SUPERINTENDENCIA DE BANCOS

RESOLUCIÓN No. SB-2026-3743

Magister Francisco Xavier Garzón Cisneros
SUPERINTENDENTE DE BANCOS, SUBROGANTE

CONSIDERANDO:

Que, el artículo 82 de la Constitución de la República del Ecuador indica: *"El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes."*;

Que, el artículo 204 de la Constitución de la República del Ecuador determina que: *"(...) La Función de Transparencia y Control Social estará formada por el Consejo de Participación Ciudadana y Control Social, la Defensoría del Pueblo, la Contraloría General del Estado y las superintendencias. Estas entidades tendrán personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa. (...);*

Que, la Constitución de la República del Ecuador, en su artículo 213, prescribe que: *"Las Superintendencias son organismos técnicos de vigilancia, auditoria, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujetarán al ordenamiento jurídico y atiendan al interés general";*

Que, el artículo 226 del mismo cuerpo legal manifiesta: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución."*;

Que, el artículo 227 ibidem: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación."*

Que, el artículo 59 del Código Orgánico Monetario y Financiero establece que *"La Superintendencia de Bancos es un organismo técnico de derecho público, con personalidad jurídica, parte de la Función de Transparencia y Control Social, con autonomía administrativa, financiera, presupuestaria y organizativa, cuya organización y funciones están determinadas en la Constitución de la República y la ley"*;

Que, el artículo Art. 64 de Código Orgánico Monetario y Financiero dispone: "*La Superintendencia de Bancos podrá establecer intendencias regionales dentro del territorio nacional. // La estructura administrativa de la Superintendencia contará con las instancias, intendencias especializadas en los sectores financieros público y privado, unidades, divisiones técnicas y órganos asesores que se establezcan en el respectivo estatuto orgánico por procesos, que deberá ser aprobado de conformidad con lo que dispone la Ley Orgánica del Servicio Público"*;

Que, el artículo 67 ibidem establece: *"La Superintendencia de Bancos estará dirigida y representada por la o el Superintendente."*;

Que, los numerales 3 y 4 del artículo 69 del mismo cuerpo legal manifiestan: *"3. Dirigir, coordinar y supervisar la gestión administrativa de la Superintendencia, para lo cual expedirá los reglamentos internos correspondientes; // 4. Acordar, celebrar y ejecutar, a nombre de la Superintendencia los actos, contratos, convenios y negocios jurídicos que requiera la gestión institucional y las obligaciones que contraiga;"*;

Que, el artículo 14 del Código Orgánico Administrativo indica: *"La actuación administrativa se somete a la Constitución, a los instrumentos internacionales, a la ley, a los principios, a la jurisprudencia aplicable y al presente Código."*

Que, el artículo 20 de mismo cuerpo legal dispone: *"Las administraciones públicas actuarán bajo los criterios de certeza y previsibilidad. // La actuación administrativa será respetuosa con las expectativas que razonablemente haya generado la propia administración pública en el pasado. // La aplicación del principio de confianza legítima no impide que las administraciones puedan cambiar, de forma motivada, la política o el criterio que emplearán en el futuro. // Los derechos de las personas no se afectarán por errores u omisiones de los servidores públicos en los procedimientos administrativos, salvo que el error u omisión haya sido inducido por culpa grave o dolo de la persona interesada."*;

Que, el artículo 47 de Código Orgánico Administrativo establece: *"La máxima autoridad administrativa de la correspondiente entidad pública ejerce su representación para intervenir en todos los actos, contratos y relaciones jurídicas sujetas a su competencia. // Esta autoridad no requiere delegación o autorización alguna de un órgano o entidad superior, salvo en los casos expresamente previstos en la ley."*;

Que, la Contraloría General del Estado mediante el Acuerdo No. 004-CG-2023 de 07 de febrero de 2026; expidió las Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos;

Que, el artículo 2 del Acuerdo No. 004-CG-2023 de 07 de febrero de 2026 indica: *"Las Normas de Control Interno se aplicarán en todas las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos, a las que se refiere la Constitución de la República del Ecuador y la Ley Orgánica de la Contraloría General del Estado."*;

Que, la Norma 300 *"EVALUACIÓN DEL RIESGO"* indica: "*La máxima autoridad y el personal de la institución establecerán los mecanismos necesarios para identificar, analizar, valorar y responder a los riesgos a los que está expuesta la organización para el logro de sus objetivos, el cumplimiento de las disposiciones legales, la protección de recursos públicos y la generación de información oportuna y confiable. El riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o su entorno. La máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán, valorarán y responderán a los potenciales eventos que pudieran afectar la ejecución de sus procesos, el logro de sus objetivos, la protección de sus recursos y la generación de información; y emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos";*

Que, mediante resolución Nro. SB-2026-02293 de 23 de julio de 2026, la máxima autoridad de la Superintendencia de Bancos, expidió el Estatuto Orgánico de Gestión Organizacional por Procesos de la Superintendencia de Bancos;

Que, en el numeral 1.3.1.3. "GESTIÓN DE CONTROLLER" en el literal c y f de sus atribuciones y responsabilidades establece:" *"c) Proponer políticas de mitigación de riesgos institucionales y monitorear su implementación"* y *"f) Supervisar la correcta aplicación de manuales, políticas, procedimientos internos y otras que la máxima autoridad disponga"*;

Que, mediante *"INFORME TÉCNICO No. SB-DPS-2026-105-I "* de 13 de octubre de 2026, suscrito por el Coordinador General de Planificación, la Directora de Planificación y Seguimiento y el Experto en Administración Técnica 3, concluyen :*" Con la vigencia del nuevo Estatuto Orgánico de Gestión Organizacional por Procesos, emitido con resolución Nro. SB-2026-02293 de 23 de julio de 2026, y la nueva designación del puesto de Controller, es necesario continuar con el trámite de aprobación de la propuesta de la "Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos"...,"*;

Que, mediante memorando Nro. SB-INJ-2026-1096-M de 23 de octubre de 2026, la Intendencia Nacional Jurídica emitió el respectivo criterio jurídico para la aprobación de la "Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos

y concluyo entre otros aspectos: *"(...)En consecuencia, existe fundamento constitucional, legal, orgánico y técnico para que el Superintendente de Bancos para expedir la metodología mediante resolución cuyo proyecto se adjunta , como una medida dirigida a fortalecer la gestión institucional, el control interno y el cumplimiento de los objetivos de la entidad por lo que desde el ámbito estrictamente jurídico, se considera viable la expedición de la "Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos", y procedente continuar con el trámite para la suscripción de la resolución por parte de la máxima autoridad.(...)";*

Que, mediante Memorando Nro SB-IGGI-2026-0400-M de 23 de octubre de 2026, la Intendencia General de Gestión Institucional recomendó a la máxima autoridad la suscripción de la resolución de aprobación de la "Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos", de acuerdo con lo establecido en los informes y demás documentación de sustento; y,

Que, mediante acción de personal Nro. 0787 de 21 de octubre de 2026 se me designó Superintendente de Bancos subrogante; y, por ende, máxima autoridad de este Organismo de Control.

En ejercicio de las facultades y atribuciones conferidas por la Constitución de la República del Ecuador, el Código Orgánico Monetario y Financiero, demás normativa legal vigente; y el Estatuto Orgánico Organizacional por Procesos.

RESUELVE:

Artículo 1.- EXPEDIR la Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos.

Artículo 2.- DISPONER a el Controller la ejecución e implementación de la Metodología para la Gestión de Riesgos Institucionales de la Superintendencia de Bancos, para lo cual presentará el correspondiente plan de trabajo.

Artículo 3.- ENCARGAR a la Secretaría General la notificación a todo el Nivel Jerárquico Superior de la Superintendencia de Bancos, difusión y publicación de la presente Resolución en la página web institucional de la Superintendencia de Bancos, de conformidad con la normativa legal y administrativa aplicable.

DISPOSICIÓN GENERAL

ÚNICA. - Los casos de duda que se presenten en la aplicación o interpretación de la presente Resolución serán resueltos por la Superintendencia de Bancos, en el ámbito de sus competencias.

DISPOSICIÓN FINAL

ÚNICA.- La presente Resolución entrará en vigencia a partir de su expedición, sin perjuicio de su publicación en el Registro Oficial y en la página web institucional de la Superintendencia de Bancos.

COMUNÍQUESE.- Dada en la Superintendencia de Bancos, en Quito, Distrito Metropolitano, a los veinte y tres días del mes de octubre de dos mil veintiséis.

Firmado electrónicamente por:
FRANCISCO XAVIER
GARZON CISNEROS

Magister Francisco Xavier Garzón Cisneros
SUPERINTENDENTE DE BANCOS, SUBROGANTE

LO CERTIFICO. - En Quito, Distrito Metropolitano, el veinte y tres de octubre de dos mil veintiséis.

Firmado electrónicamente por:
DELIA MARIA
PENAFIEL GUZMAN

Magister Delia María Peñafiel Guzmán
SECRETARIA GENERAL

METODOLOGÍA PARA LA GESTIÓN DE RIESGOS INSTITUCIONALES

1. OBJETIVO 7

2. ALCANCE 7

3. MARCO METODOLÓGICO 7

4. DIRECTRICES GENERALES 8

5. DESARROLLO DEL DOCUMENTO 9

A. IDENTIFICACIÓN DE RIESGOS 9
B. ANÁLISIS DE RIESGOS 11
C. EVALUACIÓN DE RIESGOS 12
D. TRATAMIENTO DE RIESGOS 13
E. SEGUIMIENTO AL PLAN DE MITIGACIÓN DE RIESGOS 16
F. COMUNICACIÓN Y REVISIÓN 17

6. GLOSARIO DE TÉRMINOS 17

7. ANEXOS 18

1. OBJETIVO

Establecer una metodología para la gestión integral de riesgos institucionales que permita **identificar, analizar, evaluar, tratar y monitorear los riesgos**, internos y externos, que puedan afectar el cumplimiento de los objetivos estratégicos institucionales, asegurando su gestión sistemática, continua y articulada con la planificación institucional, conforme a lo dispuesto en la Norma de Control Interna 300.

2. ALCANCE

La presente metodología es de aplicación institucional y comprende de manera integral las etapas de **identificación, análisis, evaluación, tratamiento y monitoreo de riesgos**, incluyendo el seguimiento al cumplimiento de las acciones definidas en los planes de tratamiento.

Aplica a todos los procesos institucionales y unidades administrativas, y se ejecuta de forma continua, dinámica y actualizada, en función de cambios en el entorno interno y externo que puedan incidir en el perfil de riesgo institucional.

3. MARCO METODOLÓGICO

La presente metodología se fundamenta en principios, normas y buenas prácticas de gestión de riesgos, que aseguran su consistencia técnica y alineación con estándares nacionales e internacionales, las mismas que se señalan a continuación:

- **Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos**, emitidas por la Contraloría General del Estado: establecen el marco para la implementación de sistemas de control interno, incorporando la evaluación de riesgos como un proceso esencial para la consecución de objetivos estratégicos institucionales y la adecuada administración de recursos públicos.

- **Guía para Gestionar los Riesgos de un Proceso – Ministerio del Trabajo**: proporciona lineamientos para la identificación y tratamiento de riesgos operativos, considerando factores internos como: infraestructura, talento humano, sistemas de información y modelo de gestión.

- **ISO 31000:2018**: define principios y directrices para la identificación, análisis y evaluación de riesgos, promoviendo su integración en todos los niveles organizacionales y su utilización como herramienta para la generación y protección de valor.

4. DIRECTRICES GENERALES

Las disposiciones contenidas en la presente metodología son de **cumplimiento obligatorio** para todas las unidades administrativas y servidores/as de la Superintendencia de Bancos, en el ámbito de sus competencias, conforme a las siguientes directrices:

4.1 La gestión de riesgos deberá ejecutarse bajo un enfoque **sistemático, estructurado, continuo y documentado**, en concordancia con la Norma de Control Interno 300, asegurando su integración con la planificación estratégica y operativa .

4.2 En los aspectos no previstos en este documento, se deberá observar lo dispuesto en la normativa vigente aplicable y en la normativa interna institucional.

4.3 Los responsables de las unidades administrativas deberán:

- Identificar y evaluar los riesgos asociados a los objetivos institucionales.
- Proponer e implementar acciones de tratamiento.
- Monitorear de forma permanente la efectividad de los controles establecidos.
- Reportar oportunamente el estado de los riesgos y el avance de las acciones de mitigación al Controller.

4.4 El Controller será responsable de:

- Diseñar, implementar y mantener actualizada la metodología de gestión de riesgos institucionales con el apoyo de las unidades administrativas en el ámbito de sus respectivas competencias.
- Coordinar con las diferentes unidades administrativas la identificación, análisis, evaluación y tratamiento de riesgos.
- Elaborar y actualizar anualmente la **Matriz de Riesgos Institucionales (Anexo No. 1)**, que incluirá el registro de riesgos, su valoración, controles existentes, acciones de tratamiento y seguimiento.
- Consolidar y reportar información a la máxima autoridad o su delegado y a los Intendentes Generales para la toma de decisiones a nivel institucional, en el ámbito de sus respectivas competencias.

4.5 Para la identificación de riesgos se deberán considerar, entre otros, los siguientes insumos:

- Marco normativo interno y externo aplicable.
- Plan Estratégico Institucional y Plan Operativo Anual.

- Portafolio o taxonomía de servicios.
- Informes de auditoría interna y externa.
- Resultados de evaluaciones de la planificación institucional.

4.6 La gestión de riesgos deberá ser objeto de **monitoreo y revisión periódica**, a fin de asegurar su vigencia, efectividad y capacidad de respuesta frente a cambios en el entorno institucional.

5. DESARROLLO DEL DOCUMENTO

La presente metodología describe los mecanismos para identificar, analizar, valorar y responder a los riesgos a los que está expuesta la institución para el logro de sus objetivos, todas las etapas se registrarán en la Matriz de Riesgos Institucionales (Anexo No. 1), así como, el plan de mitigación que define las acciones necesarias a tomar para cada uno de los riesgos, de acuerdo con su valoración y tratamiento.

a. Identificación de Riesgos

La identificación de riesgos constituye un proceso sistemático y estructurado orientado a reconocer los eventos potenciales, internos y externos, que podrían afectar el cumplimiento de los objetivos institucionales.

Este proceso se realizará considerando el contexto estratégico, operativo y normativo de la institución, así como el análisis de procesos, servicios y factores críticos de gestión. Los riesgos deberán formularse en términos de **causa – evento – efecto**, a fin de facilitar su comprensión y posterior tratamiento.

Para la identificación se utilizarán, entre otros, los siguientes mecanismos:

- Análisis de los objetivos institucionales
- Revisión de información histórica y lecciones aprendidas.
- Resultados de auditorías internas y externas.
- Talleres de trabajo con responsables de las unidades involucradas.
- Análisis del entorno: político, económico, social, tecnológico, legal y ambiental.

Los riesgos identificados deberán ser registrados en la Matriz de Riesgos Institucionales, especificando su descripción, causas, consecuencias y unidad responsable.

Los factores internos incluyen la infraestructura, talento humano, cultura organizacional, cumplimiento de objetivos, tecnologías y procesos.

Es necesario definir el "Generador" o el qué o quién puede generar o provocar el evento (riesgo), que podrá guardar relación con:

- Talento humano
- Materiales/Insumos/Información
- Equipos y/o Tecnología
- Instalaciones / Infraestructura física
- Metodologías, procesos, servicios
- Situaciones políticas, financieras o sociales
- Condiciones culturales
- Medioambientales
- Normativa y/o regulaciones
- Tiempos de ejecución
- Manejo de información

El Controller, en conjunto con el responsable de la unidad respectiva y con base en los objetivos estratégicos definidos en el PEI, determinará las posibles causas, condiciones o circunstancias específicas por las cuales el generador puede ocasionar un riesgo.

Es necesario resaltar que, una vez identificado el "*Generador*", se define el "*Efecto o Consecuencia*" que es la materialización del riesgo para la institución, por ejemplo:

- Disminución de la calidad del servicio
- Reprocesos
- Incumplimiento o suspensión de actividades y/o servicios
- Afectación del clima laboral / Desempeño del personal
- Insatisfacción del usuario
- Afectación de imagen institucional
- Pérdida de credibilidad en los procesos
- Pérdida de información
- Procesos disciplinarios
- Reducción en el presupuesto
- Demora (mayores tiempos de ejecución)

El planteamiento del riesgo se definirá de acuerdo con la siguiente premisa:

Evento + "causaría" + Consecuencia

Por ejemplo:

La insuficiente asignación de recursos para la adquisición de equipos tecnológicos causaría disminución en la calidad de la atención al ciudadano.

b. Análisis de Riesgos

El análisis de riesgos tiene por objeto comprender la naturaleza de los riesgos identificados y determinar su nivel de exposición, considerando la probabilidad de ocurrencia y el impacto en el cumplimiento de los objetivos institucionales.

Para este propósito:

- Se evaluará la **probabilidad de ocurrencia** del riesgo, en función de su frecuencia o posibilidad de materialización.
- Se analizará el **impacto**, considerando las posibles consecuencias en términos operativos, financieros, legales, reputacionales y de cumplimiento.
- Se identificarán y valorarán los **controles existentes**, con el fin de determinar su efectividad en la reducción del riesgo.

El resultado del análisis permitirá establecer el nivel de riesgo inherente y residual, constituyendo la base para su priorización y tratamiento. Además, este análisis permitirá, a los responsables de las unidades, comprender cómo los riesgos pueden afectar el logro de los objetivos estratégicos, considerar sus particularidades y el contexto en el que se desarrollan.

La calificación de la probabilidad se realiza acorde a lo siguiente:

CALIFICACIÓN	PROBABILIDAD	DESCRIPCIÓN	FRECUENCIA
5	Muy alta	La ocurrencia del evento es certera e inminente	Se presenta más de una vez al año.
4	Alta	Existe una gran probabilidad de que el evento ocurra.	Se presenta por lo menos una vez al año.
3	Media	El evento podría o no ocurrir en algún momento. Las probabilidades de que suceda son 50/50.	Se presentó una vez dentro de los últimos dos (2) años.
2	Baja	El evento podría ocurrir en algún momento no tan esperado.	Se presentó una vez dentro de los últimos cinco (5) años.
1	Muy baja	El hecho de que el evento ocurra es una posibilidad muy remota.	No se tiene registros de que el evento haya ocurrido

La calificación del impacto se realiza acorde a la siguiente tabla:

CALIFICACIÓN	VALORACIÓN	DESCRIPCIÓN
5	Catastrófico	Muy alta afectación, cuando pone en peligro aspectos cruciales en la institución.
4	Grave	Afectación alta al cumplimiento de objetivos.
3	Moderado	Afectación media al cumplimiento de objetivos.
2	Leve	Baja afectación al cumplimiento de objetivos.
1	Insignificante	Muy Baja afectación al cumplimiento de objetivos.

c. Evaluación de Riesgos

La evaluación de riesgos consiste en comparar los niveles de riesgo obtenidos en la fase de análisis con los criterios de aceptación definidos por la institución, a fin de determinar su prioridad y necesidad de tratamiento.

Para la valoración de los riesgos:

- Se aplicará una **matriz de probabilidad e impacto**, que permita clasificar los riesgos en niveles (por ejemplo: bajo, medio, alto, extremo).
- Se definirán **umbrales de tolerancia o apetito de riesgo**, en función de la capacidad institucional para asumir riesgos.
- Se priorizarán los riesgos que requieran intervención inmediata o medidas de control adicionales.

Los resultados de la evaluación deberán ser documentados y servirán como insumo para la toma de decisiones y la definición de estrategias de tratamiento.

Para la estimación del riesgo se consideran los valores de la probabilidad y el impacto de acuerdo con la siguiente fórmula:

Nivel de Riesgo = Probabilidad * Impacto

IMPACTO		Insignificante	Leve	Moderado	Grave	Catastrófico
PROBABILIDAD		1	2	3	4	5
Muy baja	1	1 BAJO	2 BAJO	3 BAJO	4 MEDIO	5 MEDIO
Baja	2	2 BAJO	4 MEDIO	6 MEDIO	8 ALTO	10 ALTO
Media	3	3 BAJO	6 MEDIO	9 ALTO	12 ALTO	15 EXTREMO
Alta	4	4 MEDIO	8 ALTO	12 ALTO	16 EXTREMO	20 EXTREMO
Muy alta	5	5 MEDIO	10 ALTO	15 EXTREMO	20 EXTREMO	25 EXTREMO

Con la matriz de calificación de riesgo se establecen las zonas para determinar el nivel del riesgo, la misma que se asocia a un color lo cual permite determinar las acciones que se deben tomar para gestionarlo.

Para definir la gravedad de los riesgos se determinan cuatro (4) zonas:

- **Nivel VERDE (BAJO):** Cuando el impacto por la ocurrencia es menor o igual a 3.
- **Nivel AMARILLO (MEDIO):** Cuando el impacto por la ocurrencia es mayor a 3 y menor o igual a 5.
- **Nivel NARANJA (ALTO):** Cuando el impacto por la ocurrencia es mayor a 5 y menor o igual a 12.
- **Nivel ROJO (EXTREMO):** Cuando el impacto por la ocurrencia es mayor a 12 y menor o igual a 25.

d. Tratamiento de Riesgos

El tratamiento de riesgos comprende la definición e implementación de acciones orientadas a modificar el nivel de riesgo, con el fin de reducir su probabilidad de ocurrencia, su impacto, o ambos.

Las estrategias de tratamiento estarán orientadas a:

- **Evitar el riesgo:** eliminando la actividad que lo genera.
- **Mitigar o reducir el riesgo:** implementando controles preventivos
- **Compartir el riesgo:** involucrar a un tercero en el manejo del riesgo.
- **Aceptar el riesgo**, cuando se encuentre dentro de los niveles de tolerancia establecidos.

Para cada riesgo priorizado se deberá definir un **plan de tratamiento**, que incluya:

- Acciones específicas por implementar y/o indicadores de seguimiento.
- Responsables de su ejecución.
- Plazos de cumplimiento.
- Las acciones definidas deberán integrarse en la gestión operativa de las unidades responsables.

Una vez evaluados los riesgos, se adoptan medidas para el tratamiento de estos, las cuales se pueden describir como:

TRATAMIENTO	DESCRIPCIÓN

EVITAR	Evitar el riesgo implica prevenir las actividades que los originan. Anticiparse a los eventos que pueden suceder y establecer políticas, normas, controles y/o procedimientos que hagan que el evento no ocurra o que disminuya la probabilidad de su ocurrencia. Algunas de las medidas para prevenir los riesgos son: ● Acciones preventivas derivadas de informes de auditorías ● Inspecciones y pruebas de seguridad ● Capacitación y/o entrenamiento ● Aumentar el nivel de información disponible para tomar decisiones ● Disminuir el nivel de exposición ● Eliminar o modificar la actividad ● Mantenimiento preventivo ● Expedir políticas y normas internas de seguridad
REDUCIR	La reducción incluye los métodos y técnicas específicas para tratar con ellos, identificándolos y proveyendo acciones para la reducción de su probabilidad e impacto. Busca proteger los recursos que amenazan los riesgos (personas, materiales, información, etc.) para evitar pérdidas en el evento de ocurrir un riesgo. Existen muchas formas de reducir la probabilidad e impacto de un riesgo, algunas son activas y otras pasivas; las activas requieren de la intervención humana para su funcionamiento y control, las pasivas actúan sin necesidad de intervención: ● Sistemas automáticos de protección ● Equipos de protección personal ● Plan de contingencia ● Planes de comunicaciones ● Sistemas de información
COMPARTIR	El compartirlo reduce la probabilidad y el impacto mediante la transferencia u otra manera de compartir una parte del riesgo. Consiste en involucrar a un tercero en el manejo del riesgo, el que, en algunos casos, podría absorber parte de las pérdidas ocasionadas por su ocurrencia e incluso responsabilizarse de la aplicación de medidas de control para reducirlo. Por ejemplo, a través de cláusulas de contratos o contratos de seguros en los cuales el asegurador se hace responsable de las pérdidas que ocasionen los riesgos.
ACEPTAR	La aceptación no realiza acción alguna para minimizar la probabilidad o el impacto porque su evaluación da como resultado un riesgo poco significativo, es decir, su ocurrencia no tendría un efecto importante o la probabilidad de que ocurra es muy remota y en caso de materializarse el riesgo, las pérdidas que ocasione son asumibles. Debe mantenerse en observación a un riesgo identificado que no representa una gran amenaza; esta decisión es analizada con la información disponible debido a la ocurrencia que resulte rara o improbable y de ocurrir no es necesario reaccionar de manera inmediata.

TRATAMIENTO IMPACTO / PROBABILIDAD		Insignificante	Leve	Moderado	Grave	Catastrófico
		1	2	3	4	5
Muy baja	1	1 BAJO	2 BAJO	3 BAJO	4 MEDIO	5 MEDIO
		ACEPTAR	ACEPTAR	ACEPTAR	REDUCIR COMPARTIR	REDUCIR COMPARTIR
Baja	2	2 BAJO	4 MEDIO	6 MEDIO	8 ALTO	10 ALTO
		ACEPTAR	REDUCIR COMPARTIR	REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR
Media	3	3 BAJO	6 MEDIO	9 ALTO	12 ALTO	15 EXTREMO
		ACEPTAR	REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR
Alta	4	4 MEDIO	8 ALTO	12 LTO	16 EXTREMO	20 EXTREMO
		REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR
Muy alta	5	5 MEDIO	10 ALTO	15 EXTREMO	20 EXTREMO	25 EXTREMO
		REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR	EVITAR REDUCIR COMPARTIR

Para los riesgos que se encuentren en el nivel verde (bajo) el riesgo se considera aceptable, por lo cual no se establecerá una medida de tratamiento.

Para los riesgos que se encuentren en el nivel amarillo (medio), nivel naranja (alto) y nivel rojo (extremo) se debe analizar la medida de tratamiento aplicable (evitar, reducir, compartir) y se generará el respectivo "*Plan de mitigación de riesgos*".

e. Seguimiento al Plan de mitigación de riesgos

El monitoreo y seguimiento tiene por finalidad verificar la implementación y efectividad de las acciones de tratamiento, así como detectar cambios en el comportamiento de los riesgos.

Este proceso deberá realizarse de manera continua e incluir:

- Seguimiento periódico al cumplimiento de las acciones definidas en los planes de tratamiento.
- Evaluación de la efectividad de los controles implementados.
- Actualización de la valoración de riesgos en función de cambios en el entorno o en los procesos.
- Identificación de nuevos riesgos emergentes.

Los responsables de las unidades deberán reportar el estado de los riesgos y de las acciones de mitigación conforme a los lineamientos institucionales. El Controller consolidará esta información y generará reportes para la alta dirección.

El plan de mitigación estará incluido dentro de la matriz de riesgos institucionales y contendrá las actividades de control y contingencia establecidas para manejar los riesgos, fechas y responsables por áreas relacionadas.

El Controller, coordinará los talleres de construcción del plan de mitigación de riesgos en conjunto con los responsables de las unidades, que deberán entender y aportar con información para la toma decisiones y para la definición de acciones dentro de la gestión de riesgos, así como, cumplir las acciones bajo su responsabilidad dentro de su ámbito de gestión y en los plazos establecidos.

Los responsables de las unidades administrativas y el Controller deben promover acciones para facilitar el intercambio de información veraz, pertinente, precisa y fácil de entender.

El Controller, de manera semestral, realizará el seguimiento al cumplimiento del plan de mitigación mediante reuniones de trabajo.

Además, debido a que los riesgos son dinámicos y están en constante cambio, algunos riesgos tienden a desaparecer, mientras que otros riesgos pueden aparecer o pueden cambiar su “Nivel de riesgo” por lo que se deberá realizar un análisis anual con los responsables de éstos, para la actualización de la matriz de riesgos institucionales, siguiendo la misma metodología.

f. Comunicación y revisión

La gestión de riesgos deberá ser comunicada de manera oportuna y transparente a los niveles pertinentes de la organización, asegurando que la información relevante esté disponible para la toma de decisiones.

Asimismo, la metodología y la matriz de riesgos deberán ser objeto de revisión periódica, con el fin de garantizar su pertinencia, actualización y mejora continua, en concordancia con cambios institucionales, normativos o del entorno.

6. GLOSARIO DE TÉRMINOS

- **Análisis del riesgo:** Proceso llevado a cabo para identificar y evaluar la severidad de los riesgos, definidos a partir de la consecuencia y probabilidad de ocurrencia de cada riesgo.
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis de riesgos con los criterios de los riesgos con el fin de tomar las acciones necesarias para evitar, reducir, compartir o aceptar os riesgos.
- **Evento:** Acontecimiento imprevisto o cambio de un conjunto particular de circunstancias.
- **Factor de riesgo:** Circunstancia o situación interna y/o externa que aumenta la probabilidad de que un riesgo se materialice.
- **Identificación de los riesgos:** Identificar los sucesos que se pueden producir en la institución y las consecuencias que puedan tener sobre los objetivos.
- **Impacto**: Representación del efecto o de las consecuencias que la ocurrencia del evento pueda representar para la gestión institucional, afectando de diversas formas la implementación y/o ejecución de estos.
- **Matriz de riesgos:** Es la herramienta que permite evidenciar el diagnóstico general de los riesgos, las medidas pertinentes para su tratamiento, las acciones de mitigación y el seguimiento de su ejecución.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de varios. Se expresa en términos de combinación de la probabilidad y el impacto de éstos.
- **PEI:** Plan Estratégico Institucional.
- **Probabilidad:** Se refiere a la posibilidad de ocurrencia del evento y está basada en un marco temporal considerado de un año (1) correspondiente al período fiscal en curso; es decir, el número de veces al año que puede presentarse un hecho. Adicional se tomará como referencia general el período total de duración de la administración institucional, cinco (5) años.
- **Riesgo:** Evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto que pudiera obstaculizar o impedir el logro de los objetivos, procesos y metas institucionales.

- **Tratamiento del riesgo:** Se desarrollan e implementan estrategias específicas y eficaces con relación a costos y planes de acción para incrementar los beneficios potenciales y reducir las pérdidas potenciales.
- **Objetivo:** es el enunciado que define los resultados específicos y medibles que una institución o el Estado buscan alcanzar a mediano y largo plazo. Estos deben estar articulados al Plan Nacional de Desarrollo (PND) y orientados a la gestión por resultados
- **Proceso:** es el conjunto de actividades, tareas y recursos interrelacionados que transforman insumos en productos o servicios. Su propósito central es cumplir con la misión institucional de la organización y satisfacer las demandas de los ciudadanos de manera eficiente.

7. ANEXOS

Anexo No. 1. Matriz de Riesgos Institucionales. (sujeta actualización conforme alineaciones instrumentos de planificación)