MANUAL PARA LA ADMINISTRACIÓN DEL SISTEMA DE RIESGO OPERATIVO (SARO)

APROBADO

proinvioriente
Proyectos de Inversión Vial del Oriente

CORREDOR VILLAVICENCIO - YOPAL

APROBADO	FERNANDO REYES GIRALDO Director General EPC – PROINVIORIENTE	Aprobado en acta de junta directiva N.º 61 del 18 de julio de 2024

TABLA DE CONTENIDO

1. PRESENTACIÓN 3
2. INTRODUCCIÓN 3
3. OBJETIVOS 4
4. ALCANCE 4
5. PRINCIPIOS DE GESTIÓN DEL RIESGO OPERATIVO 5
6. DEFINICIONES 5
7. POLÍTICAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO 9
8. ROLES Y RESPONSABILIDADES 11
9. ADMINISTRACIÓN DEL RIESGO OPERATIVO 13
10. METODOLOGÍA 13
11. REGISTRO DE EVENTOS DE RIESGO OPERATIVO 27
12. REPORTES 31
13. ESCALAMIENTO 31
14. ACTUALIZACIÓN 31
15. DIVULGACIÓN 32
16. CAPACITACIÓN 34
17. ANEXOS 35
18. CONTROL DE CAMBIOS 35

APROBADO

1. PRESENTACIÓN

El presente Manual de Riesgo Operativo de **PROYECTOS DE INVERSIÓN VIAL DEL ORIENTE S.A.S,** en adelante **PROINVIORIENTE**, fue elaborado con base en las mejoras prácticas emitidas a través de circulares normativas por entes reguladores para este tipo de sistemas, adicionalmente incorporando como marco de referencia, el modelo corporativo de Corficolombiana y las iniciativas de Gobierno Riesgos y cumplimiento de casa matriz.

Se definen las políticas, metodologías y etapas requeridas para la administración del Riesgo Operativo de la actividad empresarial de **PROINVIORIENTE**, para fortalecer los mecanismos de control para la minimización de los riesgos operativos a los cuales pueda estar expuesta su operación.

La información contenida en este documento es de uso exclusivo de **PROINVIORIENTE**. Se prohíbe su divulgación y conocimiento a cualquier ente externo sin la debida autorización, a excepción de los organismos de vigilancia y supervisión facultados con autorización previa del responsable del Sistema de Administración de Riesgo Operativo (SARO). En caso de su reproducción y divulgación sin previa autorización, se someterá a las disposiciones conferidas en el reglamento interno de trabajo, Código de ética y la Política de seguridad de la información y Ciberseguridad de **PROINVIORIENTE**.

El contenido del presente Manual será sometido a revisión cada vez que se requiera la cual será realizada por la Coordinación de Gobierno, Riesgo y Cumplimiento (en adelante Coordinación de GRC) con el fin de incorporar, si procede, las modificaciones necesarias para la adaptación de su contenido a las normas o lineamientos que casa matriz dicte o la mejora de los criterios y procedimientos establecidos a sugerencia de la propia experiencia de **PROINVIORIENTE**. Las modificaciones que sean necesarias al presente Manual con posteridad a su aprobación se adoptaran por decisión de la Junta Directiva o quien haga sus veces en **PROINVIORIENTE**.

El presente Manual se aplica a partir de su aprobación y actualizaciones por parte de la Junta Directiva o quien haga sus veces en **PROINVIORIENTE**, según se muestra en la sección de control de cambios que se encuentra al final de este documento.

2. INTRODUCCIÓN

El presente modelo tiene como objetivo definir los elementos necesarios para la adecuada gestión y control del Sistema de Administración de Riesgo Operativo, en adelante “SARO”. El modelo deberá fortalecer y mejorar las políticas y prácticas en cuestiones de gestión, control y mitigación del SARO, para así reducir las pérdidas derivadas del mismo en el futuro.

APROBADO

La directriz para la elaboración de este manual está contemplada en el Marco de Gestión de Riesgo Operativo, normatividad, y disposiciones a nivel corporativo (emitidas por Corficolombiana y/o Grupo Aval). En ese mismo orden, **PROINVIORIENTE** estará focalizando los esfuerzos en la implantación y constante mejora de la Gestión de Riesgo Operativo que permita alcanzar los siguientes objetivos.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Documentar la metodología utilizada para identificar, medir, tratar, monitorear y reportar el riesgo operativo (incluido el riesgo de fraude) de **PROINVIORIENTE**. Asimismo, este Manual está dirigido a todas las contrapartes vinculadas con **PROINVIORIENTE** con las cuales se establezca una relación de negocio.

3.2. OBJETIVOS ESPECÍFICOS

- Identificar, evaluar y realizar el seguimiento de los riesgos operativos de **PROINVIORIENTE**.
- Controlar y mitigar los riesgos operativos de todas las líneas de negocio y unidades, identificando y mitigando focos de riesgo en cualquier ubicación dentro de la operación del negocio.
- Impulsar la cultura y conciencia organizacional en materia de riesgo operativo.
- Contar con una estructura organizacional efectiva y responsable de la coordinación para la administración del riesgo operativo.
- Establecer las metodologías para la identificación, medición, tratamiento y monitoreo de los riesgos operativos.

4. ALCANCE

El Manual SARO de **PROINVIORIENTE**, está dirigido a todos los accionistas, miembros de Junta Directiva o quienes hagan sus veces, colaboradores, clientes y proveedores, y demás terceros vinculados con **PROINVIORIENTE**. El proceso inicia con la identificación de riesgos operativos y finaliza con su tratamiento, monitoreo y reportes relacionados, de acuerdo con los procesos identificados en el mapa de procesos de **PROINVIORIENTE**.

Dado los factores de riesgo que incorpora en su definición el Riesgo Operativo, su alcance involucra la totalidad de proceso representados en el 4GL-MP-DIR-001 MAPA DE PROCESOS SIG PROINVIORIENTE.

APROBADO

5. PRINCIPIOS DE GESTIÓN DEL RIESGO OPERATIVO

A continuación, se establecen principios generales del SARO en el marco normativo y en consonancia con las buenas prácticas para la gestión y supervisión del Riesgo Operativo:

- La Junta Directiva o quien haga sus veces deberá conocer los principales aspectos del Riesgo Operativo y aprobar y revisar el marco de gestión.
- El marco de gestión del Riesgo Operativo debe estar sujeto a revisiones de Auditoría Interna.
- La gestión del Riesgo Operativo forma parte de las responsabilidades de la Junta Directiva o quien haga sus veces, que debe velar por la implantación del marco de gestión en **PROINVIORIENTE**.
- Todos los colaboradores de **PROINVIORIENTE** son considerados gestores del Riesgo Operativo inherente a los procesos y sistemas, con los que interactúa en su actividad diaria.
- La gestión directa y activa del Riesgo Operativo recae en cada una de las diferentes unidades o áreas de **PROINVIORIENTE**, determinada por el mapa de procesos.
- El control del Riesgo Operativo, de forma adicional e independiente a la gestión, la realiza el responsable de Riesgo Operativo (Coordinación de GRC) y tiene por objeto su identificación, evaluación, tratamiento y monitoreo por medio de herramientas cualitativas y cuantitativas.
- Se dispondrá de planes de contingencia y de continuidad de negocio para mantener su operatividad y reducir las pérdidas en caso de interrupciones del negocio.
- Se dispondrá de información suficiente para cubrir lo requerido por la Junta Directiva o quien haga sus veces en **PROINVIORIENTE**, con el fin de cumplir con toda la normativa emitida por el ente regulador en esta materia.

Adicionalmente, anualmente se llevará a cabo la revisión y si procede, la modificación del apetito de Riesgo de **PROINVIORIENTE**, a través de la definición de perfiles que deberán conducir al establecimiento de umbrales de Riesgo Operativo. Estas definiciones deberán ser presentadas para su aprobación por parte de la Junta Directiva o quien haga sus veces en PROINVIORIENTE.

6. DEFINICIONES

Ambiente de control: Conjunto de estándares, procesos y estructuras que proveen la base para ejecutar el control interno a través de la organización.

Análisis de Riesgos: Uso sistemático de la información disponible, para determinar la probabilidad/frecuencia con la que pueden ocurrir eventos y la magnitud de sus impactos (consecuencias).

Apetito al riesgo: Se refiere a la medida de riesgos que la organización está dispuesta a aceptar para cumplir su misión, visión y objetivos estratégicos.

APROBADO

Asociación (Listado de riesgos corporativo): Se refiere a la combinación de tipo, categoría y subcategoría para un riesgo corporativo genérico de SARO.

Consecuencia: Resultado o impacto de un evento.

Control (Actividad de control): Acciones establecidas a través de las políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos.

Control Clave: Son controles que operan a un nivel de precisión que les permite cumplir con los objetivos para los cuales fueron diseñados y mitigar de manera significativa la exposición al riesgo.

Control Compensatorio: Son controles que operan a un nivel de precisión menor que el de un control clave pero que mitigan la posibilidad de que exista una exposición al riesgo cuando otro control es deficiente.

Control Complementario: Son controles que funcionan en conjunto con otros controles para cumplir con el mismo objetivo de control. Una falla en estos controles puede generar que no se cumpla con el objetivo de control o que se cumpla en un nivel diferente de precisión.

Control del Riesgo: Parte de la administración del riesgo que involucra la implementación de políticas, normatividad, procedimientos y cambios físicos a fin de eliminar o minimizar los riesgos adversos.

Cultura de gestión de riesgos operativos: conjunto de valores, actitudes, competencias y comportamientos individuales y corporativos que conforman el compromiso y estilo de una empresa para la gestión del riesgo operativo. – Fuente: BCBS-Gestión y supervisión del Riesgo Operativo.

Dueño del proceso: Es el representante del proceso, que conoce sus expectativas y necesidades y las traduce en requerimientos (acuerdos de niveles de servicio - ANS) al interior de **PROINVIORIENTE**. En coordinación con los ejecutores, diseña el proceso y asigna responsables dentro de las etapas o subprocesos.

Asimismo, es el encargado de reportar los eventos de riesgo operativo que puede a la vez ser responsable del proceso impacto. Es quien establece también los planes de acción del evento operativo reportado.

Evaluación del Riesgo: Proceso usado para determinar las prioridades de administración del riesgo mediante la comparación de la probabilidad del riesgo, contra impacto.

APROBADO

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

Eventos Materializados por Riesgo Operacional / Evento de riesgo operativo (ERO): Son aquellos incidentes que generan pérdidas por riesgo operacional que se haya materializado en la empresa.

Fraude: Actividad deshonesta u omisión intencional o negligente diseñada para engañar a otros y generar sobre la víctima una pérdida y/o sobre el autor un beneficio. El fraude puede contextualizarse según las fuentes que lo originan de la siguiente manera.

Fraude Interno: Evento de riesgo por actos causados por un funcionario de **PROINVIORIENTE**, ya sea presidente, vicepresidentes, gerentes, directivos, administradores, representante o cualquier trabajador o colaborador.

Fraude Externo: Eventos de riesgo generados por un tercero sin la asistencia de un funcionario.

Fraude mixto: Fraude cometido conjuntamente por colaboradores y/o administradores de PROINVIORIENTE en coalición con un tercero.

Gestión de Riesgo: Actividades para dirigir y controlar una organización con respecto al riesgo.

Impacto: Índice que mide las consecuencias que tendría la materialización del riesgo sobre los procesos de negocio. Pérdida potencial que se puede generar en caso de ocurrencia del evento de riesgo operativo.

Mapa térmico: Representación gráfica del nivel de severidad de un riesgo.

Materialización (de un riesgo): Ocurrencia de un evento considerado como incierto (riesgo) y que su desarrollo implica una consecuencia positiva o negativa a la organización.

Mitigar: Reducción del nivel de riesgo existente a un nivel aceptable por la organización.

NAS (Network Attached Storage): Corresponde al dispositivo de almacenamiento mediante el cual es posible compartir la estructura de carpetas y archivos a través de la red.

Nivel de Precisión: Grado de detalle y/o alcance bajo el cual opera el control. Indica la cobertura respecto a la exposición al riesgo.

Nivel de Severidad: Es el indicador cualitativo que resulta de multiplicar el impacto por su probabilidad/frecuencia.

APROBADO

Normatividad: Conjunto de disposiciones de carácter jurídico que permite regular una materia, actividad o sector específico. Incluyen la Constitución Nacional, leyes, decretos, resoluciones, reglamentos técnicos, entre otros.

Pérdida: Cuantificación económica del impacto derivado de la ocurrencia de un evento de riesgo operacional, así como los gastos derivados de su atención.

Perfil de riesgo: Resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la compañía.

Plan de Contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de Continuidad de Negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Probabilidad/frecuencia: Índice por medio del cual se mide que tan factible es que se materialice el riesgo.

Proceso: Es un conjunto de actividades y recursos interrelacionados que transforman elementos de entrada en elementos de salida o resultados.

Requisitos: Circunstancia o condición necesaria para una cosa o actividad.

Riesgo: Son eventos futuros inciertos, tanto positivos como negativos, que tienen el potencial de afectar el logro de las metas y objetivos de una Entidad.

Riesgo de Fraude: Posibilidad de ocurrencia para la ejecución de un evento de fraude.

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

Riesgo Operativo: Es la posibilidad de ocurrencia de pérdidas financieras, originadas por fallas o insuficiencias de procesos, personas, sistemas internos, tecnología, y en la presencia de eventos externos imprevistos. Esta definición incluye el riesgo legal.

Riesgo Residual: Es el riesgo que subsiste después de haber implementado controles.

Sistema de Administración de Riesgo Operativo (SARO): Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgos

APROBADO

operacional, órganos de control, divulgación de información y capacitación, mediante los cuales la empresa que adopta este modelo identifica, mide, controla y monitorea el riesgo operacional.

Subproceso: Es una parte bien definida y delimitada de un proceso. Una actividad o una secuencia ordenada de actividades con compañía propia dentro de un proceso.

7. POLÍTICAS PARA LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

PROINVIORIENTE acoge como suyos los principios sobre los cuales se fundamenta y estructura su sistema de administración de riesgo operativo. Tales principios son expresiones de la Alta Dirección para una presentación y valoración justa y transparente del riesgo operativo, permitiendo la adecuada identificación de controles a nivel de proceso que mitigan razonablemente los riesgos identificados. Estos principios están documentados en la 4GL-PO-GRC-001 Política de Riesgo Operativo.

La Administración de riesgos operativos de **PROINVIORIENTE** involucra a los diferentes procesos y/o áreas de esta y a cada una se le asignan responsabilidades diferentes:

- **Junta Directiva o quien haga sus veces**

Las responsabilidades de la Junta Directiva o quien haga sus veces, respecto a la aplicación de SARO son:

- Aprobación de las Políticas de Riesgo Operativo.
- Aprobación del Manual de Riesgo Operativo y sus posteriores actualizaciones.
- Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo de **PROINVIORIENTE.**
- Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo de **PROINVIORIENTE** (definición de las escalas de medición de Probabilidad/ frecuencia e impacto).
- Toma de decisiones sobre los puntos de los informes que la Coordinación de GRC emite periódicamente.
- Emitir su pronunciamiento sobre la evaluación que los órganos de control realizan de forma periódica sobre SARO.
- Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.
- Aprobación de los planes de contingencia y de continuidad de negocio.

- **Representante Legal**

APROBADO

Se ocupará de:

- Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva o quien haga sus veces.
- Adelantar el seguimiento de los elementos y etapas de SARO.
- Garantizar el cumplimiento de estrategias que permitan implementar una adecuada cultura de gestión de riesgos operativos en **PROINVIORIENTE.**
- Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.
- Evaluar los informes que recibe de la Coordinación de GRC y de los Órganos de control.
- Garantizar la implementación de procedimientos para la administración adecuada de riesgos operativos.
- Presentación de informes sobre la evaluación del SARO ante la Junta Directiva o quien haga sus veces.

- **Coordinación de GRC**

Es el área la encargada de presentar el modelo de riesgo operativo dispuesto, para su evaluación y hacer los ajustes necesarios para su buen funcionamiento. Tendrá dentro de sus funciones:

- Diseño e implementación del Manual de Riesgo Operativo.
- Establecer los instrumentos, métodos y procedimientos para que sea posible una administración eficaz de los riesgos.
- Desarrollo e implementación del sistema de reportes de los riesgos administrados.
- Seguimiento del perfil de riesgo.
- Seguimiento de las etapas de SARO.
- Asegurar que los procedimientos contemplen una adecuada administración, gestión y control de los riesgos operativos.
- Emitir informes sobre la evolución de SARO al Representante Legal o la Junta Directiva o quien haga sus veces.
- Seguimiento de los procedimientos y planes de acción implementados por los procesos.
- Diseño de sistemas de medición de SARO.
- Implementar Programas de capacitación en SARO para todos los colaboradores de **PROINVIORIENTE**.
- Evaluación y seguimiento a las medidas implementadas (controles) para la administración de los riesgos inherentes.
- Informar al Representante Legal sobre la evolución de riesgos y los controles del SARO.
- Proponer actualizaciones del Manual de procedimientos.
- Evaluación de los informes que presente la Auditoría Interno o externa referentes al SARO.
- Definir un procedimiento para el registro de los eventos de riesgo operativo.

APROBADO

- Administrar los registros de Eventos de Riesgo Operativo (ERO).
- Garantizar la integridad, confiabilidad, cumplimiento, disponibilidad, eficiencia, efectividad y confidencialidad en el registro de eventos de riesgo operativo.

- **Responsabilidades generales de todas las áreas**

Dentro de la estructura organizacional y responsabilidades definidas para una adecuada gestión del SARO, es importante considerar el hecho de que los eventos de riesgo pueden afectar a todas las áreas de **PROINVIORIENTE**, por lo que los responsables de los procesos asumirán responsabilidades sobre los riesgos operativos de sus áreas, adelantando la gestión de estos y su materialización, cuando se produzcan.

También tendrán la responsabilidad de fomentar la cultura de administración del riesgo al interior de sus equipos de trabajo. Asimismo, tienen la obligación de desarrollar todas y cada una de las etapas del SARO.

8. ROLES Y RESPONSABILIDADES

Para la adecuada implementación, ejecución y monitoreo del SARO, la Junta Directiva de **PROINVIORIENTE**, ha definido los roles y responsabilidades de cada uno de sus actores. Estos se encuentran establecidos en el documento 4GL-PO-GRC-001 Política de Riesgo Operativo. A continuación, se presentan en un detalle más específico los roles de: dueño de proceso, funcionarios de **PROINVIORIENTE** y el área de Auditoría Interna.

8.1. DUEÑO DE PROCESO

Los dueños de cada uno de los procesos de PROINVIORIENTE tendrán las siguientes responsabilidades:

- Identificar y medir los riesgos asociados a los procesos que lideran, de conformidad con la metodología aprobada, con apoyo de la Coordinación de GRC.
- Documentar con el apoyo de la Coordinación de GRC, los controles en la Matriz ERM, con el fin de mitigar las causas identificadas, los cuales deben ser evaluados frente a los criterios establecidos.
- Gestionar y documentar la ejecución de los controles asociados a su proceso.
- Cumplir con las acciones establecidas para el mejoramiento de los controles en materia de riesgo operativo.

APROBADO

- Coordinar la formulación, el seguimiento y la ejecución de planes de acción que permitan mitigar las causas que se encuentren asociadas a cada riesgo, soportándose en los demás colaboradores del área.
- Promover entre todos los colaboradores de su proceso, la identificación y reporte de alertas sobre situaciones que pueden ser eventos de riesgo operativo.
- Realizar el registro de los eventos de riesgo materializados, definir los planes de acción necesarios para prevenir que éstos se presenten nuevamente y velar por su implementación oportuna y de manera eficaz.
- Certificar mensualmente a la Coordinación de GRC la ausencia de eventos de riesgo operativo cuando no se hayan materializado eventos de riesgo en los procesos a cargo
- Mantener y fortalecer la cultura de gestión de riesgo operativo al interior de cada proceso.
- Validar la efectividad de los controles implementados para los riesgos operativos de sus procesos a cargo.
- Comunicar a la Coordinación de GRC el incumplimiento de las políticas, procedimientos y planes de acción asociados al SARO.

8.2. FUNCIONARIOS

Los funcionarios de **PROINVIORIENTE** tendrán las siguientes responsabilidades:

- Dar soporte al dueño de proceso en la identificación, medición y actualización de los riesgos operativos inherentes a su actividad.
- Gestionar y documentar la ejecución de los controles que le sean asignados asociados a sus procesos.
- Cumplir con las acciones establecidas para el mejoramiento de los controles en materia de riesgo operativo.
- Gestionar y documentar la ejecución de los planes de acción para el establecimiento o mejoramiento de controles, cuando se les asigne.
- Alertar y reportar oportunamente al Dueño de proceso respecto a eventos riesgo operativo.
- Atender oportunamente los requerimientos del dueño de proceso o a la Coordinación de GRC para documentar y soportar el evento de riesgo reportado.

8.3. AUDITORÍA

Las siguientes son responsabilidades adicionales a las indicadas en el documento 4GL-PO-GRC-001 Política de Riesgo Operativo:

- Conocer en detalle los procesos a evaluar, su documentación, riesgos y controles asociados.
- Conocer en detalle el contenido y funcionamiento del SARO.
- Validar el cumplimiento de lo dispuesto en este manual.

APROBADO

- Verificar que los controles identificados se encuentren diseñados de acuerdo con los parámetros indicados en este documento, que mitiguen el riesgo al que se encuentran asociados y que se estén ejecutando tal y como han sido documentados.
- Proveer una visión independiente respecto a la efectividad del enfoque usado en la identificación de riesgos y la metodología empleada en su gestión.
- Generar informes de auditoría donde se resuman las oportunidades de mejora y hallazgos encontrados. Estos deberán ser compartidos con la Coordinación de GRC, el Director General EPC y la Junta Directiva.

9. ADMINISTRACIÓN DEL RIESGO OPERATIVO

Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores. El riesgo operacional se relaciona con las actividades propias de **PROINVIORIENTE**. En otras palabras, se refiere a los posibles fallos o deficiencias en los recursos y procesos de las actividades del día a día.

- **Riesgo legal**

Es la posibilidad de pérdida en que incurre una empresa 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.

- **Riesgo reputacional**

Es la posibilidad de pérdida en que incurre una empresa por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto a sus prácticas de negocios y que cause pérdida de clientes o accionistas, disminución de ingresos o procesos judiciales.

10. METODOLOGÍA

La metodología establecida por **PROINVIORIENTE** para la administración del riesgo operativo se fundamenta en cuatro etapas: identificación, medición, control y monitoreo, las cuales, a su vez, deben cumplir con unos pasos para su debida implementación.

APROBADO

La administración/gestión de los riesgos operativos involucra la ejecución de un proceso iterativo cuyas etapas permiten disminuir la probabilidad de ocurrencia y el impacto del riesgo en caso de materializarse.

PROINVIORIENTE adopta la norma técnica, Gestión de Riesgo- Principios y Directrices, como referente técnico para llevar a cabo el proceso de administración de los riesgos operativos, el cual será soportado por infraestructura tecnológica y políticas y lineamientos que dirigirán su ejecución, con ilustra la gráfica a continuación:

Las distintas etapas del Modelo de Gestión del Riesgo Operativo implican:

- Identificar el Contexto interno y externo de **PROINVIORIENTE**. Determinar la estrategia de **PROINVIORIENTE** para el periodo en el que se realiza la evaluación del riesgo, de la misma forma la misión, visión, objetivos, cultura, modelo de operación y estructura de **PROINVIORIENTE** que permitirán el entendimiento de factores que se tendrán en cuenta posteriormente en la identificación de los riesgos. Por otro lado, en el contexto externo se determinan los factores sociales, económicos, tecnológicos, político, competitivo y legales para entender los factores externos a **PROINVIORIENTE** que pueden generar un riesgo.
- Identificar el Riesgo Operativo inherente a todas las actividades, productos, procesos y sistemas de **PROINVIORIENTE**, tanto existentes como de nueva definición, en cuanto a factores de tipo interno y externo, el proceso se desarrolla a través de la implementación de las diferentes técnicas de identificación del riesgo con los encargados con cada uno de los procesos.
- Medir y evaluar el Riesgo Operativo de forma objetiva, continuada y coherente con los estándares de la industria, y definir objetivos y niveles de tolerancia (umbrales) de riesgo.

APROBADO

- Realizar un seguimiento continuo de las exposiciones de Riesgo Operativo, con el fin de detectar niveles de riesgo no asumidos, implantar procedimientos de control, mejorar conocimiento interno y mitigar las pérdidas.
- Establecer medidas de mitigación que eliminen o minimicen el Riesgo Operativo.
- Generar informes periódicos sobre la exposición al Riesgo Operativo.
- Definir y documentar las políticas para la gestión del Riesgo Operativo, e implementar metodologías de gestión de este riesgo acordes con la normativa y las mejores prácticas.

10.1. IDENTIFICACIÓN

Consiste en reconocer y determinar las causas (factores de riesgo) y riesgos inherentes a los procesos de **PROINVIORIENTE** con los responsables de los procesos y subprocesos, es decir, el riesgo puro sin el efecto del control, que impedirían la consecución de los objetivos propios del negocio.

10.1.1. Entendimiento del proceso (Análisis de contexto).

El entendimiento del proceso es el punto de partida de una identificación eficiente de los factores internos o externos que pueden generar riesgos y que, por lo tanto, atenten contra el cumplimiento de la misión y objetivos de **PROINVIORIENTE.**

El análisis del contexto externo se realiza a partir del conocimiento e identificación de situaciones que pueden ser de carácter: social, económico, tecnológico, político, competitivo, ambiental y legal, bien sean locales, de la industria, regionales, nacionales o internacionales. Igualmente, implica el entendimiento de los clientes, proveedores, competidores y rivalidad entre competidores.

Las situaciones internas están relacionadas con la estrategia, objetivos de la organización, estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes, programas y proyectos, los sistemas de información, los procesos, procedimientos y los recursos humanos y económicos con los que cuenta **PROINVIORIENTE**, como ayuda en la determinación del contexto del proceso, es necesario realizar el análisis de flujo o caracterización del proceso (representación esquemática de interrelaciones de entradas, tareas, salidas y responsabilidades).

Como resultado de este análisis la Coordinación de GRC diligenciará el formato CVO-RE-GRC-004 Contexto externo e interno de la organización. Este se debe presentar como una guía a los dueños de proceso para las sesiones de identificación de riesgos, de tal manera que permita darles información de referencia respecto a **PROINVIORIENTE**. Sin embargo, esta información podrá ser modificada y corregida durante la ejecución de las sesiones con los aportes de los participantes.

10.1.2. Alcance de la identificación

APROBADO

El alcance de la identificación se encuentra determinado por los procesos que se encuentren totalmente documentados en **PROINVIORIENTE**, debido a que cuenta con un mapa de todos los procesos y subprocesos y que implican y, por tanto, es posible listar más fácilmente los eventos de riesgo posibles.

10.1.3. Sesiones de identificación

Luego de definir el alcance, es necesario seleccionar el método para identificar las situaciones de riesgo y el espacio en el que se ejecutarán. En el formato CVO-RE-GRC-009 Técnicas de Identificación de Riesgos se encuentran algunas opciones para ejecutar esta actividad.

Para ejecutar la identificación del proceso será necesario desarrollar sesiones de identificación con el dueño de proceso, directivos (si se considera necesario) y funcionarios que participan en el proceso implementando la técnica seleccionada. La identificación del riesgo debe tener en cuenta el conocimiento previo de situaciones como:

- Retroalimentación de los hallazgos de las auditorías internas y/o externas realizadas a los procesos de **PROINVIORIENTE**.
- Base de datos del registro de eventos de riesgo operativo Formato CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo (ERO).
- Sesiones periódicas de monitoreo de los procesos con el acompañamiento de la Coordinación de GRC y los dueños de procesos.
- Identificación y análisis de nuevos proyectos, servicios o procesos en **PROINVIORIENTE.**

Líneas base de riesgos y controles definidas por el Grupo Aval o Corficolombiana para los diferentes procesos (de existir).

Al ejecutar la técnica de identificación de riesgos seleccionada es posible determinar las situaciones o eventos de riesgo operacional, estos pueden resultar de:

- Falta de adecuación.
- Fallo en los procesos.
- Personal.
- Sistemas internos.
- Acontecimientos externos.

Se deben tener en cuenta los siguientes parámetros:

- El objetivo del proceso.
- Partes involucradas, interacciones internas o externas, roles y responsabilidades.
- Los productos y/o servicios que genera el proceso.

APROBADO

- Sistemas de información que participan en el proceso.
- Eventos o situaciones que pueden causar fallas en el proceso.
- Las contingencias del proceso.

Para cada evento identificado, es necesario redactar un riesgo, al momento de redactar los riesgos deberán tenerse en cuenta los siguientes criterios:

- El riesgo debe estar escrito en un lenguaje claro, común y comprensible para toda la Compañía.
- Se deben emplear verbos en infinitivo.
- Evitar las negaciones para expresar el Riesgo. Ejemplo: No realizar la actualización de una información.
- El riesgo no debe ser el efecto o el impacto de este. Ejemplo: Sanciones, multas, sobrecostos.
- La ausencia o deficiencia de un control no es un riesgo.

Para la documentación de los riesgos operativos identificados, sus causas y controles, se utilizará la Matriz ERM, de acuerdo con lineamiento emitido por la Vicepresidencia Corporativa de Gobiernos Riesgos y Cumplimiento de Corficolombiana.

El alcance del formato toma como base el mapa de procesos y subprocesos definidos y aprobados en **PROINVIORIENTE**. La Coordinación de GRC es la responsable de acompañar al dueño de proceso en la identificación y documentación de la información requerida en el formato, adicional tiene bajo su responsabilidad la administración del documento evaluando la razonabilidad de las modificaciones que sean requeridas. La Matriz ERM se desarrollará conjuntamente para el proceso y sus subprocesos para así identificar correctamente los riesgos aplicables y que a su vez se puedan establecer causas, controles, entre otros. El desarrollo de las actividades de documentación de los riesgos se dará como aprobada por el dueño de proceso a través del formato CVO-RE-GRC-003 Acta de formalización riesgos y controles SARO.

10.1.4. Definir Causas del Riesgo

Además de identificar el riesgo, es necesario que se determinen las causas y efectos (consecuencias) de la materialización del riesgo.

Las causas son las fuentes generadoras de riesgos operativos que pueden o no generar pérdidas. El riesgo se describe como una combinación de categoría de riesgo y causa raíz en una actividad determinada.

APROBADO

Las causas del riesgo (factores internos o externos) son los medios, circunstancias y agentes que solos o en combinación tienen el potencial de ocasionar un riesgo. Generando o no pérdidas para PROINVIORIENTE.

Cuando se generen dudas con respecto a si se identificó un riesgo o realmente lo identificado es una causa, se sugiere recordar la frase del riesgo:

"Debido a _CAUSA_ puede ocurrir _RIESGO_ lo que conllevaría a _EFECTO_"

Como resultado de la ejecución de este ejercicio, la Coordinación de GRC documentará en la Matriz ERM los riesgos identificados por proceso y subproceso.

10.1.5. Definir Factores que generan el Riesgo Operacional

Así mismo, las causas identificadas están asociadas a tipos de agentes generadores, los cuales se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

Por lo tanto, es necesaria que a cada causa le sea asignada una categoría de acuerdo con la siguiente clasificación:

- Recurso Humano.
- Procesos.
- Tecnología.
- Infraestructura.
- Eventos Externos.

- **Recurso Humano:** Posibilidad de pérdidas financieras y/o reputacionales asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores.

  Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación de personal.

- **Procesos:** Posibilidad de pérdidas financieras y/o reputacionales relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes dentro de la empresa, que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de estos.

APROBADO

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.

- **Tecnología de Información:** Posibilidad de pérdidas financieras y/o reputacionales derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la empresa al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

  Se puede considerar el incluir en esta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología, entre otros aspectos.

  Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

- **Infraestructura:** Posibilidad de pérdidas financieras y/o reputacionales asociadas con la inadecuada existencia o falta de elementos de apoyo para el adecuado y eficiente funcionamiento de la empresa. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

- **Eventos Externos:** Posibilidad de pérdidas financiera y/o reputacionales derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información.

  Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen el continuo cambio en las leyes, regulaciones o normativas.

10.1.6. ALINEACIÓN CON RIESGOS GENÉRICOS

Una vez identificados los riesgos para **PROINVIORIENTE**, es necesario asociar cada uno de ellos con un Riesgo Corporativo SARO. Para esto, el Grupo Aval ha definido un Catálogo de Riesgos Genéricos SARO, el cual deberá ser utilizado en cumplimiento del M-AR-RO-01 Manual Políticas

APROBADO

SARO Corporativo del Grupo Aval, esto con el fin de permitir la consolidación de riesgos a Corficolombiana.

La asociación debe ejecutarse teniendo en cuenta la descripción riesgo identificado en **PROINVIORIENTE** el cual debe compararse con el tipo, categoría y subcategoría del riesgo corporativo para lograr el mejor ajuste posible entre ambos listados.

El resultado de este la homologación de los riesgos de proceso a los riesgos genéricos es documentado en la Matriz ERM.

10.2. MEDICIÓN

Luego de identificar la totalidad de los riesgos es necesario medirlos y evaluarlos. Esta etapa tiene como objetivo establecer el nivel de riesgo inherente al cual está expuesto cada uno de los procesos de **PROINVIORIENTE**, teniendo en cuenta los criterios definidos por la Junta Directiva, en consonancia con lo establecido en la 4GL-PO-GRC-001 Política de Riesgo Operativo.

10.2.1. Probabilidad/frecuencia de Ocurrencia:

Consiste en determinar qué tan factible es la materialización de un riesgo respecto a la frecuencia de ejecución de la actividad ligada al riesgo a evaluar. Para determinar la probabilidad se utiliza el análisis cualitativo o cuantitativo (probabilidad/frecuencia). Ver anexo Matriz ERM.

Se fundamenta en estimar las consecuencias que tendría la materialización del riesgo sobre los procesos de **PROINVIORIENTE**.

El impacto será representado en escala de pérdida económica de **PROINVIORIENTE** o pérdida reputacional por deterioro en la interacción con los grupos de interés y en la imagen de la compañía o del Grupo Empresarial, por divulgación mediática de eventos. La medición se realiza basada en el juicio del dueño del proceso y los asistentes a la sesión de identificación, junto con el apoyo de la Coordinación de GRC y teniendo en cuenta los criterios definidos previamente.

El resultado de este análisis es documentado por la Coordinación de GRC en el anexo **Matriz ERM** durante la sesión de identificación de riesgos, con ello se obtiene el perfil de riesgo inherente, el cual se define como aquél al que se enfrenta la Compañía en ausencia de acciones por parte de la administración para modificar su probabilidad/frecuencia o impacto.

El riesgo inherente es clasificado según una severidad y se ubica en el mapa térmico de **PROINVIORIENTE**.

APROBADO

10.2.2. Severidad

El nivel de severidad es el indicador cualitativo que resulta de multiplicar el impacto por la probabilidad. Este resultado, permite establecer el grado de cada uno de los riesgos identificados, de acuerdo con las siguientes consideraciones:

NIVEL DE SEVERIDAD O PERFIL DE RIESGO	Extremo
	Alto
	Moderado
	Bajo

- **Zona de Severidad Extrema (Rojo): Riesgos Inaceptables**

Se debe dar tratamiento a las causas que generan el riesgo. Es decir, se deben implementar controles de prevención para reducir la probabilidad del riesgo y/o disminuir el impacto de los efectos a través de la adopción de medidas de protección para compartir o transferir el riesgo, por ejemplo, a través de pólizas de seguros u otras opciones que estén disponibles. Las acciones que se definan como tratamiento se deben establecer a corto plazo.

- **Zona de Severidad Alta (Amarilla): Riesgos Importantes**

Se deben tomar medidas para llevar los riesgos al nivel de severidad “bajo”, fortaleciendo los controles existentes o implementando controles complementarios.

- **Zona de Severidad Moderada (Verde): Riesgos Inferiores**

Se deben tomar medidas para llevar los riesgos al nivel de severidad “bajo”, fortaleciendo los controles existentes o implementando controles complementarios.

- **Zona de Severidad Baja (Azul): Riesgos Aceptables**

El riesgo se encuentra en un nivel que puede ser aceptado sin necesidad de tomar otras medidas de control diferentes a las que se poseen. No obstante, deben ser monitoreados para prevenir que a mediano o largo plazo se incremente su nivel de severidad.

10.3. TRATAMIENTO DE LOS RIESGOS

El tratamiento de los riesgos involucra:

- Identificar las opciones para actuar sobre el riesgo.

APROBADO

- Evaluarlas según criterios como: Costo-beneficio, viabilidad operativa, técnica y jurídica, entre otros.
- Preparar planes para tratamiento, es decir la implementación de la opción.

10.3.1. Opciones de tratamiento de riesgo

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

- **Evitar el riesgo:** No incurrir o terminar actividades que potencialmente podrían generar la materialización del riesgo identificado, o sustituir la actividad por una menos riesgosa.

- **Reducir el riesgo:** Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles.

- **Compartir o Transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras empresas, como en el caso de los contratos de seguros, cláusulas contractuales, garantías entre otros. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

  Esta opción de tratamiento también puede significar la tercerización, es decir, la transferencia de la totalidad o una parte de la actividad a un tercero externo a **PROINVIORIENTE** para su ejecución.

  Los mecanismos de para compartir o transferir el riesgo deben ser formalizados a través de un acuerdo contractual. Sin embargo, la utilización de estas medidas puede ser fuente generadora de otros riesgos operativos, los cuales también debe ser administrados.

- **Asumir el riesgo:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el dueño del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

El nivel permitido o aceptado por PROINVIORIENTE en su evaluación residual son los riesgos cuya severidad sea **moderada o baja**. Para los riesgos residuales con **severidad alta y extrema**, el dueño de proceso deberá establecer planes de acción que tengan como objetivo disminuir su probabilidad y/o su impacto, ya sea a través de la creación de nuevos controles, la implementación de

APROBADO

modificaciones a los controles existentes o la creación de actividades de corrección inmediata, con el fin de disminuir su severidad al nivel aceptado por la empresa.

Los riesgos que en su nivel residual se clasifiquen como altos o extremos, así como los planes de acción planteados por los dueños de proceso tendientes a la disminución de su severidad, deberán ser presentados a la Coordinación de GRC para su evaluación.

Dichos planes deben ser aprobados formalmente por el dueño de proceso y/o la Alta Dirección y la Coordinación de GRC será la encargada de realizarles seguimiento, reportando su avance.

Las causas de los riesgos clasificados como moderados y bajos deben ser evaluadas continuamente por los dueños de proceso, garantizando la eficacia de los controles en el tiempo, ya sea mejorándolos o planteando unos nuevos, cuando haya lugar.

Si el dueño de proceso percibe un incremento en el nivel del riesgo en las actividades que ejecuta, debe informarlo inmediatamente a la Coordinación de GRC, con el fin de realizar la respectiva reclasificación, con el fin de evitar que exista un deterioro.

Si el dueño de proceso percibe un incremento en el nivel del riesgo en las actividades que ejecuta, debe informarlo inmediatamente a la Coordinación de GRC, con el fin de realizar la respectiva reclasificación.

10.3.2. CONTROL

Para aquellos riesgos que se encuentran en un nivel de severidad superior al nivel “bajo” es necesario definir un plan de tratamiento a implementar. El plan de tratamiento busca determinar los controles que se tienen implementados como medios de mitigación de los riesgos inherentes identificados, así como el evaluar la efectividad de estos y el efecto en la reducción que estos producen en los factores generadores del riesgo.

Cada uno de los riesgos evidenciados dentro de la etapa de identificación deberá poseer como mínimo un control documentado, que ayude a la mitigación de este riesgo.

En caso de que el riesgo definido no se tenga implementado ningún control, se deberá diseñar e implementar uno.

APROBADO

10.3.3. Diseño de Controles.

Los controles se definen como mecanismos, políticas, prácticas u otras acciones existentes que actúan para minimizar el riesgo o potenciar oportunidades positivas en su gestión, con el fin de garantizar el desarrollo y cumplimiento de las actividades acorde a los requisitos de la organización.

Los controles de acuerdo con su naturaleza se pueden clasificar en:

- **Control Preventivo:** Acciones aplicadas previamente al inicio de una actividad. Se emplean para que, dadas unas condiciones, el resultado final sea el esperado. Se utilizan para minimizar la probabilidad de materialización del evento de riesgo.

- **Control Detectivo:** Son las acciones que se toman para identificar desviaciones o errores y que permiten servir de alarmas respecto a situaciones anormales, operaciones inusuales u operaciones sospechosas que requieran ser reportadas a las autoridades competentes. Un control detectivo mitiga el impacto de un evento de riesgo.

- **Control Correctivo:** Son las acciones que se toman una vez materializado el evento de riesgo, pueden ser correcciones para eliminar la situación indeseable o las acciones correctivas para eliminar la causa del evento de riesgo.

Los controles de acuerdo con su modo de ejecución se pueden clasificar en:

- **Control Manual:** Control que es ejecutado por completo con intervención humana.

- **Control Automático:** Control que es ejecutado sin necesidad de intervención humana.

- **Dependiente de TI:** Control que efectúa parte de su funcionamiento de manera automática tras una ayuda manual o que requiere de un componente tecnológico para poder ser ejecuta.

Los controles acordes a su tipo (detectivo, correctivo o preventivo) o a su modo de ejecución (manual, dependiente de TI o automático), deben tener en cuenta la viabilidad de implementación y el costo de estos. Sin embargo, siempre será más favorable para **PROINVIORIENTE** el implementar controles preventivos y automáticos.

10.3.4. Lineamientos o mejores prácticas sobre Controles de Riesgo Operativo.

Con el fin de tener un criterio de referencia para documentar los controles de los riesgos operativos, a continuación, se mencionan algunos aspectos para tener en cuenta como mejores prácticas para la redacción de estos dentro de la Matriz ERM (Enterprise Risk Management).

APROBADO

- El control ha de ser coherente en relación con el riesgo y/o causa a la cual se le asocia, es decir, debe mitigarla.
- El control ha de estar incluido en los Procedimientos del proceso analizado. Los procedimientos y controles deben garantizar la efectividad en el desarrollo de las tareas, la integridad de la información, el cumplimiento de los requerimientos regulatorios, enfocados a minimizar el riesgo de la operación cumpliendo con los estándares de calidad definidos por **PROINVIORIENTE**.
- Los controles deberán ser claros tanto para quienes hayan de usarlos como por aquellos que de un modo u otro consulten la matriz ERM. La redacción de los controles ha de ser compresible, exponiendo claramente la acción que realizan.

El control deberá atender a los siguientes interrogantes:

1. ¿Qué se está controlando?
2. ¿Quién ejecuta el control?
3. ¿Cuál es la frecuencia del control?
4. ¿Cómo se realiza la actividad de control?
5. Evidencia de la actividad de control.

Adicionalmente, el control debe tener en cuenta el nivel de precisión que se desea tener para mitigar efectivamente el riesgo, este se puede ver afectado por:

- **Objetivo de la revisión:** El grado en que se revisa a detalle el paso a paso del proceso para prevenir o detectar errores, más allá de solamente identificar y explicar diferencias encontradas.

- **Alcance del control:** Un control que se realiza a un nivel más granular generalmente es más preciso que uno realizado en un nivel superior. Por ejemplo, un análisis de variación de costos por etapa de proyecto normalmente es más preciso que un análisis a nivel general de proyecto.

- **Consistencia de los resultados:** Un control que se lleva a cabo de forma rutinaria y consistente, es generalmente más preciso que uno que se lleva a cabo de forma esporádica. Se recomienda que el control esté en función directa de la periodicidad de la operación generadora del riesgo.

- **Previsibilidad de las expectativas:** Algunos controles están diseñados para detectar errores mediante el uso de indicadores clave sobre situaciones inusuales reportadas u otra información desarrollada sobre expectativas. La precisión de los controles depende de la

APROBADO

capacidad para desarrollar las expectativas suficientemente precisas para resaltar discrepancias o errores potenciales.

- **Población objeto de control:** Un control puede ejecutarse en la totalidad de elementos en los que se realiza la revisión (es decir, en la población o mediante censo) o puede tomarse una muestra representativa que permita extrapolar los resultados de la validación. Un control dará mayor seguridad cuando se ejecuta sobre la totalidad de la población.

10.3.5. Implementación y evaluación de controles.

La implementación de controles se asocia a que estén claramente definidos, documentados, implementados, conocidos (divulgados) y puestos en marcha acorde a los criterios establecidos.

En la valoración de los riesgos identificados, se tendrán en cuenta la calidad de los controles establecidos para el tratamiento de estos, para así valorar el riesgo residual.

La calificación de estos criterios arroja la valoración de efectividad y ejecución de cada control, para así definir el nivel de exposición por causa, una vez aplicados los controles.

Después de evaluados los controles, se diligencia la sección de "Resultado" en el anexo **Matriz ERM (Enterprise Risk Management),** el cual determinará el nivel de Riesgo Residual. Finalmente, el dueño de proceso autorizará mediante firma o correo electrónico su matriz de riesgos identificados y controles implementados para su proceso.

El coordinador y el analista GRC, semestralmente, realizarán validación al diseño de los controles de la matriz SARO en compañía de los dueños de procesos. En caso de encontrar oportunidades de mejora o cambios en los procedimientos, realizarán el respectivo ajuste y se documentará en la sección control de cambios. Como evidencia se deja el formato "Evaluación de diseño de controles" y el control de cambios en la matriz de riesgos SARO.

10.4. MONITOREO

Es necesario monitorear continuamente los riesgos, la efectividad de los planes de tratamiento, las estrategias y el sistema de administración que se establece para controlar la implementación.

Los riesgos y la efectividad de las medidas de control necesitan ser revisadas constantemente para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos o la aparición de riesgos remanentes.

APROBADO

Es importante tener en cuenta que pocos riesgos permanecen estáticos. Es esencial realizar una revisión periódica con el fin de asegurar que el plan de administración mantiene su relevancia. Pueden cambiar los factores que generar los riesgos o las condiciones usadas para calificar la probabilidad/frecuencia y el impacto sobre los resultados, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento.

Los dueños de proceso son responsables de contactar a la Coordinación de GRC en los casos en que existan cambios significativos en sus procesos y se requiera ejecutar nuevamente el proceso de identificación, medición y tratamiento de riesgos operativos.

En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos, por lo tanto, el monitoreo será una parte integral de la administración de riesgos de **PROINVIORIENTE.**

En el monitoreo anual al sistema, se enfocará en:

- Verificar que los controles estén funcionando en forma oportuna, eficiente y efectiva.
- Verificar que los riesgos residuales se encuentren en los niveles de aceptación establecidos y aprobados por la Junta Directiva.
- Validar los cambios en el monto del criterio base de impacto usado para la calificación de riesgos.

De esta etapa, se desprenden continuos ajustes al sistema para hacerlo efectivo de acuerdo con sus propósitos, que son:

- Asegurar que los riesgos residuales con severidad, moderada y alta cuenten con planes de tratamiento acordes para su mitigación.
- Mantener actualizados los mapas de riesgos de los procesos de PROINVIORIENTE, teniendo en cuenta los cambios que se den en éstos.
- Analizar el comportamiento de los eventos de pérdida, con el fin de determinar su incidencia en la probabilidad e impacto de los riesgos.
- Asegurar que los nuevos procesos, actividades y sistemas usados sean incluidos en el sistema.

11. REGISTRO DE EVENTOS DE RIESGO OPERATIVO

La Coordinación de GRC es la responsable de establecer y mantener actualizado un registro de eventos de riesgo operativo para PROINVIORIENTE.

El registro de eventos de riesgo operativo es un inventario de los eventos que implican la materialización de un riesgo operativo, esto con el objetivo de:

APROBADO

- Generar los planes de acción y modificación necesaria en los controles, procesos, perfil de riesgo, riesgos y supuestos usados en la ejecución del SARO.
- Ser una fuente de información para el Comité de GRC, Representante legal y Junta Directiva respecto a la exposición de PROINVIORIENTE al riesgo operativo.
- Servir de insumo para la generación de revelaciones en los estados financieros en caso de que el evento de riesgo operativo tenga la materialidad suficiente.

El Registro de eventos de riesgos operativo llevará cuenta de todos los eventos que impliquen los siguientes tipos de pérdidas:

- Tipo A: Generan pérdidas y afectan el estado de resultados de la compañía.
- Tipo B: No generan pérdidas y por lo tanto no afectan el estado de resultados de la compañía.

En la situación en la que cualquier funcionario de **PROINVIORIENTE** identifique y reporte que se ha presentado un evento que implica la materialización de un riesgo operacional (sea que este riesgo haya o no sido identificado con antelación en el formato Matriz ERM, es decir, si el evento comprende la falla en un proceso, persona, sistema informático, infraestructura o representa un perjuicio para **PROINVIORIENTE** debido a un acontecimiento externo), deberá dirigirse al/los dueño(s) del/los proceso(s) afectado(s) y a la Coordinación de GRC para notificar respecto a la existencia de un "evento de riesgo operativo" (ERO).

El funcionario que identifique el evento deberá llevar la información soporte de este al dueño de proceso al que corresponda el ERO, quién, en primer lugar, identificará:

- Si el evento implica otros procesos. En cuyo caso contactará a los demás dueños de proceso para realizar un solo análisis del evento. El primer dueño de proceso contactado debido al evento será el responsable del ERO ante la Coordinación de GRC y ejecutará toda su documentación.
- Si existen controles que hayan fallado durante la ejecución del evento.
- Qué riesgos dentro de sus procesos (y los de los demás dueños de proceso, si aplica) se materializaron con el evento.
- Si el impacto en términos financieros del evento lo hace o no material para la PROINVIORIENTE (ver numeral 10.1.2 Afectación de estados de resultados).
- Si existen controles, circunstancias o acciones que la compañía puede ejecutar para mitigar el impacto del evento.
- La cuantía de dinero que es posible mitigar gracias a los controles, circunstancias o acciones identificadas.

APROBADO

Posterior a la identificación, el responsable del ERO diligenciará el formato CVO-RE-GRC-007 Registro de Evento de Riesgo Operativo y lo remitirá mediante correo electrónico a la Coordinación de GRC para su validación.

Una vez validado por la Coordinación de GRC, ésta se encargará de documentarlo en el formato CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo y será el responsable de ejecutar seguimiento a los planes de acción definidos. por el dueño de proceso donde se presentó el evento.

Los correos del dueño de proceso con el formato CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo definitivo será custodiado por la Coordinación de GRC y nombrados con la referencia asignada al ERO, por ejemplo:

El evento número 1 del año 202X tendrá el siguiente código: ERO2021-1.

La versión en uso del formato CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo se encontrará disponible en la carpeta One Drive de la Coordinación de GRC.

Cuando no se hayan materializado eventos de riesgo en un año, los dueños de proceso deberán certificar dicha condición de forma semestral a la Coordinación de GRC haciendo uso del formato CVO-RE-GRC-005 Declaración Ausencia de Eventos de Riesgo Operativo.

11.1FORMULACIÓN DE PLANES DE ACCIÓN A EVENTOS DE RIESGO OPERATIVO

Los planes de acción que defina el dueño de proceso a cargo del Evento de Riesgo Operativo (ERO) para subsanar las causas generadoras del mismo deberán contemplar:

- **Especifico:** Presentar un nivel de detalle adecuado que permita identificar las actividades a ser ejecutadas y que subsanarían la causa generadora, así como los entregables que las soportarían.
- **Medible:** Indicar un criterio de medición que permita conocer si el plan ha sido o no ejecutado o estimar de forma razonable el avance de este.
- **Alcanzable:** El plan puede ser ejecutado con los recursos disponibles de PROINVIORIENTE o comprender la destinación de los recursos adicionales para su ejecución (tiempo, personal, infraestructura, etc.). Asimismo, puede implicar la elección de la mejor relación “calidad, tiempo y costo” para cumplir eficientemente el objetivo.
- **Relevante:** Estar alineado con la causa generadora de tal forma que, al ejecutarlo, la subsane a totalidad, de no ser así, podrían requerirse mayor cantidad de actividades.
- **Fecha de ejecución:** Debe indicar la fecha de implementación del plan.
- **Oportuno:** el plan se ejecuta en el momento adecuado que prevenga la materialización del riesgo.

APROBADO

- **Responsable(s) definido(s):** Debe indicar la(s) persona(s) a cargo de implementar el plan de acción en PROINVIORIENTE.

11.2 SEGUIMIENTO A LA GESTIÓN DE EVENTOS DE RIESGO OPERATIVO.

Con el fin de asegurar que los planes de acción se ejecuten según lo definido y se generen alertas oportunas para asegurar la adecuada gestión del riesgo, la Coordinación de GRC realizará seguimiento sobre los planes de acción definidos.
En el seguimiento de los planes de acción, el dueño de proceso debe reportar:

1. El avance en la implementación de los planes de acción a la fecha de corte del seguimiento. Para aquellos casos en los que se presenten desviaciones en el cumplimiento de los planes de acción, el dueño de plan deberá presentar las justificaciones de dicha desviación

   En caso de requerir modificaciones o cancelaciones a los planes de acción establecidos, el dueño del plan deberá realizar la solicitud a la Coordinación de GRC por correo electrónico, justificando las razones de su modificación o cancelación. Asimismo, debe establecer cuál va a ser el plan de acción alterno en el tratamiento de la(s) causa(s) generadora(s) de la situación, considerando que debe cumplir con el objetivo de reducir la exposición o impacto al riesgo.

2. Las evidencias que soporten el estado de avance del plan de acción. El dueño del plan de acción es el único responsable de certificar que el plan ha sido cerrado a conformidad ante la Coordinación de GRC.

   El estado de los planes de acción se definirá de la siguiente manera:

- No definido: Evento de riesgo que no cuenta con un plan de acción definido a la fecha de seguimiento.
- No aprobado: evento de riesgo con un plan de acción formulado pero que no ha sido aprobado por parte de la Coordinación de GRC.
- En ejecución: El plan de acción presenta avance a la fecha de seguimiento conforme a lo planeado y la fecha de finalización no ha ocurrido.
- Vencido: el plan de acción no se ha completado en el tiempo planeado y no ha sido mitigada la causa originadora del plan.
- Sin gestión: el plan de acción no presenta avance a la fecha de seguimiento y la fecha de finalización no ha ocurrido.
- Cancelado: el plan de acción fue cancelado debido a que hubo cambios en la situación del proceso, análisis costo beneficio o un incidente externo, antes de lograr el 100% de su implementación.

APROBADO

- Cerrado: el plan de acción fue implementado al 100% conforme a lo planeado y la causa generadora del evento de riesgo fue mitigada o eliminada.

El resultado del seguimiento de los eventos de riesgo se diligenciará en el formato CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo.

Los registros de seguimiento a planes de acción y sus respectivos soportes quedarán almacenados en la carpeta de One Drive de la Coordinación de GRC.

El dueño del plan de acción es el único responsable de certificar que el plan ha sido cerrado a conformidad ante la Coordinación de GRC.

12. REPORTES

La Coordinación de GRC reportará semestralmente a la Alta Dirección, el desempeño del SARO teniendo en cuenta:

- Nivel de implementación del sistema.
- Eventos de Riesgo Operativo presentados y planes de acción generados.
- Estatus de los planes de acción vigentes.
- Eventos relacionados con el curso del negocio, procesos o actividades identificados que puedan afectar el SARO o requerir una modificación de este.
- Mapas de calor de riesgos inherentes y residuales.

13. ESCALAMIENTO

La Coordinación de GRC escalará los siguientes casos a la Alta Dirección para definir las medidas a tomar:

- En caso de que un ERO permanezca por un mes sin un plan de acción definido (si el dueño del plan de acción no ha hecho entrega del cronograma de implementación, si aplica, se entiende que el ERO no tiene un plan de acción).

- En el caso en que un plan de acción definido se venza sin justificación.

14. ACTUALIZACIÓN

APROBADO

Actualizar periódicamente y/o de acuerdo con las actualizaciones realizadas de los riesgos y controles de cada uno de los procesos de **PROINVIORIENTE**, junto con los dueños de los procesos y/o ejecutores de estos, o sus delegados; con el fin de actualizar los mapas de riesgos existentes, de acuerdo con los cambios, observaciones, hallazgos y/o eventos materializados que se hayan presentado.

Todo cambio en los procedimientos de los procesos tiene una afectación directa sobre el mapa de riesgos operacionales generado.

De igual manera, otros insumos utilizados para la actualización y/o ajuste a los mapas de riesgos son las observaciones u oportunidades de mejoras, tanto de entes de control externos como internos, respecto de los procesos auditados, lo cual hará más precisa la medición de los riesgos.

Como consecuencia del proceso de actualización anual se generará un acta indicando los cambios ejecutados. Ésta será firmada por la Coordinación de GRC y el Dueño de proceso respectivo.

14.1 FACTORES QUE AFECTAN EL RIESGO RELACIONADOS A LA ACTUALIZACIÓN DE UN CONTROL

Los siguientes son factores por considerar en el momento de analizar los controles implementados del SARO:

- La naturaleza y materialidad de los errores que el control pretende impedir o detectar, al igual que los errores que se han presentado para éste.
- Si ha habido cambios en el volumen o en la naturaleza de las transacciones que podrían afectar de manera adversa al diseño o a la efectividad operativa del control.
- La competencia del personal que ejecuta el control o monitorea su desempeño y si ha habido cambios en el personal clave que ejecuta el control o monitorea su desempeño.
- La complejidad del control y la importancia de los juicios que se deben hacer en conexión con su operación.
- Si el control es ejecutado de forma descentralizada, es decir, en múltiples localidades.

15. DIVULGACIÓN

De forma adicional a la divulgación generada durante el proceso de entrenamiento, el mapa de calor generado como resultado de la ejecución del SARO y este manual se encontrarán disponibles en el

APROBADO

sistema integrado de gestión (SIG) de **PROINVIORIENTE**, para acceso y consulta de todos los funcionarios de la compañía.

PROINVIORIENTE consciente de la importancia que tiene la identificación, captura y comunicación de la información que se genera con la administración del "Riesgo Operativo", entre los niveles de la organización, ya sea que provenga de fuentes externas o internas, es requerido para llevar a cabo sus responsabilidades frente a la identificación, valoración y respuesta a los riesgos.

La divulgación de la Información deberá realizarse de forma periódica y estar disponible, cuando así se requiera. Se implementan dos sistemas de divulgación de información: interno y externo.

a. INTERNA

Lo constituye la presentación y conocimiento formal de PROINVIORIENTE de los reportes generados por la Coordinación de GRC y las disposiciones que emite la Junta Directiva en materia de normas y las recomendaciones y evaluaciones realizadas tanto por los Órganos de control interno como las realizadas por la Alta Dirección.

Tiene como objeto generar conciencia frente a la importancia y relevancia del riesgo, así como identificar los roles y responsabilidades que se generan al implementar y dar apoyo a los componentes que conforman la administración de los riesgos operativos.

La Alta Dirección de **PROINVIORIENTE** establece una estructura de informes con el fin de mantener actualizada a la Junta Directiva o quien haga sus veces sobre el desempeño, los desarrollos y el funcionamiento del Sistema de Administración de Riesgos Operativos. De la misma forma, la Junta Directiva o quien hagas sus veces de **PROINVIORIENTE** debe comunicar de manera clara y explícita sus disposiciones y requerimientos, y disminuir de esta forma el nivel de criticidad que pueda.

Los canales de información internos de **PROINVIORIENTE** deben facilitar a los empleados comunicar lo concerniente a los riesgos a través de las unidades de negocio, procesos o canales que ha dispuesto **PROINVIORIENTE** para dicho fin. Para llevar a cabo lo anterior, se ha previsto el registro de los eventos de riesgo operativo.

Debe ser del conocimiento de los empleados y **PROINVIORIENTE**.

- Políticas, objetivos, metodologías y documentos que hacen parte del Sistema de Administración de Riesgo Operativo.
- Apetito al riesgo de la Entidad y tolerancia al mismo.
- Los mapas de riesgo por Proceso y consolidado.
- Las medidas de mitigación y control.
- Planes de mejora para cada proceso.

APROBADO

- Revelación contable de los eventos Ocurridos.

Para tal fin, el responsable de Riesgos Operativo trabajará de manera integrada con los responsables de Recursos Humanos y Formación.

b. EXTERNA

Los canales de comunicación externos a **PROINVIORIENTE** se convierten en entradas significativas frente a la manera en que los clientes y el mercado en general perciben los productos y servicios que presta **PROINVIORIENTE**.

PROINVIORIENTE, entonces, ajusta su nivel de riesgo permitido con el de sus clientes y socios, asegurando que no asume, inadvertidamente, un nivel de riesgo elevado en los procesos de negocio y operaciones que ejecuta, disminuyendo así cualquier tipo de riesgo sistémico que amenace la estabilidad del mercado y la buena reputación y continuidad de la empresa.

Con base en lo anterior, el sistema de divulgación externo lo conforma el conjunto de Comunicaciones sobre información definida como importante de la administración del riesgo operativo de **PROINVIORIENTE** referente a la gestión realizada y los resultados obtenidos frente a la administración de los riesgos.

16. CAPACITACIÓN

La Coordinación de GRC se encargará de que todos los trabajadores de **PROINVIORIENTE**, sean capacitados en: cultura de riesgo, estructuras y metodología del SARO. De igual manera, los nuevos funcionarios serán capacitados durante la inducción a **PROINVIORIENTE**.

A partir de los reportes generados, la Coordinación de GRC deben dar a conocer los resultados, experiencias y oportunidades de mejora del SARO. Igualmente, con el apoyo de la Dirección General EOC generarán las herramientas y espacios para la capacitación de todos los funcionarios de **PROINVIORIENTE.** en cuanto a temas de a la cultura de gestión de riesgos, la estructura y funcionamiento del sistema. Para impulsar cultura de riesgo operativo se debe dar cumplimiento a las siguientes políticas:

- Concientizar a los Órganos de Administración y Dirección.
- Diseñar y actualizar permanentemente los programas de capacitación (inducción y reinducción)
- Dictar capacitación periódica a todo el personal de **PROINVIORIENTE**, enfatizando, además, en la transparencia y consistencia de la información entre todas las Direcciones de

APROBADO

PROINVIORIENTE en lo que respecta a la gestión y control del Riesgo Operativo, para que obtenga confiabilidad en la toma de decisiones.

- Evaluar la efectividad de la capacitación.

De forma anual, se ejecutará una sesión de capacitación respecto al SARO, el método de capacitación definido por la Coordinación de GRC contará con un mecanismo de evaluación de los resultados obtenidos con el fin de determinar la eficacia de dichos programas y el alcance de los objetivos propuestos.

17. ANEXOS

I. 4GL-PO-GRC-001 Política de Riesgo Operativo.
II. CVO-RE-GRC-003 Acta de Formalización de Riesgos y Controles RO.
III. CVO-RE-GRC-004 Contexto externo e interno de la organización.
IV. CVO-RE-GRC-005 Declaración Ausencia de Eventos de Riesgo Operativo (ERO)
V. CVO-RE-GRC-006 Matriz ERM
VI. CVO-RE-GRC-007 Registro de Eventos de Riesgo Operativo (ERO)
VII. CVO-RE-GRC-008 Reporte Eventos de Riesgo con Alto Impacto
VIII. CVO-RE-GRC-009 Técnicas de Identificación de Riesgos

18. CONTROL DE CAMBIOS

FECHA	VERSIÓN	DESCRIPCIÓN DEL CAMBIO
04-06-2021	01	Creación
15-05-2024	02	• Se cambia acontecimientos externos a Eventos externos de acuerdo con el listado de factor de riesgo definido por CFC en el numeral 10.1.5 Definir Factores que generan el riesgo operacional • Se agrega control semestral de evaluación de diseño en el numeral 10.3.5 Implementación y evaluación de controles.

APROBADO