POLITICA DE ADMINISTRACIÓN DEL RIESGO

INTRODUCCIÓN

Este manual contiene la metodología para llevar a cabo la identificación, análisis y valoración del riesgo dentro de cada uno de los procesos, iniciando con la identificación del contexto estratégico, además de establecer los actores y responsables del proceso de administración del riesgo y define las políticas generales de administración del riesgo aplicables para TEVEANDINA – Canal Trece.

Para la elaboración del presente Manual se tomaron como referencia los lineamientos del Departamento Administrativo de la Función Pública DAFP, establecidos mediante la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5 del DAFP, la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5 y 6 del DAFP, los Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas de MinTic y la Norma NTC ISO 31000:2018. Gestión del Riesgo.

TEVEANDINA SAS – Canal Trece, está comprometida con la administración efectiva de riesgos que incluya los riesgos de corrupción, riesgos de seguridad informática, riesgos fiscales y riesgos por proceso, identificándolos, promoviendo las acciones y controles necesarios que le permitan al canal mitigarlos evitando que se materialicen afectando negativamente los logros y los objetivos institucionales.

1. OBJETIVO

Establecer, definir e implementar el marco general para la administración de riesgos, mediante el análisis de las estrategias, la formulación de objetivos y su implementación para la toma de decisiones cotidiana, lo que permitirá una identificación del riesgo adecuada a las necesidades conforme al cumplimiento de las metas del plan estratégico, con un enfoque preventivo que permita la protección de los recursos contribuyendo al mejoramiento continuo mediante el tratamiento de los riesgos identificados, con el fin de mitigar los efectos no deseados.

2. ALCANCE

Es aplicable a todos los programas, proyectos, procesos y procedimientos que desarrolla TEVEANDINA SAS– Canal Trece para el logro de sus objetivos conforme al cumplimiento de requisitos legales y técnicos aplicables, incluidos los controles para mitigar el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Canal mediante criterios de responsabilidad por parte de los servidores públicos en el ejercicio de sus funciones.

3. DEFINICIONES

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros que utiliza la organización para funcionar en el entorno digital.

Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

a. **Bien de uso público:** aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b. **Bienes fiscales:** aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la entidad.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

Confidencialidad: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Control: Medida que permite reducir o mitigar un riesgo.

Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

Control fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.
Factores de riesgo: son las fuentes generadoras de riesgos.

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas,

jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes.

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Infraestructura critica cibernética: infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Integridad: propiedad de exactitud y completitud.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la formula del nivel del riesgo poder ser probabilidad * impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de probabilidad – impacto.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza publica, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C- 340-07).

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota: los eventos potenciales hacen referencia a 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.

Riesgo de Corrupción: Posibilidad de que, por acción y omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Contratación: Son los eventos que pueden afectar la realización de la ejecución contractual y cuya ocurrencia no puede ser predicha de manera exacta por las partes involucradas en el Proceso de Contratación.

Riesgo Fiscal: Es el efecto dañoso sobre los recursos Públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial2. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel de riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Vulnerabilidad: representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. GENERALIDADES

El manual toma como base fundamental los lineamientos establecidos por el Departamento Administrativo de la Función Pública (DAFP), en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas actual, así como la NTC ISO 31000.

Para ello, TEVEANDINA S.A.S. – Canal Trece, adopta esta metodología de gestión del riesgo con el interés de formalizar y fortalecer el compromiso de la entidad en el tema, al estar conscientes que una adecuada gestión de riesgos permite:

- Aumentar la probabilidad de alcanzar los objetivos
- Establecer una base confiable para la toma de decisiones y la planificación.
- Preparar a la organización para eventos no esperados “Evitar sorpresas”

- Cuidar nuestros principales activos: Los recursos de la Nación, las Personas
- Prevenir amenazas y aprovechar oportunidades
- Mejorar la presentación de informes obligatorios y voluntarios
- Mejorar el aprendizaje organizacional

Los principios de la gestión de riesgos son:

- Crear y proteger el valor contribuyendo al logro demostrable de los objetivos y a la mejora del desempeño
- Ser parte integral de todos los procesos de la organización, no una actividad independiente
- Ser parte de la toma de decisiones
- Abordar explícitamente la incertidumbre
- Debe ser sistemática, estructurada y oportuna contribuyendo a la eficiencia y resultados consistentes, comparables y confiables
- Establecer la mejor información disponible basándose en datos históricos, experiencia, retroalimentación, observación, previsiones y examen de expertos.
- Intervención por aquellos que toman decisiones en todos los niveles de la organización, garantizando de esta forma que sea transparente e inclusiva
- Alinear el contexto externo e interno y el perfil de riesgo de la organización a la gestión del riesgo.
- Ser parte de las responsabilidades de la alta dirección
- Considerar los factores humanos y culturales
- Es dinámica, reiterativa y receptiva al cambio
- Facilitar la mejora continua en la organización

5. POLITICA GENERAL DE ADMINISTRACIÓN DEL RIESGO

La gestión del riesgo en TEVEANDINA SAS – Canal Trece, genera un entorno permanente de lucha y cero lins contra la corrupción, integrando sus procesos enfocados a la prevención y detección de hechos asociados a este fenómeno, tomando las medidas necesarias para combatirlo mediante la política de administración de riesgos y cuenta con un carácter estratégico, fundamentado en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores públicos y contratistas del Canal.

La presente política involucra la participación de las líneas de defensa las cuales a través del Modelo Integrado de Planeación y Gestión (**MIPG**) se desarrolla en la **Dimensión 7 *Control Interno*** para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores públicos del Canal.

Es de recordar que el modelo integrado de planeación y gestión (MIPG) es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades para el cumplimiento de los objetivos institucionales de TEVEANDINA SAS – Canal Trece a través de sus 7 dimensiones (talento humano, direccionamiento estratégico, gestión con valores para el resultado, evaluación de resultados, información y comunicación, gestión del conocimiento y la innovación y, finalmente, control interno) que agrupan las políticas de gestión y Desempeño institucional y que, implementadas de manera articulada e interrelacionada, permitirán la funcionalidad y operación adecuada del modelo.

Dentro de la gestión institucional, TEVEANDINA SAS – Canal Trece, cuenta con acciones articuladas al sistema de control interno para la prevención del riesgo de gestión, de corrupción y fiscal bajo la base de un ejercicio preventivo frente a la concreción del daño patrimonial de naturaleza pública.

En este sentido, TEVEANDINA SAS– Canal Trece a través de la presente política, identifica y valora los riesgos los cuales se integra en el desarrollo del plan estratégico y a su vez, la formulación de los objetivos y su implementación a través de la toma de decisiones cotidiana en cada uno de los procesos.

Imagen No. 1

5.1. POLÍTICAS ESPECIFICAS DE ADMINISTRACIÓN DEL RIESGO

- El representante legal en el seno del comité institucional de coordinación de control interno aprueba la política de administración del riesgo.
- Antes de iniciar con los compromiso de la dirección frente al riesgo es necesario aclarar que la política de administración de riesgos contiene los lineamientos para la gestión efectiva de los riesgos por proceso, los riesgos de corrupción y los riesgos de seguridad de la información.
- Establecer, dar a conocer y mantener las estrategias de mitigación o tratamiento de los riesgos, como pilares fundamentales en la administración de los riesgos.
- Divulgar en toda la Institución la misión, visión, estrategias, políticas, responsabilidades y procedimientos de manera que todos los funcionarios se sientan involucrados y compartan su responsabilidad en el proceso de administración de riesgos.
- Vigilar el cumplimiento y entendimiento de las normas, políticas y procedimientos tendientes a minimizar el riesgo en cada una de las áreas expuestas en la Institución.

5.2. LINEAMIENTOS GENERALES PARA GESTIÓN DEL RIESGO

La Matriz de Gestión del Riesgo que contiene los riesgos institucionales, de seguridad de la información y de corrupción, se debe:

- Elaborar anualmente por cada responsable de los procesos, junto con su equipo.
- Elaborar y consolidar con el liderazgo de planeación junto a los líderes de cada proceso.
- Publicar en la página web, a más tardar el día 31 del mes de enero y realizar su divulgación interna y externa a través de la sección de Transparencia y Acceso a la Información Pública.
- Realizar el seguimiento de Control Interno con corte a las siguientes fechas: 30 de abril, 31 de agosto y 31 de diciembre.
- Anualmente, en el último trimestre del año se revisarán los riesgos de gestión y de corrupción por proceso, identificados de acuerdo con los parámetros vigentes definidos por el DAFP.

5.3. LINEAMIENTOS ESPECIFICOS DE LA POLÍTICA DE GESTIÓN DE RIESGOS

En TEVEANDINA SAS– Canal Trece, la Política de Gestión de Riesgos se define de conformidad a los parámetros del Modelo Integrado de Planeación y Gestión MIPG tomando como referente las líneas de defensa dentro de la estructura del Sistema Integrado de Gestión implementado.

La presente política involucra todos los procesos y dependencias, quienes deben establecer los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco del Plan estratégico, mediante:

- ✓ El establecimiento de acciones de control detectivas y preventivas para los riesgos identificados.
- ✓ La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

Para gestionar adecuadamente los riesgos TEVEANDINA SAS– Canal Trece determina las acciones para asumir, reducir y mitigar el riesgo al igual que establece acciones cuando se presente la materialización de los riesgos.

i. Aplicabilidad de Política de Operación

La política de riesgos es aplicable a todos los procesos, proyectos, productos de TEVEANDINA SAS– Canal Trece, y a las acciones ejecutadas por los servidores públicos durante el desarrollo de sus funciones en cumplimiento de los objetivos institucionales.

ii. Determinación de la capacidad de riesgo

TEVEANDINA SAS – Canal Trece, aplica los valores de probabilidad e impacto sugeridos mediante metodología suministrada por el Departamento Administrativo de la Función Pública contenidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas y con base en esta, determina, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la misión del Canal, puede ser resistido antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad de riesgo”.

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que el Canal puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos institucionales.

iii. Determinación del apetito al riesgo

Una vez se determine la capacidad de riesgo por parte de la alta dirección del Canal, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del Modelo Integrado de Planeación y Gestión.

Este valor se denomina ***"apetito de riesgo"***, dado que equivale al nivel de riesgo que el Canal puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

iv. Tolerancia de riesgo

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por TEVEANDINA SAS– Canal Trece.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y no puede ser superior al valor de la capacidad de riesgo.

Para el canal, la determinación de la tolerancia de riesgo es optativa y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

La política de gestión de riesgos en TEVEANDINA SAS– Canal Trece, genera un entorno permanente de lucha y cero tolerancias contra la corrupción, integrando sus procesos con enfoque a la prevención y detección de hechos asociados a este fenómeno, tomando las medidas necesarias para combatirlo mediante la aplicación de los requisitos de la presente política de gestión de riesgos la cual cuenta con un carácter estratégico y está fundamentada en el Modelo Integrado de Planeación y Gestión MIPG, con un enfoque preventivo de evaluación permanente sobre la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores, trabajadores y contratistas y el análisis de los siguientes riesgos:

- Riesgos de gestión de proceso bajo el efecto que se causa sobre los objetivos del Canal, debido a eventos potenciales.

- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los por acción u omisión, se use el poder para desviar la gestión delo público hacia un beneficio privado.

- Los riesgos de seguridad de la información como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un

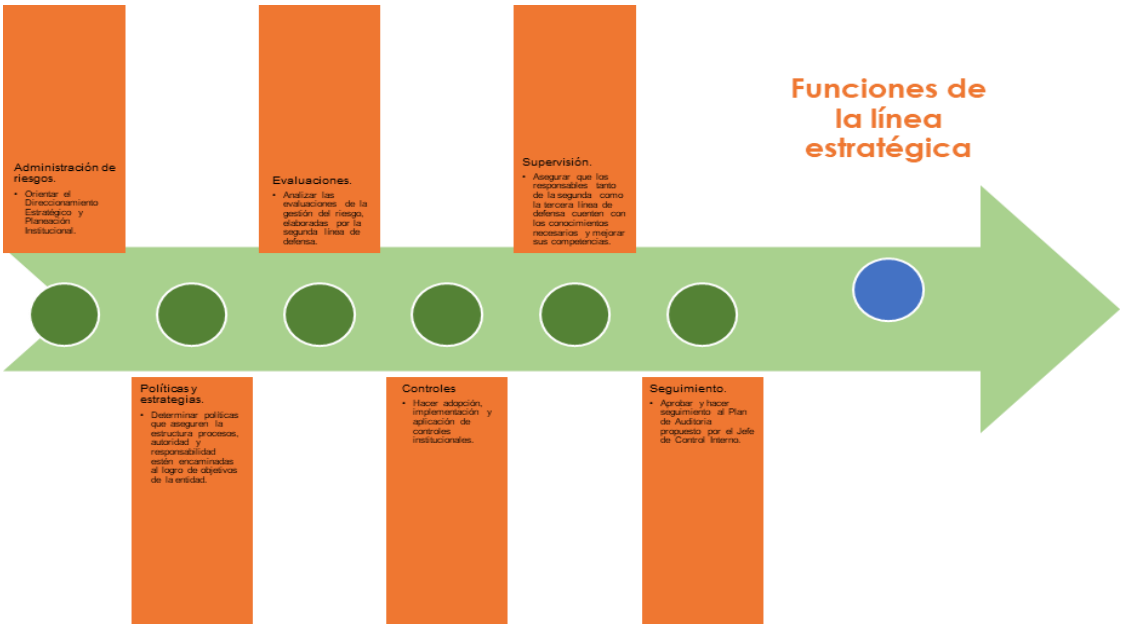
activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Los Riesgos de Contratación CCE como los eventos que pueden afectar la realización de la ejecución contractual y cuya ocurrencia no puede ser predicha de manera exacta por las partes involucradas en el Proceso de Contratación.
- Riesgo Fiscal con el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

La presente política involucra la gestión de los Servidores, trabajadores y contratistas de TEVEANDINA SAS– Canal Trece, permitiendo la Identificación, el análisis, la valoración, el tratamiento, el registro y el seguimiento de las acciones con el fin de mitigar los riesgos que pudieran afectar el logro de los objetivos por proceso y por ende los institucionales, para lo cual la Alta Dirección, representada en el comité Institucional de Gestión y Desempeño como línea estratégica define el marco general para la gestión del riesgo y supervisa su cumplimiento.

Línea estratégica, **A cargo de** la gerencia y el comité institucional de gestión y desempeño con las siguientes obligaciones:

• Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control.
• Recomendaciones de mejoras a la política de operación para la administración del riesgo.
• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad.

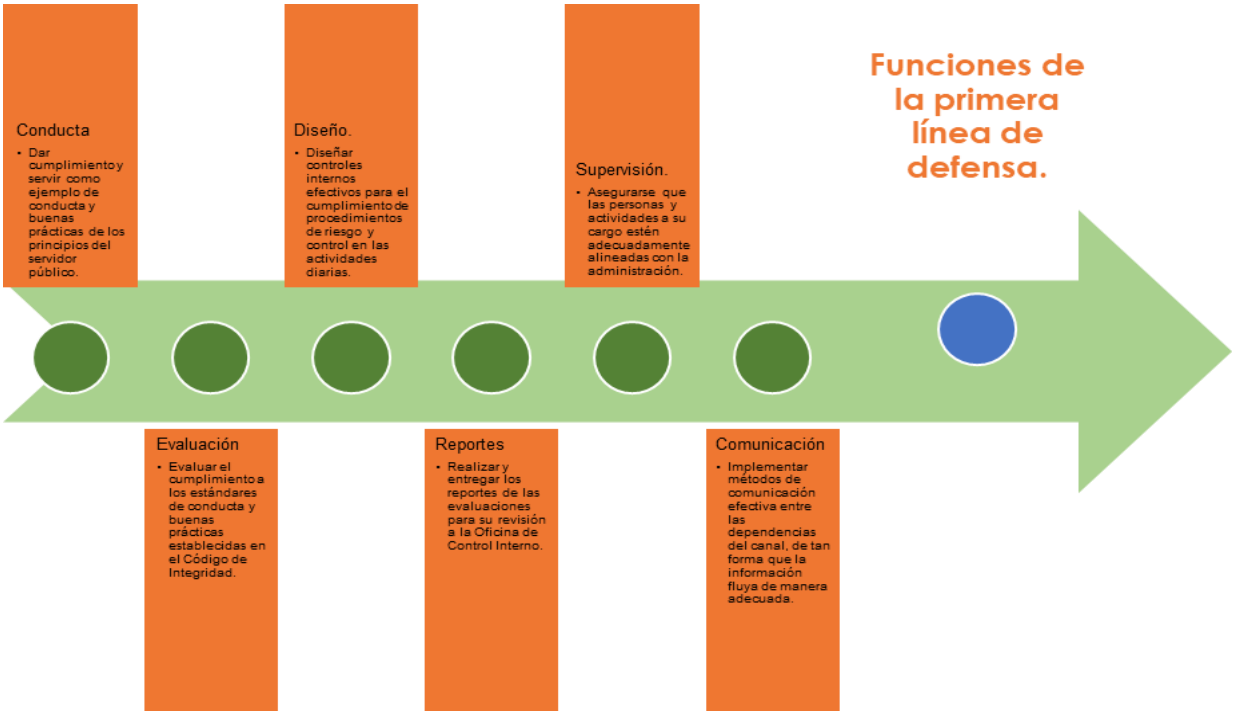


La primera línea de defensa **A cargo** de: líderes de los procesos, programas y proyectos en su

i. **Rol principal:** de Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos del Canal.

   Así mismo, orientar el desarrollo e implementación de:

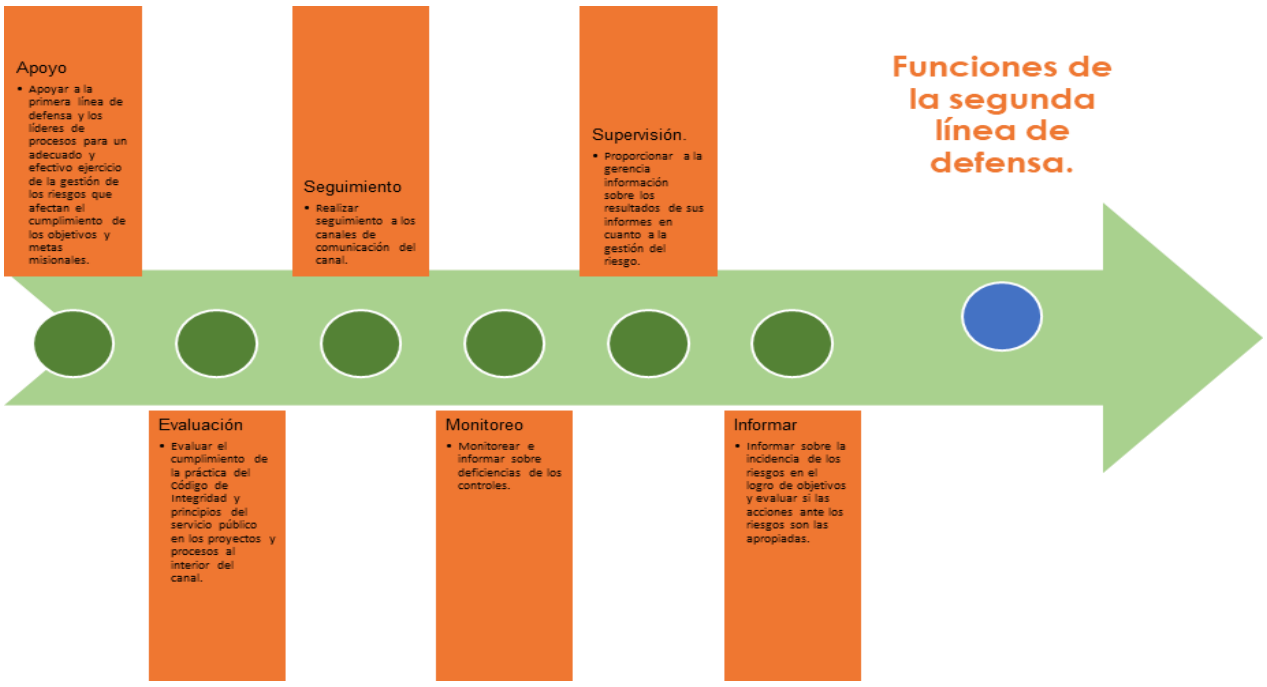
ii. Políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos del Canal y emprender las acciones de mejoramiento para su logro.



La segunda línea de defensa **A cargo de**: Los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo.

Planeación en su

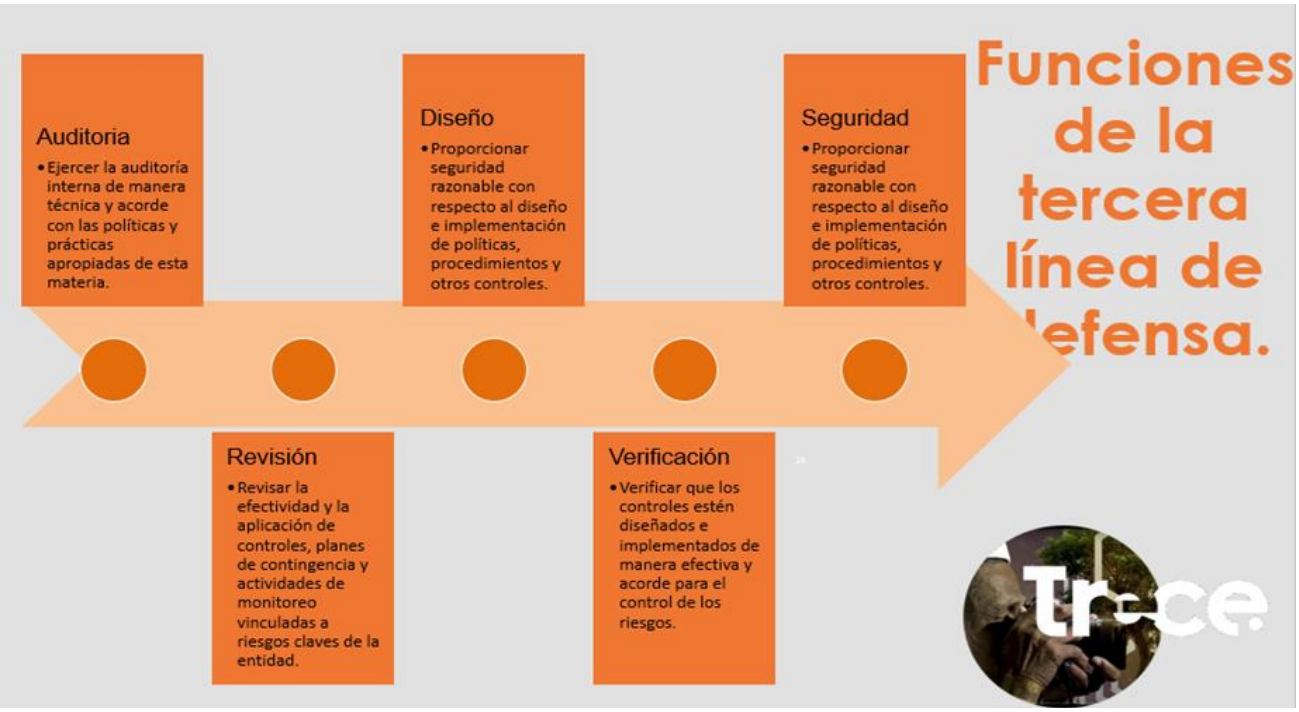
i. **Rol principal:** Soporta y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la operación de riesgos.



Y, la tercera línea de defensa **A cargo de:** área de Control Interno y revisoría fiscal,

El rol principal de proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la operación de riesgos.

El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del Sistema de Control Interno.

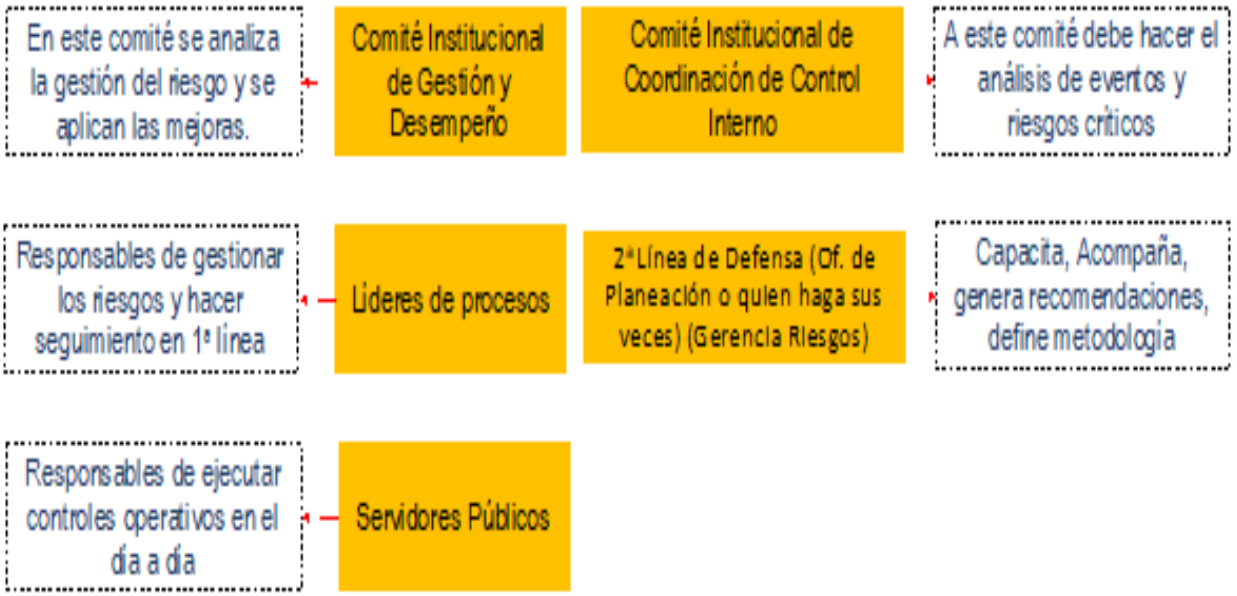


5.4. RESPONSABILIDADES

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección y por todos los servidores públicos y contratistas de TEVEANDINA SAS– Canal Trece, con el propósito de proporcionar en el desarrollo de su gestión, un aseguramiento razonable con respecto al logro de los objetivos se debe tener en cuenta los siguientes beneficios:

- Apoyo a la toma de decisiones
- Fortalecimiento en la operación organizacional
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos y sus servidores públicos y contratistas (la calidad va de la mano con la gestión del riesgo)
- Fortalecimiento de la cultura de control
- Incrementa la capacidad del Canal para alcanzar sus objetivos
- Dota al canal de herramientas y controles para hacer una administración más eficaz y eficiente.

Imagen No. 2 INSTITUCIONALIDAD PARA LA GESTIONDEL RIESGO

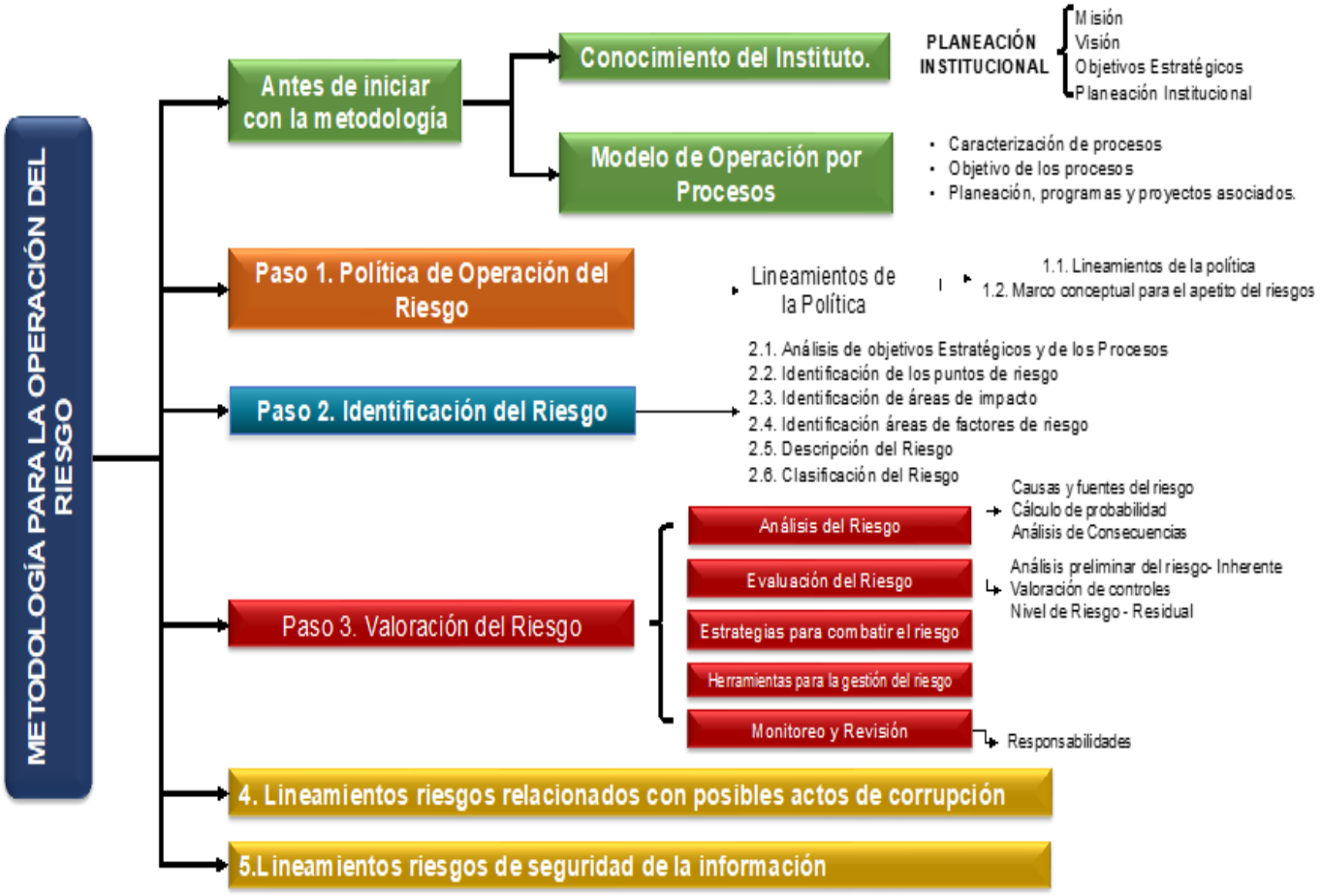


Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6. METODOLOGÍA DE GESTIÓN DEL RIESGO

TEVEANDINA SAS– Canal Trece, establece la metodología para la gestión del riesgo previo al análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión, además del conocimiento de la metodología desde un punto de vista estratégico y de la aplicación de tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la administración para que su efectividad pueda ser evidenciada.

Estructura con sus desarrollos básicos:



6.1. IDENTIFICACIÓN DE LOS RIESGOS.

TEVEANDINA S.A.S. – Canal Trece identifica las fuentes de riesgo, las áreas de impacto, los eventos, causas y consecuencias potenciales generando una lista con base en los eventos que puedan crear, aumentar, degradar, acelerar o retrasar el logro de sus objetivos.

Para ello incluye riesgos sin importar si su origen está o no bajo el control de la entidad, aun cuando su causa pueda no ser evidente. Para ello se realiza un análisis del entorno interno y externo en que opera el canal y desde la caracterización de cada uno de los procesos se analizan todos los factores que puedan generar que un riesgo afecte el cumplimiento de los objetivos estratégicos.

Una vez se identifiquen los posibles riesgos se deben aplicar los siguientes pasos:

6.1.1. Análisis de objetivos estratégicos y de los procesos: Todos los riesgos que se identifiquen deberán cumplir con un criterio que impacte los objetivos estratégicos o de los procesos de TEVEANDINA S.A.S.. – Canal Trece.

Así las cosas, se realizarán los siguientes análisis:

6.1.1.1. Análisis de objetivos estratégicos. la entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

Es necesario revisar que los objetivos estratégicos se encuentren alineados con la misión y la visión institucional, así como, analizar su adecuada formulación, es decir que contengan las siguientes características mínimas: especifico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en ingles).

A continuación, se explican las características SMART.

- **Specific (Especifico):** Lo importante es resolver cuestiones como: qué, cuándo, cómo, con qué, quién. Considerar el orden y los necesarios para el cumplimiento de la misión.
- **Mensurable (Medible):** Para ello es necesario involucrar algunos números en su definición, por ejemplo, porcentajes o cantidades exactas (cuando aplique)
- **Achievable (Alcanzable):** Para hacer alcanzable un objetivo se necesita un previo análisis de lo que se ha hecho y logrado hasta el momento. Esto ayudará a saber si lo que se propone es posible o cómo resultaría mejor.
- **Relevant (Relevante):** Considerar recursos, factores externos e información de actividades previas, a fin de contar con elementos de juicio para su determinación.
- **Timely (Temporal):** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y mediciones finales.

6.1.1.2. Análisis de los objetivos por proceso. los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la misión y la visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

6.1.2. Identificación de los puntos de riesgo. Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo

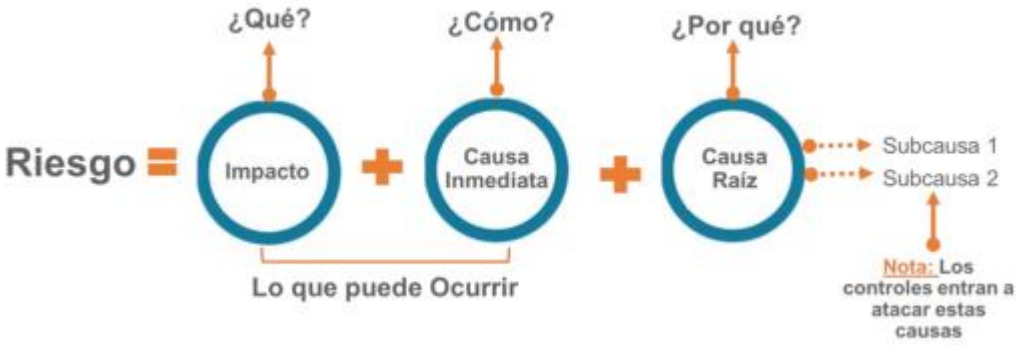
6.1.3. Identificación de las áreas de impacto. El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

6.1.4. Identificación de las áreas de factores de riesgo. Son las fuentes generadoras de riesgos. En la siguiente tabla se encontrará un listado con los factores de riesgo que puede tener TEVEANDINA S.A.S. – Canal Trece.

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externos
		Falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
Evento externo	Situaciones externas que afecten la entidad.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

6.1.5. Descripción del Riesgo. La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. El Departamento Administrativo de la Función Pública propone la siguiente estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

De acuerdo con la anterior estructura tenemos:

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa Inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

6.2. IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN.

Los riesgos de corrupción deben ser establecidos sobre los procesos de la entidad. Para facilitar su identificación y no confundirlo con otra clase de riesgo, la entidad sigue las recomendaciones de la Secretaría de Transparencia de la Presidencia de la República, teniendo en cuenta la siguiente matriz:

MATRIZ DEL RIESGO DE CORRUPCIÓN				
Descripción del Riesgo	**Acción u omisión**	**Uso del Poder**	**Desviar la gestión de lo público**	**Beneficio Privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República

Si se marca con una X las opciones de cada casilla para la Descripción del Riesgo significa que el riesgo identificado es de corrupción.

6.3. IDENTIFICACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:

Para lograr identificar los riesgos de seguridad de la información TEVEANDINA S.A.S. – Canal Trece realizara primero la identificación de sus activos de información de acuerdo con los lineamientos del "Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas." De acuerdo con este modelo se podrán identificar los siguientes tres riesgos de seguridad de la información:

- Perdida de confidencialidad
- Perdida de integridad
- Perdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

6.3.1. Identificación de activos de seguridad de la información. Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Para identificar los activos la primera línea de defensa deberá realizar los siguientes pasos:

- Listar los activos por cada proceso
- Identificar el dueño de los activos
- Clasificar los activos
- Clasificar la información

- Determinar la criticidad del activo
- Identificar si existe infraestructura critica cibernética

6.3.2. Identificación de amenazas en activos de seguridad de la información. TEVEANDINA S.A.S. – Canal Trece se acoge al listado de amenazas que representan las situaciones o fuentes que pueden dañar los activos de información de la ISO 27005:2009: y que pueden generar materialización en los riesgos.

6.3.2.1. Amenazas comunes. A continuación, se presenta un listado de las amenazas más comunes de los activos de seguridad de la información y su origen:

- **Deliberadas (D):** Se utiliza para todas las acciones deliberadas de forma voluntaria e intencionada que tienen como objetivo causar daño a los activos de la información, tales como información, procesos y sistemas.
- **Fortuitas (F):** se utiliza para todas las acciones humanas que pueden dañar accidentalmente los activos de la información, tales como información, procesos y sistemas.
- **Ambientales (A):** Se utiliza para todos los incidentes que no se basan en las acciones humanas.

Tipo	Amenaza	Origen
Daño Físico	Fuego	F, D ,A
	Agua	F, D ,A
Eventos Naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	A
	Fallas en el suministro de aire acondicionado	F, D ,A
Perturbación debida a la radiación	Radiación electromagnética	F, D ,A
	Radiación térmica	F, D ,A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas Técnicas	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F

Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

6.3.2.2. Amenazas dirigidas por el hombre. A continuación, se presenta un listado de las amenazas que pueden ser dirigidas por empleados, proveedores y/o piratas informáticos entre otros con o sin intención de dañar los activos de información:

Fuente o Amenaza	Motivación	Acciones Amenazantes
Pirata informático, intruso ilegal	• Reto • Ego	• Piratería • Ingeniería social
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información	• Crimen por computador • Acto fraudulento
Terrorismo	• Chantaje • Destrucción	• Ataques contra el sistema DDoS • Penetración en el sistema
Espionaje Industrial (Inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Hurto de información
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ganancia monetaria	• Asalto a un empleado • Chantaje

Fuente: ISO/IEC 27005:2009

6.3.2.3. Identificación de vulnerabilidades.
A continuación, se presenta un listado de las vulnerabilidades más comunes:

Tipo	Amenaza
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección

	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envió o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/IEC 27005:2009

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda

causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

6.4. IDENTIFICACIÓN DE LOS RIESGOS FISCALES

Para la Identificación del **riesgo fiscal** es necesario establecer los puntos de riesgo y las circunstancias Inmediatas.

Los puntos de riesgos: son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Las circunstancias inmediatas: se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz- para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Sirve para identificar	Preguntas y respuestas para la Identificación
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la entidad), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno.
	Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.
	Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.

	Nota 3: Los fallos con responsabilidad fiscal en firme son información publica, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado.
	Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la Republica y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?
	Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catalogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

6.5. TÉCNICAS PARA LA IDENTIFICACIÓN DE LOS RIESGOS

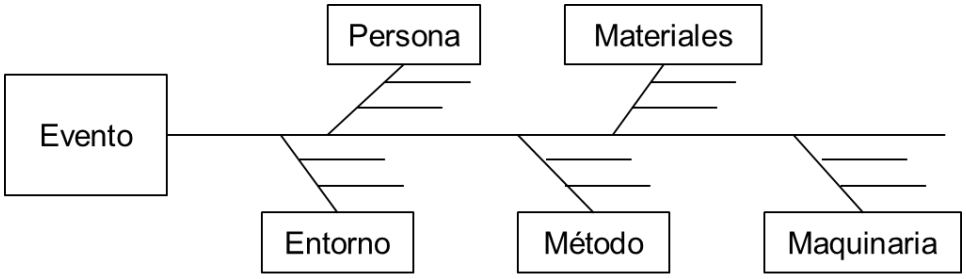
Para identificar los riesgos, TEVEANDINA S.A.S. – Canal Trece realiza mesas de trabajo por proceso donde se lista una serie de posibles eventos que se adecuen de acuerdo con los objetivos de su proceso y su entorno. Esta información es analizada por cada proceso, realizando una depuración de los riesgos que no los afectan y determinando su impacto y probabilidad basados en la ejecución en un periodo de tiempo (día, mes, año) de acuerdo con los parámetros de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5 del Departamento Administrativo de la Función Pública.

A continuación, se listan las técnicas usadas para identificar los riesgos:

6.5.1. Lluvia de Ideas. De una manera organizada y en un período mu y breve de tiempo los actores que intervienen en el proceso lanzan creativamente diferentes ideas teniendo en cuenta el contexto.

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

6.5.2. Espina de pescado. Es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo.



- La causa principal debe ir pegada a la “cabeza”.
- Pregúntese, ¿Qué podría causar el problema?
- Coloque las causas en cada una de las áreas

6.5.3. Método de la escalera (5 porqués). Es un método basado en realizar preguntas para explorar las relaciones de causa-efecto que generan un problema en particular. El objetivo final de los 5 Porqué ’s es determinar la causa raíz de un defecto o problema.

6.6. ERRORES FRECUENTES EN LA IDENTIFICACIÓN DE LOS RIESGOS

- **Referencia circular:** Esto es, identificar un riesgo simplemente como el contrario de un objetivo. Ejemplo: si el objetivo es “asegurarse que todas las facturas son aprobadas antes de su pago”, el riesgo se identifica como “las facturas pueden ser pagadas antes de ser aprobadas”. Esto agrega muy poco valor al proceso de identificación de riesgo.

- **Iniciar la redacción con palabras negativas:** Para la redacción de un riesgo se debe evitar iniciar con palabras negativas como “No, Que no, etc”.

6.7. CLASIFICACIÓN DEL RIESGO

La clasificación del riesgo permite agrupar los riesgos identificados en las siguientes categorías:

- **Ejecución y administración de procesos:** Agrupa los riesgos que generen pérdidas derivadas de errores en la ejecución y administración de procesos
- **Fraude Externo:** Agrupa los riesgos que generen pérdidas derivadas de actos de fraude por personas ajenas a la organización.
- **Fraude Interno:** Agrupa los riesgos que generen pérdida debido a actos de fraude, acciones irregulares, comisión de hechos delictivos, abuso de confianza entre otras.
- **Fallas Tecnológicas:** Agrupa los riesgos que generen errores de hardware, software, telecomunicaciones e interrupciones de servicio.
- **Relaciones laborales**: Agrupa los riesgos que generen pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
- **Usuarios productos y prácticas:** Agrupa los riesgos que generen por fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
- **Daños a activos fijos / eventos externos:** Agrupa los riesgos que generen pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo y orden público.

6.8. VALORACIÓN DEL RIESGO.

Para valorar el Riesgo inicial o Inherente TEVEANDINA S.A.S. – Canal Trece establecerá la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos. La valoración del riesgo consta de 2 pasos:

6.8.1. Análisis de Riesgos. busca establecer la prioridad de ocurrencia de los riesgo y sus consecuencias o impacto, con el fin de estimar el Riesgo inicial o Inherente.

6.8.1.1. Determinar la probabilidad de los Riesgos Institucionales, de corrupción y de seguridad de la información. La probabilidad de ocurrencia estará asociada a la exposición del riesgo de la actividad que se esté analizando.

Para TEVEANDINA S.A.S. – Canal Trece el nivel de exposición a un riesgo estará asociada al proceso o actividad que se este analizando, es decir, al número de veces que al realizar una actividad se pasa por el punto de riesgo en un periodo de un año, a continuación, se relaciona la tabla de criterios para definir los niveles de probabilidad de la entidad:

Nivel	Probabilidad	Descripción
20%	Muy Baja	La actividad se realiza entre 0 a 50 veces al año.
40%	Baja	La actividad se realiza entre 51 a 151 veces al año.
60%	Media	La actividad se realiza entre 152 a 252 veces al año.
80%	Alta	La actividad se realiza entre 253 a 353 veces al año.
100%	Muy Alta	La actividad se realiza entre 354 a 500 veces al año.

6.8.1.3. Determinar el impacto de los Riesgos Institucionales y de Seguridad de la Información. El impacto de ocurrencia estará asociada a la exposición del riesgo de la actividad que se esté analizando. A continuación, se relaciona la tabla de criterios para definir los niveles de impacto de los riesgos institucionales y de seguridad de la información:

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
20%	Leve	Pérdida económica desde 12.22 hasta 19.99 SMLMV	Solo de conocimiento de algunos funcionarios.
40%	Menor	Pérdida económica de 20 hasta 34,44 SMLMV	De conocimiento general de la entidad a nivel interno, Gerencia y Comités
60%	Moderado	Pérdida económica de 34, 45 hasta 51,66 SMLMV	Deterioro de imagen con algunos usuarios de relevancia frente a cumplimiento de objetivos. Deterioro de imagen con algunos usuarios de relevancia frente a cumplimiento de objetivos.
80%	Mayor	Pérdida económica de 51.67 hasta 68,88 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel Territorial.
100%	Catastrófico	Pérdida económica de 68,89 hasta 86.13 SMLMV	Deterioro de imagen a nivel Nacional con efecto publicitario sostenido a nivel Nacional

6.8.1.4. Determinar el impacto de los Riesgos de Corrupción. Para el impacto de los riesgos de corrupción se tendrán en cuenta solamente en los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos. A continuación, se relaciona la tabla de criterios para definir los niveles de impacto de los riesgos de corrupción:

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERUALIZA PODRÍA…	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado Responder afirmativamente de SEIS a ONCE preguntas genera un impacto Mayor Responder Afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico			
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Fuente: Secretaría de Transparencia de la Presidencia de la Republica

6.9. EVALUACIÓN DE RIESGOS

A partir del análisis de la probabilidad de ocurrencia del riesgo y de su impacto o consecuencias, la evaluación de los riesgos busca determinar la zona de Riesgo inicial o Inherente.

6.9.1. Análisis preliminar (Matriz de Riesgo Inicial o Inherente para riesgos institucionales y de seguridad de la información). Se obtiene ubicando el grado de calificación de la probabilidad y el impacto definidos anteriormente y determina la zona de riesgo donde se ubicará el riesgo inicial o inherente.

Probabilidad	Impacto				
	Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)
Muy Alta (100%)	Alto	Alto	Alto	Alto	Extremo
Alta (80%)	Moderado	Moderado	Alto	Alto	Extremo
Media (60%)	Moderado	Moderado	Moderado	Alto	Extremo
Baja (40%)	Bajo	Moderado	Moderado	Alto	Extremo
Muy baja (20%)	Bajo	Bajo	Moderado	Alto	Extremo

6.9.2. Análisis preliminar (Matriz de Riesgo Inicial o Inherente para riesgos de corrupción). Se obtiene ubicando el grado de calificación de la probabilidad y el impacto definidos anteriormente y determina la zona de riesgo donde se ubicará el riesgo inicial o inherente. Cabe resaltar que, los riesgos de corrupción no contemplan los impactos leves ni menores ya que su materialización siempre será significativa.

Probabilidad	Impacto				
	Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)
Muy Alta (100%)	NO APLICA PARA RIESGOS DE CORRUPCIÓN DADO QUE EL IMPACTO DE ESTOS RIESGOS SIEMPRE SERA SIGNIFICATIVO		Alto	Alto	Extremo
Alta (80%)			Alto	Alto	Extremo
Media (60%)			Moderado	Alto	Extremo
Baja (40%)			Moderado	Alto	Extremo
Muy baja (20%)			Moderado	Alto	Extremo

Nota: A estos riesgos inicialmente identificados se les conocerá como Riesgos Inherentes y pueden afectar el cumplimiento de los objetivos estratégicos y de cada proceso, es importante entonces definir las causas que pueden dar origen a la materialización de un riesgo, teniendo en cuenta que para cada causa identificada se debe diseñar también un control. Para efectos de la matriz de riesgos consolidada las

causas deberán manejarse en celdas separadas. Importante tener en cuenta que un control puede ser tan eficiente que podría mitigar varias causas.

6.10. VALORACIÓN DE CONTROLES.

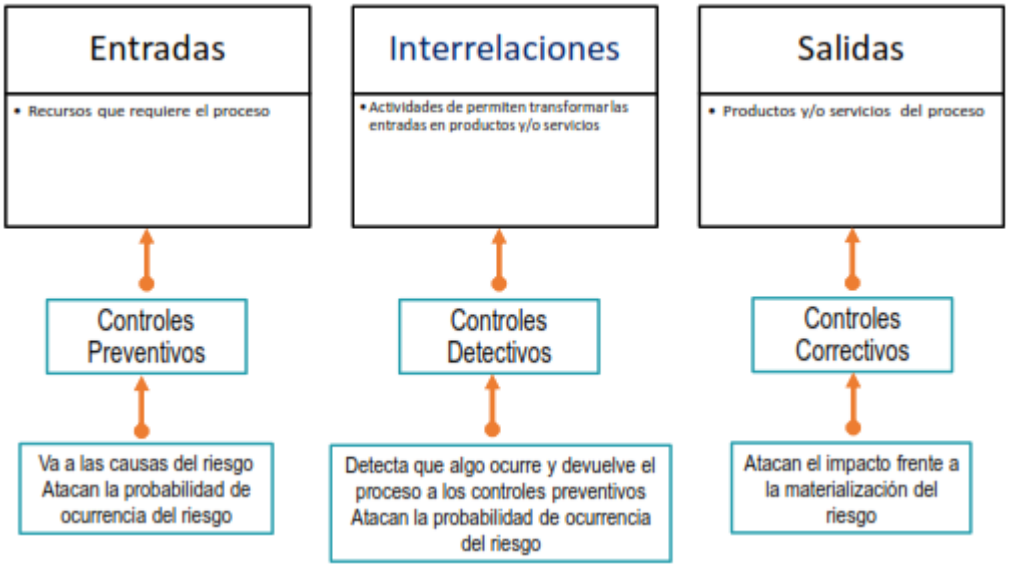
Para realizar una valoración de los controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

6.10.1. Estructura para la descripción del control. Para redactar un control adecuadamente se propone la siguiente estructura que facilitara entender su tipología y otros atributos para su valoración.

- **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

6.10.2. Tipología de los controles y los procesos. A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. En la siguiente figura se consideran las 3 fases globales del ciclo de un proceso:



Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

De acuerdo con lo anterior, tendremos las siguientes tipologías de controles:

- **Controles Preventivos:** Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Controles Detectivos:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Controles Correctivos:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control Manual:** Controles que son ejecutados por personas.
- **Control Automático:** Controles que son ejecutados por un sistema.

6.10.3. Análisis y evaluación de los controles - Atributos. A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la tabla 6 se puede observar la descripción y peso asociados a cada uno así:

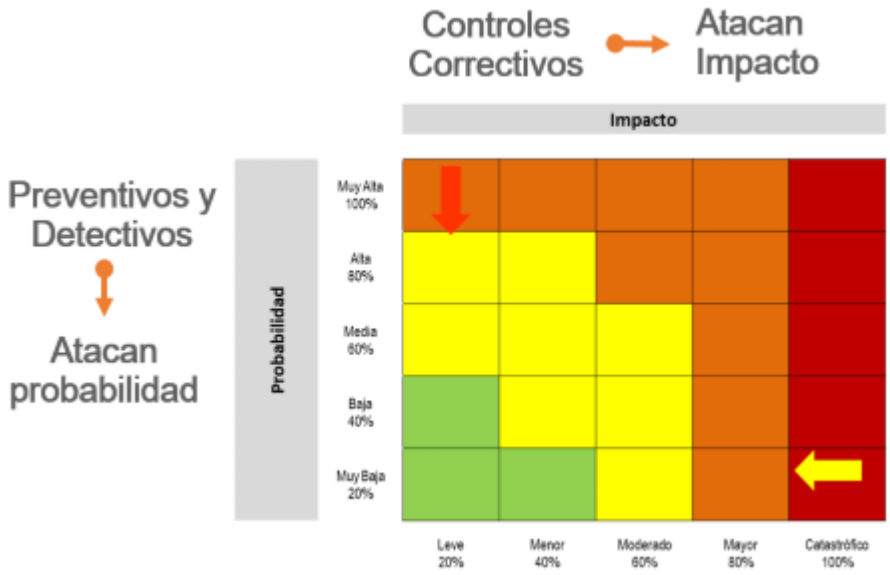
Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%

		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio de proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio de proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo.	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control	-
		Sin registro	El control no deja registro de la ejecución del control	-

Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la siguiente matriz de calor, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.



Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

Ejemplo:

Proceso: Gestión de Recursos
Objeto: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación
Riesgo identificado: posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos
Probabilidad Inherente: moderada 60%
Impacto Inherente: Mayor 80%
Zona de riesgo: alta

Controles identificados:

Control 1: el profesional de área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor los contratos que cumplen son registrados en el sistema de información de contratación.
Control 2: el jefe del área de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para la firma del ordenador de gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

En la siguiente tabla se observa la aplicación de la tabla de atributos, esta servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

6.10.4. Nivel de Riesgo (Riesgo Residual). Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

A continuación, se da continuidad al ejemplo propuesto, permitiendo observar los cálculos requeridos para la aplicación de los controles

Riesgo	Datos Relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60% * 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36% * 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2%**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A

requisitos normativos.	**Impacto Residual**	**80%**			

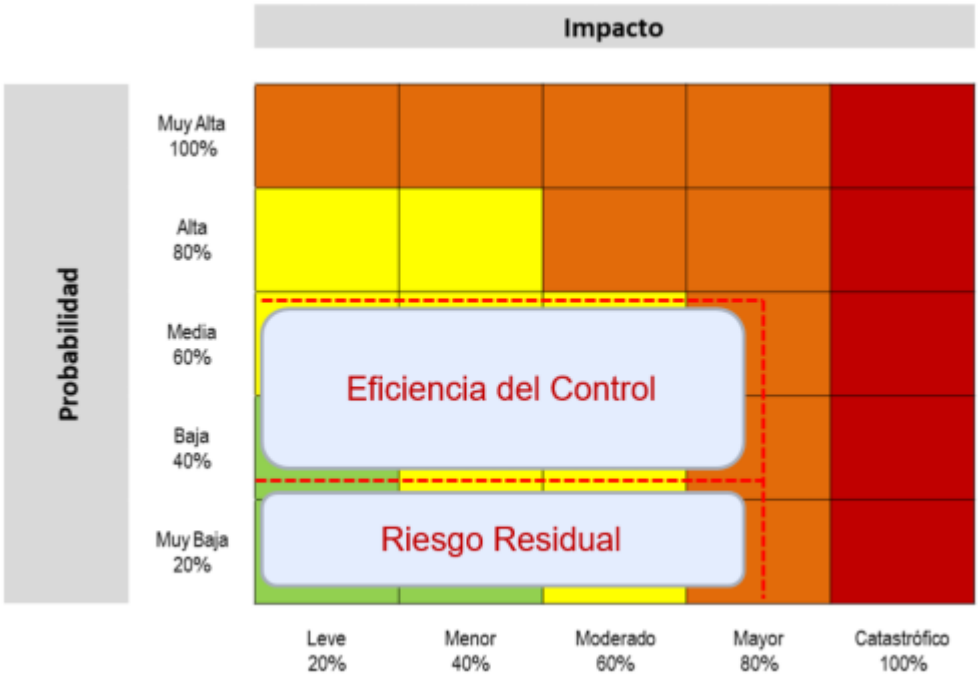
Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

Ejemplo (Continuación):

Proceso: Gestión de Recursos
Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.
Riesgo Identificado: posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
Probabilidad residual: Baja 26.8%
Impacto residual: Mayor 80%
Zona de riesgo residual: Alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

A continuación, se observa el movimiento en la matriz de calor.



Fuente: Adaptado del curso riesgo operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública 2020.

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

6.11. NIVELES DE AUTORIDAD Y SEGUIMIENTOS.

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión de Control interno del MIPG de "Control Interno" que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, distribuido de la siguiente manera:

LÍNEA DE MONITOREO Y REVISIÓN	RESPONSABILIDAD	ROL
Línea Estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno	Tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantizar el cumplimiento de los planes de la entidad. Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).
Primera Línea de Defensa	Líderes de proceso y sus equipos de trabajo.	Garantizan la gestión en el día a día, en conjunto con sus equipos de trabajo. Se encarga de identificar, evaluar, controlar y mitigar los riesgos. Son responsables de implementar acciones correctivas y detectar fallas en los controles.
Segunda Línea de Defensa	Media y alta gerencia: jefes de planeación, coordinadores de equipo de trabajo, comités de riesgo, comité de contratación, áreas financieras, de TIC etc.	Corresponde establecer mecanismos que les permitan ejecutar un seguimiento o autoevaluación permanente de la

		gestión, orientando y generando alertas a la 1ra línea de defensa. Supervisa la implementación de prácticas de gestión eficaces por parte de la primera línea.
Tercera Línea de Defensa	Oficina de control interno, auditoría interna o quien haga sus veces.	A través de un enfoque basado en riesgos, proporciona aseguramiento sobre la eficacia de la gestión del riesgo y control interno a la alta dirección.

7. BIBLIOGRAFÍA

DAFP. (2022). GUIA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS v6.- CAPITULO RIESGO FISCAL. Bogotá D.C.: Departamento Administrativo de la Función Pública. (DAFP)

DAFP. (2020). GUIA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS v5. Bogotá D.C.: Departamento Administrativo de la Función Pública. (DAFP)

DAFP. (2018). GUIA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS v4. Bogotá D.C.: Departamento Administrativo de la Función Pública. (DAFP)

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2011). NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

ICONTEC Internacional. (2013). NORMA TÉCNICA COLOMBIANA NTC-IEC/ISO 31010. GESTION DE RIESGOS. TÉCNICAS DE VALORACIÓN DEL RIESGO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

8. CONTROL DE CAMBIOS

Versión	FECHA	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE
0	Marzo 2015	Documento Original	Asesor Planeación y Calidad
1	31-05-2016	Se incluye descripción de herramientas para el análisis de causas, se incluye numeral de roles y responsabilidades, se amplía el alcance a los riesgos de corrupción.	Asesor Planeación y Calidad
2	13/09/2018	Actualización de la política de gestión de riesgos, actualización del manual bajo los parámetros actualizados de la Norma Iso 31000 y DAFP	Líder de Planeación
3	15/05/2019	Actualización del manual bajo los parámetros de la guía del DAFP y la Norma ISO 31000, contenido agregado y bibliografía.	Líder de Planeación
4	09/11/2020	Actualización del manual bajo los parámetros de la guía del DAFP	Líder de Planeación
5	Xx/xx/xxxx	Actualización del manual bajo los parámetros de la guía del DAFP v5	Líder de Planeación

9. CONTROL DE APROBACION

Elaboró:	Aprobó:
Víctor Andrés Pinzón Mora **Líder de Planeación**	Jhon alejandro Linares Camberos **Gerente**

Angela Milena Hoyos Pulido **Aseor de planeación y calidad**	
Fecha de aprobación: XX/XX/XXX	