decisiones tomadas por una única persona.

Deben de tener la autoridad suficiente para poder detectar las incidencias identificadas.

Tipología: Suelen ser controles detectivos, normalmente de baja frecuencia. Encaminados a identificar errores una vez que se han producido.

Ejemplo: Comité de Auditoría, Comité de Riesgos y en general Comités con carácter de supervisión.

2.- CONTROLES GENERALES

2.1 Formación

Definición: Diseño, comunicación e impartición de actividades formativas o de entrenamiento, encaminadas a que el personal cuente con los conocimientos y habilidades necesarias para la realización de las actividades inherentes a su puesto de trabajo. De esta forma mediante la capacitación y el adiestramiento, los riesgos inherentes, principalmente operativos, se verán reducidos.

Tipología: Suelen ser controles preventivos de baja frecuencia.

Ejemplo: Curso de suscripción, cursos para evaluación y ajustes de siniestros, cursos de paquetería Excel, Word, Power Point...

2.2 Políticas y procedimientos

2.2.1 Definición de normas y manuales.

Definición: Preparación, elaboración y publicación de documentación estándar con los procedimientos y operación desarrollada por la compañía.

Con este tipo de controles se pretende reducir las interpretaciones subjetivas del personal que interviene en las mismas, homogeneizando el comportamiento de los empleados y por tanto evitando irregularidades que podían haber pasado por alto.

Tipología: Suelen ser controles preventivos.

Ejemplo: En la atención y pago de reclamaciones por siniestros del ramo de automóviles, el personal de siniestros debe proceder hacer la validación administrativa de la reclamación, consultando para el efecto la vigencia de las pólizas de seguros, coberturas contratadas, datos del vehículo y el estatus de la cobranza de las pólizas.

2.2 Políticas y procedimientos

2.2.2 Comunicaciones internas

Definición: Implica el establecimiento de líneas de comunicación claras en las que se fijen fechas de comunicaciones y responsables, garantizando la recepción de información en los plazos adecuados.

Se pretende reducir las posibles interpretaciones subjetivas del personal que interviene en las mismas.

Tipología: Suelen ser controles preventivos.

Ejemplo: Cada vez que existe una modificación de tarifas, el área técnica avisa de las modificaciones efectuadas, realizando una publicación en Intranet y mandando un e-mail informativo a cada uno de los empleados relacionados con la suscripción de negocios.

2.2 Políticas y procedimientos

2.2.3 Códigos de conducta

Definición: Actividad que define y desarrolla los fundamentos de comportamiento ético que han de aplicarse a los negocios y actividades que desarrolla la compañía, y las pautas de actuación que han de ejercer los empleados.

Permite reducir los riesgos, principalmente de fraude de los empleados mediante la concientización corporativa y la creación y mantenimiento de una cultura interna.

Tipología: Suelen ser controles preventivos.

Ejemplos: Código de conducta en el que se establecen los valores a seguir por parte del personal, y definido por la Dirección General y comunicado o distribuido a través de la Intranet.

2.3 Atribuciones y funciones

2.3.1 Establecimiento de límites-facultades

Definición: Fijación y asignación de perfiles, importes y funciones, claramente definidos, que permitan determinar las distintas líneas de aprobación y supervisión a lo largo de un proceso, de forma que se garantice la revisión interna de todas las actividades realizadas.

La asignación de perfiles de responsabilidad a distintas áreas dentro de un mismo proceso, facilita la detección de posibles errores y su resolución a lo largo de la sucesión de las distintas actividades.

Tipología: Suelen se controles preventivos.

Ejemplos: La Dirección de la compañía XZY, ha definido un procedimiento por el cual se establecen los niveles de aprobación de la compra-venta de inversiones realizadas por la compañía en función de la cuantía de los importes comprometidos.

Las inversiones inferiores a $250,000 serán aprobadas por el responsable del área Tesorería. Para aquellas que se encuentren entre $250.000 y $500.000 se requerirá también la firma del Director Financiero y para las que sobrepasen la cantidad de $500.000, el Director General deberá dar su aprobación.

2.3 Atribuciones y funciones

2.3.2 Segregación de funciones

Definición: Fijación y asignación de perfiles, funciones y puestos entre diferentes áreas/departamentos, separando normalmente, la toma de la decisión de la ejecución de la actividad.

Tipología: Suelen ser controles preventivos.

Ejemplos: La compañía XZY decide que en el proceso de cuentas por pagar, las aprobaciones de facturas recibidas, y las aprobaciones de pagos sean realizadas por distintas áreas. El responsable de las aprobaciones de facturas recibidas pertenece al Área de Administración y Finanzas el que aprobará las órdenes de pago a proveedores será un responsable del Área de Tesorería.

2.3 Atribuciones y funciones

2.3.3 Otros Comités

Definición: Órganos caracterizados por tomar las decisiones de forma conjunta que permiten reducir y minimizar el riesgo de decisiones erróneas o tomadas sin facultades de forma fraudulenta.

La principal diferencia con las comisiones es el carácter preventivo que tiene estos riesgos.

Tipología: Suelen ser controles preventivos.

Ejemplos: Comité de Compras, Comité de Nuevos Productos, Comité de riesgos.

2.4 Control de accesos

Definición: Restricción de accesos (a sistemas, archivos, información, almacenes, etc.) a personal que no esté autorizado según los diferentes niveles identificados, minimizando el impacto de errores producidos por registros no autorizados o manipulación de información almacenada. Por la naturaleza de la restricción, el control de accesos puede ser de dos tipos:

- Control de acceso a sistemas, con claves de entrada o passwords, accesos de sólo lectura.
- Control de acceso a archivos u otras instalaciones protegidas de la compañía.

Tipología: Suelen ser controles preventivos.

Ejemplos: Solo el personal del Área de Recursos Humanos del departamento de nómina de la Compañía XZY, tienen perfiles de acceso al Sistema de Gestión de Recursos Humanos para modificar las cantidades registradas como retribuciones de los empleados.

2.5 Salvaguardas físicas

Definición: Actividades de control encaminadas a la protección física de activos tangibles, propiedad intelectual e información de gestión / financiera de la compañía, de su destrucción accidental o intencionada, robo, pérdida o acceso no autorizado.

Tipología: Suelen ser controles preventivos / detectivos.

Ejemplos: Para activos tangibles estas actividades de control pueden corresponder al aseguramiento de los mismos. Para activos intangibles o financieros las actividades de control que minimizarían el impacto de una pérdida de valor, serían por ejemplo, la contratación de coberturas cambiarias.

2.6 Control de cambios

Definición: Actividades que tratan de prevenir o detectar si se realizan cambios no autorizados en actividades críticas del proceso, personal o información y sistemas de información clave.

Tipología: Suelen ser controles preventivos / detectivos.

Ejemplos: Los cambios deben hacerse acordes a lo establecido en los manuales y sólo por parte del personal autorizado.

3.- CONTROLES ESPECÍFICOS

3.1 Autorizaciones

Definición: Aprobación de operaciones, resultados, informes, tareas, etc. tanto automática, como manual, asegurándose que los individuos apropiados aprueban las transacciones realizadas conforme a los criterios de la gerencia.

Tipología: Suelen ser controles preventivos / detectivos.

Ejemplos: El responsable de compras de la compañía XZY, debe aprobar todas las facturas recibidas con anterioridad a su registro para posterior pago.

3.2 Verificaciones

3.2.1 Verificación de existencias

Definición: Consiste en la identificación de errores en activos registrados a partir de la observación física. Las actividades de control más significativas serían:

Inventarios de existencias en los que además de realizar una comprobación visual de la presencia de las referencias registradas, se verifica que las mismas no presenten problemas de obsolescencia o deterioro.

Arqueos de caja.

Tipología: Suelen ser controles detectivos.

Ejemplos: En la compañía XZY el personal de las áreas técnicas realizan inventarios de las pólizas perfoliadas, no sólo para corroborar el registro contable de la prima y su cobranza sino también para detectar posibles disposiciones de primas. El procedimiento de verificación en este caso consiste en determinar el estatus de cada una de las pólizas perfoliadas emitidas.

3.2 Verificaciones

3.2.2 Confirmaciones

Definición: Verificación sobre la veracidad de determinados datos básicos, es decir, se trata de actividades de control encaminadas a contrastar los registros en distintos sistemas con la documentación soporte que los originó.

Estarían incluidos dentro de estos controles también las verificaciones de entradas de datos y cualquier tipo de comparación de datos.

Tipología: Suelen ser controles preventivos / detectivos.

Ejemplos: En el proceso de otorgamiento de préstamos hipotecarios, antes de proceder a su autorización, se requiere al empleado la documentación de carácter personal necesaria y se procede a verificar que tiene capacidad de pago.

3.2 Verificaciones

3.2.3 Validación contra parámetros definidos

Definición: Verificación de los datos introducidos y los cambios y conversión / procesamiento de los resultados contra parámetros establecidos para asegurar la exactitud y evitar que continúen las actividades del proceso y comunicar las excepciones.

Estarían incluidos los chequeos de datos (datos faltantes, comprobaciones de campo, auto-comprobación de dígitos, combinaciones no válidas,...)

Tipología: suelen ser controles preventivos.

Ejemplos: En la compañía XZY el formulario de alta de un nuevo asegurado, el sistema valida que todos los datos incluidos en el campo para el documento de identidad, se correspondan realmente con el algoritmo que presenta un documento de identidad, asimismo, el sistema también verifica que no existe ningún campo vacío o en blanco que falte por cumplimentar.

3.2 Verificaciones

3.2.4 Recálculo

Definición: Validación de la exactitud del procesamiento recalculando y replicando independiente las operaciones o transacciones afectadas, para contrastar normalmente cálculos realizados por medios automáticos.

Tipología: Suelen ser controles detectivos.

Ejemplos: En la compañía XZY el área de Administración vuelve a realizar el cálculo del Impuesto sobre la renta realizado previamente por el Área Fiscal para verificar, dada la trascendencia y materialidad del importe, que no existen errores en el proceso de cálculo del impuesto.

3.2 Verificaciones

3.2.5 Seguimiento de indicadores clave

Definición: Seguimiento de la evolución de índices, datos, ratios, etc. que permitan analizar y poder concluir sobre el correcto desarrollo del proceso.

Tipología: Suelen ser controles detectivos.

Ejemplos: En la compañía XZY realiza un seguimiento semanal de la evolución del número de reclamaciones y quejas interpuestas por clientes, para determinar, en el caso de que el número de éstas aumenten, acciones que determinen la causa del incremento de insatisfacción de clientes.

3.3 Conciliaciones

Definición: Comparación de información de dos fuentes distintas, para la que se identifican las diferencias, se obtiene una justificación y se analiza, de modo que en el caso de que se detecten

errores en alguna de las fuentes, se toman las medidas oportunas (registros contables, modificación de proceso, etc.) para su resolución.

Pueden ser conciliaciones contables o no contables.

Tipología: Suelen ser controles detectivos.

Ejemplos: En la compañía XZY el Área de Contabilidad realiza mensualmente las conciliaciones de las cuentas bancarias que tiene, comparando el saldo registrado en las cuentas de bancos del activo de la Compañía, con los saldos reportados por las Entidades Bancarias.

En este cuadro se muestra un resumen de las características de los tipos de controles.

Clases de Controles	Preventivos	Detectivos o Correctivos	Automáticos	Manuales
Auditoría interna		X		X
Comités / Comisiones		X		X
Formación	X			X
Definición de normas y manuales	X			X
Comunicaciones internas	X			X
Códigos de conducta				X
Establecimiento de límites-facultades	X			X
Segregación de funciones.	X			X
Otros Comités	X			X
Control de accesos	X		X	X
Salvaguardas físicas	X	X	X	X
Control de cambios	X	X	X	X
Autorizaciones	X	X		X
Verificación de existencias		X		X
Confirmaciones	X	X	X	X
Validación contra parámetros definidos	X		X	X
Recálculo		X	X	X
Seguimiento de indicadores clave		X		X
Conciliaciones		X	X	X

4.2.3 Identificación de controles.

Los controles están integrados dentro de la operación y procesos diarios desarrollados por la entidad, por lo que algunas veces no es sencillo poder separar los controles de la operación, puesto que tienden a verse como parte de ésta, es importante abstraerse de la operación y poder

pensar de forma global para poder reconocer los controles de la entidad así como hacer una labor exhaustiva de rastreo e identificación de controles.

- Identificar todas las actividades de control existentes para mitigar los riesgos críticos dentro de la organización.

- Es posible que algunas de las actividades de control o riesgos a gestionar, no sean responsabilidad del propietario del proceso y se desarrollen en otras unidades distintas, por lo tanto la labor del propietario del proceso será identificar la actividad de control y luego que el área/departamento encargado sea el que la documente.

¿Qué preguntas deberán plantearse para la identificación de controles?

No existe una fórmula única para la identificación de controles, pero será de ayuda preguntarse lo siguiente:

- ¿Qué medidas pueden ser adoptadas para la mitigación del riesgo?

- ¿Qué actividades podrían haber impedido que ocurriese el riesgo?

- ¿Cuáles son las causas de origen del riesgo?

Cuanto mejor definido esté el riesgo, más fácil será entender cuáles son los controles que contribuyen a su mitigación.

Generalmente todos los riesgos se encuentran ubicados a nivel de subproceso, en consecuencia todos los controles se situarán también en este nivel, puesto que es donde deben de actuar para mitigar el riesgo.

¿Cuántos controles hay que identificar y documentar?

Todos los controles existentes para mitigar los riesgos críticos. Normalmente cada riesgo, estará sujeto a más de un control, que podría ser combinación de controles preventivos y detectivos.

Se debe tener en cuenta que el número de controles puede afectar a la evaluación, si existen demasiados puede ser señal de que:

- El riesgo no ha sido bien definido.

- Seguramente, habrá controles que se pueden eliminar.

- Pueden aportar más ineficiencias y es indicador de que pueden haber debilidades de control.

Controles insuficientes:

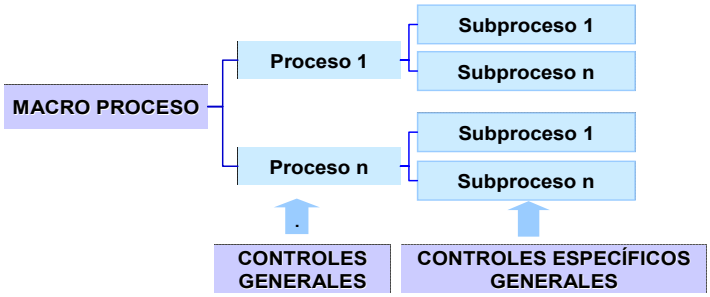
- Seguramente, será necesario implementar más controles.

- Si han sido identificados todos los controles, se deberá evaluar si existen otros tipos de medidas de control para asegurar la mitigación del riesgo.

4.2.4. Documentación de controles.

Una vez identificados y conocidos todos los controles que resultan de aplicación para mitigar el riesgo crítico, se procederá a su documentación.

Para los controles generales, será recomendable el documentarlo a nivel de proceso.



Este cuadro muestra el objetivo de cada uno de los requisitos de documentación de controles:

Descripción de la actividad del control	❖ Permite comprender en qué medida la actividad de control mitiga el riesgo al cual está asociado.
Tipología de control	❖ Determina si existe un adecuado equilibrio de controles preventivos y detectivos para mitigar los riesgos.
Grado de automatización	❖ Delimita el alcance de las pruebas de testing para verificar el funcionamiento del control, puesto que el alcance de las pruebas varía en función de la automatización del mismo (Automático o manual).
Clase de control	❖ Cataloga el control dentro del modelo de control.
Frecuencia del control	❖ Delimita el alcance de las pruebas de testing para verificar el funcionamiento del control, puesto que el alcance de pruebas varía en función de la frecuencia del control.
Responsable	❖ Es un factor a considerar para evaluar la eficacia del control.
Evidencia generada	❖ Verifica la aplicación de los controles es un requerimiento necesario para poder efectuar las pruebas de control.

4.2.4.1 Definición de los requisitos de documentación.

Descripción de la actividad del control

Explicación detallada de en que consiste la actividad de control, debe ser lo suficientemente exhaustiva para que pueda responder a las siguientes cuestiones:

- ¿En qué consiste el control?

  Descripción y detalle del contenido y en qué consiste la actividad de control por parte del responsable de la misma y como se realiza cuando el responsable no está presente.

- ¿Cuál es el objetivo del control?

  Todo control tiene su por qué, se debe de explicar cual es el objetivo de control y qué se pretende conseguir con el control.

- ¿Cómo contribuye el control?

  Justificación de cómo el control contribuye a reducir el riesgo inherente del proceso.

- ¿Cuánto detalle es necesario?

  Será necesario aquel nivel de detalle que permita posteriormente, de forma clara y unívoca poder concluir y evaluar el control.

Ejemplo:

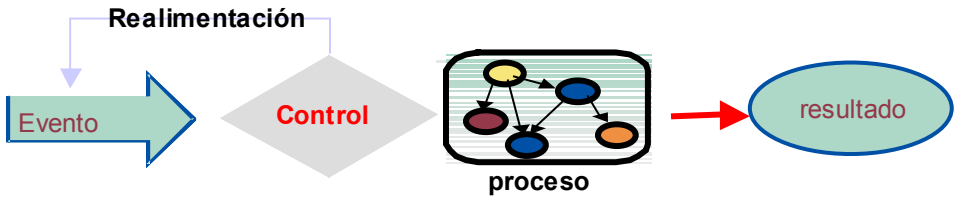
I	**¿En qué consiste el control?**	Existe una normativa interna para el aseguramiento de una unidad automotriz, que detalla los requerimientos entre los que se encuentra, el que el agente de seguros que este tramitando la expedición de la póliza de seguros, obtenga directamente del automóvil las calcas de los números de la placa bin que contienen los números de motor y de serie de la unidad.
II	**¿Cuál es el objetivo del control?**	La actividad de control pretende reducir el riesgo de fraude externo, ya que con el procedimiento establecido la Compañía asegura que el agente de seguros verificó la existencia del bien asegurable (Inspección de riesgo) y que no presenta daños que afecten el valor de unidad.
III	**¿Cómo contribuye el control?**	Mediante la inspección del riesgo realizada sobre la unidad asegurada la Compañía reduce en forma significativa el riesgo del fraude externo al evitar pagar siniestros por pérdidas totales por daños materiales o robo o en su caso, por daños materiales parciales sobre unidades en las que el siniestro se hubiera realizado anticipadamente al inicio de vigencia del seguro.

Tipología del control

Clasificación del control en función del momento en que actúa.

Controles preventivos: El objetivo del control se consigue antes de que ocurra el evento de riesgo, es decir, previene desviaciones antes de comenzar un proceso.

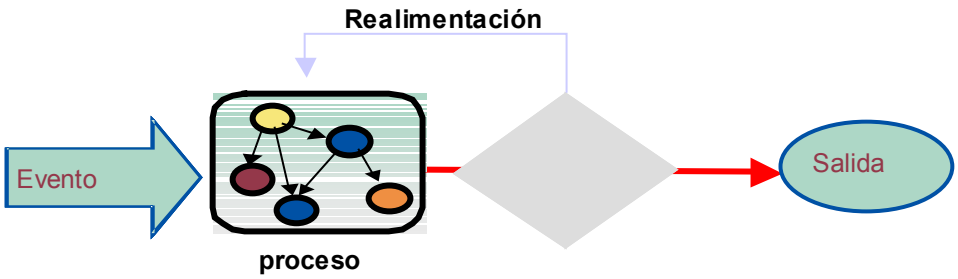
¿Cuándo se aplican?: Se suelen emplear para eliminar los problemas en origen. Se pueden predecir las posibles excepciones, muchos pueden ser de tipo informático.



Controles detectivos o correctivos: El objetivo de control se consigue después de que ocurra el evento de riesgo, es decir, identifica desviaciones cuando ya han ocurrido.

¿Cuándo se aplican?:

- Se suelen utilizar para detectar errores que son difíciles de definir y predecir.
- Normalmente las consecuencias del error no son muy elevadas.
- Si los controles no son prácticos podrían estancar el flujo normal del negocio.



Grado de automatización

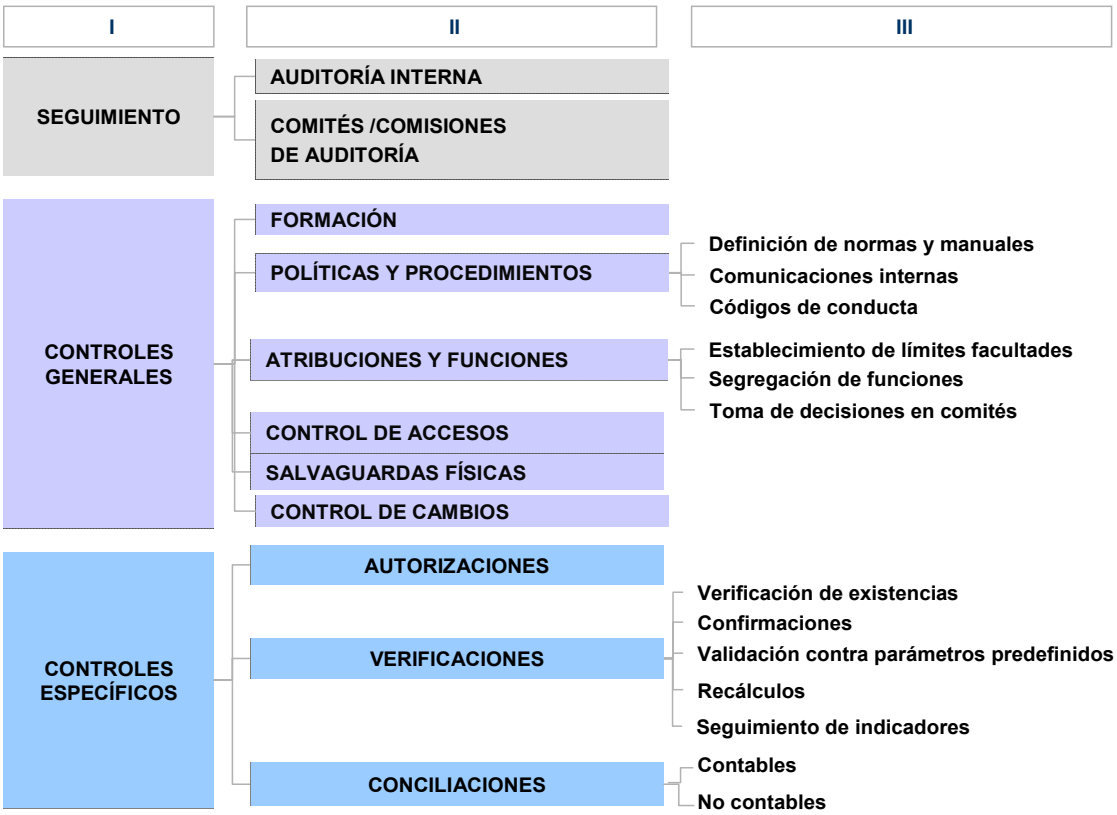
Clasificación del control en función de la naturaleza y grado de automatización del mismo.

Automáticos: Actividades de control desarrolladas de forma mecánicas (normalmente por o a través de alguna aplicación) y que no requieren de ningún juicio o valoración personal, funciona el control por sí solo.

Manuales: Siempre que en el control intervenga una persona (porque existe riesgo de que se equivoque o de que no lo haga) el control será manual, normalmente se debe de aplicar juicio o valoración a la actividad.

Clase de control

Selección de la clase de control de acuerdo al pertenezca dentro de este esquema.



Periodicidad

Frecuencia con la que se realiza o ejecuta el control.

¿Cuándo actúa el control?

En todas las operaciones	**Cuando el control es realizado cada vez que se lleva a cabo el proceso / subproceso.**
Diaria	Cuando el control es realizado una vez al día.
Semanal	Cuando el control es realizado una vez a la semana.
Mensual	Cuando el control es realizado una vez al mes.
... etc.	

Responsable

Se define la persona o puesto y departamento o unidad encargada de realizar el control. Es importante determinar quién es el responsable de realizar el control, para poder gestionar posteriormente las debilidades y los planes de acción. Además, en determinadas ocasiones la definición del puesto y la persona servirá como ayuda para poder valorar positiva o negativamente el control.

Ejemplo: Director de área, Gerente de Riesgos, Gerente de Oficina y Sucursal, Administrativo de Oficina, etc.

Evidencia generada

Se trata de tener constancia física o contrastable de que el control se ha llevado a cabo, sin embargo puede que existan determinados controles que en función de la naturaleza de los mismos no se genere evidencia alguna.

La documentación del resultado del control, debería responder a las siguientes preguntas:

I. ¿Qué genera el control?
II. ¿Dónde esta el control?
III. ¿Durante cuanto tiempo está?

Ejemplo de evidencia generada

I	¿Qué genera el control?	La aplicación genera un listado con las partidas pendientes, que el empleado interpreta y analiza y sobre las cuales genera un informe en el que se queda de manifiesto el tratamiento que ha dado a cada una de ellas.
II	¿Dónde está el control?	Se ha anexado el último informe efectuado por el empleado, así como la ruta para poder encontrar todos los informes que efectúa. 
III	¿Durante cuanto tiempo está?	Esta disponible el último informe efectuado por el empleado, por tanto como el control tiene una periodicidad mensual, la evidencia esta disponible durante 1 mes.

4.2.4.2 Control de calidad en la documentación de controles.

Finalmente, para comprobar y verificar si el control ha sido bien documentado, y con el fin de facilitar la labor de evaluación posterior, se podrán plantear las siguientes cuestiones:

- ¿El control es auto explicativo?
- ¿Alguien ajeno al proceso sería capaz de entenderlo?
- Si alguien externo tuviese que hacer el control, ¿sería capaz de replicarlo?
- ¿El control lo hace una persona o una máquina?
- ¿Es posible comprobar de manera clara y rápida que el control se ha llevado a cabo?
- En el caso de tener que pedir explicaciones sobre la realización del control ¿sé a quién acudir?

La documentación de controles y la calidad con la que se efectúe, es la base para poder concluir sobre el diseño y el funcionamiento de los controles. Toda la documentación de controles se debe efectuar.

4.2.4.3 Ejemplo de documentación del control.

Control	Operación de comprobación y verificación de documentación presentada
Tipología	Preventivo
Grado de automatización	Manual
Clase de control	Confirmaciones
Periodicidad	En cada una de las operaciones

Responsable	Analista de indemnizaciones vida individual
Evidencia generada	La sistemática para llevar a cabo el control se encuentra recogido en el Manual de Operación SVI-PYM-021-03, con fecha de emisión 01/09/03 y con entrada en vigor 18/02/05

¿En qué consiste el control?

En el Manual de Operación SVI-PYM-021-03 se establecen las políticas y procedimientos para la atención de reclamaciones de siniestros del Seguros de Vida Individual a los asegurados de la Institución a nivel nacional, así mismo se señala qué información y documentación se debe requerir de los beneficiarios para su análisis, valuación, registro y pago de las reclamaciones.

Dado que existe la posibilidad de que el beneficiario presente información y documentación falsa para cumplir con los requisitos establecidos para obtener el pago de la indemnización derivada del seguro de vida contratado, se lleva a cabo una comprobación de la veracidad de dicha documentación y la comparación de los datos incluidos en la misma, mediante la intervención de un investigador contratado para el efecto.

El Manual establece que cuando al personal de la Gerencia de Indemnizaciones Vida se le presente una duda razonable de la veracidad u originalidad de un documento o dato proporcionado por los beneficiarios de los seguros, deberá presentarlo a la consideración del Gerente de indemnizaciones vida, quien después de un primer análisis y a su juicio podrá solicitar la intervención de un investigador contratado especialmente para el efecto. Para realizar la contratación del investigador el Gerente deberá contar con la autorización del Director Técnico Vida, de acuerdo con el punto 2.6 del manual de procedimientos, siempre y cuando la suma asegurada reclamada ascienda a más de $500 mil pesos, si es inferior el propio Gerente podrá autorizar dicha contratación. De esta manera, se evita que se pueda incurrir en riesgo de fraude externo, dado que se mitiga la posibilidad de que el solicitante presente documentación falsa.

¿Cuál es el objetivo del control?

Se trata de evitar el pago de reclamaciones por siniestros improcedentes a personas que pretenden defraudar a la Institución a través de la presentación de documentos oficiales alterados o con datos falsos, que se constituyen en una omisión o inexacta declaración. Es decir, el objetivo es mitigar la posibilidad de que se cometa fraude externo por parte del beneficiario del seguro, comprobando la veracidad de la documentación presentada y comparándola con los datos reflejados en archivos oficiales, comprobando que dichos datos coincidan.

¿Cómo se contribuye el control?

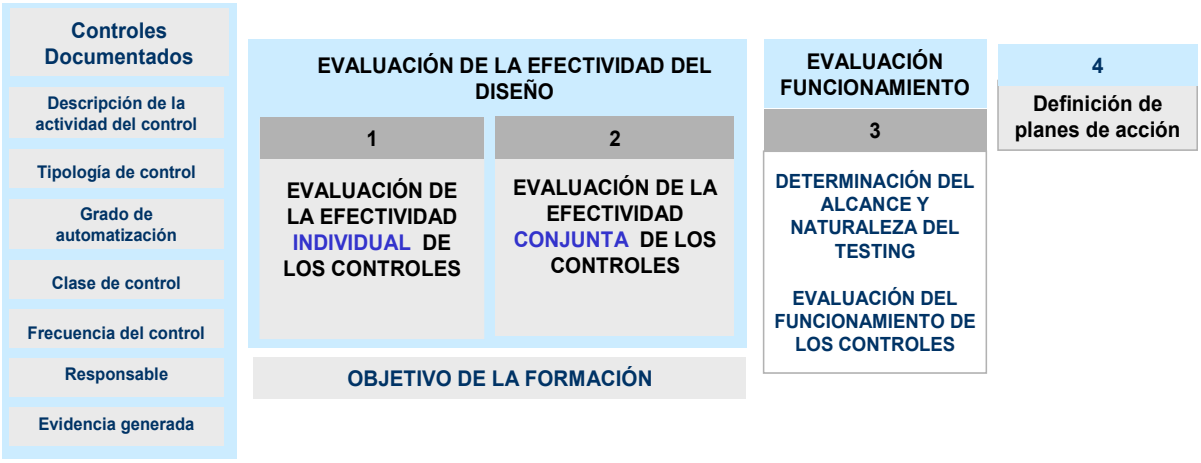
A través de la corroboración de la igualdad entre los datos presentados por el beneficiario del seguro y la existente en la documentación oficial se mitiga la posibilidad de que la Compañía realice pagos fraudulentos, que afecten su economía y sus resultados de operación.

4.2.5 Evaluación de controles

El modelo establece realizar una evaluación a un doble nivel:

La situación de la que partimos es que se han descrito todos los procesos, identificado y clasificados los riesgos inherentes que pueden afectar los objetivos de negocio y documentado todos los controles que mitigan a esos riesgos.

4.2.5.1 Esquema para la evaluación de controles y selección para pruebas (testing).

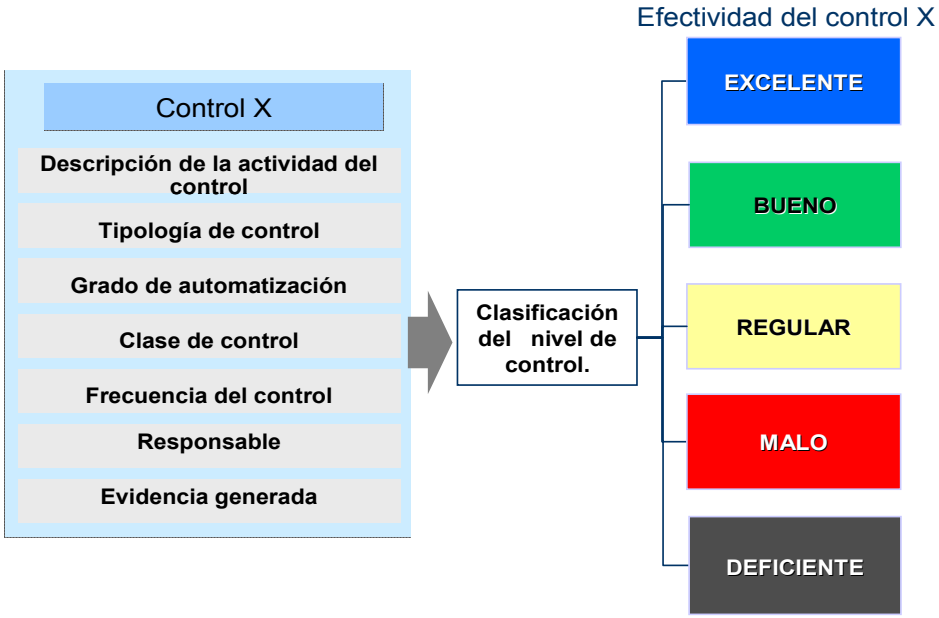


La evaluación que se va a efectuar sobre la razonabilidad de los controles, debe concluir sobre la efectividad individual de cada uno de los controles y principalmente, a nivel global sobre todos los controles que existan para un determinado riesgo.

4.2.5.2 Evaluación del diseño de controles

4.2.5.2.1 Evaluación de la efectividad individual

Evaluación de cómo la actividad de control, individualmente, contribuye a mitigar el riesgo considerando exclusivamente su diseño.



Definición de las calificaciones de evaluación

Hay que tener en cuenta que siempre pueden existir circunstancias particulares y remotas que podrían hacer que ocurra el riesgo, lo que se deberá valorar es si esas circunstancias tienen la suficiente relevancia como para poder concluir positiva/negativamente.

Efectividad Excelente: Su diseño se encuentra bien definido, se aplican al pie de la letra y evitan prácticamente la incidencia del peligro analizado.

Efectividad Bueno**:** Su diseño y aplicación es adecuado, pero generalmente necesitarán actuar conjuntamente con otros controles para mitigar el riesgo, además de que pueden tener mejoras.

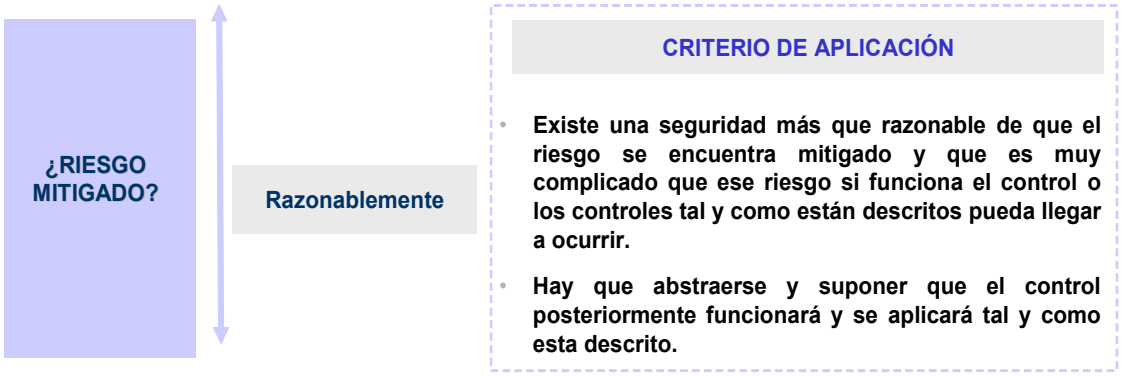
Efectividad Regular: Son medianamente adecuados y requieren una revisión más detallada para implementar mejoras para su diseño y aplicación.

Efectividad Malo: Existen pero son muy deficientes y requieren una renovación exhaustiva.

Efectividad Deficiente**:** Son inexistentes o hay pocos controles y son inadecuados.

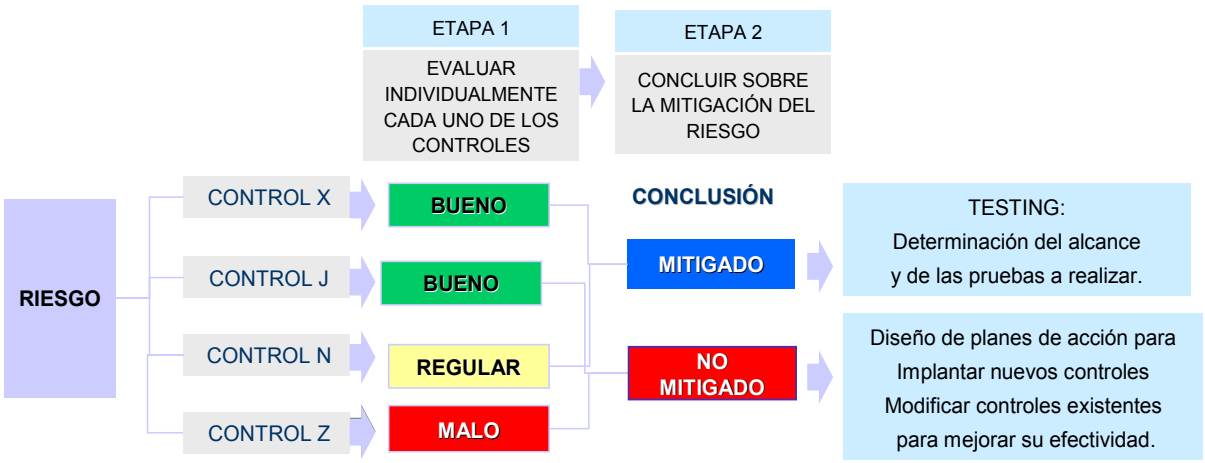
4.2.5.2.2 Evaluación de la efectividad conjunta

Debe de haber un criterio homogéneo compartido y aplicado por todos los evaluadores de controles para poder concluir que el riesgo se encuentra mitigado.



Verificación de que la actividad o conjunto de actividades de control identificadas permiten obtener una seguridad razonable sobre la mitigación del riesgo asociado.

¿Cómo mitiga cada uno de los controles el riesgo?



4.2.5.2.3 Premisas para la evaluación del diseño.

Cada una de las situaciones descritas en las que habrá que evaluar la idoneidad y suficiencia de los controles será distinta, no existen reglas ni pautas únicas, no obstante, a continuación se detallan una serie de criterios de referencia para que sirvan de ayuda y soporte en la decisión a tomar.

1) Hay que tener en cuenta que siempre pueden existir circunstancias particulares y remotas que podrían hacer que ocurriese el riesgo, lo que se deberá valorar es si esas circunstancias tienen la suficiente relevancia como para poder concluir positiva/negativamente, debemos preguntarnos si, él o los controles funcionan, ¿existe riesgo?.

2) Hay que abstraerse y suponer que el control posteriormente funcionará y se aplicará tal y como esta descrito.

3) Debe existir una adecuada combinación entre controles preventivos y detectivos.

4) Normalmente demasiados controles no son síntoma de un buen diseño o de efectividad de controles.

5) Varios controles de efectividad media pueden mitigar un riesgo de la misma manera que lo hace un solo control de efectividad alta.

6) Un mismo control, dependiendo del grado de automatización que tenga puede ser más o menos efectivo.

7) Es necesario tener en cuenta quién realiza la actividad de control, dado que ha de tener la autoridad suficiente para la toma de decisiones en el caso de detección de incidencias.

8) También habrá de considerarse el momento en el que se realiza el control, dado que llevarlo a cabo antes o después de determinado hecho puede afectar seriamente a la efectividad del mismo: preventivo/detectivo.

9) La frecuencia de la realización del control es otro elemento de relevancia, dado que cuanto más frecuentemente se realice, por lo general será más efectivo (dependiendo del riesgo del que se trate).

10) Habrá que considerar si la realización de un control genera una evidencia y si ésta es mantenida y guardada a lo largo del tiempo, con carácter general, la no-existencia de evidencia será indicativo de una debilidad de control.

    No obstante, en determinadas situaciones la propia naturaleza del control puede ocasionar que no exista ninguna evidencia de la realización del control.

4.2.5.2.4 Casos prácticos

Evaluación de la efectividad individual

Riesgo	Control	Efectividad del control
Establecimiento de importes de nóminas por parte de personal no autorizado.	Establecimiento de contraseñas para acceso a sistema de nóminas accesible sólo a personal específico del departamento de RRHH.	REGULAR

Administrativo de suscripción: Emisión de pólizas de seguros.

Riesgo: Errores tipográficos en contratos de seguros.
Descripción del control: Comprobación de datos grabados con documentación de expediente.

	CASO 1
Tipología	Detectivo
Automatización	Manual
Clase de control	Validación
Periodicidad	Todas las operaciones
Propietario	Áreas emisoras.
Evidencia	Documentación expediente e impreso de confirmación
EFECTIVIDAD	BUENA

Recursos Humanos: Nóminas Mensuales

Riesgo: Errores / incidencias en el proceso de liquidación de nóminas.
Descripción del control: Revisión de importes nóminas previo a la orden de pago.

	CASO 1	CASO 2
Tipología	Detectivo	Preventivo
Automatización	Manual	Manual
Clase de control	Confirmaciones	Confirmaciones
Periodicidad	Mensual	Mensual
Propietario	Responsable RRHH	Responsable RRHH
Evidencia	OK en aplicación	OK en aplicación
Momento	**Después de la orden de pago**	**Previo a la orden de pago**
EFECTIVIDAD	MALO	EXCELENTE

Evaluación de la efectividad conjunta

Información Financiera: Generación de estados financieros

Riesgo	Controles	Efectivo	¿Mitigación del riesgo?
Errores en los datos consignados en la información financiera correspondiente a la Empresa, en base a la cual se generan los estados financieros para el Consejo de Administración y autoridades.	Verificación de que el activo, el pasivo y capital de los estados financieros de la Empresa, tienen idéntico valor.	R	SÍ
	Verificación de que la utilidad / pérdida que refleja el estado de resultados coincide con el presentado en el balance.	R	
	Dictamen de los estados financieros de parte de los auditores externos que certifica que la información financiera es correcta.	E	
	Pruebas de razonabilidad sobre los datos presentados en los estados financieros, comparándolos con meses / ejercicios anteriores.	R	
	Conciliación de cuentas y auxiliares contables.	B	

Gestión Administrativa: Registro contable

Riesgo	Controles	Efectivo	¿Mitigación del riesgo?
Errores en la contabilización y registro de las operaciones, por una inadecuada interpretación de la normativa contable vigente.	Revisiones de Auditoría Interna.	M	NO
	Auditorías Externas periódicas.		
	Inspección de la CNSF.		

No se pueden considerar los controles externos (Auditores externos y de la CNSF) como parte efectiva del modelo de control interno de la compañía.

Gestión Administrativa: Tesorería (Compra venta de deuda pública)

Riesgo	Controles	Efectivo	¿Mitigación del riesgo?
Contratación de productos no autorizados por la Compañía que no puedan ser adecuadamente tratados ni contabilizados en los sistemas de la Empresa.	Conocimiento por parte de los empleados actividades y productos autorizados en cada momento, así como los límites establecidos para los mismos, de acuerdo a un Manual de Procedimientos.	B	SÍ
	Existencia de responsables independientes para cada tarea: mantenimiento de registros, autorización, contratación y supervisión.	R	
	Control diario del consumo de límites y de la operación.	B	

4.2.5.3 Evaluación del funcionamiento de controles

Solamente se efectuará testing de aquellos controles sobre los que se haya concluido positivamente a nivel conceptual.

4.2.5.3.1 Objetivo de las pruebas (testing)

- Probar, en base a muestras, que los controles están funcionando tal y como han sido diseñados.

- El grupo de trabajo va a buscar tener la equivalencia de un 95% de nivel de confianza en el funcionamiento del control, por tanto el nivel de desviación no debe de ser superior a un 5%, para concluir que el objetivo del control ha sido conseguido y el riesgo sobre el cual estaba actuando se encuentra mitigado.

4.2.5.3.2 Alcance del testing

El número de pruebas a realizar variará en función de:

- Frecuencia de realización del control
- Naturaleza del control (automatización)
- Importancia del riesgo
- Importancia del proceso
- Programas de Auditoría Interna

4.2.5.3.3 Realización de pruebas

Las pruebas para verificar el funcionamiento de los controles consistirán, según los casos, en:

Examen de la evidencia del control*:* Revisión de la documentación y evidencia que ha dejado la actividad de control al ser ejecutada.

Observación de la realización del control: La observación de la realización del control puede proveer una cierta seguridad de su aplicación, sin embargo esto no garantiza la aplicación de la actividad de control a lo largo del tiempo, por tanto deberá ser combinada con alguna de las otras técnicas.

Replicación de la actividad de control: Realización de la actividad de control nuevamente para garantizar que la actividad de control se esta desarrollando tal y como esta descrita.

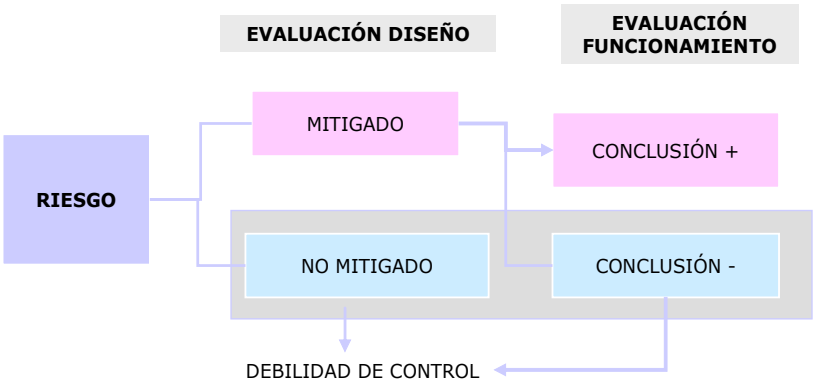
Se suelen utilizar para verificar las actividades de control automáticas (normalmente con un alto componente tecnológico). Por ejemplo, en un control de cambios, verifica que no es posible realizar ninguna modificación en la aplicación.

Las tareas a realizar por el responsable de aplicar las pruebas son:

I. Describir y documentar como se va a hacer la prueba para verificar el adecuado funcionamiento del control.
II. Analizar los programas de Auditoría interna para verificar si esa prueba que conceptualmente se ha definido esta dentro del alcance de sus programas de trabajo, de no estar se incorpora la prueba a los planes y programas.
III. Determinar el alcance de la prueba, número de muestras, fechas en las que se prueba.
IV. Realización de las pruebas.
V. Análisis e interpretación de los resultados.
VI. Conclusión.

4.2.5.3.4 Conclusión de resultados y establecimiento de planes de acción.

Es necesario efectuar una conclusión para determinar si el control funciona de acuerdo a su diseño y si su aplicación es adecuada.



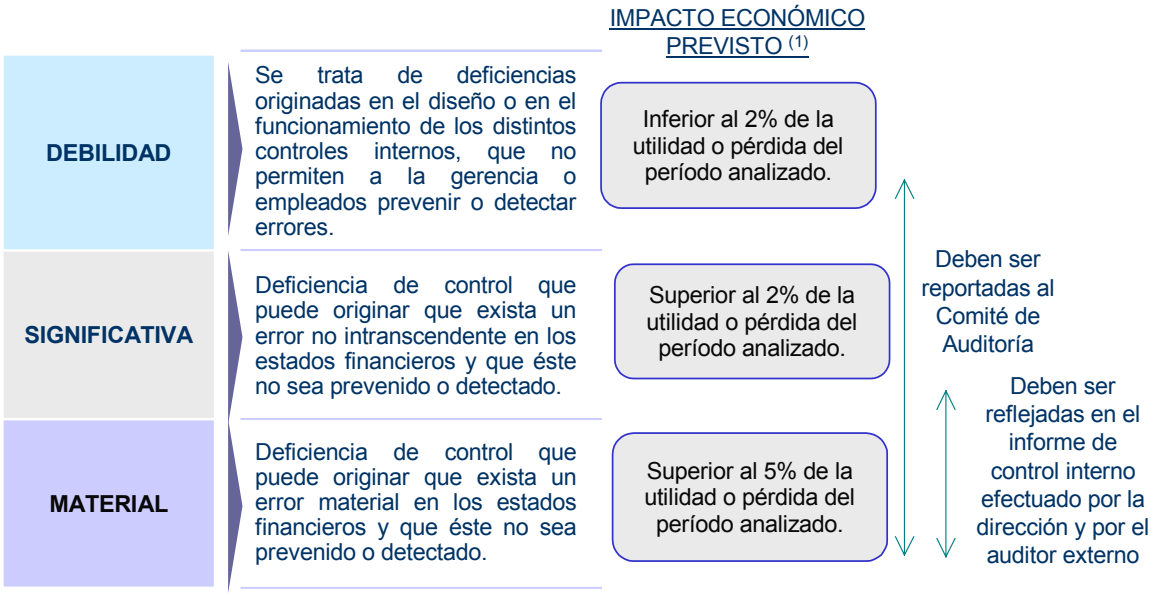
Conclusión positiva sobre el funcionamiento del control:

El control funciona tal y como esta diseñado y se esta aplicando adecuadamente.

Conclusión negativa sobre el funcionamiento del control:

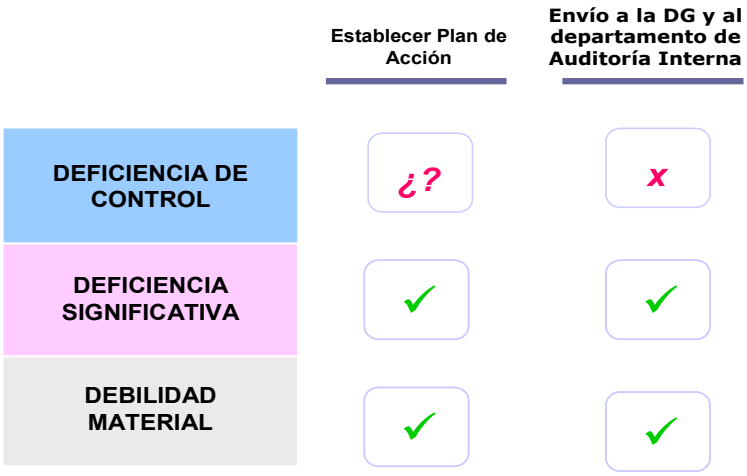
a) No se esta aplicando por el usuario.
b) No funciona tal y como estaba descrito.
c) Funciona como esta descrito pero falla y no consigue su objetivo.

No obstante, no todas las debilidades de control tienen la misma relevancia ni la misma importancia económica, para cada una de las desviaciones identificadas, habrá que realizar una estimación del impacto económico y clasificarlas en función del mismo.



Una vez que se haya determinado el tipo de debilidad, habrá que establecer el plan de acción.

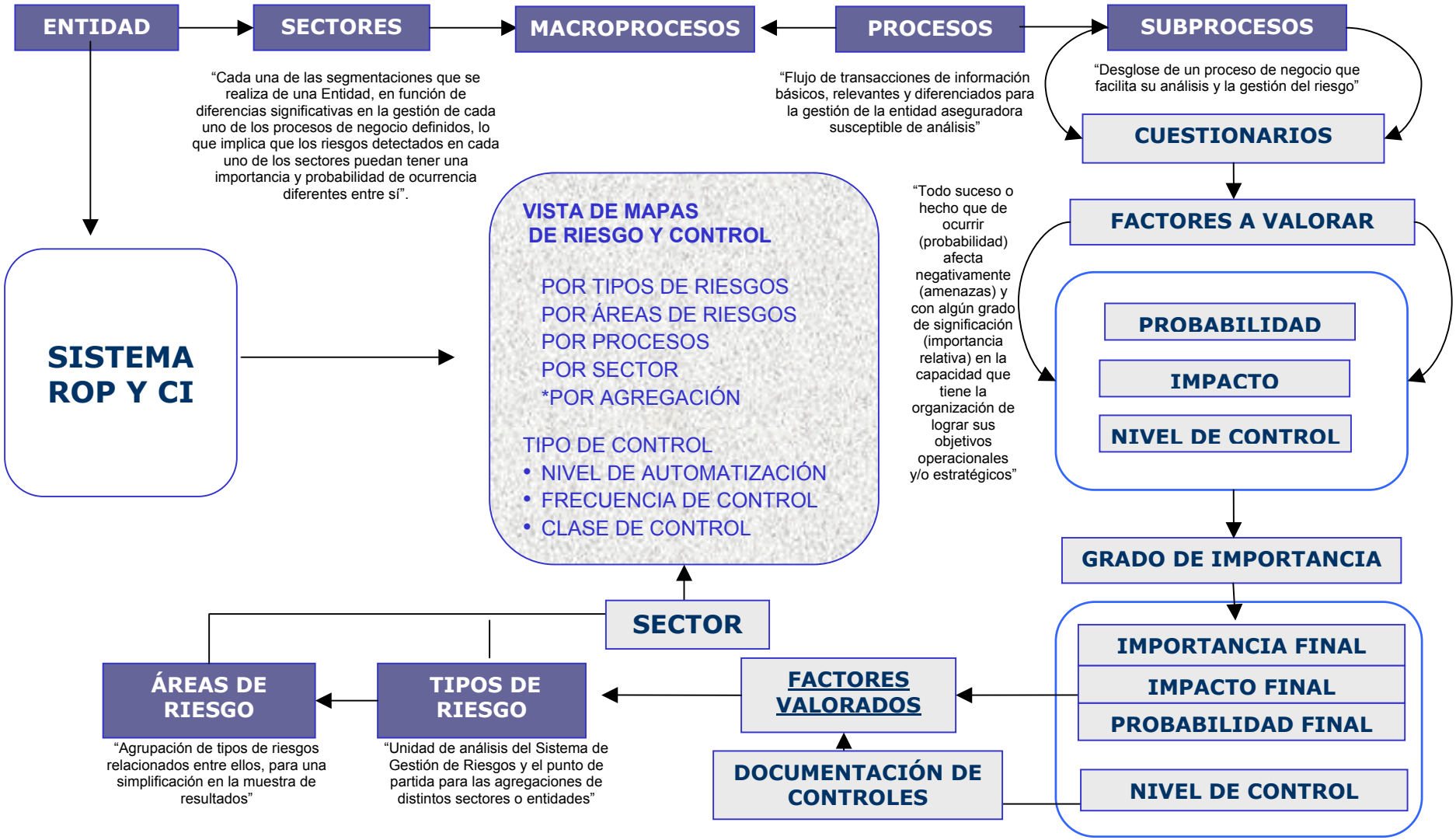
Todas las deficiencias significativas o materiales será necesario remitirlas a la Dirección General (DG), incluido la metodología de cálculo y el plan de acción previsto.



En los casos que se presenten numerosos planes de acción, será complicado e inviable el poder aplicar todos ellos en un tiempo, por tanto será recomendable el priorizar los mismos de acuerdo al mayor impacto económico.

La gestión e implantación de los Planes de Acción es responsabilidad última del propietario del control.

ESQUEMA DEL SISTEMA DE RIESGOS Y CONTROL INTERNO.



Conclusiones

Los riesgos operacionales han existido siempre, se cometen errores y fallas en la Organización, algunos cuyo impacto no es relevante, otros más serios y rara la vez muy graves, pero el riesgo esta latente en todo momento y se ha gestionado con un enfoque básico de controles internos, cada área de negocio gestiona su riesgo operacional estableciendo los controles y medidas que estima oportunos, también se apoya en la confianza y competencia de los empleados, así como en el área de Auditoría Interna que realiza inspecciones periódicas de los procesos. Bajo este esquema tradicional predomina el enfoque reactivo y correctivo, lo cual es una clara manifestación de la falta de cultura de prevención y conciencia del impacto que pueden tener los riesgos operacionales.

La Administración de Riesgos establece un marco de referencia formal con un enfoque proactivo y preventivo, con lo que se mejora las decisiones de respuesta al riesgo, ajustando los procesos a resultados y al cumplimiento de objetivos, haciendo análisis de costo beneficio para desplegar recursos eficaz y eficientemente.

La Administración de Riesgos Operativos y el Control Interno es un proceso continuo que fluye por toda la entidad y que requiere que sea realizado por su personal en todos los niveles de la Organización, ya que todos tienen responsabilidad en este proceso, empezando por el Consejo de Administración y la Alta Dirección que tienen el compromiso de incentivar y permear este nuevo enfoque, dándole seguimiento para poder establecer una cultura Institucional.

Una vez definida la estrategia y las metodologías a utilizar para la gestión de riesgos operacionales y control, el reto ha sido obtener el compromiso de la alta Dirección para incentivar este nuevo enfoque, reiterando la necesidad de constituirlo dentro de la estructura de la Organización no sobre de ella, además de promoverlo para que forme parte de la cultura, incorporando su filosofía a las prácticas y procesos de negocio.

Destacamos la necesidad de que el proceso de gestión y control de riesgos operacionales no debe ser visto o practicado como una actividad separada, porque finalmente quien identifica, documenta, controla y administra sus procesos, riesgos y controles es el personal que realiza la operación. Las áreas de Administración de Riesgos, Auditoría y Contraloría, son responsables de establecer mecanismos y dar asesoría sobre el manejo del marco de referencia y metodologías, son áreas de apoyo para incentivar la cultura y la implementación de este proceso.

Es importante destacar que con la adecuada implementación de este proyecto el Consejo de Administración y la alta Dirección van adoptar una perspectiva del riesgo a nivel conjunto de la entidad y que los resultados van a proporcionar información con una seguridad razonable para apoyar la toma de decisiones en la Organización.

Bibliografía

Instituto Mexicano de Auditores Internos.
"Curso de Administración de Riesgos Corporativos Marco Integrado COSO / ERM".
Duración 16 hrs. 30 y31 de agosto 2006.

Jornadas Internacionales de desarrollo profesional Prevención del Fraude y Administración de Riesgos Control, Auditoría y Seguridad.
"Curso de Elaboración del mapa de Riesgos, Control y Auditoría".
Duración 24 hrs. 11, 12 y 13 de mayo 2004.

Shirebrook Commodities
"Curso Programa Integral de Administración del Riesgo Operacional".
Duración junio y julio 2003.

PriceWateHouseCoopers, COSO The Committee of Sponsoring Organizations of the Tread way Commission, FILA Federación Americana de Auditores Internos, 2005.
Administración de Riesgos Corporativos Marco Integrado.
Resumen Ejecutivo Marco
Diciembre

PriceWateHouseCoopers, COSO The Committee of Sponsoring Organizations of the Tread way Commission, FILA Federación Americana de Auditores Internos, 2005.
Administración de Riesgos Corporativos Marco Integrado.
Técnicas de Aplicación
Diciembre

Comité de Basilea, Supervisión del Riesgo Operativo, 2001.
Prácticas Sólidas para la Administración y Supervisión del Riesgo Operativo.
Diciembre.

Comisión Nacional de Seguros y Fianzas, 2000.
Circular S-11.6.
Lineamientos de carácter prudencial en materia de Administración Integral de Riesgos.
Octubre.

Luis A. Chichilla Salazar "Administración de Riesgos Operacionales"
http://www.ccpl.org.pe/colegio/revista/contador2001/Noviembre%202001/administracion_de_riesgos_operac.htm