GESTIÓN INTEGRAL DE RIESGOS

El FSV posee una estructura normativa interna compuesta por un conjunto de manuales, políticas y procedimientos para cada una de las unidades organizativas involucradas en la identificación, medición, control y mitigación, así como el monitoreo y comunicación de las diferentes tipologías de riesgos a los que se encuentran expuestas sus operaciones. Tales como: Crédito, Operacional (incluye riesgo legal, de fraude, entre otros), Mercado, Liquidez, Reputacional, Continuidad del Negocio, Seguridad de Información, Lavado de Dinero y de Activos y Financiamiento al Terrorismo; entre otros, de acuerdo a la normativa externa aplicable y las mejores prácticas vigentes. La gestión de riesgos es fortalecida por el Sistema de Gestión de la Calidad, certificado bajo la norma ISO 9001:2015, el cual es sometido a auditorías anuales de seguimiento y de recertificación cada tres años (renovó su certificado en el primer semestre 2024).

La Junta Directiva, Administración Superior y Plana Gerencial ejercen control y supervisión permanente sobre los tipos de riesgos antes citados, a través de los diferentes Comités autorizados por Junta Directiva, Comités de apoyo y de la Unidad de Riesgos; con lo cual se asegura una adecuada gestión y además garantiza que la toma de decisiones sea congruente con los riesgos identificados y las políticas aprobadas para gestionarlos.

1) Riesgo de Crédito.

Es la probabilidad que la institución pueda tener pérdidas económicas, debido a que un deudor incumpla total o parcialmente sus obligaciones de pago de acuerdo con los términos establecidos en su contrato, por diferentes motivos.

Debido a que este riesgo se origina con la actividad propia del FSV, la institución cuenta con lineamientos, manuales y procedimientos; así como un sistema informático para la determinación de reservas y provisiones que mitigan el riesgo crediticio y para la adecuada administración de éste, mediante el monitoreo, análisis, seguimiento y comunicación. El FSV posee además modelos estadísticos de calificación y medición de riesgo de crédito, que sirven para determinar el valor mínimo de reservas para la cobertura de la pérdida esperada.

2) Riesgo Operacional.

Son posibles eventos de carácter aleatorio que pueden afectar el cumplimiento de los objetivos institucionales generados por factores internos y/o externos, tales como: procesos, recurso humano, tecnología y eventos externos. Se incluye la gestión del Riesgo Legal y Riesgo de Fraude. El FSV utiliza el marco de gestión basado en las tres líneas de defensa, definidas así: 1) Unidades organizativas o de negocio que desarrollan los procesos y ejecutan las principales actividades; además son las responsables de identificar y evaluar los riesgos, dar seguimiento a indicadores y registrar los eventos materializados en el momento que son detectados, así como establecer controles y medidas de mitigación, 2) Unidades especializadas en gestión, verificación y mitigación de riesgos (Unidad de Riesgos), y 3) Unidades de control y vigilancia (Auditoría Interna), lo cual permite mantener una adecuada gestión del riesgo operacional; además, desarrolla e implementa una metodología que comprende 4 fases: Identificación, Medición, Control y Mitigación, Monitoreo y Comunicación; facilitando así, un método sistemático para asegurar que cada proceso identifique y cuantifique sus potenciales riesgos operacionales de mayor relevancia, basados en los controles existentes y estableciendo estrategias de gestión de riesgos para mitigarlos.

3) Riesgo de Liquidez.

Considera la posibilidad que una entidad no sea capaz de atender sus compromisos de pago y costos de operación principalmente en el corto y mediano plazo, o tenga que vender sus activos por debajo del valor de mercado cuando se presente una brecha de liquidez desfavorable.

Se cuenta con una estructura organizativa definida, con funciones y responsabilidades específicas para la gestión de ese riesgo, mediante la cual se han establecido estrategias de mitigación para anticipar la ocurrencia de eventos inesperados a través de políticas, tales como: disponibilidad mínima mensual, cobertura de obligaciones, límites de colocación de recursos, depósitos en instituciones

financieras según su calificación de riesgo y fuentes de fondeo, entre otros. Además, cuenta con normativa interna que regula la gestión del riesgo como: Instructivo para el Manejo de Disponibilidades, Manual para la Gestión de los Riesgos de Mercado y Liquidez y el Manual de Contingencia de Liquidez; donde se definen los escenarios que podrían generar alertas de iliquidez, estableciendo responsabilidades y estrategias para afrontar dichas situaciones.

4) Riesgo de Mercado.

Se refiere al riesgo de incurrir en pérdidas, debido a las variaciones del precio de mercado como resultado de movimientos adversos de las variables financieras a las que puedan estar expuestas las posiciones dentro y fuera del balance, tales como: la fluctuación en las tasas de interés o el tipo de cambio. La volatilidad en las tasas de interés puede tener un impacto negativo en el ingreso anual y en el valor económico del capital del FSV, por ese motivo se han implementado políticas para la gestión de las tasas de interés activas y pasivas, margen financiero y costos de fondeo, además se utilizan técnicas que permiten medir la sensibilidad de los activos y pasivos sujetos a variaciones, entre otros.

El riesgo por tipo de cambio representa la potencial pérdida como consecuencia de las fluctuaciones de las divisas de acuerdo con la volatilidad y posición en un momento determinado, es decir, el cambio en la cotización de una moneda frente a otra que puede hacer ganar o perder posiciones de valor; en ese sentido el FSV estaría expuesto a este factor de riesgo en caso realizará operaciones con monedas diferentes al dólar estadounidense o criptomonedas. También cuenta con normativa específica para la gestión de este riesgo como el Manual para la Gestión de los Riesgos de Mercado y Liquidez.

5) Riesgo Reputacional.

Es aquel que se produce por una percepción desfavorable de la imagen de la institución por parte de usuarios, deudores, proveedores y entes reguladores, entre otros; debido al incumplimiento de leyes, normas internas, códigos de gobierno corporativo, códigos de conducta, lavado de dinero, entre otros; con la posibilidad de incurrir en pérdidas.

El FSV cuenta con el Manual de Comunicación Reputacional para la gestión del riesgo, cuyo alcance aplica a toda la estructura de la institución en la ejecución de los mecanismos básicos de respuesta y acciones a ejecutar antes, durante y después de un evento que puedan derivar en un riesgo reputacional para la institución, estableciendo un protocolo de acción y comunicación para actuar de acuerdo a la situación identificada aplicando la metodología definida.

6) Continuidad del Negocio.

Para desarrollar la Gestión de la Continuidad del Negocio, el FSV ha diseñado normativa interna con el objetivo de: *Establecer los lineamientos para desarrollar la gestión de la continuidad del negocio, que permita minimizar las consecuencias e impactos de cualquier incidente de interrupción que afecte el funcionamiento de la institución, ya sea por siniestros, daños a la reputación, riesgos internos o externos*; de tal forma que se determine la estructura de funcionamiento del plan de continuidad del negocio que delimite claramente las funciones, los roles, las responsabilidades, los eventos que ponen en riesgo la continuidad del negocio, las actividades a realizar para mitigar dichos eventos, las alternativas de operación ante contingencias, el retorno a las actividades normales y realizar pruebas para evaluar la eficacia del plan; permitiendo evitar y/o minimizar los efectos ante alguna falla en las operaciones por cualquier incidente de interrupción, que afecte su funcionamiento y restablecer en el menor tiempo posible las operaciones de la Institución.

7) Riesgo de Seguridad de la Información.

Es la probabilidad de pérdidas derivadas de un evento que afecta el desarrollo de los procesos de la entidad en términos de confidencialidad, integridad y disponibilidad de la información que se administra.

La gestión está orientada a fortalecer el proceso de mitigación de riesgos de Seguridad de la Información y Ciberseguridad basados en un marco de referencia constituido por las normativas y leyes vigentes, mejores prácticas y alineado a la Gestión Integral de Riesgos. El alcance de la gestión realizada comprende las siguientes áreas: Promoción de una cultura de Seguridad de la Información y

Ciberseguridad por medio de campañas permanentes de concientización al personal, buscando sensibilizar sobre la importancia que cada uno de los que integra la institución desempeña para minimizar los riesgos de fraude y robo asociados a integridad, confidencialidad y disponibilidad de la información, ya sea por ataques de ingeniería social o factores internos; desarrollo, implementación y actualización de procedimientos de seguridad informática, implementación de infraestructura tecnológica orientada a brindar controles de ciberseguridad ante amenazas, control interno mediante evaluaciones de cumplimiento desarrolladas por Auditoría Interna y la definición de controles para la mitigación de los riesgos operativos identificados por las áreas de tecnología de la información.

Se mantiene un monitoreo 24/7 sobre recursos tecnológicos críticos prestando especial atención ante los riesgos relacionados con la ciberseguridad, adoptando medidas preventivas para estar preparados ante eventos de esta naturaleza; así mismo se continúa fortaleciendo, a través de un proceso de mejora continua, los lineamientos y controles implementados a nivel institucional para la gestión de la Seguridad de la Información y Ciberseguridad; para lo cual se cuenta con un sistema informático que automatiza la gestión.

8) Riesgo de Lavado de Dinero y de Activos, Financiamiento al Terrorismo y financiación a la proliferación de armas de destrucción masiva (LDA/FT/FPADM).

Es la probabilidad de pérdida o daño que puede sufrir una entidad por su propensión o vulnerabilidad a ser utilizada de manera directa o indirectamente a través de sus operaciones como instrumento para el lavado de dinero o de activos, canalización de recursos hacia la realización de actividades terroristas, financiamiento del terrorismo y de armas de destrucción masiva.

Con el fin de tratar adecuadamente el riesgo LDA/FT/FPADM, se ha diseñado un esquema de gestión de riesgos que comprende dos fases:

I. Prevención del Riesgo. El objetivo de esta fase es prevenir que se introduzcan a la entidad recursos financieros provenientes de actividades relacionadas con el lavado de dinero y activos o se canalicen recursos para la financiación al terrorismo y/o de armas de destrucción masiva. La prevención incluye la realización de las siguientes acciones:
   a. La creación de una estructura organizacional para la gestión del riesgo LDA/FT/FPADM.
   b. La definición de políticas, procedimientos, lineamientos, pautas y directrices para la gestión del riesgo LDA/FT/FPADM.
   c. Capacitación permanente a todo el personal del FSV, Administración Superior, Consejo de Vigilancia, Junta Directiva y Asamblea de Gobernadores.
   d. La definición de una metodología que permite valorar eventos de riesgo en función de su probabilidad de ocurrencia y nivel de severidad, considerando los factores de riesgo que afectan a la Institución, dando seguimiento a los resultados, a través de una matriz de riesgos y mapas de calor revisados y avalados por el Comité de Prevención de Lavado de Dinero y Activos, así como por la Junta Directiva.

II. Control del Riesgo. En esta fase se monitorean las operaciones realizadas con el fin de detectar y reportar transacciones vinculadas al lavado de dinero o activos, financiación al terrorismo o financiación a la proliferación de armas de destrucción masiva, que se pretendan realizar o se hayan realizado en la entidad, con el fin de intentar dar la apariencia de legalidad. Para ejercer un efectivo control interno, se realiza lo siguiente:
   a. La implementación de herramientas especializadas que monitorean las operaciones realizadas por los clientes del FSV.
   b. La realización de la Debida Diligencia (Simplificada, estándar o Intensificada) en función del nivel de riesgo determinado.
   c. La realización de auditorías internas y externas que ofrecen una garantía independiente y objetiva de la gestión de riesgos implementada en la entidad, así como la atención de las recomendaciones determinadas.
   d. Revisiones de los lineamientos establecidos de forma periódica.