METODOLOGIA ARO DE SMITHSON C.W. PARA ISO 31000

INSTRUCTIVO PARA IDENTIFICAR, MEDIR, CONTROLAR Y MONITOREAR LOS RIESGOS OPERACIONALES.

Riesgo: Toda posibilidad de ocurrencia de aquella situación que pueda entorpecer el desarrollo normal de las funciones de la entidad y le impidan el logro de sus objetivos.

La metodología esta enfocada en identificar las situaciones que se puedan presentar en la ejecución de un proceso, que impida el desarrollo de las actividades o el logro del objetivo del mismo.

1- CLASIFICACIÓN DE LOS PROCESOS

Procesos Estratégicos: "Incluyen los relativos al establecimiento de políticas y estrategias, fijación de objetivos, comunicación, disposición de recursos necesarios y revisiones por la Dirección".

Procesos Misionales: "Incluyen todos aquellos que proporcionan el resultado previsto por la entidad en el cumplimiento del objeto social o razón de ser".

Procesos de Apoyo: Incluyen aquellos que proveen los recursos necesarios para el desarrollo de los procesos estratégicos y misionales".

2- IDENTIFICACIÓN DE RIESGOS OPERACIONALES

La identificación de riesgos comprende tanto en los procesos estratégicos, misionales como los de apoyo.

En una primera etapa, se identifican los riesgos operacionales potenciales en los diferentes procesos, con base a la experiencia de los responsables de los mismos, clasificándolos inicialmente de acuerdo a su buen criterio, por lo tanto, el riesgo descrito es perceptivo ya que en ocasiones no se cuenta con una base de datos que indique un registro de eventos.

Los riesgos se ponderan bajo los criterios establecidos en la siguiente metodología y con la ayuda de un consultor que guía la sesión.

Los gestores de riesgo operativo designados por los directivos de cada área identificarán los riesgos inherentes a los procesos respondiendo el siguiente formato.

El riesgo se describe en un lenguaje sencillo propio de la actividad que se realiza, posteriormente asocie el riesgo descrito con uno de los riesgos identificados y descritos en la entidad.

Dependencia:	**Fecha:**
Funcionario:	
Cargo:	
Nombre del Proceso:	
Nombre del Subproceso:	**No aplica:** ☐
1- Objetivo del proceso:	
2- Actividad del proceso en que podría presentarse la situación describir. (identificarla en la caracterización).	
3- Descripción detallada de una situación o evento que impida el cumplimiento del objetivo.	
4- Agentes generadores de la situación de descrita (quién o, qué). Ejemplo: Personas, Procesos, Equipos,	
5- Activos tangibles o intangibles afectados por la situación. (información, infraestructura, equipos, económicos, imagen)	
6- Causas que permitieron que se generara la situación. (vulnerabilidades, debilidades). Ejemplo: Falta de personal debidamente capacitado, Falta de unidad de criterios, Falta de equipos adecuados, Falta de mantenimiento y actualización de software, otros	
7- Frecuencia de ocurrencia de la situación (número de veces al año) ☐ **Alta** (Ocurre una vez ala trimestre) ☐ **Baja** (Superior al Semestre) ☐ **Media** (Ocurre una vez al semestre)	
8- Consecuencias de la materialización de la situación (personas, bienes materiales o inmateriales con incidencias importantes como daños físicos, sanciones, pérdidas económicas de información de bienes, de imagen, de credibilidad y de confianza, daño ambiental).	

9- Impacto de Materialización de la Situación.

☐ **Catastrófico** Demandas, sanciones por entes de control, imagen negativa de la entidad).

☐ **Moderado** Quejas por mala gestión o falta en la prestación del servicio, investigaciones de los entes de control, comentarios negativos en los medios de comunicación de la entidad)

☐ **Leve** Quejas por demoras en la prestación del servicio, recomendaciones de los entes de control, comentarios no favorables en los medios de comunicación

10- Identifique el riesgo presentado en la situación (tener en cuenta que no sea causa, ni consecuencia según lo identificado en el punto 2 de este documento).

11- Con relación al control del riesgo:

¿Existen tareas de control para prevenir o mitigar el riesgo? Si ☐ No ☐

¿Se están aplicando en la actualidad? Si ☐ No ☐

¿Son efectivas para prevenir o mitigar el riesgo? Si ☐ No ☐

12- ¿las tareas de control existentes están documentados en algún procedimiento?

Si ☐ No ☐

¿En cuál? (Nombre)_____

(Código)_____

13- Describa las tareas de control para prevenir o mitigar el riesgo: (pueden ser actividades o controles definidos en un procedimiento asociado al proceso o, de lo contrario defínalos)
Ejemplo: Contratación de personal, Capacitación del personal, Revisión del trabajo ejecutado etc.

14- ¿Cuando se deben aplican las tareas de control?
☐ Antes de la actividad ☐ Durante la actividad ☐ Después de la actividad

3- CLASIFICACIÓN DE LOS RIESGOS OPERACIONALES

La entidad puede realizar un agrupamiento de riesgos por afinidad y de esta manera designar un **nombre general** que permita optimizar su administración e identificación, el agrupamiento se puede efectuar por causas o por consecuencias, siendo esta última la más recomendable.

Entre los ejemplos de clasificación de riesgos tenemos:

3.1 Daño y Destrucción de activos.

Hace referencia principalmente a las consecuencias operacionales que tendría que afrontar la entidad por el daño o destrucción de sus activos. (Informáticos, instalaciones, equipos, vehículos).

Se puede originar de manera accidental o intencional. Por ejemplo: actos vandálicos en las instalaciones de cómputo de la entidad o en las instalaciones externas donde se tienen las copias o backups de información. También, por falta de medidas de seguridad físicas en los sitios neurálgicos de la entidad. La falta de políticas, normas y procedimientos, para el adecuado manejo y mantenimiento de los diferentes equipos, por parte de los usuarios.

Daños **a activos Físicos:** "Perdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales y otros acontecimientos".

3.2 Pérdida de imagen pública.

Este riesgo potencial hace referencia, principalmente, a las pérdidas de imagen y, por consiguiente, de dinero que tendría que afrontar la entidad, cuando por actos accidentales o mal intencionados de los empleados o terceros, los clientes pierden confianza en la entidad.

3.3 Decisiones erróneas.

La ocurrencia de este riesgo obedece principalmente al uso de información errónea o inexacta, ocasionada por fallas en los procedimientos de manejo de la información. Puede involucrar todas las dependencias. Cabe recordar que, una decisión de tipo gerencial, con base en información errónea, puede ocasionar un impacto negativo altamente significativo. Una proyección de la operación de la entidad, con base en información errónea, inoportuna o no confiable, podría indicar desconocimiento de la institución.

3. 4 Sanciones legales.

La ocurrencia de este riesgo obedece al incumplimiento del marco legal dentro del cual se desarrolla la institución, ocasionando pérdidas económicas por el pago de las multas y sanciones disciplinarias a sus empleados. En las entidades se puede presentar si no se cumple con la normatividad vigente y/o no se produce a tiempo la información exigida por las normas legales.

3.5 Desventaja competitiva.

Pérdidas de dinero que resultan de divulgar datos de información confidencial y de uso interno, administrada por las direcciones. También está dado por ofrecer servicios de inferior calidad que los socios comerciales.

3.6 Hurto / Fraude.

Hace referencia a las pérdidas que podría tener la institución por la apropiación indebida, por parte de un funcionario o de terceros, de los activos de esta. Este puede ser causado por alteración de la información (registros contables o financieros) que representan operaciones de los servicios de la institución.

3.7 Fraude Interno.

Perdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas institucionales en las que se encuentra implicada, al menos, una parte interna de la entidad.

3.8 Fraude Externo.

Perdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero.

3.9 Pérdidas por exceso de egresos.

Pérdidas de dinero causadas por exceso en los desembolsos, ocasionadas por errores y omisiones de los empleados en la ejecución de sus actividades y tareas.

3.10 Pérdidas en ingresos.

Pérdidas de dinero causadas por cobrar (recaudar) o registrar cantidades inferiores, originadas por errores y omisiones de los empleados en la ejecución de sus actividades y tareas.

3.11 Derechos Humanos.

La ocurrencia de este riesgo obedece a la falta de control por de parte de las entidades públicas para garantizar el conjunto de prerrogativas inherentes a la naturaleza de la persona, cuya realización efectiva resulta indispensable para el desarrollo integral del individuo que vive en una sociedad jurídicamente organizada, mediante el establecimiento de límites a las actuaciones de todos los servidores públicos, sin importar su nivel jerárquico o institución gubernamental, con el fin de prevenir los abusos de poder, negligencia o simple desconocimiento de la función.

Las entidades deben establecer de políticas, normas, procedimientos, canales y mecanismos de participación que faciliten a todas las personas tomar parte activa en el manejo de los asuntos públicos y en la adopción de las decisiones comunitarias.

3.12 Clientes, productos y prácticas comerciales.

Perdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto"

3.13 Administración de procesos, ejecución y entrega.

Perdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores".

3.14 Interrupción de las actividades y problemas del sistema.

Perdidas derivadas de incidencias en el negocio y de fallos en los sistemas.

3.15 Riesgos Profesionales.

Hace referencia al conjunto de situaciones que contribuyen a mantener y controlar los niveles de eficiencia en las operaciones de una organización pública, para brindar a sus trabajadores un medio laboral seguro evitando los riesgos que se presenten específicamente en los efectos de las enfermedades y los accidentes que pueden ocurrirles con ocasión o como consecuencia del trabajo que desarrollan.

3.16 Prácticas Laborales y seguridad en el lugar de trabajo.

Perdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad / discriminación.

3.17 Medio Ambiente.

Hace referencia a las consecuencias operacionales que tendría que afrontar la entidad por no controlar los procesos y actividades para prevenir y minimizar los efectos sobre el entorno, ocasionando incumplimiento de los requisitos de la legislación medioambiental vigente, la protección ambiental y los impactos de la propia organización sobre el medio ambiente, impactando negativamente el crecimiento económico continuado de manera sostenible a largo plazo.

4- MEDICIÓN DEL RIESGO OPERACIONAL

Para medir la probabilidad de ocurrencia de un evento de riesgo operativo se establecieron los siguientes criterios:

La medición del riesgo operacional se define por dos variables (frecuencia por impacto) el resultado del mismo debe ser cuantitativo para determinar su valor.

4.1 Escala definida para medir la frecuencia de los eventos.

La frecuencia de los eventos se califica de acuerdo a las siguientes categorías; alta, media o baja, así mismo se asigna uno de los siguientes valores dependiendo de la categoría (uno (1), dos (2) o tres (3).

- **Alta:** El evento ocurre (1) una vez al TRIMESTRE, este nivel tendrá una calificación de “3”.

- **Media:** El evento ocurre de (1) una vez al SEMESTRE, este nivel tendrá una calificación de “2”.

- **Baja:** El evento ocurre con una periodicidad superior al SEMESTRE, este nivel tendrá una calificación de “1”.

4.2 Escala definida para medir el impacto por la materialización de los eventos.

El impacto del evento se califica de acuerdo a las siguientes categorías; catastrófico, moderado o leve, de igual manera se asigna uno de los siguientes valores dependiendo de la categoría treinta (30), veinte (20), diez (10).

- **CATASTROFICO:** El impacto es “CATASTROFICO”, cuando se genere alguno de los elementos que se describen a continuación, ésta categoría tendrá una calificación de treinta (30).

Objetivos / Proyectos/Proceso: El evento afectó el cronograma establecido para uno o varios de los objetivos primarios, generando una ampliación en las fechas para el cumplimiento de los mismos.

Demandas: Se impusieron demandas en contra de la entidad por fallas en la prestación del servicio, con indemnizaciones por parte de la entidad.

Entidades de control: Impusieron sanciones a la entidad con reportes y recomendaciones críticas.

Publicidad adversa / Efectos reputacionales: El evento tuvo cobertura en los medios de comunicación, se generó una imagen negativa de la institución.

- **MODERADO:** El impacto es "MODERADO", cuando se genere alguno de los elementos que se describen a continuación, ésta categoría tendrá una calificación de diez (10).

  Objetivos / Proyectos/Proceso: El evento afectó el cronograma establecido para uno o varios de los objetivos secundarios, generando una ampliación en las fechas para el cumplimiento de los mismos.

  Quejas: Se recibieron múltiples quejas por mala gestión o faltas en la prestación del servicio de la entidad.

  Entidades de control: El evento ameritó una investigación por parte de las autoridades de control.

  Publicidad adversa / Efectos reputacionales: El evento tuvo comentarios negativos en los medios de comunicación.

- **LEVE:** El impacto es "LEVE", cuando se genere alguno de los elementos que se describen a continuación, ésta categoría tendrá una calificación de cinco (5).

  Objetivos / Proyectos/Procesos: El evento tuvo un efecto menor en el alcance de los objetivos.

  Quejas: Se recibieron quejas por demoras en la prestación del servicio de la entidad fácilmente solucionables.

  Entidades de control: Las autoridades de control realizaron unas recomendaciones para la entidad.

  Publicidad adversa / Efectos reputacionales: Se presentaron algunos comentarios no favorables en los medios de comunicación.

Matriz: Nivel de Riesgo Inherente de la entidad (Frecuencia vs Impacto).

VALORACION DEL RIESGO	
NIVEL DE RIESGO INHERENTE	CALIFICACION
INACEPTABLE	60
IMPORTANTE	30 - 40
MODERADO	15 - 20
TOLERABLE	10
ACEPTABLE	5

5- CONTROLES

Los controles son las acciones que mitigan el riesgo, reduciendo la probabilidad de ocurrencia, o el impacto en los activos, los ejecutores de los controles existentes se encargaran de valorar su eficacia de acuerdo a su buen criterio y guiados con las opciones enunciadas a continuación.

5.1 Aplicación del control:

- **Preventivo:** Sí el control se aplica ANTES o al INICIAR un proceso, ésta categoría tendrá una calificación de cuatro (4).

- **Correctivo:** Sí el control se aplica durante el proceso y permite corregir las deficiencias que se encuentran, ésta categoría tendrá una calificación de tres (3).

- **Detectivo:** Sí el control se aplica cuando el proceso ha terminado, ésta categoría tendrá una calificación de dos (2).

- **Inexistente:** Si no existe control definido ésta categoría tendrá una calificación de uno (1).

5.2 Periodicidad del control:

- **Permanente:** El control se realiza durante todo el proceso, es decir, en cada actividad, ésta categoría tendrá una calificación de tres (3).

- **Periódico:** El control se realiza transcurridas un número de actividades o un tiempo determinado, ésta categoría tendrá una calificación de dos (2).

- **Ocasional:** El control se realiza solo en forma ocasional en un proceso, ésta categoría tendrá una calificación de uno (1).

5.3 Escala para medir la eficacia de los controles:

APLICACIÓN		PERIODICIDAD		PRODUCTO	EFICACIA	VALORACION
PREVENTIVO	4	PERIODICO	3	12	ALTA	4
PREVENTIVO	4	PERMANENTE	2	8	MEDIA	3
PREVENTIVO	4	OCASIONAL	1	4	BAJA	2
CORRECTIVO	3	PERIODICO	3	9	ALTA	4
CORRECTIVO	3	PERMANENTE	2	6	MEDIA	3
CORRECTIVO	3	OCASIONAL	1	3	BAJA	2
DETECTIVO	2	PERIODICO	3	6	MEDIA	3
DETECTIVO	2	PERMANENTE	2	4	BAJA	2
DETECTIVO	2	OCASIONAL	1	2	BAJA	2
INEXISTENTE	1	- -		1	INEXISTENTE	1

EFICACIA DEL CONTROL	
ALTO	4
MEDIO	3
BAJO	2
INEXISTENTE	1

6- VALORACIÓN DE LOS RIEGOS

6.1 Metodología para calcular el Riesgo Residual

El riesgo residual es el nivel resultante del riesgo después de aplicar controles.

La formula para determinar el nivel de exposición del riesgo es la división entre el nivel del riesgo dividido entre el nivel de eficacia del control que se encuentra asociado al riesgo.

$$\textbf{Riesgo Residual} = \frac{\text{Nivel de Riesgo Inherente.}}{\text{Control (eficacia)}}$$

Escala definida para determinar el Riesgo Residual en la entidad:

VALORACION DEL RIESGO (residual)	
NIVEL DE RIESGO RESIDUAL	CALIFICACION
INACEPTABLE	> 30
IMPORTANTE	20 a 30
MODERADO	10 a 20
TOLERABLE	5 a 9,9
ACEPTABLE	< 5

- **INACEPTABLE:** El resultado de la operación (*Nivel de Riesgo / Eficiencia del control*) da un valor superior a 30.
- **IMPORTANTE** El resultado de la operación (*Nivel de Riesgo / Eficiencia del control*) da un valor entre 20 y 30.
- **MODERADO:** El resultado de la operación (*Nivel de Riesgo / Eficiencia del control*) da un valor entre 10 y 20.

- **TOLERABLE:** El resultado de la operación (*Nivel de Riesgo / Eficiencia del control*) da un valor entre 5 y 9,9.

- **ACEPTABLE:** El resultado de la operación (*Nivel de Riesgo / Eficiencia del control*) da un valor inferior a 5.

VALORACION DEL RIESGO (residual)	
NIVEL DE RIESGO RESIDUAL	CALIFICACION
INACEPTABLE	> 30
IMPORTANTE	20 a 30
MODERADO	10 a 20
TOLERABLE	5 a 9,9
ACEPTABLE	< 5

Ejemplo:
Nivel de Riesgo Inherente Moderado (20)

Eficacia de Control **Media (3)**

$$\text{Riesgo Residual} = \frac{20}{3} = 6{,}66$$

Este valor corresponde a un nivel de riesgo residual de **tolerable**.

6.2 Monitoreo de los eventos de riesgo Operativo:

Periódicamente se revisa el perfil de riesgo de la entidad para asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos por el comité de control interno y se implementan las siguientes medidas de acuerdo al nivel.

- Sí el riesgo residual tuvo una calificación de **"INACEPTABLE"** se debe informar a la alta dirección, se requiere de acción inmediata.

- Sí el riesgo residual tuvo una calificación de **"IMPORTANTE"** se debe informar a los subgerentes de área y se deben establecer planes para tratar el riesgo.

- Sí el riesgo residual tuvo una calificación de **"MODERADO"** se deben establecer puntos de control que permitan mitigarlo.

- Sí el riesgo residual tuvo una calificación de **"TOLERABLE - ACEPTABLE"** no se requiere de ninguna acción adicional, el riesgo genera impactos bajos y estos son fácilmente remediados.

6.3 Mapa de Riesgos.

Con el nivel de riesgo residual defina el mapa de riesgos

6.4 Niveles de aceptación del riesgo operativo.

El nivel de riesgo será aceptado para aquellos eventos cuya calificación de riesgo inherente se encuentren en las categorías de medio o bajo y se toleraran aquellos riesgos operacionales cuyo costo de controlar o tratar sea superior a la pérdida potencial que éstos puedan ocasionar.

6.5 Registro de eventos.

Para registrar los eventos de riesgo operativo se diseñó una plantilla adjunta con las siguientes características:

- Matriz de Identificación de Riesgos

PROCESO	SUBPROCESO	OBJETIVO DEL PROCESO	DESCRIPCION DEL RIESGO O AMENAZA	CAUSAS	CONSECUENCIAS	RIESGO ASOCIADO	PROBA-BILIDAD	IMPACTO	GRADO DE EXPOSICIÓN

- Matriz de Valoración de Riesgos.

PROCESO	RIESGO O AMENAZA	CONTROLES	TIPOS DE CONTROL		CALIFICACIÓN DEL CONTROL	VALORACIÓN DEL RIESGO (r residual puntaje)	GRADO DE EXPOSICIÓN (letra)	ACCIONES A SEGUIR LINEAMIENTOS	ACCIÓN DE TRATAMIENTO	RESPONSABLE	FECHA DE IMPLEMENTACIÓN

El registro de eventos debe ser realizado por los gestores de calidad. Sí algún funcionario desea reportar un evento de riesgo debe acercarse al gestor de calidad designado y juntos diligenciar los campos requeridos por la plantilla y evaluar los efectos del riesgo.

7. POLITICA DE RIESGOS

Con el mapa de riesgos, defina una política que permita implementar acciones para mitigar los riesgos, esto puede ser minimizando las probabilidades de ocurrencia o minimizando el impacto del riesgo cuando este se materialice.