I. Objetivo

Sensibilizar a los proveedores del Banco de la República (Banrep) sobre la gestión de riesgos, con el fin de afianzar sus conocimientos sobre los riesgos y prácticas en el desarrollo de sus procesos para el cumplimiento adecuado de los productos y servicios entregados al Banrep en el marco del acuerdo contractual efectuado.

II. Contenido

1. CONCEPTOS CLAVES

1.1 Conceptos claves

- **Gestión Integral de Riesgos**: la Gestión Integral de Riesgos (Enterprise Risk Management – ERM) se refiere a la identificación, medición, monitoreo, control y reporte de los tipos riesgos en todas las categorías y sus interrelaciones que afectan el desempeño y la continuidad de los procesos de la organización.
- **Riesgo**: efecto de la incertidumbre sobre los objetivos.
- **Riesgo operacional**: 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 estos. Incluye el riesgo legal.
- **Riesgo de terceros – proveedores**: riesgo de incurrir en pérdidas derivado de incumplimientos o deficiencias en la prestación de servicios a la entidad por parte de terceros.
- **Evento de riesgo**: hecho o cambio que puede afectar el logro de los objetivos de la entidad. En términos de riesgo operacional, es aquel hecho o cambio que puede generar impactos financieros o reputacionales a la entidad.

1.2 Principales riesgos asociados a la gestión de terceros

- **Operacional:** 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 estos.
- **Lavado de activos y financiación del terrorismo (LAFT):**riesgo de que una entidad sea utilizada para dar apariencia de legalidad a activos provenientes de actividades delictivas o para la canalización de recursos hacia la realización de actividades terroristas. Lavado de activos: conjunto de actividades encaminadas a ocultar el origen ilícito o a dar apariencia de legalidad a recursos obtenidos producto de la ejecución de actividades ilícitas. Financiación del terrorismo: conjunto de actividades encaminadas a canalizar recursos lícitos o ilícitos para promover, sufragar o patrocinar individuos, grupos o actividades terroristas.
- **No disponibilidad:** riesgo de incurrir en pérdidas derivadas de la interrupción de los procesos internos producto de la no disponibilidad del recurso humano, la información, la tecnología o la infraestructura propia del Banco o de fuentes externas.
- **Seguridad de la información y ciberriesgo:**seguridad de la información: riesgo de incurrir en pérdidas derivado de la afectación de la integridad, confidencialidad o disponibilidad de información de la entidad. Ciberriesgo: riesgo de incurrir en pérdidas derivado de fallas, uso no autorizado o errado de los sistemas de información del Banco o de ataques cibernéticos.
- **Legal:** riesgo de incurrir en pérdidas derivado de sanciones o indemnizaciones como resultado del incumplimiento de regulaciones o de obligaciones contractuales. Incluye a terceros que actúen en representación de la entidad.
- **Reputacional:** riesgo de afectación negativa de la confianza/credibilidad de la entidad por parte de uno o varios de sus grupos de interés, en cuanto a su integridad, capacidad técnica u operativa o cumplimiento. Es consecuencia de la materialización de otros riesgos.

1.3 Ciclo de gestión de riesgos

En desarrollo de sus procesos, en especial los que tienen relación directa con los servicios que prestan los proveedores, es importante identificar, medir, tratar, controlar y monitorear los riesgos asociados a estos procesos:

 **Identificación:** en esta etapa se busca determinar los riesgos (actuales y potenciales) inherentes (sin controles) a los procesos y/o las actividades que desarrolla o planea desarrollar la entidad.

 **Medición:** su objetivo es determinar el nivel de exposición de los riesgos, soportado en la medición de su probabilidad de ocurrencia e impacto potencial.

 **Tratamiento:** establecer las medidas de tratamiento de los riesgos, para tomar las decisiones respecto al manejo que se dará al riesgo residual.

 **Control y monitoreo:** realizar seguimiento al perfil de riesgos mediante diferentes mecanismos, con el fin de tomar medidas oportunamente (mejora continua) que permitan prevenir y corregir las desviaciones de los riesgos y del sistema de gestión de riesgos.

1.4 Principales riesgos y controles en la gestión de terceros - Ciclo de vida de terceros y gestión de riesgos

Durante las etapas del ciclo de vida de los terceros en el Banrep se pueden materializar diferentes riesgos; dado lo anterior, es importante contar con prácticas de control durante sus diferentes etapas:

Tipo de riesgo R1. Riesgo operacional - Fraude

Controles propuestos:

- C1. Esquemas de buen gobierno
  C2. Código de ética y conducta
  C3. Segregación de funciones

Tipo de riesgo R2. LAFT

Controles propuestos:

- C1. Políticas para prevenir riesgos de LAFT
- C2. Verificación periódica en listas de control (terceros; empleados, clientes, entre otros)

Tipo de riesgo R3. Riesgo operacional - Fallas y errores

Controles propuestos:

- C1. Controles duales
- C2. Controles automáticos
- C3. Segregación de funciones

Tipo de riesgo R4. No disponibilidad

Controles propuestos:

- C1. Planes de continuidad
- C2. Esquemas de redundancia y contingencias alternas

Tipo de riesgo R5. Seguridad de la información y ciberriesgo

Controles propuestos:

- C1. Administración de usuarios
- C2. Acuerdos de confidencialidad
- C3. Controles de acceso
- C4. Análisis de vulnerabilidades
- C5. Borrado de datos

Para una adecuada gestión de estos riesgos es importante que todos nuestros proveedores cuenten con un sistema de administración de riesgos o como mínimo con un adecuado ambiente de control que garantice que se aplican los diferentes controles operativos y de alto nivel, estableciendo las estrategias de tratamiento para minimizar la exposición de los riesgos que afecten la prestación del servicio a sus clientes.

2. Gestión Integral de riesgos en el Banco de la República

2.1 Alcance

La Gestión Integral de Riesgos se realiza a partir de la administración de los siguientes subsistemas:

Los subsistemas de gestión de riesgo pueden tener políticas individuales que disponen lineamientos respecto a la administración particular de los riesgos dentro de un proceso o tipo de riesgo según su alcance. Esas políticas se enmarcan en la sombrilla del Sistema de Gestión Integral de Riesgos del Banco de la República.

2.2 Taxonomía de riesgos

La Gestión Integral de Riesgos del Banco de la República tiene alcance sobre todos los procesos misionales y corporativos, sobre las áreas, las sucursales y agencias, todos los trabajadores del Banco, proveedores y terceras partes relacionadas con el Banrep. Es transversal a las tipologías de riesgo establecidas en la siguiente taxonomía de riesgos:

2.3 Modelo tres líneas de defensa

La Gestión Integral de Riesgos se soporta en un modelo de tres líneas de defensa que permite identificar, gestionar, controlar y supervisar los riesgos del Banrep en un esquema de pesos y contrapesos, con una unidad de riesgos independiente que reporta funcionalmente al más alto nivel de la organización.

3. Elementos del Banco de la República para la gestión de riesgos

3.1 Código de Conducta

El Banco cuenta con un Código de Conducta, el cual es un compendio de normas legales y reglamentarias internas que establecen y desarrollan los principios y valores que rigen el cumplimiento de las funciones de los trabajadores(as) del Banrep.

A su vez, es un marco de referencia para las personas naturales y jurídicas con las que el Banrep tiene alguna relación contractual, respecto de la conducta que se espera de los trabajadores(as) del Banrep, razón por la cual es importante que los proveedores conozcan el Código de Conducta y adopten las disposiciones allí establecidas.

Nuestros valores

- **INTEGRIDAD**: actuamos con independencia, responsabilidad, honestidad, coherencia, transparencia y sentido de lo público.
- **EXCELENCIA**: nos comprometemos con resultados de calidad de manera oportuna, dinámica y eficiente, tanto en los servicios a la economía como en los procesos internos.
- **SOSTENIBILIDAD**: contribuimos a generar impactos económicos, sociales y ambientales positivos con una visión de largo plazo.
- **INCLUSIÓN**: valoramos las diferencias, acogemos la diversidad, actuamos con equidad y escuchamos las distintas opiniones y puntos de vista.
- **RESPETO**: ofrecemos un trato digno y cordial a todas las personas, reconociendo y valorando todos los esfuerzos, las contribuciones y los logros.

3.2 Prácticas para la gestión de conflicto de interés, regalos o invitaciones por parte de los proveedores

Los proveedores deben conocer y adoptar el Código de Conducta del Banrep, en particular los lineamientos allí establecidos para conflictos de interés , regalos o invitaciones de terceros:

- Abstenerse de efectuar pagos, desembolsos o cualquier clase de retribuciones a favor de trabajadores(as) del Banrep.
- Validar y monitorear que no se encuentre en situación de conflicto de interés para suscribir y durante la ejecución del contrato con el Banrep.
- No ofrecer regalos, favores, premios, tratos preferenciales, invitaciones o viajes, entre otros, que comprometan o pudieran dar la apariencia de comprometer su juicio e independencia en la toma de decisiones de los trabajadores(as).
- Informar al Banrep en caso de presentarse un conflicto de interés al trabajador(a) del Banco a cargo del contrato y a través de los canales de denuncia establecidos en la sección de Atención a la Ciudadanía.

3.3 Gestión de eventos de riesgo

Los eventos de riesgo son incidentes que representan la materialización de un riesgo o que alertan sobre riesgos potenciales y que se generan por fallas en procesos internos, tecnología, infraestructura, personas o acontecimientos generados por fuentes externas.

Como proveedor del Banco de la República, ante la materialización de un evento que pueda afectar la prestación de los servicios o el cumplimiento del contrato, se debe reportar lo más pronto posible al funcionario del Banrep a cargo del contrato y a través del correo electrónico: dgrp-riesgos@banrep.gov.co relacionando la descripción del evento, sus causas y acciones tomadas para su mitigación.

4. Contactos Gestión Integral de Riesgos Banrep

Si tiene preguntas o inquietudes sobre la gestión de riesgos en su entidad, en su relación como proveedor del Banco de la República o sobre el Sistema de Gestión Integral de Riesgos del Banrep o si va a reportar algún evento de riesgos, puede escribir a los siguientes correos:

dgrp-riesgos@banrep.gov.co

Estaremos atentos a responder sus inquietudes.