

# **MANUAL DE CONTROL INTERNO**

**FORTIUS S.A. CORREDORES DE SEGUROS**

## Tabla de contenido

<b>CAPITULO PRIMERO: GENERALIDADES .....</b>	<b>4</b>
1. DEFINICIÓN Y FINALIDAD.....	4
2. PRINCIPIOS BÁSICOS:.....	4
3. OBJETIVOS DEL SISTEMA DE CONTROL INTERNO .....	6
3.1 OBJETIVO GENERAL:.....	6
3.2 OBJETIVOS ESPECÍFICOS.....	6
<b>CAPÍTULO SEGUNDO: ELEMENTOS DEL SISTEMA DE CONTROL INTERNO. ....</b>	<b>7</b>
<b>I.- SUBSISTEMA DE CONTROL ESTRATÉGICO.....</b>	<b>7</b>
1. AMBIENTE DE CONTROL: .....	8
2. DIRECCIÓN ESTRATÉGICA. ....	10
3. GESTIÓN DE RIESGOS .....	11
<b>II. SUBSISTEMA DE CONTROL DE GESTIÓN.....</b>	<b>13</b>
1. ACTIVIDADES DE CONTROL.....	13
1.1. POLÍTICAS DE OPERACIÓN.....	13
1.2. PROCEDIMIENTOS. ....	14
1.3. CONTROLES. ....	15
1.4. INDICADORES.....	16
1.5. POLÍTICAS DE CONTROL DE SEGURIDAD.....	16
1.6 CONTROLES ADMINISTRATIVOS. ....	22
1.7 CONTROLES AUTOMATIZADOS.....	24
1.8 DIFUSIÓN DE LAS ACTIVIDADES DE CONTROL. ....	24
2. INFORMACIÓN Y COMUNICACIÓN. ....	24
2.1 INFORMACIÓN.....	25
2.1.1. INFORMACIÓN INTERNA.....	25
2.1.2 INFORMACIÓN EXTERNA.....	26
2.1.3 FLEXIBILIDAD AL CAMBIO.....	26
2.1.4 COMPROMISO DE LA ALTA DIRECCIÓN. ....	26
2.1.5 SISTEMAS DE INFORMACIÓN. ....	27
2.1.6 INFORMACIÓN PRIVILEGIADA. ....	28
2.1.7. CALIDAD DE LA INFORMACIÓN.....	28
<b>III. SUBSISTEMA DEL CONTROL DE EVALUACIÓN.....</b>	<b>30</b>

1.	AUTOEVALUACIÓN DEL CONTROL.....	30
2.	AUTOEVALUACIÓN A LA GESTIÓN.....	30
3.	MONITOREO.....	31
4.	EVALUACIONES INDEPENDIENTES.....	31
<b>CAPITULO TERCERO: RESPONSABILIDADES DENTRO DEL SISTEMA DE CONTROL INTERNO .....</b>		<b>32</b>
1.	ÓRGANOS INTERNOS .....	32
1.1.	JUNTA DIRECTIVA.....	32
1.1.1	FUNCIONES GENERALES.....	32
1.2	COMITÉ DE AUDITORÍA.....	34
1.3	REPRESENTANTE LEGAL.....	34
2.	ÓRGANOS EXTERNOS.....	36
2.1	AUDITORIA EXTERNA.....	36
2.1.1	NORMAS PARA EL EJERCICIO DE LA AUDITORÍA.....	36
2.1.1.1.	NORMAS SOBRE ATRIBUTOS.....	36
2.1.1.2.	NORMAS SOBRE DESEMPEÑO.....	38
2.1.1.3.	NATURALEZA DEL TRABAJO.....	39
2.1.1.3.	PLANIFICACIÓN DEL TRABAJO.....	39
2.1.1.4.	DESEMPEÑO DEL TRABAJO.....	40
2.1.1.5.	COMUNICACIÓN DE RESULTADOS.....	40
2.1.1.6	SUPERVISIÓN.....	41
2.1.1.7.	FUNCIONES.....	42
2.3	REVISOR FISCAL.....	43
<b>CAPÍTULO CUARTO: PLANES DE MEJORAMIENTO.....</b>		<b>43</b>
1.	PLAN DE MEJORAMIENTO INSTITUCIONAL.....	43
2.	PLAN DE MEJORAMIENTO POR PROCESO.....	44
3.	PLAN DE MEJORAMIENTO INDIVIDUAL.....	44

## **CAPITULO PRIMERO: GENERALIDADES**

### **1. DEFINICIÓN Y FINALIDAD**

Se entiende por el Sistema de Control Interno, en adelante SCI, como el conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la junta directiva, la alta dirección y demás funcionarios de una organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes fines:

Mejorar la eficiencia y eficacia en las operaciones de FORTIUS S.A. CORREDORES DE SEGUROS

Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de FORTIUS S.A. CORREDORES DE SEGUROS

Orientar a los administradores de FORTIUS S.A. CORREDORES DE SEGUROS, en el cumplimiento de los deberes que les corresponde según la normatividad vigente, precisando el alcance de la responsabilidad en materia de control interno de los distintos órganos sociales.

Fomentar tanto la autorregulación como el autocontrol, dado que sin perjuicio de la responsabilidad que corresponde a los administradores, todos los integrantes de la organización deben evaluar y controlar su propio trabajo.

En ese orden de ideas y a efectos de prevalecer dentro de FORTIUS S.A. CORREDORES DE SEGUROS una cultura organizacional de control interno y crear por tanto un ambiente de control, de conformidad con lo establecido por el Numeral 7.5.1 de la Circular Externa No. 014 de mayo 19 de 2009, a continuación procedemos a enunciar los principios básicos y elementos del control interno que rigen en nuestra Sociedad:

### **2. PRINCIPIOS BÁSICOS:**

Administrar conceptualmente involucra organizar, planificar, dirigir y CONTROLAR los recursos de una empresa. Por consiguiente, FORTIUS S.A. CORREDORES DE SEGUROS establece como premisa fáctica fundamental dentro de sus procesos, la de planear, organizar, dirigir y controlar la realización de acciones suficientes para proveer SEGURIDAD RAZONABLE de que sus objetivos serán cumplidos.

Cabe acotar, que el concepto de control ha venido evolucionando y si bien se conserva su finalidad de prevenir y detectar eventos no deseados, así mismo se ha complementado su significado máxime considerando que:

“Un control es cualquier acción dispuesta por una entidad para mejorar la probabilidad de que los objetivos y metas establecidos sean logrados”.

Ahora bien, los principios fundamentan el Sistema de Control Interno y se entienden como los valores que caracterizan y personifican la naturaleza individual de FORTIUS S.A. CORREDORES DE SEGUROS y son los que se enuncian a continuación:

- a) **Autocontrol:** Es la capacidad de todos y cada uno de los funcionarios de FORTIUS S.A. CORREDORES DE SEGUROS, independientemente de su nivel jerárquico para evaluar y controlar su trabajo, detectar desviaciones y efectuar correctivos en el ejercicio y cumplimiento de sus funciones, así como para mejorar sus tareas y responsabilidades.

En consecuencia, sin perjuicio de la responsabilidad atribuible a los administradores en la definición de políticas y en la ordenación del diseño de la estructura del SCI, es pertinente resaltar el deber que les corresponde a todos y cada uno de los funcionarios dentro de la organización, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deberán procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los límites por ella establecidos.

- b) **Autorregulación:** Se refiere a la capacidad de la organización para desarrollar en su interior y aplicar métodos, normas y procedimientos que permitan el desarrollo, implementación y mejoramiento del SCI, dentro del marco de las disposiciones legales aplicables.
- c) **Autogestión:** Apunta a la capacidad de la organización para interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

Basado en los principios mencionados, el SCI establece las acciones, las políticas, los métodos, procedimientos y mecanismos de prevención, control, evaluación y de mejoramiento continuo de la entidad que le permitan tener una seguridad razonable acerca de la consecución de sus objetivos, cumpliendo las normas que la regulan.

- d) **Efectividad:** Esto es el cumplimiento de los objetivos básicos de la Sociedad, salvaguardando los recursos de la misma, que comprende los activos de la empresa y los bienes de terceros que se encuentren en su poder.
- e) **Suficiencia y confiabilidad** de la información financiera y contable, así como la preparación de todos los estados financieros
- f) **Cumplimiento** de las disposiciones legales, reglamentarias y estatutarias vigentes a las que se encuentra sujeta FORTIUS S.A. CORREDORES DE SEGUROS

Es importante resaltar que estos principios se complementan con los Principios Rectores enunciados en el Código de Ética de FORTIUS S.A. CORREDORES DE SEGUROS-

### **3. OBJETIVOS DEL SISTEMA DE CONTROL INTERNO**

#### **3.1 OBJETIVO GENERAL:**

El objetivo general del control interno es ayudar a la administración, dirección o gerencia a desempeñar eficazmente sus funciones por medio de cada una de las instancias o dependencias de FORTIUS S.A. CORREDORES DE SEGUROS, en procura de lograr una administración moderna, competitiva y transparente que consulte los distintos principios legales.

#### **3.2 OBJETIVOS ESPECÍFICOS.**

- Garantizar que la Sociedad disponga de procesos de planeación y mecanismos adecuados para el diseño y desarrollo organizativos, de acuerdo con su naturaleza y características.
- Proteger los recursos y activos de la Sociedad evitando su desaprovechamiento, pérdida y usos indebidos y propendiendo a su adecuada administración.
- Propender que se cumplan los objetivos, metas y políticas trazadas por la administración.
- Garantizar la producción de datos y estados financieros y operativos válidos, confiables y exactos.
- Garantizar la eficacia, moralidad, eficiencia y economía en todas las operaciones, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión de la empresa.

- Garantizar la observancia de las leyes, reglamentos y directrices de gestión en la Sociedad.
- Definir y aplicar medidas para prevenir los riesgos, detectar errores, fraudes o irregularidades, y corregir las desviaciones o desaciertos que se presenten en la empresa y que puedan afectar el logro de sus objetivos.
- Asegurar la oportunidad y confiabilidad de sus registros.
- Verificar y asegurar la suficiente idoneidad y eficiencia del recurso humano al servicio de FORTIUS S.A. CORREDORES DE SEGUROS.
- Garantizar la correcta y permanente evaluación, análisis y seguimiento de la gestión organizativa.
- Asegurar que todo el sistema de control interno disponga de mecanismos propios, de verificación, evaluación y examen crítico que den cuenta de su marcha y desarrollo y proponga los ajustes y correctivos pertinentes.
- El objetivo general del control interno es ayudar a la administración, dirección o gerencia a desempeñar eficazmente sus funciones por medio de cada una de las instancias o dependencias de FORTIUS S.A. CORREDORES DE SEGUROS, en procura de lograr una administración moderna, competitiva y transparente que consulte los distintos principios legales.

## **CAPÍTULO SEGUNDO: ELEMENTOS DEL SISTEMA DE CONTROL INTERNO.**

El Sistema de Control Interno está integrado por tres elementos en un enfoque sistémico, unidos por una forma de interacción o interdependencia, que tiene que ser comprendido como una unidad para el control de una gestión administrativa eficaz. Cada uno adopta el rango de subsistema por la magnitud de acciones de evaluación de las medidas de control.

Los subsistemas son: Subsistema de Control Estratégico; Subsistema de Control de Gestión Administrativa y Desarrollo Institucional; y, Subsistema de control de Evaluación.

### **I.- SUBSISTEMA DE CONTROL ESTRATÉGICO.**

Conjunto de elementos del sistema que al interactuar permiten la orientación estratégica y organizacional de la Institución.

Los componentes de este subsistema son tres:

## 1. AMBIENTE DE CONTROL:

Es generar las condiciones suficientes para que en el personal exista conciencia de la necesidad de control que impacta en la planificación, gestión y desarrollo institucional, de acuerdo a las facultades legales.

Los elementos mínimos establecidos por FORTIUS S.A. CORREDORES DE SEGUROS para crear un adecuado ambiente de control son:

- Determinación formal por parte de la alta dirección de los principios básicos que rigen la entidad, los cuales deben constar en documentos que se divulguen a toda la organización.
- Código de Ética: FORTIUS S.A. CORREDORES DE SEGUROS adoptó en su Código las pautas de comportamiento que consagran explícitamente las políticas y las directrices de la Sociedad en materia de control interno, que incluye entre otros aspectos:
  - Cumplimiento de las disposiciones legales, reglamentarias y estatutarias vigentes a las que se encuentra sujeta FORTIUS S.A. CORREDORES DE SEGUROS.
  - Situaciones generadoras de conflicto de interés
  - Políticas sobre la actuación de sus funcionarios y agentes, en forma directa o indirecta, en cualquiera de las líneas de negocios y operaciones que realicen en desarrollo de su objeto social
  - Manejo de información privilegiada
  - Relaciones con clientes y proveedores
  - Conductas relacionadas con limitación de regalos y atenciones ofrecidas y recibidas
  - Régimen sancionatorio
- Código de Buen Gobierno Corporativo: provee un marco que define derechos y responsabilidades, dentro del cual interactúan los órganos de gobierno de una entidad entre los cuales se destacan el máximo órgano de dirección, la junta o consejo directivo, los representantes legales y demás administradores y el revisor fiscal y demás órganos de control.

En ese orden de ideas, un buen gobierno corporativo es aquel que facilita los instrumentos necesarios que garanticen la existencia y puesta en práctica de mecanismos idóneos que permitan el balance entre la gestión de cada órgano y el control de la antedicha gestión, a través de un sistema de pesos y contrapesos, a efectos que las decisiones que se adopten en cada instancia se efectúen de

conformidad con el mejor interés de la persona jurídica, sus accionistas y acreedores.

Ahora bien, los últimos estudios acerca de la regulación de las sociedades como Agentes Económicos han identificado la coexistencia de tres grandes tipos de tensiones dentro de las formas asociativas:

❖ Relación entre los accionistas y los administradores: Aquí se analiza la tensión que puede presentarse en un momento dado entre los aportantes de capital y los administradores de la Sociedad. En el caso colombiano, debido al alto nivel de concentración de la propiedad en pocos accionistas, la discrepancia de intereses entre los accionistas y los administradores se resuelve de una forma ágil por medio del control que ejercen los accionistas mayoritarios.

❖ Relación entre los accionistas mayoritarios y minoritarios: En este ítem se evalúa la tensión entre estos dos tipos de accionistas, máxime cuando se indica que el accionista significativo o mayoritario es el mandatario del minoritario, dado que éste deposita su confianza en aquel cuando efectúa el aporte de capital correspondiente y en un momento determinado no pueden ejercer un control efectivo.

❖ Relación entre la sociedad y los grupos de interés: En esta relación se analiza la tensión que se presenta entre los intereses de la entidad como agente económico y sus empleados, acreedores, clientes y entes de supervisión. Aquí se encuadran todas las normas que buscan proteger a aquellos que a pesar de su calidad de terceros con relación a la entidad, han depositado su confianza de una u otra forma en la misma.

Es menester aclarar, que los accionistas no son los únicos agentes que poseen un interés legítimo en el ejercicio de la actividad societaria, los acreedores, los consumidores financieros, empleados también tienen ese interés.

Ahora bien, en torno a la Superintendencia Financiera, la relación en comento, le resulta particularmente relevante, debido a su rol fundamental frente a la seguridad, estabilidad y confianza del sistema financiero, como también la protección del consumidor financiero.

➤ Manual de Funciones y Competencias Laborales: El manual específico de funciones y de competencias es un instrumento de administración de personal a través del cual se establecen las funciones y las competencias laborales de los empleos que conforman la planta de personal de una entidad y los requerimientos exigidos para el desempeño de los mismos. Se constituye en el soporte técnico

que justifica y da sentido a la existencia de los cargos en FORTIUS S.A. CORREDORES DE SEGUROS.

Así mismo, las Competencias Laborales se pueden definir como la capacidad de una persona para desarrollar, con base en los requerimientos de calidad y resultados esperados.

Para todos los efectos, la capacidad estará determinada por los conocimientos, destrezas, habilidades, valores, actitudes y aptitudes que debe poseer y demostrar el empleado.

- Estructura Organizacional que permita soportar el alcance del SCI y que defina claramente los niveles de autoridad y responsabilidad, precisando el alcance y límite de los mismos. La estructura organizacional estará armonizada con el tamaño y naturaleza de las actividades de que FORTIUS S.A. CORREDORES DE SEGUROS soportando el alcance del SIC.
- Establecimiento de objetivos que deben estar alineados con la misión, visión y objetivos estratégicos de la Sociedad.
- Comité de Auditoría: El Comité de Auditoría de la Junta Directiva de que FORTIUS S.A. CORREDORES DE SEGUROS., es el máximo órgano de control de la Sociedad encargado de la vigilancia de la gestión y la efectividad del sistema de control interno. Es de carácter permanente y se rige por su Reglamento Interno y por la normatividad expedida por la Superintendencia Financiera de Colombia.

El Comité de Auditoría tiene como objetivo primordial apoyar a la Junta Directiva en la evaluación del control interno de la Sociedad, así como a su mejoramiento continuo, sin que ello implique en momento alguno, una sustitución a la responsabilidad que de manera colegiada le corresponde a la junta directiva.

- Manual de Recursos Humanos

## **2. DIRECCIÓN ESTRATÉGICA.**

Es el marco de referencia que orienta a la Institución hacia el cumplimiento de su Misión, alcance de su Visión y realización de los Objetivos Estratégicos.

### **- MISIÓN:**

Somos una Empresa de servicios, especializada en la colocación de seguros, asesorando eficientemente al cliente en el manejo de sus riesgos asegurables, especialmente para el

Sector Solidario, de Copropiedades y el Sector Real de la Economía, promoviendo la celebración del más competitivo contrato, liderando la ejecución del mismo y promoviendo su renovación, consiguiendo el desarrollo y realización de sus funcionarios, permitiendo así el bienestar de sus familias y obteniendo una ganancia justa para sus Socios.

#### - **VISIÓN**

Ser a corto plazo y consolidarnos en el largo plazo como una Organización sólidamente estructurada, orientada a la prestación de un eficiente servicio en la adquisición y manejo de seguros, especialmente para el Sector Solidario, el de Copropiedades y el Sector Real de la Economía, con calidad y tecnología suficientemente especializada, para ser los más competitivos.

La Dirección Estratégica se compone de planes, programas, modelos de operación y estructura organizacional:

- Manual de Calidad
- Mapa de Procesos
- Planeación Estratégica
- Planeación Estratégica de la Gestión Tecnológica
- Indicadores
- Política de Calidad
- Estructura Organizacional
- Sistema de Gestión de Calidad

### **3. GESTIÓN DE RIESGOS**

En atención a que FORTIUS S.A. CORREDORES DE SEGUROS es una entidad vigilada por la Superintendencia Financiera de Colombia, se trabajan los siguientes sistemas de administración de riesgos: Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT; y, Sistema de Administración de Riesgo Operativo –SARO-. Estos sistemas de administración de riesgos están soportados en la reglamentación legal expedida para el efecto por la Superintendencia Financiera así como por la regulación interna expedida por la Junta Directiva de la empresa para dar cumplimiento a los requerimientos legales de tales sistemas acorde con nuestra naturaleza, complejidad y tamaño.

Ahora bien, en la medida que los líderes de negocios buscan nuevas formas de agregar valor a los accionistas, éstos han comenzado a pensar en nuevas maneras de cómo la administración del riesgo se encuentra unida a la creación del valor. Más aún, muchas

industrias y organizaciones, están reconociendo que los riesgos ya no son simplemente peligros que evitar, sino que en muchos casos, oportunidades que aprovechar.

Y es precisamente, dentro de este contexto que FORTIUS S.A. CORREDORES DE SEGUROS ha enfocado sus líneas operativas, dentro de un ambiente de identificación y administración del riesgo operativo inherente al objeto social de la empresa.

Para el efecto, ha desarrollado e implementado un Sistema de Administración de Riesgo Operativo (SARO), acorde con nuestra estructura, tamaño y objeto social, que nos permite identificar, medir, controlar y monitorear eficazmente este riesgo.

Cabe indicar, que atendiendo las normas que reglamentan el SARO, dicho sistema se encuentra conformado por elementos básicos, tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información, planes de continuidad del negocio y procesos capacitación e inducción, a través de los cuales se busca obtener una efectiva administración del riesgo operativo.

Todo lo anteriormente expresado, se encuentra contemplado en su respectivo Manual evaluado y aprobado por la Junta Directiva y el cual es de obligatoria y constante consulta por parte de nuestros empleados.

Por su parte, la Superintendencia Financiera emitió la Circular Externa No. 22 de 2007 y demás normas que reglamentan la materia, cuyo objetivos general consiste en que las entidades vigiladas implementen un Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT.

Por tal razón, FORTIUS S.A. CORREDORES DE SEGUROS diseñó e implementó su Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT, acorde con su infraestructura, volumen y complejidad de sus operaciones.

El SARLAFT se compone de dos fases a saber: la primera que corresponde a la prevención del riesgo y cuyo objetivo es evitar que se introduzcan al sistema financiero recursos provenientes de actividades relacionadas con el lavado de activos y/o de la financiación del terrorismo ,y la segunda, que corresponde al control y cuyo propósito consiste en detectar las operaciones que se pretendan realizar o se hayan realizado, para intentar dar apariencia de legalidad a operaciones vinculadas al LA/FT.

Ahora bien, es importante comprender que según la normatividad anteriormente mencionada, se entiende por riesgo de Lavado de Activos y Financiación del Terrorismo, **la posibilidad de pérdida o daño** que puede sufrir una entidad vigilada por su propensión

a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

El riesgo de LA/FT se materializa a través de los riesgos asociados, estos son: el legal, reputacional, operacional y de contagio, a los que se expone la entidad, con el consecuente efecto económico negativo que ello puede representar para su estabilidad financiera cuando es utilizada para tales actividades.

Resulta de suma importancia, informar que la administración de dicho riesgo es responsabilidad de todos y cada uno de los empleado de FORTIUS S.A. CORREDORES DE SEGUROS quienes en el desarrollo de sus labores llegaren a detectar una operación de carácter inusual, es decir, que se salga de los parámetros de normalidad, tienen la obligación de reportarlo inmediatamente al Oficial de Cumplimiento.

Finalmente, cabe resaltar que las pautas de conducta incorporadas en el Código de Ética así como los lineamientos procedimentales y políticas establecidas en el Manual SARLAFT son de obligatorio cumplimiento y la violación de sus disposiciones se considera falta grave y constituye justa causa de despido.

## **II. SUBSISTEMA DE CONTROL DE GESTIÓN**

Tiene como finalidad asegurar el control a la ejecución de los procesos de la entidad orientándola a la consecución de los resultados y productos necesarios para el cumplimiento de su misión.

### **1. ACTIVIDADES DE CONTROL**

Para el cumplimiento de los requisitos y aplicación de este componente FORTIUS S.A. CORREDORES DE SEGUROS I se apoya en las siguientes herramientas:

#### **1.1. POLÍTICAS DE OPERACIÓN.**

FORTIUS S.A. CORREDORES DE SEGUROS cuenta con una Junta Directiva que es la máxima autoridad. A ella le corresponde fijar las políticas que deben aplicarse para la ejecución de la función misional y administrativa de la empresa cuando la norma legal lo permite. Al efecto, se cuenta con un documento denominado Código de Buen Gobierno Corporativo

El Buen Gobierno Corporativo cada vez adquiere una mayor importancia entre las entidades, tanto en el ámbito nacional como internacional. Lo anterior, debido a que un

Buen Gobierno Corporativo genera confianza y en coadyuvancia con el Código de Ética, establecen unas reglas de actuación , homologables e intersubjetivas, que constituyen la plataforma ética para la realización de la gestión inherente al desarrollo del objeto social de las empresas.

Los procesos de globalización de la economía y de la sociedad coetáneamente con el desarrollo de los mercados financieros, el incremento de la complejidad de la gestión económico-financiera de las compañías, las nuevas morfologías del riesgo (riesgo operacional, riesgo corporativo, riesgo reputacional, entre otros ), han contribuido a que las empresas, siguiendo los lineamientos claramente trazados por la Superintendencia Financiera, hayan empezado a mostrar una mayor sensibilidad hacia el Buen Gobierno Corporativo y su codificación.

Asimismo, el Gobierno Corporativo provee un marco que define derechos y responsabilidades, dentro del cual interactúan los órganos de gobierno de una entidad entre los cuales se destacan el máximo órgano de dirección, la junta o consejo directivo, los representantes legales y demás administradores y el revisor fiscal y demás órganos de control.

En ese orden de ideas, un buen gobierno corporativo es aquel que facilita los instrumentos necesarios que garantice la existencia y puesta en práctica de mecanismos idóneos que permitan el balance entre la gestión de cada órgano y el control de la antedicha gestión, a través de un sistema de pesos y contrapesos, a efectos que las decisiones que se adopten en cada instancia se efectúen de conformidad con el mejor interés de la persona jurídica, sus accionistas y acreedores.

En desarrollo de lo anterior y en cumplimiento de la normatividad legal expedida por la Superintendencia Financiera FORTIUS S.A. CORREDORES DE SEGUROS adoptó su CÓDIGO DE BUEN GOBIERNO CORPORATIVO, aprobado por su Junta Directiva.

## **1.2. PROCEDIMIENTOS.**

Fortius Corredores de Seguros S.A. cuenta con unos procedimientos definidos dentro de su Sistema de Gestión de Calidad, que contiene:

Mapa de procesos
Tabla de contenido
Generalidades
Historia

Ubicación
Alcance y campo de acción de este manual
Exclusiones
Misión
Visión
Valores
Control del manual
Responsabilidad de la dirección
Compromiso de la dirección
Propiedad del cliente
Enfoque al cliente
Política de calidad
Planificación
Cambios al sistema de gestión de calidad
Divulgación de los cambios al sistema de gestión de calidad
Responsabilidad, autoridad y comunicación
Organigrama
Responsabilidad
Representante de la dirección
Comunicación interna
Revisión por la dirección
Interrelación de procesos
Matriz de procesos vs. Norma
Procesos
Matriz de responsabilidades norma iso 9001
Infraestructura
Ambiente de trabajo
Anexo de caracterizaciones

### 1.3. CONTROLES.

Los controles que aplican a los diferentes procesos se encuentran referenciados, de manera principal, en los mapas de riesgo asociados a los mismos. También hay otras observaciones o controles para la ejecución de actividades en los procedimientos y la definición de puntos de control en las caracterizaciones de proceso. En el diseño del Sistema de Medición de FORTIUS S.A. CORREDORES DE SEGUROS se cuenta con el Plan Operativo de Calidad que identifica algunas variables críticas asociadas a los procesos, junto con el tipo de seguimiento, el factor crítico de éxito y el registro que evidencia el cumplimiento de controles. De otra parte, al

tener implementado un Sistema de Gestión de Calidad están definidos los procedimientos y formatos necesarios para la implementación de acciones preventivas, correctivas y de mejora por proceso.

Adicionalmente, en los Manuales SARO y SARLAFT se establecen las políticas y los controles internos relacionados con los procesos, actividades y productos de cada una de ellas.

#### **1.4. INDICADORES.**

Para dar cumplimiento a los aspectos relacionados con medición, análisis y mejora de los procesos de la Sociedad, teniendo en cuenta como factores críticos de éxito la eficacia, la eficiencia y la efectividad se ha diseñado un sistema de medición conformado por unos indicadores de gestión por proceso que se elaboran y consolidan en el formato Ficha técnica indicador; de otra parte, a partir de la información generada por cada uno de los procesos de la entidad, se ha diseñado el Plan Operativo de Calidad cuya descripción se hizo en el numeral 1.3.

#### **1.5. POLÍTICAS DE CONTROL DE SEGURIDAD.**

##### **PRIMERA POLÍTICA: ACCESO A LA INFORMACIÓN.**

Todos los empleados, directivos y colaboradores que laboran para FORTIUS S.A. CORREDORES DE SEGUROS deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Sociedad, el Gerente responsable de generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus Servicios a la Entidad.

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Sociedad, la cual deberá realizarse de acuerdo con la importancia de la

información en la operación normal de la Entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

## **SEGUNDA POLÍTICA: SEGURIDAD DE LA INFORMACIÓN**

Todos los empleados, directivos y colaboradores que laboran para FORTIUS S.A. CORREDORES DE SEGUROS son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los empleados, directivos y colaboradores no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas.

Todo funcionario que utilice los Recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los empleados, directivos y colaboradores deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. Después de que el trabajador deja de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario, deben comprometerse a no utilizar, comercializar o divulgar los productos o a información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los empleados que detecten el mal uso de la información está en la obligación de reportar el hecho al Gerente General para que tome las medidas del caso.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

### **TERCERA POLÍTICA: SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS**

El sistema de correo electrónico, grupos de charla y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los colaboradores.

FORTIUS S.A. CORREDORES DE SEGUROS se reserva el derecho de acceder y develar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, la Sociedad realizará las auditorías respectivas directamente o a través de terceros.

Los empleados no deben utilizar versiones escaneadas de Firmas de terceras personas para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la entidad. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual.

Los empleados y colaboradores que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar al responsable de sistemas, no utilizar el computador y desconectarlo de la red.

### **CUARTA POLÍTICA: SEGURIDAD EN RECURSOS INFORMÁTICOS**

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece como deben ser utilizadas las claves de ingreso a los recursos informáticos.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles. También deben permitir que un rol de usuario administre el Administrador de usuarios.

Plan de auditoria: Hace referencia a las pistas o registros de los sucesos relativos a la operación.

Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas en la mayoría de los sistemas operacionales, bases de datos, aplicativos y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.

Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los empleados y colaboradores son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con las políticas internas de la empresa.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

## **QUINTA POLÍTICA. ALMACENAMIENTO Y RESPALDO**

Contamos con un sistema de backups de información el cual se realiza de forma incremental de manera semanal y una copia completa anual la cual se envía a custodia a Informática Consultoría de Servicios, este sistema permite realizar mensualmente una imagen del servidor la cual puede ser restaurada en caso de emergencia o desastre sobre cualquier máquina sin importar su tecnología en un tiempo aproximado de 48 horas, también contamos con el acceso a los archivos logs del sistema, los cuales son analizados por medio de informes y son creados y visualizados de acuerdo a las necesidades de consulta.

FORTIUS S.A. CORREDORES DE SEGUROS cuenta con un firewall central con todas sus características antivirus, antispam e intermediario para consulta fuera de la red.

Para la protección de ataques externos tenemos instalado un firewall (iptables), el cual nos permite filtrar el tráfico de paquetes que circulan por nuestra red por medio de la creación de reglas de filtrado de puertos y realizar tareas de net de origen y destino de los paquetes que viajan a través de nuestra red.

Dentro de los parámetros para la entrega de copias documentales se efectúa a través de memorandos suscritos por el jefe del área respectiva.

## **SEXTA POLÍTICA: SEGURIDAD FÍSICA**

FORTIUS S.A. CORREDORES DE SEGUROS cuenta con mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión para entrar al edificio.

Los visitantes de las oficinas de la empresa deben ser escoltados durante todo el tiempo por un empleado autorizado. Esto significa que se requiere de un escolta tan pronto como un visitante entra a un área y hasta que este mismo visitante sale del área controlada. Todos los visitantes requieren una escolta incluyendo clientes, antiguos empleados, miembros de la familia del trabajador.

Siempre que un trabajador se de cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Los centros de cómputo o áreas que la entidad considere críticas, deben ser lugares de

acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en un lugar visible.

En los centros de cómputo o áreas que la entidad considere críticas deberán existir elementos de control de incendio, inundación y alarmas.

Los centros de computo o áreas que la entidad considere críticas deberán estar demarcados con zonas de circulación y zonas restringidas.

Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles, módems y equipos de comunicación se deben registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva.

Los equipos de microcomputadores (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa.

Los particulares en general, entre ellos, los familiares de los empleados, no están autorizados para utilizar los recursos informáticos de la entidad.

#### **SÉPTIMA POLÍTICA: ESCRITORIOS LIMPIOS**

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, usb memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

#### **OCTAVA POLÍTICA: ADMINISTRACIÓN DE LA SEGURIDAD**

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

## **NOVENA POLÍTICA: CONTINGENCIAS**

La administración de la Entidad cuenta con Plan de Continuidad del Negocio y con Planes de Contingencia que permite a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación etc.

### **1.6 CONTROLES ADMINISTRATIVOS.**

- Análisis efectuados por la Alta Dirección. Revisiones periódicas sobre el desempeño de la Compañía en aspectos como presupuestos, pronósticos, periodos anteriores y competidores. Estos análisis se efectúan con el fin de analizar y monitorear el progreso de la entidad y adoptar los correctivos necesarios

-Comprobación de las operaciones en cuanto a su exactitud y conformidad con los procedimientos de la Compañía. Los actos y operaciones relevantes sólo pueden ser autorizados y ejecutados por funcionarios que actúen dentro del ámbito de sus competencias.

-Registro oportuno y adecuado de los actos y operaciones. Los actos y operaciones y las circunstancias que afectan a una Compañía deben registrarse inmediatamente y ser debidamente clasificados con el fin de garantizar su relevancia y utilidad.

-Dispositivos de seguridad para restringir el acceso a los activos y registros. El acceso a los recursos, activos, registros y comprobantes, debe estar protegido por mecanismos de seguridad y limitado a personas autorizadas.

-Indicadores de desempeño. La empresa cuenta con métodos de medición de desempeño que permitan la preparación de indicadores para su supervisión y evaluación.

-Segregación de funciones. Las responsabilidades se dividen entre diferentes funcionarios con el fin de minimizar el riesgo de error o de acciones inapropiadas. Las responsabilidades de autorizar, ejecutar, registrar y comprobar una operación, es conveniente que queden claramente diferenciadas y asignadas a personas diferentes.

- Confidencialidad. La información suministrada y toda la que llegue a conocer un empleado o contratista de FORTIUS S.A. CORREDORES DE SEGUROS en razón al desarrollo de sus funciones o cumplimiento del objeto contractual, tendrá el carácter de confidencial

y deberá ser mantenida bajo estricta reserva. Solamente se podrá revelar información confidencial a quienes se encuentren debidamente autorizados por el Gerente o quien este delegue o por mandato legal, so pena de incurrir en responsabilidad civil y penal de conformidad con lo prescrito por las normas que regulan la materia.

-Asignación de autoridad y responsabilidad. Cada funcionario debe conocer sus deberes y responsabilidades. Esto contribuye a desarrollar la iniciativa de los mismos y a solucionar los problemas, actuando siempre dentro de sus responsabilidades.

Asimismo, los funcionarios deben conocer los objetivos del área donde se desempeñan y cómo su función contribuye al logro de los objetivos generales. Esto es fundamental para lograr un compromiso mayor en las personas que se desempeñan en una Organización. Los funcionarios conocen los cometidos de la Organización y cómo su función contribuye al logro de los mismos.

Existe una clara asignación de responsabilidades, lo que implica que cada funcionario desarrolla sus propias iniciativas y actúa dentro de sus responsabilidades.

La asignación de responsabilidad está directamente vinculada con la asignación de autoridad. Los funcionarios que tienen asignadas responsabilidades deben rendir cuentas periódicamente por tal asignación

-Coordinación entre áreas. Las áreas que componen una Organización deben actuar coordinadamente entre ellas. Esto redundará en la consecución de los objetivos generales de la Organización.

Que exista coordinación implica que los funcionarios conozcan las consecuencias de sus acciones respecto a la Organización en su conjunto. Existe un flujo de información adecuado entre las distintas áreas.

Los funcionarios deben ser conscientes de cómo impactan sus acciones en la Organización en su conjunto.

- Documentación. La estructura de control interno y todas las transacciones y hecho significativos de la empresa deben estar claramente documentados y disponibles para su control. Para el efecto, existen documentos escritos acerca de la estructura de control interno de la Sociedad y los mismos se encuentran disponibles y al alcance de todos los funcionarios.

- Niveles definidos de autorización. Los hechos significativos de una organización deben ser autorizados y realizados por funcionarios que actúen dentro del ámbito de su competencia.

La Dirección deberá autorizar los hechos significativos a realizar y los funcionarios deberán ejecutar las tareas que les han sido asignadas, de acuerdo a los lineamientos establecidos.

Los procedimientos de control aseguran que las tareas son realizadas exclusivamente por los funcionarios que tienen asignada la tarea. La delegación de tareas se encuentra dentro de los lineamientos establecidos por la Dirección.

-Rotación del personal en las tareas sensibles. Las personas que llevan adelante tareas que puedan dar lugar a cometer irregularidades, deben ser regularmente rotadas en sus puestos. Se rota a los funcionarios en las tareas que pueden dar lugar a irregularidades (fraude, actos de corrupción).

### **1.7 CONTROLES AUTOMATIZADOS.**

- Cartera: Teniendo en cuenta que en los seguros no existen facturas porque son las mismas pólizas, como intermediarios emitimos una remisión cuyo número consecutivo lo arroja el sistema, permitiendo así la no duplicidad de dichas remisiones e información.

-Control de vencimientos

### **1.8 DIFUSIÓN DE LAS ACTIVIDADES DE CONTROL.**

Una vez que la Junta Directiva haya analizado y aprobado el Manual de Control Interno, se procederá a realizar una capacitación a todos los empleados de FORTIUS S.A. CORREDORES DE SEGUROS y se pondrá a disposición de ellos para su constante consulta.

Adicionalmente, dentro de los procesos de inducción de nuevos empleados se incluirá un capítulo específico de Control Interno.

Ahora bien, conscientes de la importancia del tema se tiene previsto efectuar una capacitación anual sobre el tema.

Finalmente, cuando se presente una relación contractual con terceros y éstos desempeñen funciones en FORTIUS S.A. CORREDORES DE SEGUROS se les dictará una capacitación sobre el Sistema de Control Interno.

## **2. INFORMACIÓN Y COMUNICACIÓN.**

Hay que identificar, recopilar y comunicar información pertinente en tiempo y forma que permitan cumplir a cada empleado con sus responsabilidades.

También deberá existir una comunicación eficaz en un sentido amplio, que fluya en todas las direcciones a través de todos los ámbitos de la empresa, de arriba hacia abajo y a la

inversa. La Dirección debe comunicar en forma clara las responsabilidades de cada empleado dentro del sistema de control interno implementado. Los funcionarios tienen que comprender cuál es su papel en el sistema de control interno y cómo las actividades individuales están relacionadas con el trabajo del resto. Asimismo, deben contar con los medios para comunicar la información significativa a los niveles superiores.

## **2.1 INFORMACIÓN.**

### **2.1.1. INFORMACIÓN INTERNA.**

Elemento de control que orienta la difusión de políticas y la información generada al interior de la empresa para una clara identificación de los objetivos, las estrategias, los planes, los programas, los proyectos y la gestión de operaciones hacia los cuales se enfoca el accionar de la entidad.

Se lleva a cabo a través de los siguientes elementos y acciones:

- *Intranet.* Es el canal interno de comunicación electrónica.
- *Manual.* Instrumento que contiene instrucciones detalladas y precisas para realizar de forma ordenada y sistemática los objetivos, políticas, atribuciones, funciones y procedimientos.
- *Circular.* Orden de autoridad competente dirigida a subalternos y obligados.
- *Informe periódico.* Contiene los datos a través de los cuales es posible evaluar cada cierto lapso de tiempo los resultados alcanzados, contra las metas establecidas.
- *Formato.* Facilita el cumplimiento de requisitos y obligaciones específicas que se deben contener en un acto de acuerdo con su naturaleza.
- *Plan.* Disposición detallada de una obra o acción y del modo de realizarla, expresados por escrito, sujetos a una autorización para ser ejecutado y controlado.
- *Capacitación.* La capacitación transmite información. En la implantación del Sistema de Control Interno constituye factor primordial e imprescindible la capacitación y

el entrenamiento, como paso inicial al nuevo esquema administrativo que exige la cultura del control interno.

La cultura del control exige que cada quien identifique sus responsabilidades en la empresa y las afronte con dedicación y esmero, buscando en todo momento la mejor calificación y perfeccionamiento en su cargo, como paso fundamental para el logro de la competitividad personal y empresarial.

### **2.1.2 INFORMACIÓN EXTERNA.**

Elemento de Control, conformado por el conjunto de datos de fuentes externas provenientes de las instancias con las cuales la organización está en permanente contacto, así como de las variables que no están en relación directa con la Entidad, pero que afectan su desempeño. FORTIUS S.A. CORREDORES DE SEGUROS ha identificado las siguientes fuentes de información externa: Bancos, Aseguradoras, Superfinanciera, Fasecolda y ACOAS.

### **2.1.3 FLEXIBILIDAD AL CAMBIO.**

El sistema de información debe ser revisado, a los efectos de comprobar que sigue siendo eficaz para la toma de decisiones a lo largo del tiempo.

Se debe constatar que la información elaborada sigue siendo relevante para los objetivos de la Organización.

Toda vez que el organismo cambie su estrategia, misión, política u objetivos, se debe analizar el impacto sobre su sistema de información.

El sistema de información es revisado a lo largo del tiempo, a los efectos de comprobar que sigue siendo eficaz para la toma de decisiones y que la información elaborada sigue siendo relevante para los objetivos de la Organización.

Se analiza el sistema de información cada vez que el organismo cambia su estrategia, misión, política u objetivos.

### **2.1.4 COMPROMISO DE LA ALTA DIRECCIÓN.**

Es imprescindible que la Dirección tome conciencia del grado de importancia del sistema de información organizacional, para poder cumplir con sus objetivos. Este compromiso se debe explicitar mediante la procura de recursos suficientes para poder mejorarlo y volverlo más eficaz.

La Dirección es consciente de la importancia del sistema de información organizacional y este compromiso se explicita por ejemplo mediante la procura de recursos suficientes para poder mejorarlo y volverlo más eficaz.

### **2.1.5 SISTEMAS DE INFORMACIÓN.**

En materia de Sistemas de Información y desde el punto de vista informático se utilizan algunos sistemas cuyo desarrollo es interno como son Alfasis Visual Net, que comprende los siguientes procesos:

- **Cartera General de Seguros:** Control total de la producción, recaudos, cuadros diarios, pólizas, vencimientos, cartera general e individual, banco de clientes. Permite además la generación automática de las planillas de pago o cortes de cuenta, manejo de observaciones, generación automática de la información de cada factura de venta, impresión de las facturas sobre documentos preimpresos.

#### **- Características:**

- ✓ Control de producción con generación del cobro al cliente.
- ✓ Consultas e informes múltiples (Más de 700 opciones combinadas)
- ✓ Informe de producción diaria
- ✓ Control de recaudos con impresión de 9 tipos básicos de recibos diferentes(creados por Alfasis)
- ✓ Control independiente de consecutivos en cada tipo de recaudo
- ✓ El usuario puede crear nuevos tipos de modo abierto
- ✓ Manejo de otros recaudos por cada tipo como Anticipos, Mayores y menores valores, reintegros y muchos más conceptos que no afectan primas pero si caja y contabilidad
- ✓ Cuadre diario de recaudos y de caja
- ✓ Control y facturación de comisiones, manejo de planillas y cortes de cuentas, manual y automático
- ✓ Facturación de venta por conceptos tanto de comisiones como de otros rubros diferentes.
- ✓ Manejo de impuestos abierto con rangos de fechas
- ✓ Informes de cartera con edad de mora
- ✓ Cartas de estado de cuentas
- ✓ Control de cartera provisionada y conciliación mensual de la recuperación de cartera
- ✓ Control de vencimientos por muchas opciones
- ✓ Informes estadísticos de producción, recaudos y cartera.
- ✓ Módulo de administración del sistema.
- ✓ Control de auditoría, a las claves, recaudos y producción.
- ✓ Claves de acceso personalizadas.
- ✓ Control de recaudos de modo multiusuario

- ✓ Control comisiones por el sistema de conciliación con las aseguradoras
- ✓ Consulta del estado de cuenta de la póliza
- ✓ Reclasificación de remisiones, recaudos, pólizas y clientes
- ✓ Anulación automática y manual de remisiones y recaudos
- ✓ Control de auditoría histórica en los movimientos hechos a la base de datos

### **2.1.6 INFORMACIÓN PRIVILEGIADA.**

En concordancia con lo expresado en el Código de Ética de la Sociedad, el uso de la información privilegiada debe ceñirse a las limitaciones de revelación establecidas por la Entidad. Se prohíbe expresamente a los empleados que tienen acceso a dicha información en razón a sus cargos, revelarla en tiempo, espacio y lugar que no corresponda a las limitaciones antes mencionadas.

La información interna debe ser protegida y no está autorizada la entrega de ningún tipo de reportes, bases de clientes, planes estratégicos, software, etc., que no hayan sido requeridos por las autoridades judiciales, administrativas y de control, dentro de la órbita de su competencia y cumpliendo con los procedimientos oficialmente establecidos para la formulación de requerimientos de información, y con las reglamentaciones internas de verificación de la autenticidad de las personas que solicitan, y, la ejecución del procedimiento establecido para esta finalidad.

No se debe comunicar información a ninguna persona fuera de la Sociedad, exceptuando los requeridos por las autoridades.

### **2.1.7. CALIDAD DE LA INFORMACIÓN.**

La información disponible en la entidad debe cumplir con los atributos de: contenido útil, oportuna, comprensible, completa y exacta, y además concisa. Dichos atributos hacen imprescindible su confiabilidad.

- Útil: Es decir que supla o apunte a las necesidades
- Oportuna: Que se genere en el momento preciso y requerido y además sea fiable.
- Comprensible: Es decir, que sea inteligible para todo aquel a quien vaya dirigida. Debe presentarse en forma clara y en un lenguaje de fácil comprensión, que permita así mismo una adecuada interpretación.

- Completa y exacta: Debe contener todos los datos y aspectos necesarios sobre lo que intenta comunicar, ha de ser íntegra y exacta
- Concisa: No debe estar sobresaturada de ideas o sobrecargada de datos secundarios de poca relevancia, sino que debe destacar la información más importante en forma clara y concisa. Se requiere orden de la información que presente y exponga en primer lugar lo esencial para continuar con lo menos significativo.

Es deber de la Alta Gerencia el control interno y esforzarse por obtener un grado adecuado de cumplimiento de cada uno de los atributos mencionados.

Ahora bien, la información procesada tendrá que ser comunicada al usuario, interno y externo que la necesite, en forma y en el plazo requerido sin perder el principio de confidencialidad.

La frecuencia de la comunicación será continua y estará supeditada a los siguientes factores externos, entre otros:

- Modificación del objeto social de la empresa
- Modificaciones a las regulaciones por parte de entes externos de control
- Personal nuevo
- Cambio en los sistemas de información
- Pueden introducirse nuevas tecnologías en los procesos de producción o en los sistemas de procesamiento de información.
- Recomendaciones de entes externos de control, revisoría fiscal o auditoría interna.

Los responsables y destinatarios de la comunicación son todos los empleados, colaboradores así como la Alta Dirección, Comité de Auditoría, Comité de Riesgos y Junta Directiva.

## **2.2 COMUNICACIÓN.**

**2.2.1. COMPONENTE COMUNICACIÓN PÚBLICA.** Conjunto de Elementos de Control, que apoya la construcción de visión compartida, y el perfeccionamiento de las relaciones humanas de la Sociedad con sus grupos de interés internos y externos, facilitando el cumplimiento de sus objetivos institucionales y sociales.

**2.2.1.1. COMUNICACIÓN ORGANIZACIONAL.** Elemento de Control, que orienta la difusión de políticas y la información generada al interior de la Sociedad para una clara identificación de los objetivos, las estrategias, los planes, los programas, los proyectos y la

gestión de operaciones hacia los cuales se enfoca el accionar de la Entidad.

**2.2.1.2. COMUNICACIÓN INFORMATIVA.** Elemento de Control, que garantiza la difusión de información de la Entidad sobre su funcionamiento, gestión y resultados en forma amplia y transparente hacia los diferentes grupos de interés y externos.

**2.2.13. MEDIOS DE COMUNICACIÓN.** Elemento de Control que se constituye por el conjunto de procedimientos, métodos, recursos e instrumentos utilizados por la Entidad, para garantizar la divulgación, circulación amplia y focalizada de la información y de su sentido, hacia los diferentes grupos de interés.

Los responsables de la comunicación tanto interna como externa son el Gerente Administrativo y Financiero y el Gerente General.

### **III. SUBSISTEMA DEL CONTROL DE EVALUACIÓN**

Este subsistema se orienta principalmente a los mecanismos de medición, evaluación y verificación que permitan demostrar que el Sistema de Control Interno de la entidad es eficaz, eficiente y efectivo. Ante las desviaciones que se puedan presentar proporciona las herramientas para subsanar las deficiencias encontradas con el fin de alcanzar los estándares y metas propuestos acordes con la función legal asignada a la entidad.

#### **1. AUTOEVALUACIÓN DEL CONTROL.**

Para el cumplimiento de los requisitos y aplicación de este componente la Sociedad se apoya en las siguientes herramientas:

Los responsables de los diferentes procesos definidos por FORTIUS S.A. CORREDORES DE SEGUROS hacen seguimiento a las actividades que ejecutan de manera periódica. Se utilizan las diferentes herramientas de seguimiento que contempla el Sistema de Gestión de Calidad, como son la revisión del SGI por la Dirección; el análisis de datos; la medición periódica a los procesos para determinar el cumplimiento de los factores críticos; la formulación de correcciones de producto no conforme, de acciones preventivas, correctivas o de mejora. La Junta Directiva hace un seguimiento mensual a las actividades del FORTIUS S.A. CORREDORES DE SEGUROS a partir de los temas que se presentan a la misma.

#### **2. AUTOEVALUACIÓN A LA GESTIÓN.**

A partir de la implementación el Sistema de Gestión de Calidad FORTIUS S.A.

CORREDORES DE SEGUROS definió un Sistema de Medición de sus procesos basado en los factores críticos de eficacia, eficiencia y efectividad para lo cual se utilizan los indicadores de gestión y el Plan Operativo de Calidad que complementa los indicadores. Con estas dos herramientas se garantiza que cada proceso tiene al menos una medición respecto a cada uno de los factores críticos de éxito. Semestralmente y con miras a la evaluación del Sistema de Medición dentro de la revisión gerencial del Sistema de Gestión de Calidad se consolidan los resultados que reporta cada proceso y se analiza el cumplimiento de metas y la corrección de desviaciones que puedan presentar.

### **3. MONITOREO.**

Le corresponde a la alta dirección de FORTIUS S.A. CORREDORES DE SEGUROS garantizar la existencia de una estructura de control interno idónea y eficiente, así como de mecanismos que permitan su revisión y actualización periódica, el cual se establece cada seis (6) meses. De esta forma, se establecen procedimientos de evaluación de las actividades de control de los sistemas, para determinar su eficacia e identificar aquellos aspectos susceptibles de mejoramiento.

Con este propósito, FORTIUS S.A. CORREDORES DE SEGUROS implementó controles automáticos o alarmas tanto en los sistemas automatizados como en manuales, así como adoptar indicadores de gestión y desempeño que contribuyan a monitorear el SCI. Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión que se adopten deben ser comunicadas a efectos de que se adopten las medidas de ajuste correspondientes. Según el impacto de las deficiencias y la materialidad del asunto, los destinatarios de la información pueden ser tanto las personas responsables de tomar acciones correctivas sobre la función o actividad implicada, como la Junta Directiva de la Compañía.

Igualmente, le corresponde a la auditoría interna realizar evaluaciones periódicas puntuales.

### **4. EVALUACIONES INDEPENDIENTES.**

FORTIUS S.A. CORREDORES DE SEGUROS efectuará evaluaciones independientes sobre la efectividad del SCI, con el objetivo de adoptar medidas correctivas y de mejoramiento e independizar el control que se realiza al interior de la empresa.

De acuerdo con lo establecido por la Superintendencia Financiera, estas evaluaciones se efectuarán por parte del AUDITOR INTERNO Y EL REVISOR FISCAL de FORTIUS S.A.

CORREDORES DE SEGUROS, sin perjuicio que, como práctica de buen gobierno corporativo, la administración opte por efectuar auditorías externas.

Para revisar la efectividad del SCI estos controles y auditorías internas y externas deben contribuir a que los funcionarios mejoren los procesos, optimicen recursos y renueven su compromiso institucional. De igual forma, a través de ellos deben definirse y ponerse en práctica planes de mejoramiento al SCI.

Las debilidades resultado de esta evaluación y sus recomendaciones de mejoramiento, deben ser reportadas de manera ascendente, informando sobre asuntos representativos de manera inmediata al Comité de Auditoría, y haciéndoles seguimiento.

## **CAPITULO TERCERO: RESPONSABILIDADES DENTRO DEL SISTEMA DE CONTROL INTERNO**

### **1.ÓRGANOS INTERNOS**

#### **1.1. JUNTA DIRECTIVA.**

Los miembros de las juntas directivas como principales gestores del gobierno corporativo, deben realizar su gestión con profesionalismo, integridad, competencia e independencia, dedicándole el tiempo necesario. Así mismo deben ser transparentes en su gestión, procurando tener un buen conocimiento de los riesgos que involucran los productos que ofrece la empresa; evaluar con profundidad los riesgos asociados a los instrumentos de inversión que ésta utiliza y apoyar la labor de los órganos de fiscalización y control.

De la junta directiva debe provenir la autoridad, orientación y vigilancia al personal directivo superior, de manera que sus miembros deberán contar con experiencia y conocimientos adecuados acerca de las actividades, los objetivos y la estructura de la respectiva entidad.

##### **1.1.1 FUNCIONES GENERALES.**

Sin perjuicio de las obligaciones especiales asignadas a este órgano en otras disposiciones legales, estatutarias o en reglamentos, en materia de control interno, en cumplimiento de los deberes que le señala el artículo 23 de la Ley 222 de 1995, la junta directiva es la instancia responsable de:

- i. Participar activamente en la planeación estratégica de la sociedad, aprobarla y efectuar seguimiento, para determinar las necesidades de redireccionamiento estratégico cuando se requiera.
- ii. Definir y aprobar las estrategias y políticas generales relacionadas con el SCI, con fundamento en las recomendaciones del Comité de Auditoría.
- iii. Establecer mecanismos de evaluación formal a la gestión de los administradores y sistemas de remuneración e indemnización atados al cumplimiento de objetivos a largo plazo y los niveles de riesgo.
- iv. Definir claras líneas de responsabilidad y rendición de cuentas a través de la organización.
- v. Analizar el proceso de gestión de riesgo existente y adoptar las medidas necesarias para fortalecerlo en aquellos aspectos que así lo requieran.
- vi. Designar a los directivos de las áreas encargadas del SCI y de la gestión de riesgos, salvo que el régimen aplicable a la respectiva entidad o sus estatutos establezcan una instancia diferente para el efecto.
- vii. Adoptar las medidas necesarias para garantizar la independencia del auditor interno y hacer seguimiento a su cumplimiento.
- viii. Conocer los informes relevantes respecto del SCI que sean presentados por los diferentes órganos de control o supervisión e impartir las órdenes necesarias para que se adopten las recomendaciones y correctivos a que haya lugar.
- ix. Solicitar y estudiar, con la debida anticipación, toda la información relevante que requiera para contar con la ilustración suficiente para adoptar responsablemente las decisiones que le corresponden y solicitar asesoría experta, cuando sea necesario.
- x. Requerir las aclaraciones y formular las objeciones que considere pertinentes respecto a los asuntos que se someten a su consideración.
- xi. Aprobar los recursos suficientes para que el SCI cumpla sus objetivos.
- xii. Efectuar seguimiento en sus reuniones ordinarias a través de informes periódicos que le presente el Comité de Auditoría, sobre la gestión de riesgos en la entidad y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada seis (6) meses, o con una frecuencia mayor si así resulta procedente.
- xiii. Evaluar las recomendaciones relevantes sobre el SCI que formulen el Comité de Auditoría y los otros órganos de control interno y externos, adoptar las medidas pertinentes y hacer seguimiento a su cumplimiento.
- xiv. Analizar los informes que presente el oficial de cumplimiento respecto de las labores realizadas para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, evaluar la efectividad de los controles implementados y de las recomendaciones formuladas para su mejoramiento.
- xv. Evaluar los estados financieros, con sus notas, antes de que sean presentados a la asamblea de accionistas o máximo órgano social, teniendo en cuenta los informes y recomendaciones que le presente el Comité de Auditoría.
- xvi. Presentar al final de cada ejercicio a la Asamblea General de Accionistas, junta de socios o máximo órgano social un informe sobre el resultado de la evaluación del SCI y sus actuaciones sobre el particular.

Todas las decisiones y actuaciones que se produzcan en desarrollo de las atribuciones antes mencionadas deberán constar por escrito en el acta de la reunión respectiva y estar debidamente motivadas. La junta directiva u órgano equivalente determinará la información que deba ser divulgada a los diferentes niveles de la organización, de acuerdo con lo que considere pertinente.

## **1.2 COMITÉ DE AUDITORÍA.**

El Comité de Auditoría de la Junta Directiva de FORTIUS S.A. CORREDORES DE SEGUROS, es el máximo órgano de control de la Sociedad encargado de la vigilancia de la gestión y la efectividad del sistema de control interno. Es de carácter permanente y se rige por su Reglamento Interno y por la legislación que le resulte aplicable.

El Comité de Auditoría tiene como objetivo primordial apoyar a la Junta Directiva en la supervisión de la efectividad de los sistemas contables y financieros de la Sociedad y vigilar que los procedimientos de control interno se ajusten a las necesidades, objetivos, metas y estrategias financieras determinadas por OPCIONES BURSÁTILES DE COLOMBIA S.A.

Su reglamentación fue aprobado por Junta Directiva el 29 de julio de 2009.

## **1.3 REPRESENTANTE LEGAL.**

Sin perjuicio de las obligaciones especiales asignadas al representante legal en otras disposiciones legales, estatutarias o en reglamentos, en materia de control interno el representante legal es la instancia responsable de:

- i. Implementar las estrategias y políticas aprobadas por la junta directiva en relación con el SCI.
- ii. Comunicar las políticas y decisiones adoptadas por la junta directiva u órgano equivalente a todos y cada uno de los funcionarios dentro de la organización, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deberán procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los lineamientos por ella establecidos.
- iii. Poner en funcionamiento la estructura, procedimientos y metodologías inherentes al SCI, en desarrollo de las directrices impartidas por la junta directiva, garantizando una adecuada segregación de funciones y asignación de responsabilidades.
- iv. Implementar los diferentes informes, protocolos de comunicación, sistemas de información y demás determinaciones de la junta relacionada con SCI.

- v. Fijar los lineamientos tendientes a crear la cultura organizacional de control, mediante la definición y puesta en práctica de las políticas y los controles suficientes, la divulgación de las normas éticas y de integridad dentro de la institución y la definición y aprobación de canales de comunicación, de tal forma que el personal de todos los niveles comprenda la importancia del control interno e identifique su responsabilidad frente al mismo.
- vi. Realizar revisiones periódicas a los manuales y códigos de ética y de gobierno corporativo.
- vii. Proporcionar a los órganos de control internos y externos, toda la información que requieran para el desarrollo de su labor.
- viii. Proporcionar los recursos que se requieran para el adecuado funcionamiento del SCI, de conformidad con lo autorizado por la junta directiva u órgano equivalente.
- ix. Velar porque se de estricto cumplimiento de los niveles de autorización, cupos u otros límites o controles establecidos en las diferentes actividades realizadas por la entidad, incluyendo las adelantadas con administradores, miembros de junta, matriz, subordinadas y demás vinculados económicos.
- x. Certificar que los estados financieros y otros informes relevantes para el público no contienen vicios, imprecisiones o errores que impidan conocer la verdadera situación patrimonial o las operaciones de la correspondiente entidad.
- xi. Establecer y mantener adecuados sistemas de revelación y control de la información financiera, para lo cual deberán diseñar procedimientos de control y revelación para que la información financiera sea presentada en forma adecuada.
- xii. Establecer mecanismos para la recepción de denuncias (líneas telefónicas, buzones especiales en el sitio Web, entre otros) que faciliten a quienes detecten eventuales irregularidades ponerlas en conocimiento de los órganos competentes de la entidad.
- xiii. Definir políticas y un programa antifraude, para mitigar los riesgos de una defraudación en la entidad.
- xiv. Verificar la operatividad de los controles establecidos al interior de la entidad.
- xv. Incluir en su informe de gestión un aparte independiente en el que se de a conocer al máximo órgano social la evaluación sobre el desempeño del SCI en cada uno de los elementos señalados en el numeral 7.5 de la Circular Externa No. 38 de 2009. En el caso de los grupos empresariales, la evaluación sobre la eficacia del SCI que expida el representante legal de la matriz debe incluir también a las entidades subordinadas (filiales o subsidiarias).

En general el representante legal es el responsable de dirigir la implementación de los procedimientos de control y revelación, verificar su operatividad al interior de la correspondiente entidad y su adecuado funcionamiento, para lo cual debe demostrar la ejecución de los controles que le corresponden.

El representante legal debe dejar constancia documental de sus actuaciones en esta materia, mediante memorandos, cartas, actas de reuniones o los documentos que resulten pertinentes para el efecto.

Adicionalmente, debe mantener a disposición del auditor interno, el revisor fiscal y demás órganos de supervisión o control los soportes necesarios para acreditar la correcta implementación del SCI, en sus diferentes elementos, procesos y procedimientos.

## **2. ÓRGANOS EXTERNOS.**

### **2.1 AUDITORIA EXTERNA.**

La auditoría es una actividad que se fundamenta en criterios de independencia y objetividad de aseguramiento<sup>1</sup> y consulta<sup>2</sup>, concebida para agregar valor y mejorar las operaciones de una organización, ayudándola a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

#### **2.1.1 NORMAS PARA EL EJERCICIO DE LA AUDITORÍA.**

En el desarrollo de la actividad de Auditoría o su equivalente, deberá darse aplicación, entre otras a las siguientes normas:

##### **2.1.1.1. NORMAS SOBRE ATRIBUTOS.**

- Propósito, Autoridad y Responsabilidad

El propósito, la autoridad y la responsabilidad de la actividad de Auditoría deben estar formalmente definidos en un estatuto (documento) debidamente aprobado por la junta directiva u órgano equivalente, en donde quede establecido un acuerdo con la alta dirección de la entidad respecto de la función y responsabilidad de la actividad de

---

<sup>1</sup> Se entiende por aseguramiento el examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una organización. Por ejemplo trabajos financieros, de desempeño, de cumplimiento y de seguridad de sistemas. (Texto tomado del documento “Normas Internacionales para el ejercicio profesional de la Auditoría Interna” – Instituto de Auditores Internos de Colombia).

<sup>2</sup> Se denomina Consultoría, a las actividades de asesoramiento y servicios relacionados, proporcionadas a los clientes, cuya naturaleza y alcance estén relacionados con los mismos y estén dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos y control, de una organización sin que el auditor interno asuma responsabilidades de gestión.

Auditoría, su posición dentro de la organización, la autorización al auditor para que tenga acceso a los registros, al personal y a los bienes relevantes para la ejecución de los trabajos y la definición del ámbito de actuación de las actividades de auditoría interna.

➤ **Independencia y Objetividad**

La actividad de auditoría interna debe ser independiente, y los auditores internos deben ser objetivos en el cumplimiento de sus trabajos a través de una actitud imparcial y neutral, buscando siempre evitar conflictos de intereses. Dentro de este contexto, como una práctica de buen gobierno corporativo, se considera conveniente que el auditor o quien haga sus veces sea nombrado por la junta directiva u órgano equivalente.

Si la independencia u objetividad en cualquier momento se viese comprometida de hecho o en apariencia, los detalles del impedimento deben darse a conocer por escrito a la junta directiva u órgano equivalente.

➤ **Pericia y debido cuidado profesional.**

Tanto el auditor como su equipo de trabajo deben reunir los conocimientos, las aptitudes y las competencias necesarias para cumplir con sus responsabilidades. El auditor debe contar con asesoría y asistencia competente para aquellas áreas especializadas respecto de las cuales él o su personal no cuenten con los conocimientos necesarios.

Los auditores internos deben cumplir su trabajo con el cuidado y la pericia que se esperan de un especialista razonablemente prudente y competente.

➤ **Programa de Aseguramiento de Calidad y Cumplimiento**

El auditor debe desarrollar y mantener un programa de aseguramiento de calidad y mejora que cubra todos los aspectos de la actividad de auditoría interna y revise continuamente su eficacia. Este programa incluye evaluaciones de calidad externas e internas periódicas y supervisión interna continua. Cada parte del programa debe estar diseñada para ayudar a la actividad de auditoría interna a añadir valor y a mejorar las operaciones de la organización y a proporcionar aseguramiento de que la actividad de

auditoría interna cumple con las normas aplicables a esta actividad y el Código de Ética de los auditores.

Si bien la actividad de auditoría externa debe lograr el cumplimiento total de las normas de general aceptación para esta actividad, puede haber casos en los cuales esta meta no se logre. Cuando el incumplimiento afecte el alcance general o el funcionamiento de la actividad de auditoría interna, debe declararse esta situación a la alta dirección y al consejo o junta directiva u órgano competente, informándoles los obstáculos que se presentaron para generar esta situación.

### **2.1.1.2. NORMAS SOBRE DESEMPEÑO.**

#### ➤ **Administración de la Actividad de Auditoría Externa**

El auditor interno debe gestionar efectivamente la actividad que desarrolla para asegurar que su trabajo está generando valor agregado a la organización, para lo cual debe ejercer entre otras, las siguientes actividades:

- i. **Planificación.** El Auditor debe establecer, por lo menos anualmente, planes basados en los riesgos que afecten el logro de los objetivos de la organización, a fin de determinar las prioridades de la actividad de auditoría interna, incluyendo entre otros, el derivado de las operaciones y relaciones con otras entidades del mismo grupo económico.
- ii. **Comunicación y Aprobación.** El Auditor debe comunicar los planes y requerimientos de recursos de la actividad de auditoría interna, incluyendo los cambios provisorios significativos al Comité de Auditoría y al representante legal, para la adecuada revisión y aprobación. El Auditor Interno también debe comunicar el impacto de cualquier limitación de recursos.
- iii. **Administración de Recursos.** Determinar los recursos que necesita para el adecuado ejercicio de su labor y solicitarlos a la junta directiva u órgano equivalente.

- iv. **Políticas y Procedimientos.** Establecer políticas y procedimientos para guiar la actividad de auditoría interna.
- v. **Coordinación.** El Auditor Interno debe compartir información y coordinar actividades con los otros órganos de control para lograr una cobertura adecuada y minimizar la duplicación de esfuerzos.
- vi. **Informes.** Los informes emitidos por el Auditor Interno deben ser precisos, objetivos, claros, constructivos, completos y oportunos. Igualmente, deberán estar debidamente soportados en evidencias suficientes y realizar seguimiento a las acciones tomadas por la administración frente a estas comunicaciones.

#### **2.1.1.3. NATURALEZA DEL TRABAJO.**

La actividad de auditoría externa debe evaluar y contribuir a la mejora de los procesos de gestión de riesgos, control y gobierno de la entidad, utilizando un enfoque sistemático y disciplinado, así:

- i. **Gestión de Riesgos:** El auditor interno debe evaluar la eficacia del sistema de gestión de riesgos de la organización y las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización.
- ii. **Sistema de Control Interno:** La actividad de auditoría externa debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua, sin perjuicio de la autoevaluación y el autocontrol que corresponden a cada funcionario de la organización, de conformidad con los principios señalados en el subnumeral 7.4 de la C.E. No 038 de 2009..
- iii. **Gobierno Corporativo:** La actividad de auditoría externa debe evaluar y hacer las recomendaciones apropiadas para mejorar el proceso de gobierno corporativo, para lo cual debe evaluar el diseño, implantación y eficacia de los objetivos, programas y actividades de la organización.

#### **2.1.1.3. PLANIFICACIÓN DEL TRABAJO.**

Los auditores externos deben elaborar y registrar un plan para cada trabajo, que incluya el alcance, los objetivos, el tiempo y la asignación de recursos.

#### **2.1.1.4. DESEMPEÑO DEL TRABAJO.**

Los auditores deben identificar, analizar, evaluar y registrar suficiente información, que resulte confiable y relevante, de manera tal que les permita cumplir con los objetivos del trabajo.

Adicionalmente deben establecer requisitos de custodia para los registros del trabajo que sean consistentes con las políticas de la organización en este sentido, y realizar una adecuada supervisión sobre la calidad del trabajo realizado por los integrantes de su equipo.

Los auditores deben ser proactivos al analizar, monitorear, indagar, cuestionar, verificar y en general al realizar las actividades propias del aseguramiento, sin limitarse a una simple comprobación de requisitos formales.

#### **2.1.1.5. COMUNICACIÓN DE RESULTADOS.**

Los auditores deben comunicar los resultados de su trabajo, en forma precisa, objetiva, clara, concisa, constructiva, completa y oportuna.

Si una comunicación contiene un error u omisión significativos, debe corregirse y enviarse nuevamente a todas las partes que recibieron la comunicación original.

Por lo menos al cierre de cada ejercicio, el auditor o quien haga sus veces deberá presentar un informe de su gestión y su evaluación sobre la eficacia del sistema de control interno, incluyendo todos sus elementos. Dicho informe debe contener por lo menos lo siguiente:

- i. Título.

- ii. Identificación de los temas, procesos, áreas o materias objeto del examen, el periodo y criterios de evaluación y la responsabilidad sobre la información utilizada, precisando que la responsabilidad del auditor interno es señalar los hallazgos y recomendaciones sobre los sistemas de control interno y de administración de riesgos.
- iii. Especificación respecto a que las siguientes evaluaciones se realizaron de acuerdo con la regulación, las políticas definidas por la junta directiva u órgano equivalente y mejores prácticas de auditoría sobre el particular:
  - a. Evaluación de la confiabilidad de los sistemas de información contable, financiera y administrativa.
  - b. Evaluación sobre el funcionamiento y confiabilidad del sistema de control interno.
  - c. Evaluación de la calidad y adecuación de los sistemas establecidos para garantizar el cumplimiento con las leyes, regulaciones, políticas y procedimientos.
  - d. Evaluación de la calidad y adecuación de otros sistemas y procedimientos, análisis crítico de la estructura organizacional y evaluación de la adecuación de los métodos y recursos en relación con su distribución.
- iv. Los resultados de la evaluación realizada respecto a la existencia, funcionamiento, efectividad, eficacia, confiabilidad y razonabilidad de los sistemas de control interno y de riesgos.
- v. Una declaración de la forma en que fueron obtenidas sus evidencias, indicando cuál fue el soporte técnico de sus conclusiones.
- vi. Mencionar las limitaciones que encontraron para realizar sus evaluaciones, para tener acceso a información u otros eventos que puedan afectar el resultado de las pruebas realizadas y las conclusiones.
- vii. Relación de las recomendaciones formuladas sobre deficiencias materiales detectadas, mencionando los criterios generales que se tuvieron en cuenta para determinar la importancia de las mismas.
- viii. Resultados del seguimiento a la implementación de las recomendaciones formuladas en informes anteriores.
- ix. Identificación, nombre y firma, ciudad y fecha de elaboración.

Lo anterior sin perjuicio de informes extraordinarios que el auditor interno deba presentar cuando detecte irregularidades graves que ameriten la atención inmediata de los órganos competentes.

#### **2.1.1.6 SUPERVISIÓN.**

El auditor debe establecer un proceso de seguimiento, para supervisar y verificar que las acciones de la dirección hayan sido efectivamente implantadas o que la alta dirección ha aceptado el riesgo de no tomar ninguna acción.

Cuando el auditor considere que la alta dirección ha aceptado un nivel de riesgo residual que en su concepto pueda ser inaceptable para la organización, debe discutir esta cuestión con el representante legal. Si la decisión referida al riesgo residual no se resuelve, el auditor interno y el representante legal deben informar esta situación a la Junta Directiva o quien haga sus veces, para que adopte la decisión pertinente.

#### **2.1.1.7. FUNCIONES.**

Las principales funciones del auditor o de quien tenga a su cargo responsabilidades equivalentes son las siguientes, sin perjuicio de la responsabilidad de autocontrol que corresponde a todos los funcionarios de la organización según los principios señalados en el numeral 7.4 del presente capítulo:

- i. Elaborar el plan anual de auditoría antes de finalizar el año anterior y darle estricto cumplimiento. En el caso de entidades subordinadas para las cuales la matriz (sea nacional o extranjera) establezca los lineamientos generales del plan de auditoría, deberá velar porque éstos se ajusten a las disposiciones vigentes en Colombia para la respectiva entidad, así como a las características propias de su entorno, y realizar los ajustes pertinentes de acuerdo al tipo de negocio y a la normatividad aplicable.
- ii. Someter a consideración del comité de auditoría el presupuesto anual de funcionamiento del área de auditoría interna.
- iii. Realizar una evaluación detallada de la efectividad y adecuación del SCI, en las áreas y procesos de la organización que resulten relevantes, abarcando entre otros aspectos los relacionados con la administración de riesgos de la entidad, los sistemas de información, administrativos, financieros y tecnológicos, incluyendo los sistemas electrónicos de información y los servicios electrónicos.
- iv. Evaluar tanto las transacciones como los procedimientos de control involucrados en los diferentes procesos o actividades de la entidad, en aquellos aspectos que considere relevantes.
- v. Revisar los procedimientos adoptados por la administración para garantizar el cumplimiento con los requerimientos legales y regulatorios, códigos internos y la implementación de políticas y procedimientos.
- vi. Verificar en sus auditorías la eficacia de los procedimientos adoptados por la administración para asegurar la confiabilidad y oportunidad de los reportes a esta Superintendencia y otros entes de control.
- vii. Contribuir a la mejora de los procesos de gestión de riesgos, control y gobierno de la entidad, utilizando un enfoque sistemático y disciplinado.

- viii. Adelantar las investigaciones especiales que considere pertinentes, dentro del ámbito de su competencia, para lo cual deberá contar con la colaboración de expertos en aquellos temas en que se requiera.
- ix. Presentar comunicaciones e informes periódicos al comité de auditoría o a la junta directiva o a la administración cuando lo estime conveniente, sobre el resultado del ejercicio de sus funciones.
- x. Hacer seguimiento a los controles establecidos por la entidad, mediante la revisión de la información contable y financiera.
- xi. Evaluar los problemas encontrados y solicitar las acciones de mejoramiento correspondientes.
- xii. Presentar a la Junta Directiva, por lo menos al cierre de cada ejercicio, un informe acerca de los resultados de su labor, incluyendo, entre otros aspectos, las deficiencias detectadas en el SCI.

### **2.3 REVISOR FISCAL.**

De conformidad con lo previsto en el numeral 4.4.2.2 de la Circular Externa 054 de 2008, incorporada en el Título I, Capítulo III, numeral 4 de la presente circular, el revisor fiscal de la entidad debe valorar los sistemas de control interno y administración de riesgos implementados por las entidades a fin de emitir la opinión a la que se refiere y en los términos consignados en el numeral 4.2.8 *ibídem*.

### **CAPÍTULO CUARTO: PLANES DE MEJORAMIENTO.**

Para el cumplimiento de los requisitos y aplicación de este componente FORTIUS S.A. CORREDORES DE SEGUROS se apoya en las siguientes herramientas:

#### **1. PLAN DE MEJORAMIENTO INSTITUCIONAL.**

Constituye el Plan de orden corporativo que integra las acciones de mejoramiento que en su conjunto, FORTIUS S.A. CORREDORES DE SEGUROS debe adelantar para fortalecer su desempeño institucional y cumplir con su función, misión y objetivos en los términos de la normatividad legal vigente y los compromisos adquiridos con sus grupos de interés.

Su contenido debe contemplar el análisis de las variaciones presentadas entre las metas esperadas y los resultados encontrados, analizando para cada caso las causas y consecuencias que de ello se derivan; la definición de su objetivo, alcance, acciones a implementar y metas de logro en un periodo de tiempo determinado; la asignación de los

responsables y de los recursos requeridos y las acciones de seguimiento necesarias para verificar su cumplimiento.

El seguimiento al PLAN DE MEJORAMIENTO INSTITUCIONAL se realiza a dos niveles, dependiendo del aspecto que se valide. El primero se orienta a verificar el cumplimiento de los compromisos realizados por la administración de diseñar e implementar dichas acciones; el segundo, se relaciona con la calidad, al validar la eficiencia y eficacia de las acciones emprendidas, lo que significa que no sólo se evalúa el diseño e implementación de las acciones señaladas en el Plan de Mejoramiento Institucional, sino que verifica que efectivamente se impacte la gestión de la entidad y el Sistema de Control Interno. (Ver Anexo).

## **2. PLAN DE MEJORAMIENTO POR PROCESO.**

En este punto se hace uso de las herramientas proporcionadas por el Sistema de Gestión de Calidad y en particular los procedimientos para formulación de acciones preventivas y correctivas así como los formatos utilizados para ellas y para las acciones de mejora. La aplicación de este tipo de acciones puede ser el resultado, entre otros, de no conformidades u observaciones de auditoria de calidad; de conclusiones resultantes del proceso de revisión del SGI por la Dirección; de correcciones de servicio no conforme detectadas por los distintos procesos; de autoevaluación al interior de los procesos que los lleva a formular acciones; del comportamiento de indicadores, planes operativos de calidad o de mapas de riesgo. (Ver anexo)

## **3. PLAN DE MEJORAMIENTO INDIVIDUAL.**

FORTIUS S.A. CORREDORES DE SEGUROS mide anualmente la evaluación del desempeño de sus funcionarios. Está previsto que a partir del resultado obtenido en la misma podrán surgir acciones a las que debe comprometerse el funcionario para lo cual evaluador y evaluado además de definir las en el formato anexo a la evaluación, deben establecer un plazo dentro del cual se ejecutarán y hacer seguimiento a los resultados de las mismas. En el caso de las acciones a las que debe comprometerse la entidad, el Plan de Capacitación resulta ser de gran utilidad para ayudar a corregir las debilidades o deficiencias que presenta un funcionario. Tanto los evaluadores como los evaluados deben fijar compromisos relacionados con el desempeño laboral del funcionario que redunden en una mejor prestación del servicio que se le ha encomendado a la empresa. (Ver Anexo)