MANUAL DEL SISTEMA DE CONTROL INTERNO (SCI)

Ashmore Investment Advisors S.A., Sociedad Fiduciaria

2023

ÍNDICE DE MODIFICACIONES			
Versión	Numeral Modificado o Adicionado	Fecha de Modificación por la Junta Directiva (dd/mm/aaaa)	Descripción de la modificación
0.0	Todo el documento	01/10/2019	Creación del documento.
1.0	Acápites indicados	25/08/2020	1. Se modifica la regulación a la que hace referencia el numeral 5.3 (del Decreto 661 de 2018 al Decreto 2555de 2010) 2. Se incluyen dos responsabilidades del Representante Legal, en el numeral 6.1.3 (6.1.3l y 6.1.3p)
0.2	Acápites indicados	11/10/2021	1. Se incluye referencia cruzada al protocolo de atención de PQRS de la Entidad
3.0	Todo el documento	12/10/2023	Se modifican las referencias a los manuales de gestión de riesgos de SARO, SARM y SARL, derogados e incluidos en el Manual SIAR, aprobado en 18/05/2023

CONTENIDO

1. ÁMBITO DE APLICACIÓN. 6
2. OBJETIVO DEL MANUAL Y POLÍTICAS DEL SCI. 7
2.1. Objetivos del Manual. 7
2.1.1. Objetivos generales. 7
2.1.2. Objetivos específicos. 7
2.2. Políticas del SCI. 8
2.2.1. Políticas generales. 8
2.2.2. Gestión de Riesgos. 9
2.2.3. Cumplimiento. 9
3. PRINCIPIOS DEL SISTEMA DE CONTROL INTERNO 11
3.1. Alcance: 11
3.2. Desarrollo de los principios del SCI al interior de la Entidad. 11
4. ELEMENTOS DEL SISTEMA DE CONTROL INTERNO. 13
4.1. Ambiente de Control 13
4.1.1. Código de Conducta y Cumplimiento 13
4.1.2. Procesos de selección dirigidos a las Personas Vinculadas 14
4.1.3. Estructura organizacional. 14
4.2. Gestión de riesgos. 14
4.3. Actividades de control 15
4.3.1. Revisiones de alto nivel. 16
4.3.2. Procedimientos. 16
4.3.3. Controles 16
4.3.4. Estadísticas. 18
4.3.5. Políticas de seguridad física. 19
4.3.6. Controles Administrativos. 19
4.3.7. Difusión de actividades de Control 21
4.3.8. Calidad de la Información. 21
4.4. Información y comunicación. 21
4.4.1. Información 22
4.4.2. Comunicación. 25
4.5. Monitoreo. 28
4.6. Evaluaciones independientes. 28
5. ÁREAS ESPECIALES DENTRO DEL SISTEMA DE CONTROL INTERNO 29

5.1. Control interno en la gestión contable. 29

5.2. Normas de control interno para la gestión de la tecnología. 30

5.3. De la obligación de cumplimiento del deber de asesoría. 33

6. RESPONSABILIDADES DENTRO DEL SISTEMA DE CONTROL. 34

6.1. Órganos internos. 34

6.1.1. Junta Directiva. 34
6.1.2. Comité de Auditoría. 35
6.1.3. Representante Legal. 38
6.1.4. Auditoría interna. 40

6.2. Órganos externos. 43

6.2.1. Revisor Fiscal. 43

7. DOCUMENTOS MÍNIMOS QUE DEBEN SUSTENTAR LA IMPLEMENTACIÓN DEL SCI 45

DEFINICIONES

Para todos los efectos atinentes a este Manual, los términos que a continuación se relacionan deberán entenderse de acuerdo con el siguiente significado:

a. Circular Básica Jurídica: se refiere a la Circular Externa 029 de 2014 expedida por la SFC y/o las normas que la modifiquen, adicionen o sustituyan.

b. ASHMORE: se refiere a Ashmore Investment Advisors (Colombia) S.A., Sociedad Fiduciaria. También podrá referirse a ASHMORE como la "Entidad" o la "Sociedad Fiduciaria".

c. Instrucciones del SCI: se refiere a las instrucciones relativas al Sistema de Control Interno expedidas por la SFC y que se encuentran contenidas en el Capítulo IV del Título I de la Parte I de la Circular Básica Jurídica.

d. SCI: Se refiere al Sistema de Control Interno. De conformidad con el Numeral 2 de las Instrucciones del SCI, por éste se entiende 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 la organización para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

- Mejorar la eficiencia y eficacia en las operaciones de la Entidad. Para el efecto, se entiende por eficacia la capacidad de alcanzar las metas y/o resultados propuestos; y por eficiencia la capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo.
- Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de la organización.
- Realizar una gestión adecuada de los riesgos.
- Aumentar la confiabilidad y oportunidad en la Información generada por la organización.
- Dar un adecuado cumplimiento de la normatividad y regulaciones aplicables a la organización.

e. Manual: se refiere al presente manual del SCI de ASHMORE.

f. Persona Vinculada: persona quien se vincula a ASHMORE a través de un contrato laboral o una relación legal o reglamentaria. Dentro del concepto de Persona Vinculada se encuentran los funcionarios y empleados de ASHMORE, así como el Representante Legal de la misma.

g. SFC: es la Superintendencia Financiera de Colombia.

1. ÁMBITO DE APLICACIÓN

El SCI de ASHMORE se fundamenta en políticas, normas y procedimientos establecidos, bajo la cobertura de una adecuada administración del riesgo. En este sentido, el SCI se encuadra dentro del marco de gestión integral de riesgos, el cual está diseñado para identificar los riesgos potenciales a los que se enfrenta la institución, procurando que los mismos sean gestionados dentro de los límites establecidos por la Junta Directiva, de forma que se aseguren, de manera razonable, los objetivos del negocio a través de la detección oportuna de las desviaciones en los procesos y los eventos que pueden llegar a impedir el cumplimiento de los mismos.

La Entidad ha implementado el presente Manual del SCI para dar cumplimiento a las Instrucciones del SCI, teniendo en cuenta:

- El tamaño de la organización.
- La naturaleza de las actividades propias del objeto social de la Entidad.
- La naturaleza de las actividades desarrolladas por cuenta de terceros.
- Que la Entidad no tiene la calidad de matriz.

La Junta Directiva, el Comité de Auditoría, las Personas Vinculadas y demás colaboradores deben aplicar el SCI a todos y cada uno de los procesos que se cumplen y se han establecido al interior de la organización.

Bajo este alcance el SCI impulsará a la Entidad al logro de sus metas, a asegurar el cumplimiento de la normatividad y la confiabilidad de los Estados Financieros y en general toda aquella información que genere a sus usuarios internos y externos.

2. OBJETIVO DEL MANUAL Y POLÍTICAS DEL SCI

El objetivo del presente Manual es generar, establecer políticas, procedimientos, controles, mediciones, atribuciones, responsabilidades y reportes para las Personas Vinculadas de la Entidad en desarrollo de las instrucciones del SCI.

2.1. Objetivos del Manual

2.1.1. Objetivos generales

El Manual busca recoger el proceso adelantado por la Junta Directiva y las Personas Vinculadas, bajo el cual se ha establecido el plan de la organización, los métodos a implementar y las medidas adoptadas dentro de Entidad para mejorar o mantener los siguientes objetivos de la misma:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Realizar una gestión adecuada de riesgos.
- Cumplimiento de las leyes y normas aplicables.

2.1.2. Objetivos específicos

El Manual tiene por objetivos específicos, los siguientes:

a. Fijar las políticas de la Entidad para la implementación y desarrollo del SCI procurando los principios de autocontrol, autorregulación y autogestión al interior de la Entidad.

b. Consolidar en un documento el conjunto de principios y normas que orienten el desarrollo de las actividades y guías de trabajo para la realización de la implementación del SCI.

c. Adoptar las bases de reconocido valor técnico para la ejecución de las tareas para evaluar la suficiente, eficacia y efectividad del SCI y de la administración de riesgos al interior de la Entidad.

d. Constituirse en herramienta de capacitación y difusión a todo nivel de la Entidad para lograr el adecuado entendimiento de los principios y normas así como para la adecuada aplicación de la función de control interno.

e. Impulsar la cultura de control interno al interior de la Entidad para mitigar los riesgos a los cuales se encuentra expuesta.

f. Asegurar el adecuado cumplimiento por parte de la Entidad de las normas sobre la estructura de cubrimiento de riesgos.

2.2. Políticas del SCI

2.2.1. Políticas generales

Para efectos del cumplimiento de las instrucciones impartidas por la SFC en materia del SCI, ASHMORE deberá tener en cuenta las siguientes políticas generales.

a. Las Instrucciones del SCI no suspenden ni reemplazan el cumplimiento de obligaciones y deberes establecidos en disposiciones vigentes.

b. Cada Persona Vinculada a la Entidad es responsable por las relaciones, requerimientos, comunicaciones e informes que se deben presentar y velarán por el cumplimiento con prioridad y diligencia y en forma inmediata de las operaciones de la Entidad, exigiendo que se cumpla en forma la normatividad vigente externa e interna.

c. El presente Manual se aplica en todas sus sucursales y agencias si llegaren a existir.

d. Todas las Personas Vinculadas a ASHMORE son responsables por cumplir y hacer cumplir lo establecido en el presente Manual. En caso de incumplimiento las Personas Vinculadas involucradas serán responsables de los perjuicios que se ocasione o pueda llegar a ocasionar al cliente, la Entidad o mercado por una transgresión a la normativa aplicable o la relativa al SCI.

e. Todas las Personas Vinculadas a ASHMORE deben realizar las labores priopias de su encargo con profesionalismo, honestidad y transparencia.

f. La política general del SCI es definida por la Junta Directiva de la Entidad.

g. El eje de articulación del SCI es el “proceso” y con este criterio deben adaptarse las actividades orientadas a la identificación y evaluación de los factores de riesgo y el análisis causal de incidencias y eventos.

h. Todas las Personas Vinculadas deben ser capacitadas por la Entidad a efectos de dar cumplimiento a lo establecido en el presente Manual y en las Instrucciones del SCI, a fin de promover el trabajo en equipo, la permanente coordinación entre la áreas, la absoluta responsabilidad, estricta disciplina y en general el cumplimento de los valores de la Entidad.

i. El Comité de Auditoría es responsable de la articulación del SCI en la Entidad, así como de la definición de la metodología aplicable.

j. El alcance y la frecuencia de la evaluación son determinados por el Comité de Auditoría de la Entidad, cuando corresponda en el ámbito de sus responsabilidades, con las áreas específicas que el Comité de Auditoría determine.

k. El Comité de Auditoría cuenta con las facultades y recursos necesarios para el adecuado ejercicio de sus funciones y con un nivel de independencia que previene la potencial ocurrencia de conflictos de

intereses.

I. En desarrollo del principio de Autocontrol, es deber de todas las Personas Vinculadas que en desarrollo de sus funciones apliquen los procesos operativos apropiados y procuren el cumplimiento de los objetivos trazados por la Entidad, siempre sujetos a los límites por ella establecidos.

2.2.2. Gestión de Riesgos

El riesgo está en el corazón del negocio y forma parte integrante de la actividad en el mercado de valores. Por otro lado, los intensos cambios en el entorno, protagonistas fundamentales de los últimos tiempos, plantean a las entidades, en creciente medida, desafíos a los que ha de hacerse frente mediante nuevos principios de gestión del riesgo.

La Entidad dispone de un modelo de gestión del riesgo. Su principal objetivo es la configuración de un perfil de riesgo que, de un lado, facilite la consecución de objetivos estratégicos y de creación de valor para los accionistas y, de otro, garantice la solvencia a medio y largo plazo de la organización.

Esta doble perspectiva requiere una precisa gestión de los riesgos de mercado, lavado de activos y operacional y además la integración de estos riesgos en la gestión, de forma que se supere la visión de cada uno de ellos.

El objetivo es establecer e implantar metodologías y procedimientos de identificación, admisión, medición, seguimiento e integración que permitan mantener el perfil de riesgos dentro de los niveles de tolerancia al mismo fijados por la Junta Directiva. Estas metodologías y procedimientos deben ser, además, una ventaja competitiva para el crecimiento del negocio, y no un obstáculo.

La Entidad cuenta con un Sistema Integrado de Administración de Riesgos (en adelante SIAR), que incluye las politicas, procedemientos, metodologías y gobierno corporativo relacionado con:

- Gestión de Riesgo de Liquidez.
- Gestión de Riesgo de Mercado.
- Gestión de Riesgo Operacional.

Y adicionalmente, cuenta con manuales para la gestión y administración de:

- SARLAFT (Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo).
- SAC (Sistema de Atención al Consumidor Financiero).

Ashmore Investments Advisors (Colombia) S.A., como Sociedad Fiduciaria en el ejercicio del principio de autonomía de la voluntad, ha decidido implementar las metodologías estándar de valoración y calificación de riesgos, determinadas por la Superintendencia Financiera de Colombia, a través de la Circular Básica Contable Financiera y sus anexos.

2.2.3. Cumplimiento

Hace referencia al riesgo normativo y/o reputacional, el cual incluye la evaluación de los siguientes elementos:

- Código de Conducta.
- Tratamiento de los conflictos de interés.
- Prevención de lavados de activos y de la financiación del terrorismo.
- Protección del consumidor.

Estos elementos se encuentran desarrollados en los Manuales y Reglamentaciones internas de la Entidad.

3. PRINCIPIOS DEL SISTEMA DE CONTROL INTERNO

3.1. Alcance

Constituyen las condiciones imprescindibles y básicas que garantizan la efectividad del SCI. La Autorregulación, el Autocontrol y la Autogestión son los pilares esenciales que garantizan el funcionamiento del SCI y se definen por las Instrucciones del SCI de la siguiente forma:

a. Autocontrol

Es la capacidad de todos y cada uno de los funcionarios de la organización, 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.

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 aplicables.

c. Autogestión

Apunta a la capacidad de la organización para interpretar, coordinar, ejecutar y evaluar de manera efectiva, eficiente y eficaz su funcionamiento.

3.2. Desarrollo de los principios del SCI al interior de la Entidad

En desarrollo de los principios del SCI la Entidad debe determinar planes de trabajo para verificar que se estén acatando las normas y requisitos para realización de las operaciones. Lo anterior a fin de:

a. Verificar la suficiencia y confiabilidad de la información financiera y contable, así como de la preparación de todos los estados financieros e informar a la administración de la Entidad sobre la situación de la misma.

b. Asegurar el cumplimiento de las disposiciones legales, reglamentarias y estatutarias vigentes a las que se encuentra sujeta la Entidad.

c. Informar a la Junta Directiva de la Entidad sobre las deficiencias, inconsistencias o irregularidades detectadas en las revisiones, para evitar procesos posteriores ante autoridades administrativas, civiles o penales.

d. Elaborar los instructivos necesarios que se efectúen los correctivos del caso.

e. Verificar el cumplimiento de los objetivos básicos de la Entidad, salvaguardando los recursos de la misma, que comprende los activos de la organización y los bienes de terceros que se encuentren en su

poder.

f. Planificar y organizar los procedimientos de análisis y control para el desarrollo del adecuado seguimiento a las operaciones.

4. ELEMENTOS DEL SISTEMA DE CONTROL INTERNO

Para el cumplimiento de los principios y objetivos indicados en las secciones precedentes del Manual, la Entidad ha consolidado una estructura de control interno que tiene en cuenta los siguientes elementos:

4.1. Ambiente de Control

En cumplimiento del elemento de ambiente de control, la Entidad debe promover la cultura organizacional a fin de fomentar en todas las Personas Vinculadas principios, valores y conductas orientadas hacia el control. Lo anterior, a fin de que ASHMORE cuente con un personal competente y se inculque en toda la organización un sentido de integridad y concientización sobre el control.

Para los anteriores efectos, la Entidad ha acogido las siguientes políticas y procedimientos a través de los cuales se implementarán los elementos mínimos para crear un adecuado ambiente de control:

4.1.1. Código de Conducta y Cumplimiento

La Junta Directiva de ASHMORE ha acogido y adoptado los principios que rigen la Entidad, los cuales se encuentran contenidos en su Código de Conducta y Código de Buen Gobierno Corporativo. Igualmente, la Entidad ha incluido en los mencionados Códigos las políticas que contienen:

- Valores y pautas explícitas de comportamiento.
- Parámetros concretos determinados para el manejo de conflictos de interés, incluyendo expresamente, entre otros, los que regulen las operaciones con vinculados económicos, en adición a los que apliquen por disposición legal.
- Mecanismos para evitar el uso de información privilegiada o reservada.
- Órganos o instancias competentes para hacer seguimiento al cumplimiento del código.
- Consecuencias de su inobservancia, teniendo en cuenta factores tales como reincidencias, pérdidas para los clientes o a la Entidad, violaciones a límites, entre otros.

Todos las Personas Vinculadas a la Entidad deben orientar su conducta a partir de las previsiones contenidas en el Código de Conducta y el Código de Buen Gobierno Corporativo adoptado por la Junta Directiva de ASHMORE. Para los anteriores efectos, todas las Personas Vinculadas deberán suscribir el compromiso que se adjunta como **ANEXO N°1** al presente Manual, a través del cual manifiestan expresamente someterse a su cumplimiento.

El Representante Legal deberá asegurarse que el Código de Conducta y el Código de Buen Gobierno Corporativo se divulguen a todas las Personas Vinculadas. En todo caso, el citado código deberá estar disponible para todos los grupos de interés de la Entidad a través de su página web.

4.1.2. Procesos de selección dirigidos a las Personas Vinculadas

En desarrollo del elemento de ambiente de control, la Entidad ha adoptado políticas y procedimientos a fin de realizar el proceso de selección de las Personas Vinculadas que se pretendan unir a la organización. Lo anterior, a fin de garantizar que éstos cumplen con los conocimientos, habilidades y conductas necesarias para el desempeño de sus funciones.

Las políticas y procedimientos adoptadas por la Entidad contienen una guía de los términos y condiciones de contratación y las políticas y procedimientos que la Entidad implementará sobre la materia. Adicionalmente, este documento incluye todas las condiciones contractuales y no contractuales relativas al proceso y selección de personal para la Entidad, entre las cuales se encuentran incluidas:

- La política de reclutamiento y selección de la Entidad: Establece las competencias, prácticas de gestión humana que aplican a la Entidad al realizar los procesos de selección, inducción habilidades, aptitudes e idoneidad de las Personas Vinculadas.

- La política de capacitación, desempeño y desarrollo de personal al interior de la Entidad: Establece las políticas de formación, capacitación, sistemas de compensación o remuneración y de evaluación del desempeño de las Personas Vinculadas en todos sus niveles, las cuales deben ser diseñadas e implementadas para facilitar un efectivo control interno, ya sea que se realice el proceso directamente o a través de terceros.

4.1.3. Estructura organizacional

En desarrollo del elemento de ambiente de control la Entidad, ha adoptado una estructura organizacional que permite soportar el alcance del SCI y que define claramente los niveles de autoridad y responsabilidad, precisando el alcance y límite de los mismos.

La estructura organizacional de la Entidad se adjunta como **ANEXO 2** al presente Manual y se encuentra armonizada con el tamaño y naturaleza de las actividades de ASHMORE.

4.2. Gestión de riesgos

La Entidad preserva la eficacia, eficiencia y efectividad de su gestión y capacidad operativa, para salvaguardar los recursos que administra, para tal efecto cuenta con sistemas de administración de riesgo, soportados en manuales de procedimientos que determinan los métodos para el tratamiento y monitoreo de los riesgos incluidos en el SIAR.

Los manuales de los respectivos sistemas de gestión de riesgos de la Entidad han sido elaborados según las instrucciones que en materia de gestión de ciertos riesgos establece la SFC y le permiten a la Entidad:

a. Identificar las amenazas que enfrenta la Entidad y las fuentes de las mismas.

b. Autoevaluar los riesgos existentes en sus procesos, identificándolos y priorizándolos a través de un ejercicio de valoración, teniendo en cuenta los factores propios de su entorno y la naturaleza de su

actividad.

c. Medir la probabilidad de ocurrencia de los riesgos y su impacto sobre los recursos de la Entidad (económicos, humanos, entre otros), así como sobre su credibilidad y buen nombre, en caso de materializarse.

d. Identificar y evaluar con criterio conservador, los controles existentes y su efectividad, mediante un proceso de valoración realizado con base en la experiencia y un análisis razonable, y objetivo de los eventos ocurridos.

e. Construir los mapas de riesgos que resulten pertinentes, los cuales deben ser actualizados periódicamente, permitiendo visualizarlos de acuerdo con la vulnerabilidad de la organización a los mismos.

f. Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la Entidad, que incluya elementos como: prevención y atención de emergencias, administración de crisis, planes de contingencia para responder a las fallas e interrupciones específicas de un sistema o proceso, y capacidad de retorno a la operación normal.

g. Divulgar entre las Personas Vinculadas que intervienen en los procesos respectivos, los mapas de riesgos y las políticas definidas para su administración.

h. Gestionar los riesgos en forma integral, aplicando diferentes estrategias que permitan llevarlos hacia niveles tolerables. Para cada riesgo se debe seleccionar la alternativa que presente la mejor relación entre el beneficio esperado y el costo en que se debe incurrir para su tratamiento. Entre las estrategias posibles se encuentran las de evitar los riesgos, mitigarlos, compartirlos, transferirlos, aceptarlos o aprovecharlos, según resulte procedente.

i. Registrar, medir y reportar los eventos de pérdidas por materialización de riesgos.

j. Hacer seguimiento a través de los órganos competentes, de acuerdo al campo de acción de cada uno de ellos, estableciendo los reportes o acciones de verificación que la administración de la entidad y los jefes de cada órgano social considere pertinentes.

k. Definir las acciones correctivas y preventivas derivadas del proceso de seguimiento y evaluación de los riesgos (planes de mejoramiento).

4.3. Actividades de control

La Entidad tiene establecidas las políticas y procedimientos que deben seguirse para lograr que las instrucciones de la administración con relación a sus riesgos y controles se cumplan. Para tal efecto se han consagrado políticas para administrar cada uno de los riesgos a los cuales se ve expuesta la Entidad y los controles necesarios para administrarlos y mitigarlos.

Sin perjuicio de lo anterior, para el cumplimiento de los requisitos y aplicación de este componente, la Entidad

se apoya en las siguientes herramientas:

4.3.1. Revisiones de alto nivel

ASHMORE cuenta con una Junta Directiva, la cual es la máxima autoridad administrativa de la Entidad. A ella le corresponde fijar las políticas que deben aplicarse para la ejecución de la función misional y administrativa de la organización en el marco de la normativa aplicable.

El Código de Gobierno Corporativo de ASHMORE provee un marco que define los derechos y responsabilidades dentro de los cuales interactúan los órganos de gobierno de la Entidad, entre los cuales se destacan la Junta Directiva, los Representantes Legales, los directivos, el Revisor Fiscal y demás órganos de control de la organización.

La Junta Directiva de ASHMORE es la encargada del análisis de los informes y presentaciones que preparan las Personas Vinculadas y los órganos de control en virtud de la normativa vigente, para efectos de analizar y monitorear el progreso de la Entidad hacia el logro de sus objetivos, detectar problemas, tales como deficiencias de control, errores en los informes financieros o actividades fraudulentas, y adoptar los correctivos necesarios.

4.3.2. Procedimientos

La Entidad cuenta con sus procesos y procedimientos definidos dentro de su mapa de procesos.

4.3.3. Controles

Los controles de seguimiento son utilizados para supervisar la ejecución de los controles generales y específicos. El objetivo de esta clase de controles es supervisar y verificar la aplicación y cumplimiento de políticas, procedimientos, normativas internas y externas, así como aspectos legales.

Son controles normalmente de baja frecuencia, encaminados a identificar errores una vez han sido producidos. Entre estos controles se encuentran:

- Auditoria Interna: realiza un 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 operativa de los controles de riesgos específicos o probando los resultados del proceso de control.

- Comité de Auditoría: 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 tener la autoridad suficiente para poder detectar las incidencias identificadas.

4.3.3.1. Controles Generales

Son controles que afectan de forma generalizada a un grupo determinado de procesos. Esta clase de controles son generalmente de tipo preventivo y comprenden entre otras las siguientes actividades:

a. Formación: Comprenden el diseño, comunicación e instrucción de actividades formativas o de entrenamiento encaminadas a que las Personas Vinculadas cuenten con los conocimientos y habilidades necesarias para la realización de las actividades inherentes a su puesto de trabajo.

b. Políticas y procedimientos: tales como:

- Normas y manuales: Preparación, elaboración y publicación de documentación estándar con los procedimientos y operativa desarrollada por la Entidad. Con este tipo de controles se pretende reducir las interpretaciones subjetivas de las Personas Vinculadas que intervienen en las mismas, homogeneizando el comportamiento de los empleados y por tanto evitando irregularidades que podían haber pasado por alto.

- Comunicaciones internas: 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 de las Personas Vinculadas que intervienen en las mismas.

- Código de conducta: define y desarrolla los fundamentos de comportamiento ético que han de aplicarse a los negocios y actividades que desarrolla la Entidad, y las pautas de actuación que han de ejercer las Personas Vinculadas. Permite reducir los riesgos, principalmente de fraude mediante la concienciación corporativa y la creación y mantenimiento de una cultura interna.

c. Atribuciones y funciones:

- Establecimiento de límites-facultades: 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.

- Segregación de funciones: Fijación y asignación de perfiles, funciones y puestos entre las Personas Vinculadas.

4.3.3.2. Controles Específicos

Son mecanismos de control establecidos sobre procesos específicos que permiten prevenir, detectar y corregir los riesgos. Se clasifican en:

a. **Autorizaciones:** Aprobación de operaciones, resultados, informes, tareas, entre otros aspectos, tanto de forma automática, como manual, asegurándose que los individuos apropiados aprueban las

transacciones realizadas conforme a los criterios definidos. Pretenden evitar el registro de información errónea antes de su tramitación o grabación.

b. Verificaciones

- Verificación de existencias: Consiste en la identificación de errores en activos registrados a partir de la observación física como por ejemplo inventarios de existencias y arqueos de caja.

- Confirmaciones: Hace referencia a la verificación sobre la veracidad de determinados datos básicos, son actividades de control encaminadas a contrastar los registros en distintos sistemas con la documentación soporte que los originó. Están incluidos dentro de estos controles también las verificaciones de entradas de datos y cualquier tipo de comparación de datos.

- Validación contra parámetros definidos: Comprende la verificación los datos introducidos y los cambios, conversión o procesamiento de los resultados contra parámetros establecidos para asegurar la exactitud y evitar que continúen las actividades del proceso y comunicar las excepciones, entre otros como están los chequeos de datos, comprobaciones de campos, auto-comprobación de dígitos, validación de combinaciones.

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

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

c. Conciliaciones: 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.

d. Controles Realizados por Terceros: Hacer referencia a cualquier control que mitigue riesgos afectos a la operativa de la Entidad y que tienen una característica común, la de ser realizados por terceros no pertenecientes a la propia organización. Los riesgos que mitigan estos terceros han de ser riesgos inherentes a la operativa de la Entidad, no inherentes a la operativa desplegada por el tercero.

4.3.4. Estadísticas

Para dar cumplimiento a los aspectos relacionados con la medición, análisis y mejora de los procesos de la Entidad, 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. De otra parte, a partir de la información generada por cada uno de los procesos de la Entidad, se evalúan identificando factores críticos asociados a los procesos, generando seguimiento y cumplimiento de controles.

4.3.5. Políticas de seguridad física

La Entidad cuenta con mecanismos de control de acceso tales como puertas de seguridad y sistemas de control con tarjetas inteligentes, para entrar a las oficinas.

Adicionalmente, en materia de seguridad se han definido las siguientes políticas mínimas:

a. Los centros de cómputo o áreas que la Entidad considera críticas, se encuentran en lugares de acceso restringido. Cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por un funcionario de la Entidad.

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

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

d. Los centros de cómputo o áreas que la Entidad considere criticas deberán estar demarcados con zonas de circulación y zonas restringidas.

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

f. 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.

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

La evaluación de riesgos de seguridad para los recursos informáticos se debe ejecutar con una periodicidad definida por el Comité de Auditoría. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo según lo indica el Manual SIAR de la Entidad.

4.3.6. Controles Administrativos

a. Análisis y revisiones periódicas. En relación con el desempeño de la Entidad en aspectos como presupuestos, pronósticos, periodos anteriores, entre otros. Estos análisis se efectúan con el fin de analizar y monitorear el progreso de la Entidad y adoptar los correctivos necesarios.

b. Comprobación de las operaciones. En cuanto a su exactitud y conformidad con los procedimientos de la Entidad. Los actos y operaciones relevantes sólo pueden ser autorizados y ejecutados por Personas Vinculadas que actúen dentro del ámbito de sus competencias.

c. 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.

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

e. 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.

f. Confidencialidad. La información suministrada y toda la que llegue a conocer una Persona Vinculada a la Entidad 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, so pena de incurrir en responsabilidad civil y penal de conformidad con lo prescrito por las normas que regulan la materia. Para estos efectos la Entidad ha adoptado acuerdos de confidencialidad los cuales deberán ser suscritos con cualquier persona que en virtud de sus funciones deba conocer información reservada.

g. Asignación de autoridad y responsabilidad. Las Personas Vinculadas deben 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. Así mismo, las Personas Vinculadas deben conocer los objetivos del área donde se desempeñan y cómo su función contribuye al logro de los objetivos generales.

En la Entidad debe haber una clara asignación de responsabilidades, lo que implica que cada Persona Vinculada desarrolla sus propias iniciativas y actúa dentro de sus responsabilidades. La asignación de responsabilidad está directamente vinculada con la asignación de autoridad. Las Personas Vinculadas que tienen asignadas responsabilidades deben rendir cuentas periódicamente.

h. Coordinación entre Procesos. Los procesos que componen la Entidad deben actuar coordinadamente entre ellos. Esto redundará en la consecución de los objetivos generales de la organización. Que exista coordinación implica que las Personas Vinculadas conozcan las consecuencias de sus acciones respecto a la Entidad en su conjunto. Existe un flujo de información adecuado entre los distintos procesos. Las Personas Vinculadas deben ser conscientes de cómo impactan sus acciones en la organización.

i. Documentación. La estructura de control interno y todas las transacciones y hecho significativos de la Entidad deben estar claramente documentados y disponibles para su control. Para el efecto, existen documentos escritos acerca de la estructura de control interno y estos se encuentran disponibles y al alcance de todas las Personas Vinculadas.

j. Niveles definidos de autorización. Los hechos significativos de la Entidad deben ser autorizados y realizados por funcionarios que actúen dentro del ámbito de su competencia. El Representante Legal debe autorizar los hechos significativos a realizar y sus personas dependientes, en caso de existir, deben 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 individuos que tienen asignada la tarea. La delegación de tareas se encuentra dentro de los lineamientos establecidos por el Representante Legal.

4.3.7. Difusión de actividades de Control

Una vez que la Junta Directiva haya analizado y aprobado el Manual, se procederá a realizar una capacitación a todas las Personas Vinculadas a la Entidad y se pondrá a disposición de ellos para su constante consulta. Adicionalmente, dentro de los procesos de inducción de nuevas Personas Vinculadas se incluirá un capítulo específico de Control Interno.

4.3.8. Calidad de la Información

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

a. Útil: Es decir que supla o apunte a las necesidades.

b. Oportuna: Que se genere en el momento preciso y requerido y además sea fiable.

c. 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.

d. Completa y exacta: Debe contener todos los datos y aspectos necesarios sobre lo que intenta comunicar, ha de ser íntegra y exacta.

e. Concisa: No debe estar sobre saturada 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 administración 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 la forma y en el plazo requerido sin perder el principio de confidencialidad.

4.4. Información y comunicación

En desarrollo del elemento de ambiente de control, la Entidad ha suscrito un Acuerdo de Servicios que se encuentra adjunto como **ANEXO 3** al presente Manual, a fin de que ésta última desarrolle las obligaciones en materia de información.

Lo anterior, dando cumplimiento a las siguientes condiciones:

a. Identificar la información que se recibe y su fuente.

b. Asignar el responsable de cada información y las personas que pueden tener acceso a la misma.

c. Diseñar formularios y/o mecanismos que ayuden a minimizar errores u omisiones en la recopilación y procesamiento de la información, así como en la elaboración de informes.

d. Diseñar procedimientos para detectar, reportar y corregir los errores y las irregularidades que puedan presentarse.

e. Establecer procedimientos que permitan a la Entidad retener o reproducir los documentos fuente originales, para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requerimientos legales.

f. Definir controles para garantizar que los datos y documentos sean preparados por personal autorizado para hacerlo.

g. Implementar controles para proteger adecuadamente la información sensible contra acceso o modificación no autorizada.

h. Diseñar procedimientos para la administración del almacenamiento de información y sus copias de respaldo.

i. Establecer parámetros para la entrega de copias, a través de cualquier modalidad (papel, medio magnético, entre otros).

j. Clasificar la información (en pública, privada o confidencial, según corresponda).

k. Verificar la existencia o no de procedimientos de custodia de la información, cuando sea del caso, y de su eficacia.

l. Implementar mecanismos para evitar el uso de información privilegiada, en beneficio propio o de terceros.

m. Detectar deficiencias y aplicar acciones de mejoramiento.

n. Cumplir los requerimientos legales y reglamentarios.

Sin perjuicio de lo anterior, ASHMORE ha determinado adoptar las siguientes políticas generales en relación con el manejo de información al interior de la Entidad:

4.4.1. Información

4.4.1.1. Acceso a la información

a. Todas las Personas Vinculadas a ASHMORE deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas a la Entidad, el funcionario responsable de

generar la información debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación y la suscripción del correspondiente acuerdo de confidencialidad.

b. Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que la persona cesa de prestar sus servicios.

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

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

e. Mediante el registro de eventos en los diversos recursos informáticos 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 pertinentes a su solución.

4.4.1.2. Seguridad de la Información

a. Todos las Personas Vinculadas a ASHMORE son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad y por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

b. Las Personas Vinculadas y colaboradores no deben suministrar la información de la Entidad a ningún ente externo sin las autorizaciones respectivas.

c. Toda Persona Vinculada 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 privilegiada.

d. Las Personas Vinculadas deben firmar un acuerdo de confidencialidad de la seguridad de la información y el buen manejo de la información.

e. Después de que una Persona Vinculada deje 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 información generada o conocida durante la gestión en la Entidad, directamente o través de terceros, así mismo, los funcionarios que detecten el mal uso de la información está en la obligación de reportar el hecho al Representante Legal para que tome las medidas del caso.

f. 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.

4.4.1.3. Seguridad para los servicios de información

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

b. La Entidad se reserva el derecho de acceder y revelar todos los mensajes enviados por medio del sistema de correo electrónico para cualquier propósito. Para este efecto, la Entidad realizará las auditorias respectivas directamente o a través de terceros.

c. Las Personas Vinculadas no deben utilizar versiones escaneadas de firmas de terceras personas para dar la impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmado por la persona que la envía.

d. La propiedad intelectual desarrollada o concebida mientras las Personas Vinculadas 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.

e. Las personas Vinculadas 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 y correo electrónico.

f. 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.

4.4.1.4. Seguridad de Recursos Informáticos

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

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

b. 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. También deben permitir que un rol de usuario administre el Administrador de usuarios.

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.

c. Plan de auditoria: Hace referencia a los registros de las transacciones relativos a la operación.

d. Las palabras claves o contraseñas de acceso: a los recursos informáticos, que designen las personas Vinculadas 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.

e. Controles de acceso especiales: 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 cifrado 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.

4.4.1.5. Almacenamiento y Respaldo de Información

Sin perjuicio de lo establecido en el plan de continuidad de negocios de la Entidad, ASHMORE debe contar con un sistema de respaldo de información, el cual permita realizar 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 24 horas. La Entidad también debe contar 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.

De otra parte, la Entidad cuenta con un firewall central con todas sus características antivirus, anti-spam e intermediario para consulta fuera de la red. Para la protección de ataques externos se tiene instalado un firewall, el cual permite filtrar el tráfico de paquetes que circulan por la 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.

4.4.2. Comunicación

Es el medio por el cual la administración orienta al personal de la Entidad hacia el logro de los objetivos; es vital que cada área y persona pueda conocer oportunamente los aspectos relativos a las responsabilidades.

Un sistema de comunicación eficaz que fluya a través de todo ASHMORE logra que sus miembros comprendan su papel en la Entidad, su grado de interacción con otras áreas, su participación en la gestión de los riesgos y su aporte en la mitigación de los mismos.

De igual forma, es importante transmitir a los diferentes grupos de interés de forma adecuada, confiable y veraz, los aspectos relacionados con el comportamiento de la Entidad, demostrando transparencia en el ejercicio de las operaciones.

Es por esto, que la comunicación es un elemento clave dentro del SCI, en razón a que coadyuva en la generación de un adecuado entorno de control.

Como parte de una adecuada administración de la comunicación, la Entidad ha identificado los siguientes elementos a través de sus políticas y procedimientos:

- Canales de comunicación.
- Responsables de su manejo.
- Requisitos de la información que se divulga.

- Frecuencia de la comunicación.
- Responsables.
- Destinatarios.
- Controles al proceso de comunicación.

En cuanto a la transparencia de la información que se proporciona a los consumidores financieros y sus calidades se encuentran previstas en el Manual del Sistema de Atención al Consumidor Financiero de la Entidad.

4.4.2.1. Comunicación Interna

En el ámbito interno de la Entidad se manejan diversos esquemas de comunicación de acuerdo con la naturaleza de lo que se desea informar a la Entidad, estos son:

a. Responsable de cada proceso:

Se encarga de comunicar todos los aspectos relacionados con:

- Normativa interna.
- Políticas.
- Procesos.
- Procedimientos.
- Otros temas.

b. Comunicaciones Internas:

El Representante Legal debe transmitir la información emitida por las diferentes unidades de la Entidad respecto a los temas de interés general, entre ellos se encuentran:

- Comunicados.
- Boletines.
- Actividades de bienestar y de responsabilidad social.

El control que orienta la difusión de la información generada al interior 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 SCI constituye factor primordial e imprescindible la capacitación y la inducción, 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 Entidad 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.

4.4.2.2. Comunicación Externa

El manejo de las comunicaciones externas es responsabilidad del Representante Legal de la Entidad, quien se encarga de planificar e implementar el desarrollo de las comunicaciones y relaciones institucionales de ASHMORE con los diferentes grupos de interés. Adicionalmente debe planificar y ejecutar los programas de responsabilidad corporativa y de patrocinios institucionales en caso de éstos existir.

4.4.2.3. Recepción y tratamiento de denuncias

A efectos de asegurar que en el que hacer de ASHOMRE las Personas Vinculadas den cumplimiento a la normatividad interna y externa aplicable, adicional a las medidas contempladas frente a cada proceso y en los sistemas de administración de riesgo, se han dispuesto las siguientes políticas:

- Las Personas Naturales que detecten eventuales irregularidades, incumplimientos normativos, violaciones al código de ética y conducta u otros hechos o circunstancias que afecten o puedan afectar el adecuado funcionamiento del SCI o de sus funciones, deben poner en conocimiento de esta situación a través del canal establecido por el representante legal.

- El procedimiento y las instancias que intervendrán en las investigaciones derivadas de las denuncias presentadas por las Personas Vinculadas se desarrolla en el Inventario de Canales de Atención para la recepción de PQRS establecido por la Entidad, así como en el Whistleblowing Policy de la matriz

- La información objeto de denuncia y la identidad del denunciante, serán objeto de reserva y confidencialidad. La revelación de esta información de manera no autorizada será considerada como falta gravísima.

- El canal establecido por el Representante legal para la recepción de denuncias será socializado en todas las instancias de la Entidad y deberá ser un canal exclusivo para la recepción de este tipo de denuncias.

- La administración del canal de denuncias será realizada directamente por el Representante Legal, quien adelantará el procedimiento de investigación establecido en el Inventario de Canales de Atención para la recepción de PQRS establecido por la Entidad, así como en el Whistleblowing Policy de la matriz

  En el escenario en que sea el representante legal quien presuntamente ha incurrido en los hechos o circunstancias irregulares objeto de denuncia, la investigación será direccionada por la Junta Directiva o por la persona que esta designe.

4.5. Monitoreo

Es el proceso que se lleva a cabo para verificar la calidad de desempeño del SCI a través del tiempo; las actividades de monitoreo se convierten en un elemento clave dentro del SCI, ya que es necesario que la gestión del riesgo se supervise de manera constante para medir su evolución, comprobar su apropiado funcionamiento y determinar los puntos susceptibles de ser mejorados, reemplazados o derogados.

Las actividades de monitoreo se llevan a cabo mediante acciones permanentes, evaluaciones independientes o por medio de la combinación de ambas técnicas. En el primero de los casos, están inmersas dentro de la gestión normal del negocio, involucran a los propietarios de los procesos dentro del ámbito de la competencia de cada uno de ellos. Como ejemplos de esta clase de técnica están: la revisión de informes, verificación de pagos, contraste de cifras, márgenes, ratios, indicadores, entre otros.

En segunda instancia, están las evaluaciones independientes de la gestión de riesgos, que son llevadas a cabo periódicamente por el Comité de Auditoría. El propósito principal de esta técnica consiste en establecer el nivel de funcionamiento real del sistema, esto implica validar que los controles realmente existan y estén documentados, que se apliquen de forma oportuna y que cumplan con el propósito para cual fueron creados.

4.6. Evaluaciones independientes

Aunque los procedimientos de seguimiento permanente proporcionan una retroalimentación importante, es deseable realizar adicionalmente evaluaciones que se centren directamente sobre la efectividad del SCI, las cuales deben ser llevadas a cabo por personas totalmente independientes del proceso, como requisito indispensable para garantizar su imparcialidad y objetividad.

Se cumple con el requisito de estas evaluaciones independientes a través del auditor interno y del Revisor Fiscal, en la medida en que el alcance de la evaluación hecha por éstos respecto al control interno de la respectiva Entidad tenga el alcance y la cobertura requeridos en la Circular Básica Jurídica de la SFC.

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.

5. ÁREAS ESPECIALES DENTRO DEL SISTEMA DE CONTROL INTERNO

De conformidad con las Instrucciones del SCI, si bien este sistema debe abarcar todas las áreas de la organización, por su particular importancia se debe hacer un control pormenorizado de la gestión del área contable y tecnológica:

5.1. Control interno en la gestión contable

En desarrollo del elemento, la Entidad ha adoptado las políticas y procedimientos necesarios, a fin de cumplir con las obligaciones de la Entidad en materia de gestión contable.

Lo anterior, en el marco del cumplimiento de las Instrucciones del SCI las cuales requieren que los procedimientos para llevar a cabo esta actividad cuenten, por lo menos con lo siguiente:

a. Supervisión de los procesos contables. Toda la responsabilidad del proceso contable de la Entidad, está a cargo del Representante Legal y la supervisión de dicho proceso se encuentra a cargo de la Revisoría Fiscal y del Comité de Auditoría.

b. Evaluaciones y supervisión de los aplicativos, accesos a la información y archivos, utilizados en los procesos contables. Corresponde a la Revisoría Fiscal, adelantar la supervisión de los aplicativos utilizados en el proceso contable.

c. Presentación de informes de seguimiento. La Revisoría Fiscal, deberá presentar por lo menos cuatro (4) veces al año, o cuando lo considere conveniente o por solicitud de la administración de la organización, informes acerca del funcionamiento del aplicativo utilizado en el proceso contable, así como informes detallados del funcionamiento de todo el proceso contable. Así mismo corresponde a la Revisoría Fiscal realizar, de manera periódica validaciones de calidad de la información, revisando que las transacciones u operaciones sean veraces y están adecuadamente calculadas y valoradas aplicando principios de medición y reconocimiento.

d. Comparaciones, inventarios y análisis de los activos de la Entidad, realizadas a través de fuentes internas y externas. Corresponde a la Revisoría Fiscal revisar los inventarios y análisis de los activos de la organización. No obstante, ASHMORE, en cualquier momento podrá contratar una auditoría externa para tales comparaciones.

e. Supervisión de los sistemas de información. Los sistemas de información estarán permanente vigilados por el Representante Legal y por la Revisoría Fiscal de la Entidad.

f. Controles generales.

g. Autorización apropiada de las transacciones por los órganos de dirección y administración.

h. Autorización y control de documentos.

i. Autorizaciones y establecimiento de límites.

De otra parte, la Revisoría Fiscal se encarga de verificar que los Estados Financieros de la organización presenten en forma razonable la situación financiera y resultados de la Entidad, y que cumplan plenamente con las normas, principios y reglamentos que resulten aplicables, a través de la generación de información financiera oportuna, razonable y veraz que reflejen en forma fidedigna la realidad económica de la organización.

Igualmente, el Representante Legal de la Entidad es responsable de informar ante el Comité de Auditoría todas las deficiencias significativas encontradas en el diseño y operación de los controles internos que hubieran impedido a la sociedad registrar, procesar, resumir y presentar adecuadamente la información financiera de la misma.

5.2. Normas de control interno para la gestión de la tecnología

En desarrollo del elemento, la Entidad ha suscrito un Acuerdo de Servicios que se encuentra adjunto al presente Manual como **ANEXO 3 y 4**, a fin de desarrollar las obligaciones en materia de gestión de tecnología.

Las políticas adoptadas deben ser revisadas por lo menos una vez al año o al momento de presentarse cambios significativos en el ambiente operacional o del negocio y cuentan con estándares, directrices y procedimientos debidamente orientados a cubrir los siguientes aspectos:

a. Plan estratégico de tecnología.
b. Infraestructura de tecnología.
c. Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.
d. Administración de proyectos de sistemas.
e. Administración de la calidad.
f. Adquisición de tecnología.
g. Adquisición y mantenimiento de software de aplicación.
h. Instalación y acreditación de sistemas.
i. Administración de cambios.
j. Administración de servicios con terceros.
k. Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.
l. Continuidad del negocio.
m. Seguridad de los sistemas.
n. Educación y entrenamiento de usuarios.
o. Administración de los datos.
p. Administración de instalaciones.
q. Administración de operaciones de tecnología.
r. Documentación.

Por la relevancia que representan algunas de las políticas previamente identificadas, a continuación, se instruye de manera específica sobre las siguientes:

a. Plan estratégico de tecnología

Se debe realizar un proceso de planeación estratégica de tecnología, a intervalos de tiempo regulares, con el propósito de lograr el cumplimiento de los objetivos de la Entidad a través de las oportunidades que brinda la