INFORMACIÓN DEL DOCUMENTO

Estamento de Aprobación	**Junta Directiva** **Según Acta No 355 del 14-10-2020**

TABLA DE CONTENIDO

1. PROCESO

Control – Riesgo Corporativo y Conglomerado

2. OBJETIVO

- Establecer las políticas, metodologías y procedimientos para la gestión del Sistemas de Riesgo Operacional en Grupo Aval Acciones y Valores S.A (en adelante "la Entidad"), con el fin de mantener la exposición de los riesgos operacionales derivados del cumplimiento del objeto social de la entidad, dentro de los niveles aceptados.
- Fortalecer el ambiente de control en los procesos a través de la aplicación de los mecanismos definidos para la administración de los riesgos operacionales.
- Establecer los lineamientos para identificar, medir, controlar y monitorear los riesgos operacionales de la Entidad.
- Establecer un lenguaje unificado al interior de la Entidad para el fortalecimiento de la cultura de gestión de riesgos en la Entidad.
- Apoyar a los procesos en la identificación de riesgos y controles.

3. ALCANCE

El presente documento rige para los procesos de la Entidad, de acuerdo con el análisis realizado por la Vicepresidencia de Riesgos Corporativos, para su construcción se tiene en cuenta, en lo que se considere aplicable, los aspectos previstos para la gestión de riesgo operacional por la Superintendencia Financiera de Colombia, siendo este un marco de referencia. La actualización es responsabilidad de la Vicepresidencia de Riesgos Corporativos, la aprobación estará a cargo de la Junta Directiva. Es deber de todos los colaboradores conocer, acatar y aplicar las disposiciones establecidas en este documento.

4. GLOSARIO

- **Aceptación del riesgo:** decisión informada de tomar un riesgo particular, los riesgos aceptados podrán ser sujetos a monitoreo y revisión.

- **Acuerdos de Basilea:** conjunto de propuestas de reforma de la regulación bancaria, elaboradas por el Comité Bancario de Basilea para fortalecer la regulación, supervisión y gestión de riesgos del sector bancario. Estas medidas persiguen:
  - ✓ Mejorar la capacidad del sector bancario para afrontar perturbaciones ocasionadas por tensiones financieras o económicas de cualquier tipo;
  - ✓ Mejorar la gestión de riesgos y el buen gobierno en los bancos; y
  - ✓ Reforzar la transparencia y la divulgación de información de los bancos

- **Apetito riesgo:** definido como la cantidad de riesgo que la Entidad considera adecuado asumir para alcanzar sus objetivos estratégicos; ésta depende de múltiples factores como las condiciones del mercado, la economía, el sector, la capacidad económica de la Entidad, los objetivos de crecimiento y estratégicos, y la cultura institucional hacia el riesgo. El Apetito al Riesgo se expresa a través de la Declaración de Apetito al Riesgo con un conjunto de métricas cuantitativas y cualitativas.
- **Capacidad:** es la cantidad máxima de riesgo que la Entidad puede asumir en relación con su capital, gestión del riesgo, capacidades de control y restricciones regulatorias. De esta

manera, la capacidad es una medida “top-down” que se encuentra relacionada con los recursos que posee la Entidad (capital, liquidez, apalancamiento, entre otros).

- **Controles:** cualquier medida que tome la Entidad y otras partes, para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

- **COSO:** marco de referencia de control interno. por su significado en inglés (COMMITTEE OF SPONSORING ORGANIZATIONS). El cual establece los principios para un efectivo sistema de control interno.

- **Criterios de evaluación o medición de un Riesgo:** son los términos de referencia frente a los cuales la importancia de un riesgo es evaluada. Los Criterios de Riesgo se basan en los objetivos y el contexto externo e interno de la organización. También, los Criterios de Riesgo se pueden derivar de normas, leyes, políticas y otros requisitos.

- **Declaración de Apetito al Riesgo:** conjunto de umbrales y restricciones sobre métricas cuantitativas y cualitativas de riesgo, respectivamente, que expresan el Apetito al Riesgo de la Entidad.

- **Dueño de proceso / controles:** es el responsable de la gobernabilidad del proceso que tiene asignado, por cuanto se asegura que, sus controles son ejecutados, monitoreados y se deja evidencia suficiente de ambas tareas. Cuenta con una estructura funcional que aboca el proceso, sus riesgos y controles dentro de las Entidades según sus políticas internas. Cuando se menciona en este documento al dueño de proceso / controles, debe entenderse que el dueño de proceso cuenta con un grupo de personas que en conjunto se encargan de asegurar y monitorear que se ejecuten los controles tal y como fueron diseñados, de tal forma que la responsabilidad del dueño de proceso / controles involucre a todos los actores vinculados en el proceso y no sólo al colaborador jefe / gerente / vicepresidente de la misma.

- **Evento:** incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

- **Eventos de pérdida:** son aquellos incidentes que generan pérdidas por riesgo operacional a las entidades.

  ✓ Clasificación de los riesgos operacionales

  Para los efectos del presente capítulo los riesgos operacionales se clasifican de la siguiente manera:

  - Fraude Interno: actos que tienen como resultado defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales vigentes en los que se encuentra implicado, al menos, un empleado o tercero contratado para ejecutar procesos a nombre de la entidad.

  - Fraude Externo: actos, realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes, en los que se encuentra implicado un tercero ajeno a la entidad.
  - Relaciones laborales y seguridad laboral: actos que son incompatibles con la legislación laboral o con acuerdos relacionados con la higiene o la seguridad en el trabajo, o que

versen sobre el pago de reclamaciones por daños personales o casos relacionados con la diversidad y/o discriminación en el ámbito laboral.

- Clientes, productos y prácticas empresariales: incumplimiento involuntario o negligente de una obligación profesional/empresarial frente a clientes o eventos derivados de la naturaleza o diseño de un producto.

- Daños a activos físicos: pérdidas derivadas de daños o perjuicios a activos físicos de la entidad como consecuencia de desastres naturales, actos de terrorismo, vandalismo u otros acontecimientos.

- Fallas tecnológicas: hechos o cambios originados por fallas del hardware, software, telecomunicaciones o servicios públicos que puedan afectar, además de la operación interna de la entidad, la prestación del servicio a los clientes.

- Ejecución y administración de procesos: errores en el procesamiento de operaciones o en la gestión de procesos, así como en las relaciones con contrapartes comerciales y proveedores.

Adicionalmente para cada clase de evento de riesgo operacional la entidad debe establecer, como mínimo, las subcategorías que se señalan en el numeral 3.2.5.4 del capítulo XXIII de la CBCF.

- **Factores de riesgo:** se entiende por factores de riesgo las fuentes generadoras de riesgos operacionales que pueden o no generar pérdidas. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos.

  Dichos factores se deben clasificar en internos o externos, según se indica a continuación:

  ✓ Internos

  - Recurso Humano: es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad.

    Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente.

    La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

  - Procesos: es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

  - Tecnología: es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

- Infraestructura: es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

✓ Externos

Son situaciones asociadas a la fuerza de la naturaleza u ocasionadas por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

- **Indicador (KRI):** métricas cuantitativas para los riesgos materiales a los que está expuesta la entidad, que reflejan su Perfil de Riesgo y que permiten el control y seguimiento del mismo.

- **Informes de Apetito de Riesgo:** incluyen el análisis periódico del Perfil de Riesgo y los planes de acción establecidos para mantenerlo dentro de los umbrales correspondientes.

- **Impacto:** es la pérdida (monetaria o no monetaria) generada por la materialización de un riesgo, que puede ser medida de manera cualitativa y cuantitativa.

- **Manual de Riesgo Operacional:** es el documento que contiene las políticas, metodologías y procedimientos aplicables en el desarrollo, implementación y seguimiento del SARO.

- **Marco de Apetito de Riesgo:** incluye lineamientos, modelos organizativos y políticas en las que se establecen tanto principios, roles y responsabilidades; como criterios que determinan las pautas en las cuales se concreta la cultura de riesgos de la Entidad y definen mínimos comunes de aplicación transversal a diversas áreas.

- **Marco de Referencia de Control Interno:** se refiere al marco utilizado por la administración para evaluar la efectividad del diseño y operación de su sistema de control interno; para el caso de Grupo Aval, el Marco de Referencia de Control Interno es COSO en concordancia con los lineamientos de la Superintendencia, establecidos en la circular básica jurídica.

- **Perfil de Riesgo:** es la exposición a los riesgos actuales y potenciales inherentes al desarrollo del plan de negocio.

- **Pérdidas:** cuantificación económica de la ocurrencia de un evento de riesgo operacional, así como los gastos derivados de su atención.

  ✓ Pérdida Bruta: se entiende una pérdida antes de recuperaciones de cualquier tipo.

  ✓ Pérdida Neta: se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida bruta, que no necesariamente se efectúa en el mismo periodo por el que se perciben fondos o flujos económicos.

- **Probabilidad:** es la posibilidad que un riesgo se materialice. Para determinar la probabilidad se puede utilizar el análisis cualitativo o cuantitativo.

- **Procesos:** conjunto de actividades relacionadas entre sí, las cuales transforman elementos de entrada en resultados o elementos de salida y generan un valor agregado.

- **Responsable de la Información - RES:** es el ejecutivo para quien la información fue creada con el objetivo de realizar sus funciones en el negocio y tiene la responsabilidad de administrarla, clasificarla y evaluar los riesgos que pueden afectarla.

- **Riesgo Inherente:** nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

- **Riesgo Residual:** nivel resultante del riesgo después de aplicar los controles.

- **Riesgo Operacional (RO):** es la posibilidad de que la entidad incurra en pérdidas por las deficiencias, fallas o inadecuado funcionamiento de los procesos, la tecnología, la infraestructura o el recurso humano, así como por la ocurrencia de acontecimientos externos asociados a éstos. Incluye el riesgo legal.

- **Riesgo Legal:** es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones. Aplica a todas las actividades e incluye a terceros que actúen en representación de la entidad respecto de los procesos y/o actividades tercerizadas.

- **Sistema de Administración de Riesgo Operacional (SARO):** conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operacional, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las entidades vigiladas identifican, miden, controlan y monitorean el riesgo operacional.

- **Tolerancia:** es el nivel aceptable de la variación o desviación frente al apetito al riesgo que la Entidad está dispuesta a asumir en la búsqueda del logro de sus objetivos. Sirve de alerta para evitar llegar a niveles no deseados de exposición al riesgo y/o a su capacidad máxima de asunción de riesgos.

- **Unidad de Riesgo Operacional (URO):** es el área o cargo, designada por el Representante Legal de la entidad, responsable de gestionar el SARO.

5. REGULACIÓN

- Marco de referencia: Capítulo XXIII Circular Básica Contable y Financiera de la Superintendencia Financiera.

Otra Regulación:

- Norma ISO 31000
- Acuerdo de Basilea

6. RESPONSABILIDADES

6.1 CONTEXTO ORGANIZACIONAL DE GRUPO AVAL

Grupo Aval Acciones y Valores S.A. tiene como objeto social la compra y venta de acciones, bonos y títulos valores de entidades pertenecientes al sistema financiero y de otras entidades comerciales.

En desarrollo del mismo, la Sociedad puede adquirir y negociar toda clase de títulos valores de libre circulación en el mercado y de valores en general; promover la creación de toda clase de empresas afines o complementarias con el objeto social; representar personas naturales o jurídicas que se dediquen a actividades similares o complementarias a las señaladas en los literales anteriores; tomar o dar dinero en préstamos con o sin interés, dar en garantía o en administración sus bienes muebles o inmuebles, girar, endosar, adquirir, aceptar, cobrar, protestar, cancelar o pagar letras de cambio, cheques, pagarés, o cualesquiera otros títulos valores o aceptarlos o darlos en pago y ejecutar o celebrar en general el contrato de cambio en todas sus manifestaciones en todas sus modalidades o actividades afines, paralelas y/o complementarias.

Con el fin de contar con un adecuado ambiente de control, la Entidad ha adoptado como marco de referencia COSO.

6.2 LIDERAZGO Y COMPROMISO

En este capítulo se describen los compromisos de la estructura organizacional con el Sistema de Administración de Riesgo Operacional, para el cumplimiento de las políticas, funciones y responsabilidades que deben asumir los colaboradores para la implementación, y seguimiento a las actividades de mitigación de riesgos que les sean asignadas; a continuación, se muestran las políticas y funciones del sistema:

6.2.1 Compromiso de la Dirección

La Presidencia de Grupo Aval por medio de la Vicepresidencia de Riesgos Corporativos, está comprometida con la implementación y desarrollo del SARO en cuanto al cumplimiento de políticas, objetivos y estrategias para fortalecer la cultura de riesgo que la administración del SARO implica.

6.2.2 Políticas de Administración de Riesgo Operacional

Las Políticas de administración de riesgo operacional del SARO, se fundamentan en el contexto organizacional en el que se encuentra la Entidad y se enmarca bajo las siguientes políticas:

Política Estratégica

La gestión de Riesgos Operacionales está orientada en la creación y fortalecimiento de una cultura de Riesgo mediante la capacitación y concientización de todos los colaboradores de la Entidad, que permiten realizar la identificación de riesgos y controles que se pueden presentar en el desarrollo de las actividades propias de sus procesos. Para ello, es importante contar con

un flujo constante de información entre todas las áreas de la Entidad, fortaleciendo la cultura de reporte y apoyando la mitigación de los riesgos potenciales.

Política de Gobernabilidad

Los órganos de administración, de control y demás colaboradores de la Entidad, cuentan con funciones definidas en el SARO, evidenciando su rol y las responsabilidades específicas en cada una de las etapas del Sistema, asegurando su cumplimiento y alineación con los objetivos del mismo.

Política de Independencia

La URO como área independiente y manteniendo su imparcialidad, tiene acceso a toda la información que considere necesaria para la ejecución de cada una de las etapas del sistema SARO y en especial para el registro de eventos de riesgo operacional.
Para el desarrollo de sus funciones, la URO cuenta con personal con experiencia y capacitado en la administración de riesgo operacional y con recursos suficientes. Esta Unidad está a cargo de la Gerencia de Riesgos Corporativos y Normas de Conglomerado, con nivel organizacional alto y capacidad decisoria.

Política de Revelación

La URO genera el perfil de riesgo operacional, su evolución, y los cambios que se presenten en los controles implementados. Los resultados del avance de cada una de las etapas del SARO están en todo momento disponibles para consulta por parte de los miembros del Comité de Riesgos y Auditoría, para su respectiva retroalimentación y mejoramiento continuo.

Política de Continuidad de Negocio

Las Políticas de Continuidad de Negocio están establecidas en el “Manual de Continuidad de Negocio”, las cuales se basan en acciones que buscan mitigar los impactos en eventos que interrumpan la operación normal en la Entidad.

6.3 LÍNEAS DE DEFENSA FRENTE AL RIESGO

Grupo Aval ha establecido el principio de las tres líneas de defensa de acuerdo con el marco de referencia COSO.

La Entidad estructura sus funciones y responsabilidades frente a los riesgos que se expone, siguiendo el esquema de las tres líneas de defensa, esto es, considerando (i) la gestión por la línea de negocio, (ii) una función de gestión del riesgo independiente, y (iii) una revisión independiente.

Primera Línea de Defensa

La primera línea de defensa la constituyen cada una de las áreas o colaboradores de la Entidad responsable del desarrollo de su objeto social (p.e. las actividades de cara al público que están en contacto directo con los clientes y los procesos de back office necesarios para atender sus necesidades). Esto significa que tales áreas o colaboradores son responsables en primera

medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos inherentes a las actividades, procesos y sistemas de los que son responsables. Quienes conforman esta línea de defensa deben conocer sus actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

Segunda Línea de Defensa

Esta línea de defensa está conformada por la URO, es independiente a la primera línea, hace seguimiento al cumplimiento de todas las obligaciones en materia de Riesgo Operacional, es responsable de la definición de la metodología para la gestión de este riesgo, así como la identificación de las herramientas adecuadas para tal efecto.

Tercera Línea de Defensa

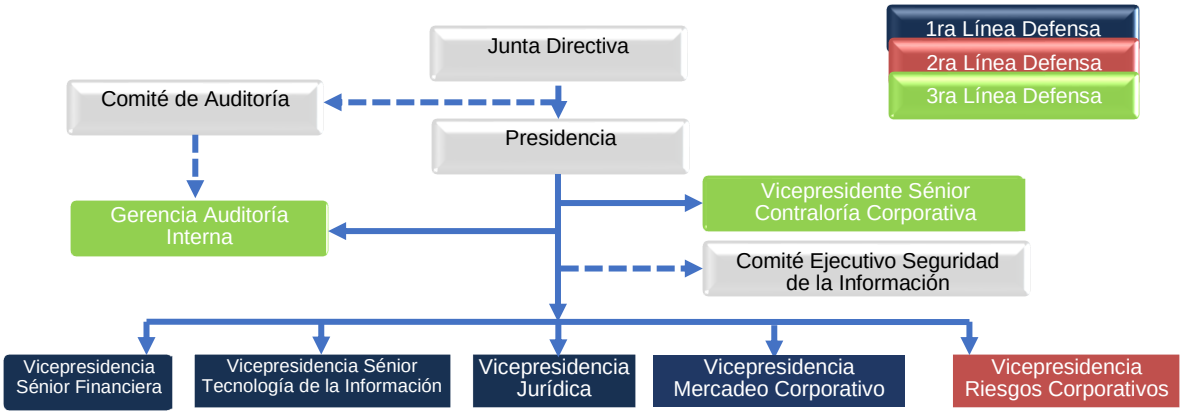
La tercera línea de defensa está conformada por la Auditoria Interna y es la responsable de realizar la evaluación independiente de la gestión de Riesgo Operacional en la entidad, así como los procesos y sistemas que conforman, rindiendo cuentas al Comité de Auditoría.

Esta revisión puede ser realizada por el personal de auditoría o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados. Los cuales proveen un aseguramiento objetivo sobre la efectividad de la gestión de riesgos a la Junta Directiva y/o Comité de Auditoria, asegurando que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno implementado está siendo operado efectivamente.

6.4 FUNCIONES DE LA ORGANIZACIÓN, RESPONSABILIDADES Y AUTORIDADES

El proceso de cumplimiento del SARO requiere de la vigilancia de la alta gerencia de la Entidad, de los órganos control y del establecimiento de los roles y responsabilidades aplicables a todos y cada uno de los colaboradores.

La siguiente es la estructura organizacional del SARO:



Junta Directiva

Sin perjuicio de las funciones asignadas en otras disposiciones, el SARO debe contemplar como mínimo las siguientes funciones a cargo de la Junta Directiva u órgano que haga sus veces:

- Aprobar el Manual para la Gestión del Riesgo Operacional, y sus actualizaciones.
- Hacer seguimiento y pronunciarse sobre el perfil de riesgo operacional de la entidad. Lo anterior, en concordancia con el Marco de Gestión de Riesgos de Grupo Aval.
- Solicitar las medidas necesarias para ajustar el perfil de riesgo operacional, cuando este se encuentre por fuera de los niveles fijados por la Junta Directiva. Lo anterior, en concordancia con el Marco de Gestión de Riesgos de Grupo Aval.
- Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.

Comité de Auditoría

El Comité como órgano de apoyo a la Junta Directiva en relación con la supervisión del sistema de control interno, y en lo que se relaciona con el SARO ejecuta las siguientes funciones:

- Evaluar el cumplimiento de la Política y solicitar la adopción de las medidas necesarias cuando se identifiquen incumplimientos. Estos serán evidenciados a través de los informes sobre la evaluación periódica del SARO que le presente la Auditoria Interna, según su plan de trabajo anual.
- Conocer y discutir los informes presentados por la Vicepresidencia de Riesgos sobre SARO de Grupo Aval.

Presidencia de Grupo Aval

Sin perjuicio de las responsabilidades asignadas en otras disposiciones, son funciones del Presidente:

- Dar conformidad para la presentación y poner a consideración y aprobación de la Junta Directiva, el Manual para la Gestión del Riesgo Operacional y sus posteriores actualizaciones.
- Velar por el cumplimiento efectivo de las políticas establecidas en el Manual de Riesgo Operacional.
- Conocer los informes sobre la evaluación periódica del SARO, que realicen los órganos de control.
- Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SARO - (Unidad de Riesgo Operacional - URO).
- Estar informado por medio de la Vicepresidencia de Riesgos Corporativos sobre la evolución del Riesgo Operacional de Grupo Aval.
- La Presidencia, a través de la Vicepresidencia de Riesgos Corporativos y los jefes de las demás áreas de Grupo Aval, debe desarrollar y velar porque se implementen las estrategias para fortalecer la cultura en la administración de este riesgo en la entidad.
- Adoptar las medidas necesarias para ajustar el perfil de riesgo operacional, cuando este se encuentre por fuera de los niveles fijados por la Junta Directiva. Lo anterior, dentro del Marco de Gestión de Riesgos de Grupo Aval.

Vicepresidencia de Riesgos Corporativos

- Revisar y someter a consideración del Presidente, el Manual para la Gestión del Riesgo Operacional y sus actualizaciones, para su aprobación por parte de la Junta Directiva.
- Velar por el cumplimiento efectivo de las políticas establecidas en el Manual para la Gestión del Riesgo Operacional.
- Presentar informes periódicos a la Presidencia y al Comité de Auditoria, sobre la evolución y aspectos relevantes del SARO.
- Efectuar seguimiento a las etapas y elementos establecidos en el SARO.
- Desarrollar y velar porque se implementen las estrategias para fortalecer la cultura de la administración del riesgo operacional en la entidad.
- Evaluar los informes presentados por la Unidad de Riesgo Operacional.
- Velar porque se implementen los procedimientos para la administración del riesgo operacional, que incluya el reporte de eventos de riesgo operacional, asegurando que cumpla con los criterios de integridad, disponibilidad y confidencialidad de la información allí contenida.
- Informar oportunamente al Comité de Auditoría, y a la Presidencia sobre cualquier evento importante que afecte el riesgo operacional de la entidad.

Unidad de Riesgo Operacional (URO)

Corresponde a la Gerencia de Riesgos Corporativos y Normas de Conglomerado, las funciones de Unidad de Riesgo Operacional, para tal efecto, cuenta con la Dirección de Riesgo Operativo y el apoyo del Analista de Riesgo Operativo, sus responsabilidades son:

- Definir las metodologías, instrumentos y procedimientos necesarios para la adecuada administración de los riesgos operacionales de la Entidad, de acuerdo con el volumen y complejidad de las operaciones que realiza.
- Desarrollar los modelos de medición del riesgo operacional, que permitan establecer el perfil de riesgo de la Entidad.

- Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operacional de la entidad.
- Monitorear el perfil de riesgo de la entidad e informarlo a la Vicepresidencia de Riesgos Corporativos.
- Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operacional y administrarlo.
- Acompañar a los procesos en la identificación de sus riesgos y controles.
- Solicitar a los procesos los planes de acción necesarios para mantener los riesgos dentro de los niveles aceptados y realizar seguimiento.
- Diseñar y ejecutar los programas de capacitación de la entidad relacionados con el SARO.
- Apoyar en la identificación de riesgos cuando el dueño de proceso lo considere y en ocasión de la implementación o modificación de cualquier proceso, producto, servicio o canal, así como en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.
- Reportar semestralmente al Vicepresidente de Riesgos Corporativos, la evolución y aspectos relevantes del SARO.
- Diseñar y proponer a la Vicepresidencia de Riesgos Corporativos el Manual para la Gestión del Riesgo operacional, así como sus actualizaciones, para su posterior presentación a la Presidencia de Grupo Aval y Junta Directiva.

Dueños de Proceso y Demás Colaboradores

- Mantener documentados y actualizados los procesos a su cargo, para ello debe contar con procedimientos claramente definidos, divulgados y comprendidos.
- Dar estricto cumplimiento a los lineamientos y políticas definidos en el presente Manual, así como a los procedimientos de gestión.
- Conocer en forma clara las actividades que conforman el proceso, el objetivo del mismo, su frecuencia de ejecución y clasificación dentro del mapa de procesos.
- Disponer de políticas y procesos adecuados para seleccionar a su personal, a fin de garantizar unos elevados principios éticos y profesionales.
- Impartir programas de inducción y formación a los colaboradores con el fin de asegurar que cuentan con las competencias para la adecuada ejecución de las actividades a su cargo.
- Participar en la etapa de Identificación, Medición, Control y Monitoreo de Riesgo Operacional.
- Mantener actualizado al personal sobre sus obligaciones y responsabilidades a cargo, las cuales deben incluir dentro de su alcance los posibles factores de riesgo a los que los colaboradores se encuentren expuestos en cumplimiento de sus responsabilidades.
- Identificar los riesgos operacionales y controles de los procesos ejecutados en el desarrollo de sus funciones.
- Conocer las normas que rigen su proceso, a fin de identificar los riesgos legales y de cumplimiento de acuerdo con los términos y definiciones del presente manual.
- Definir los planes de acción a que haya lugar para mitigar riesgos fuera de los niveles aceptados, de acuerdo con la periodicidad y metodología definida por la URO y en todo caso al menos una vez al semestre.
- Velar por la autogestión, autocontrol y autorregulación en la ejecución de sus actividades, e informar oportunamente a la URO los cambios que se presenten en sus actividades y que puedan variar la operación actual y por lo tanto los riesgos identificados.
- Realizar la evaluación de sus riesgos operacionales con los estándares definidos por la URO.

- Reportar adecuada y oportunamente los eventos de riesgo en el formato definido por la URO y los campos deben ser diligenciados en su totalidad. En el caso de conocer un evento de riesgo materializado y no sea de su responsabilidad, debe proceder con la notificación a la URO para solicitar a quien corresponda el reporte del evento.
- Verificar la implementación de los controles que hacen parte de los procesos de su área y actualizar la calificación en la matriz de riesgo Operacional. En caso de modificaciones tanto en los controles como en los riesgos de su proceso, notificar a la URO las mismas.
- Para aquellos riesgos cuya exposición a nivel residual este fuera del apetito de riesgo de la Entidad y manifieste su conformidad con dicho nivel, el RES debe realizar un proceso de Aceptación del Riesgo, de acuerdo con los protocolos definidos por la URO. La URO presentará en sus informes el resumen de aquellos riesgos que presentan esta situación.
- Reportar a la URO, situaciones potenciales que indiquen posibles nuevos riesgos en su proceso.
- Incluir a la URO en la divulgación de nuevos documentos o cambios en los procesos que se realiza a través del área de Organización y Métodos, con el fin de actualizar las matrices SARO e implementar y programar pruebas de continuidad si el cambio lo requiere.
- Participar en las capacitaciones y actividades definidas por la URO para el fortalecimiento del SARO.
- Para los procesos que en la identificación de riesgos operacionales y por su probabilidad o impacto sean considerados como riesgos críticos y que además puedan generar la interrupción de la operatividad normal del negocio, los procesos serán encargados de documentar sus contingencias en los correspondientes documentos internos. No obstante, en compañía de la URO se debe realizar valoración de inclusión en la estrategia de continuidad de negocio de la Entidad, bajo las políticas de Continuidad que se encuentran publicadas en el manual de dicho sistema de Gestión.

Incumplimiento de las normas y procedimientos establecidos. Las sanciones administrativas por el incumplimiento de lo previsto en el presente documento se aplicarán de acuerdo con lo establecido en el Reglamento Interno de Trabajo, sin perjuicio de las sanciones de tipo legal a que haya lugar.

Áreas de Apoyo a la Gestión del SARO

Algunas áreas son fuente importante para la adecuada gestión del SARO en la Entidad, ya que, por la ejecución de sus actividades y soporte a los demás procesos, presentan información relevante que para la URO son insumo para la revisión de los riesgos y controles identificados en los procesos. Esta información estará soportada y acordada mediante ANS firmado por las áreas, con el fin de acordar los parámetros mínimos en el suministro de información a la URO.

- El área de Tecnología debe informar a la URO y a la Dirección de Organización y Métodos cuando realice cambios en la infraestructura tecnológica, para así actualizar los procesos y estrategias de continuidad establecidas.

- Los eventos o incidentes que sean reportados al área de TI, deben ser notificados a la URO para que se pueda realizar el análisis de si se debe realizar un reporte de evento de riesgo operacional y algún ajuste en la matriz de SARO.

- El área de Organización y Métodos incluirá en la lista de divulgación de creación, modificación, eliminación, de los diferentes documentos de los procesos (Manuales, políticas, procedimientos, otros) a la URO para que esta pueda realizar el proceso de actualización de matriz SARO.

- La Auditoría interna podrá remitir los informes que genere de su plan de auditoria en los procesos, con el fin de evidenciar fallas en los controles y que ameriten la actualización de la matriz SARO.

- La gerencia Juridica en caso de recibir informes de entes externos y que en su buen entender considere oportuno comunicar a la URO, debe remitir la comunicación para realizar los ajustes en los riesgo y controles a que haya lugar.

- La Gerencia de Riesgo Regulatorio quien lidera el sistema de riesgo de seguridad de la información y Ciberseguridad, en caso de tener reporte de incidentes de la entidad, debe notificar a la URO para su gestión desde riesgo operacional.

Auditoría Interna

Sin perjuicio de las funciones asignadas en otras disposiciones a la Auditoría Interna, ésta debe evaluar periódicamente, de acuerdo con su plan de trabajo anual, el sistema SARO con el fin de determinar posibles debilidades en el sistema de control interno y solicitar los planes de acción que sean requeridos. Así mismo, informará los resultados de la evaluación a la Unidad de Riesgo Operacional al Vicepresidente de Riesgos Corporativos, Presidencia y Comité de Auditoria.

7. LINEAMIENTOS GENERALES

7.1 ETAPA I - IDENTIFICACIÓN DE RIESGOS OPERACIONAL

El objetivo específico de esta etapa es la identificación de los riesgos inherentes a partir del mapa de procesos o de la metodológica que la URO determine para la Entidad.

7.1.1 Identificación de Factores de Riesgo y Riesgos Operacionales

La identificación de los factores de riesgo y eventos de pérdida se lleva a cabo según lo establecido en las referencias normativas y el glosario de este documento.

7.1.2 Metodología de Identificación de Riesgos

- La determinación de los riesgos inherentes a un proceso se realizará por parte del dueño de proceso con apoyo de la URO, partiendo del conocimiento del mismo e identificando las posibles causas que puedan afectar el cumplimiento de los objetivos y estrategia de Grupo Aval.

- Quienes participen en la fase de identificación de riesgos deben apoyarse en información confiable y tener un buen conocimiento de los procesos y de la Entidad. Aparte de la

experiencia es recomendable el soporte documental que proporcionan los informes gerenciales y de auditoría, hallazgos de las entidades de vigilancia y control, planes, diagnósticos, regulaciones y normatividad, encuestas, listas de chequeo, datos estadísticos y registros de eventos.

- La identificación de los riesgos debe responder al siguiente ciclo de preguntas:

Figura No. 1

- Al efectuar el análisis se deberán tener en cuenta tanto los riesgos Operacionales que ya se han presentado como aquellos riesgos potenciales.

- La identificación de riesgos se realizará en base a los protocolos definidos por la URO.

- Una vez identificados los riesgos que podrían originar eventos de riesgo Operacional en un proceso, la información deberá registrarse en la matriz de riesgos definida por Grupo Aval.

- Previamente a la implementación o modificación de cualquier proceso, producto, servicio o canal, así como en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros, se realiza la identificación de los riesgos con el fin de prever el esquema de controles que puedan mitigar su impacto ante la materialización de los mismos.

7.1.3 Perfil de Riesgo Inherente

Corresponde al resultado de la identificación de los riesgos propios de la ejecución de la actividad sin tener en cuenta el efecto de los controles que realiza el proceso.

7.2 ETAPA II – MEDICIÓN DE RIESGOS OPERACIONALES

El objetivo específico de esta etapa es medir el nivel de Riesgo Operacional, para lo cual se realizará una medición cualitativa, y cuando se cuente con datos de eventos de Riesgo Operacional, se realizará de manera cuantitativa; para esto se establecen los siguientes lineamientos:

- La medición de la frecuencia del Riesgo Operacional se realiza con un horizonte de un año.
- Se determinan escalas de impacto y probabilidad para la medición de los riesgos.
- El perfil de riesgo inherente se realizará con base en el juicio de personas conocedoras de los procesos de la Entidad, para lo cual se aplica el esquema del método Delphi.
- Cuando se cuente con información suficiente de eventos de riesgo operacional, la valoración de probabilidad e impacto cualitativo se ajusta tomando como herramienta la base de los eventos materializados; estos eventos se cruzarán con la matriz de Riesgo Operacional cualitativa para ajustar el perfil de la valoración principal.
- Con el fin de realizar una adecuada valoración de los riesgos, se evalúa el impacto y probabilidad de variables tanto cualitativas como cuantitativas, bajo los criterios que se definen en el Anexo Metodológico de Riesgos A-R_corporativo-8.

7.3 ETAPA III – CONTROL

Con el fin de mitigar la materialización de los riesgos operacionales a los que se expone la Entidad en la ejecución de sus operaciones, se deben aplicar medidas de prevención y control, estas medidas están encaminadas a disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialice. Para efectos del SARO, se entiende que la matriz de riesgo operacional contempla aquellos controles clave que realmente mitigan el riesgo.
Durante esta etapa se establece:

- Metodología para definir las medidas de control de los riesgos operacionales.
- Medidas de control sobre cada uno de los riesgos operacionales.
- Medidas que permiten asegurar la continuidad del negocio.
- El perfil de riesgo residual de la entidad.

Sin perjuicio de lo anterior, la Entidad decide si transfiere, mitiga, acepta o evita el riesgo, en los casos en que esto sea posible. Cuando se decida la aceptación del riesgo, se deberán cumplir los protocolos que defina la URO.

La utilización de ciertas medidas, como la contratación de un seguro o tercerización (outsourcing) tanto de personas naturales y/o jurídicas, y que procedan al desarrollo de actividades de la Entidad, pueden ser fuente generadora de otros riesgos operacionales, los cuales deben ser a su vez administrados.

Para eso, la entidad debe: (i) realizar un análisis de riesgo para determinar los procesos y/o actividades a tercerizar; (ii) comprender el riesgo operacional asociado a los procesos y/o actividades tercerizadas; (iii) contar con políticas eficaces para incorporar en su estrategia de riesgos, aquellos derivados de la tercerización; y (iv) determinar dentro de los procesos y/o actividades tercerizadas aquellos que se consideren críticos.

7.3.1 Evaluación de Controles

En la evaluación de los controles se tienen en cuentan dos criterios: Cobertura y Oportunidad. Como resultado de la combinación de estos criterios se determina la eficiencia de control.

- Cobertura del control

Esta fase tiene como fin evaluar el control con respecto al riesgo que se está mitigando. Durante los ejercicios de riesgos y controles se debe tener en cuenta la experiencia del equipo de trabajo y las mejores prácticas para determinar si los controles definidos están encaminados a disminuir de una parte la probabilidad de ocurrencia o de otra el impacto del riesgo evaluado. De lo contrario, se deben establecer nuevos controles o complementarios.

- Oportunidad del control:

Es la calificación dada al nivel de ejecución del control en el proceso.

La suma de la cobertura y la oportunidad determinan la eficiencia del control:

- Si no se está ejecutando el control
- Si el control se está ejecutando en el proceso, pero no cumple con todos los parámetros establecidos en el diseño del mismo
- Si el control se está ejecutando en el proceso de acuerdo con los parámetros establecidos en el diseño del mismo

Las características de la evaluación de los controles se encuentran en el Anexo Metodológico de Riesgo Operacional.

7.3.2 Perfil de Riesgo Residual

En esta fase se tiene en cuenta el efecto de los controles sobre el perfil de riesgo inherente, el cálculo de impacto y probabilidad de ocurrencia se realiza de forma automática y evidencia los niveles de riesgo residuales para los procesos. La generación del perfil de riesgo residual incluye:

- La valoración de los controles existentes en cada proceso.
- Revisión de los eventos materializados.

7.4 ETAPA IV – MONITOREO Y REVISIÓN DEL SARO

Semestralmente la URO, realiza seguimiento a los perfiles de riesgo inherente y residual, así como a los eventos materializados, en este se revisa la valoración de nuevos procesos, nuevos controles y rediseño de los controles actuales.

Igualmente, se tiene en cuenta la evolución de las variables externas o internas que podrían estar generando una mayor probabilidad de ocurrencia o de impacto financiero.

El reporte semestral de la URO debe incluir al menos:

- Composición y Calificación de Riesgos (Informe de análisis efectuado a los factores y clases de eventos de riesgo Operacional identificados en la matriz).

- Resultados de los cambios generados por la actualización de la matriz de Riesgo Operacional, por nuevos procesos, controles, aplicación de planes de tratamiento o remediación frente al perfil.

- Informes Estadísticos de Eventos de Riesgo Operacional presentados.

- Análisis y Seguimiento a los Planes de Tratamiento.

- Reporte de aceptación de riesgos.

- Resultados de la ejecución del programa de capacitación.

En el proceso de monitoreo y seguimiento de los perfiles de riesgo, se usan como fuentes también, los indicadores descriptivos y prospectivos referenciados en el Anexo Metodológico de Riesgo Operacional, verificando el comportamiento y efectuando la valoración de estos en los casos que aplique.

Estos indicadores se enfocan en observar la gestión de control y la materialización de eventos a través del tiempo. Se pueden clasificar en indicadores de control o de desempeño (relacionados a resultados del procedimiento).

7.5 REGISTRO DE EVENTOS DE RIESGO OPERACIONAL

Los eventos de Riesgo Operacional son una fuente indispensable de información para la adecuada gestión del SARO. Para tal efecto, la Entidad cuenta con un registro de eventos de riesgo operacional el cual debe estar actualizado y su administración es responsabilidad de la URO.

El registro de eventos de riesgo operacional debe cumplir con los siguientes lineamientos:

- El registro debe contener todos los eventos de riesgo operacional ocurridos y que:
- Generan pérdidas y afectan el estado de resultados de la entidad.
- No generan pérdidas y por lo tanto no afectan el estado de resultados de la entidad.
- Las pérdidas definidas de acuerdo con el ítem anterior, cuando afecten el estado de resultados, deben registrarse en cuentas de gastos en el período en el que se materializó la pérdida.
- Las recuperaciones por concepto de riesgo operacional cuando afecten el estado de resultados deben registrarse en cuentas de ingreso en el período en el que se materializó la recuperación.
- Las cuentas de gastos e ingresos requeridas son definidas por la Superintendencia en el Catálogo Único de Información Financiera CUIF respectivo.
- Reportar todos los eventos, generen o no pérdidas. Todo el personal de la Entidad es responsable de realizar el reporte de eventos de riesgo Operacional o gestionar que estos sean reportados.
- El reporte de los eventos de Riesgo Operacional se realiza por medio del formato dispuesto por la URO, estos deben ser reportados mediante el mecanismo definido a dicha Unidad o en su defecto al Vicepresidente de Riesgos Corporativos.

- Los eventos de Riesgo Operacional generados por el factor Tecnológico (Hardware, software, telecomunicaciones) deben ser reportados al área de Soporte Técnico del Grupo Aval, con copia a la URO, para que se realice la gestión de corrección de la falla; posteriormente Soporte Técnico debe reportar la solución al proceso que reportó el evento y a la URO.
- Una vez reportado el evento a la URO, esta procederá a realizar la investigación y análisis del evento de riesgo Operacional, de manera que en conjunto con el dueño de proceso se pueda complementar el registro en los campos mínimos enunciados en el numeral anterior.
- Los eventos de riesgo Operacional que se reporten tienen como fin revisar posibles medidas que propendan por mejorar el ambiente de control del proceso. Las actividades de incumplimiento serán tratadas conforme a lo dispuesto en el Código de Ética y Conducta de Grupo Aval.
- Los registros de eventos sobre pérdidas operacionales deben ser integrales e incluir la totalidad de las actividades y exposiciones.
- Los campos mínimos para diligenciar en el Registro de eventos de Riesgo Operacional son:

Nombre	Descripción
Referencia	Código interno que relacione el evento en forma secuencial.
Fecha de inicio del evento	Fecha en que se inicia el evento.
	Día, mes, año, hora.
Fecha de finalización del evento	Fecha en que finaliza el evento.
	Día, mes, año, hora.
Fecha del descubrimiento	Fecha en que se descubre el evento.
	Día, mes, año, hora.
Fecha de registro contable	Fecha en que se registra contablemente la pérdida por el evento.
	Día, mes, año, hora.
Fecha de recuperación	Fecha en la cual se recupera total o parcialmente el dinero empleado para atender un evento de riesgo operacional.
	Día, mes, año, hora.
Divisa	Moneda extranjera en la que se materializa el evento.
Cuantía bruta	El monto de dinero (moneda legal) a que asciende la pérdida bruta.
Cuantía total recuperada	El monto de dinero recuperado por acción directa de la entidad. Incluye las cuantías recuperadas por seguros.
Cuantía recuperada por seguros	Corresponde al monto de dinero recuperado por el cubrimiento a través de un seguro.
Cuantía de otras recuperaciones	Corresponde al monto de dinero recuperado por otros mecanismos diferentes al cubrimiento a través de un seguro.
Cuantía neta de recuperaciones	El monto de dinero (moneda legal) a que asciende la pérdida teniendo en cuenta la cuantía total recuperada.
Clase de riesgo operacional	Especifica la clase de riesgo, según la clasificación indicada en el glosario de este documento.
Producto/servicio afectado	Identifica el producto o servicio afectado.
Cuentas Catálogo afectadas	Identifica las cuentas del Catálogo Único de Información Financiera con Fines de Supervisión" (CUIF) afectadas.
Proceso	Identifica el proceso afectado.
Tipo de pérdida	Identifica el tipo de pérdida, de acuerdo con lo señalado en la Etapa III – Registro de eventos de riesgo operacional
Descripción del evento	Descripción detallada del evento.
	- Canal de servicio o atención al cliente (cuando aplica)
	- Zona geográfica
Líneas de negocio	Identificación según clasificación adoptada por la SFC, estas líneas están indicadas en el formato de reporte de eventos.

7.6 DIVULGACIÓN DE INFORMACIÓN

El Manual para la gestión del Riesgo Operacional aprobado por la Junta Directiva, es divulgado por el área de Organización y Métodos en el recurso compartido de la Entidad.

7.7 CAPACITACIÓN

Es requisito indispensable tanto para colaboradores antiguos como en la inducción a nuevos Colaboradores, se efectúe la capacitación sobre el SARO. Es por esto, que la entidad organiza las jornadas de capacitación y en ellas se integran aspectos relacionados con la gestión del riesgo operacional y la continuidad de negocio, en aras de lograr que las políticas y procedimientos del SARO sean conocidos en forma adecuada por todos los Colaboradores.

Grupo Aval lleva a cabo al menos una jornada de capacitación anual para colaboradores antiguos y está enfocada en brindar conocimientos en los mecanismos y herramientas requeridos para la adecuada administración del Riesgo Operacional.

De estos programas queda como soporte el registro de asistencia para inducción y registro de participación para colaboradores antiguos, además se dispone de una evaluación o taller para medir los conocimientos adquiridos por parte de los colaboradores.

Cuando en virtud de una relación contractual existan terceros que desarrollen funciones de la entidad, se efectúa una capacitación sobre los aspectos relevantes del SARO.
Esta actividad debe es liderada la URO con el apoyo el área Administrativa y de Talento Humano.

El programa de capacitación cuenta con la evaluación de los resultados obtenidos que permite determinar la eficacia del programa.