COPIA NO CONTROLADA

Política de Administración del Riesgo		
REVISADO POR: JAIME ALBERTO ESCUDERO JIMENEZ JEFE DE LA OFICINA DE CONTROL INTERNO (C) OSCAR MARINO GOMEZ GARCIA SECRETARIO GENERAL (E) PEDRO NEL MONTOYA MONTOYA DIRECTOR DE GESTION AMBIENTAL INGRID OSPINA REALPE DIRECTOR FINANCIERO ALVARO HERNAN ROLDAN ALVAREZ DIRECTOR DE PLANEACION	**APROBADO POR:** MARCO ANTONIO SUAREZ GUTIERREZ DIRECTOR GENERAL Mediante **Resolución 0100 No.0550-0368-2024**	CVC Corporación Autónoma Regional del Valle del Cauca

CONTENIDO

INTRODUCCIÓN

El presente documento establece la política de administración del riesgo para la Corporación Autónoma Regional del Valle del Cauca – CVC, la cual expresa el compromiso de la Entidad frente a la identificación, evaluación, y tratamiento de los riesgos que puedan afectar el cumplimiento de la misión y de los objetivos institucionales.

Dando cumplimiento a las políticas de gestión y desempeño que aplican a la Corporación, se toma como referente la Política de Control Interno, a través de la cual se promueve el mejoramiento continuo y se establecen las acciones,

métodos y procedimientos de control y de gestión del riesgo. Con el cumplimiento de los aspectos que constituyen esta política, se cumple el objetivo de: “Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua”.[1]

1. OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

1.1 OBJETIVO GENERAL

Establecer un marco general de actuación de todos los servidores públicos y personal de apoyo de la Corporación para la adecuada gestión de los riesgos, mediante la identificación, evaluación y tratamiento de los mismos, con el fin de minimizar y controlar los efectos al interior, que afecten el cumplimiento de la misión y el logro de los objetivos institucionales, desde un enfoque preventivo.

1.2 OBJETIVOS ESPECÍFICOS

- Definir las metodologías para la administración de los diferentes tipos de riesgo.
- Establecer las responsabilidades en la administración de los riesgos.
- Apoyar la toma de decisiones.
- Definir estrategias de comunicación y divulgación adecuadas para la apropiación de la administración del riesgo en la Corporación.
- Incentivar el pensamiento basado en riesgos.

2. ALCANCE

La política de administración del riesgo aplica a todos los procesos adoptados por la CVC, bajo la responsabilidad de las líneas de defensa establecidas en el marco del Sistema de Control InternoInterno y abarca los siguientes:

• Riesgos por posibles actos de corrupción.
• Riesgos fiscales.
• Riesgos de seguridad de la información.
• Riesgos de seguridad y salud en el trabajo.
• Riesgos ambientales aplicables a los Sistemas de Gestión Ambiental implementados en la CVC.

3. TERMINOS Y DEFINICIONES

Alta dirección: persona o grupo de personas que dirige y controla una organización al más alto nivel. [ISO 9000:2015, 3.1.1]

Administración del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo[2]

Aplicativo: Daruma.

Control: medida que permite reducir o mitigar un riesgo.[3]

Daruma: software o aplicativo utilizado como herramienta para optimizar e integrar los diferentes sistemas de gestión corporativos (módulo Riesgos).[4]

Evaluación del riesgo: su propósito es identificar, evaluar y gestionar eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales. [Manual Operativo MIPG, pág. 117].

Factores de riesgo: Son las fuentes generadoras de riesgos.[3]

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo[3]

Líneas de defensa: asignación de roles y responsabilidades para la efectiva gestión de riesgos.[4]

Mapa de riesgos institucional: documento con la información resultante de la gestión de los riesgos en zona residual extrema.[3]

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 fórmula del Nivel del Riesgo puede 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.[3]

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 1 año.[3]

Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
NOTA 1: 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.[3]

Riesgo ambiental: posibilidad de que de manera natural o por acción humana se produzca daño en el medio ambiente. La ISO 14001:2015, define el riesgo como un efecto de incertidumbre, por lo que implica tanto efectos potenciales negativos como positivos, es decir amenazas y oportunidades.

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.[3]

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 potencial.[3]

Riesgo de gestión: son los riesgos generales incluidos en la definición para **Riesgo**.[3]

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 la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgos en seguridad y salud en el trabajo: combinación de la probabilidad de que ocurra un(os) evento(s) o exposición(es) peligroso(s), y la severidad de lesión o enfermedad, que puede ser causado por el (los) evento(s) o la(s) exposición(es) (NTC-OHSAS 18001).

Riesgo inherente: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.[3]

Riesgo residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.[3]

[1] Marco General del Modelo Integrado de Planeación y Gestión. Departamento Administrativo de la Función pública DAFP. Versión 6. 2023

[2] ICONTEC internacional. NTC ISO 31000 Gestión del riesgo – principios y directrices. 2018. P.1.

[3] Función Pública. Guía para la administración del riesgo y el diseño de controles en entidades públicas - versión 6.2022.

[4] Elaboración propia.

4. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

La CVC, entidad encargada de administrar los recursos naturales renovables y el medio ambiente del Valle del Cauca, en las áreas de su jurisdicción determinadas por la Ley, se compromete a adoptar e implementar las metodologías necesarias para la evaluación y tratamiento de todos los riesgos identificados por la Entidad, entre ellos:

- Los riesgos de gestión.
- Los riesgos por posibles actos de corrupción.
- Los riesgos fiscales.
- Los riesgos de seguridad de la información.
- Los riesgos de seguridad y salud en el trabajo.
- Los riesgos ambientales aplicables a los Sistemas de Gestión Ambiental implementados en la CVC.

La CVC cuenta con un aplicativo en donde se registrará la información correspondiente a los riesgos mencionados anteriormente y se compromete además a:

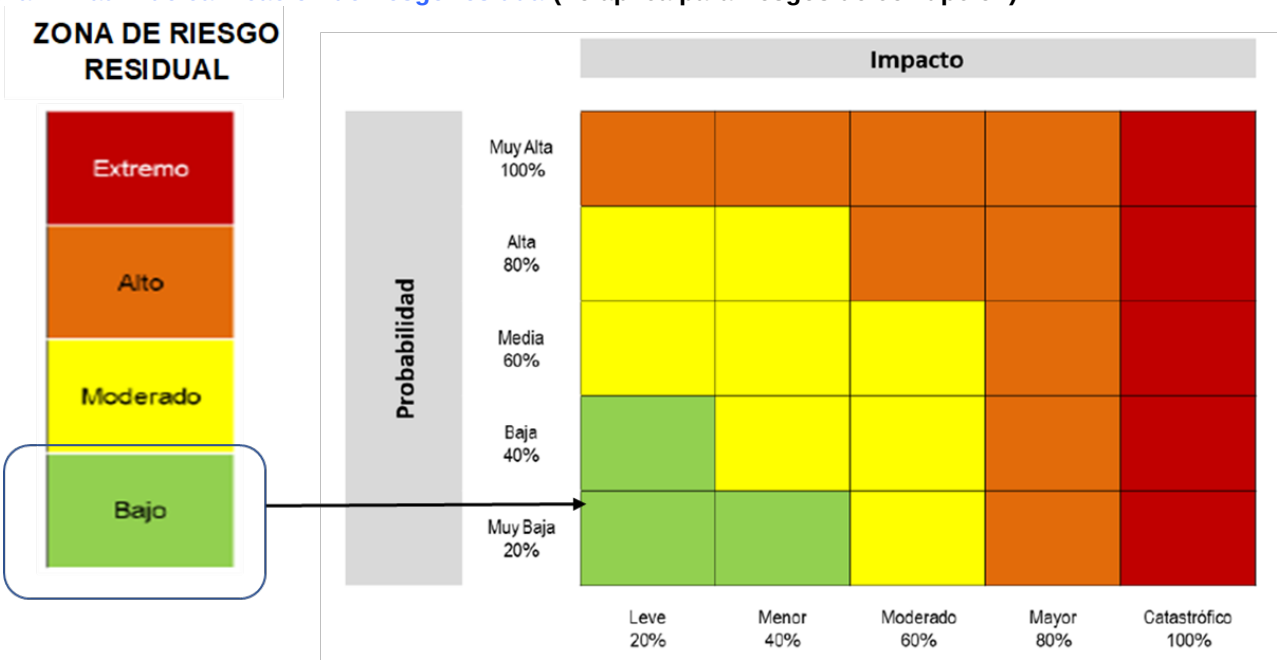
- Socializar y capacitar sobre las estrategias de mitigación o tratamiento de los riesgos.
- Capacitar en el uso del aplicativo para el manejo de los diferentes tipos de riesgos.

4.1 NIVELES DE ACEPTACIÓN DEL RIESGO

La Corporación **acepta** los riesgos identificados en la Entidad que, una vez se les hayan aplicado los controles, se encuentren en una **zona de riesgo residual baja** (ver Figura 1). Por lo tanto, para los riesgos que están ubicados en

dicha zona, no se requiere elaborar plan de acción, no obstante, sí se requiere cumplir con la implementación de los controles, así como dar cumplimiento estricto con el cronograma de seguimiento y monitoreo establecido.

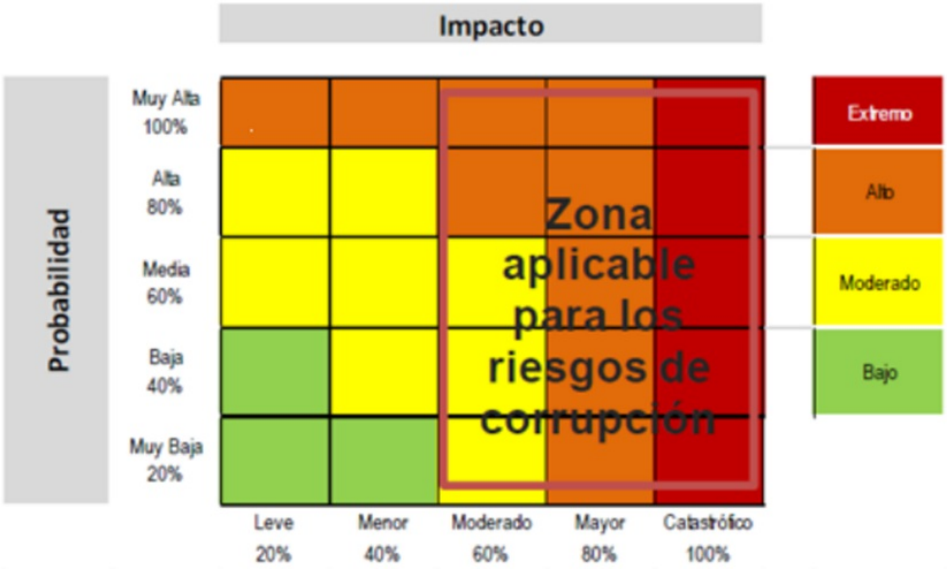
Figura 1. Matriz de calificación de riesgo residual(no aplica para riesgos de corrupción)



Fuente: Función Pública

En lo que respecta a los riesgos de corrupción, no se aceptan en ningún caso (ver Figura 2) y siempre se deben definir acciones para fortalecer el control establecido.

Figura 2. Matriz de calificación para riesgos de corrupción



Fuente: Función Pública

4.2 NIVELES PARA CALIFICAR EL IMPACTO

Los niveles para calificar el impacto se establecen en las metodologías a aplicar para cada tipo de riesgos.

4.3 NIVELES DE RESPONSABILIDAD FRENTE AL MANEJO DE RIESGOS

Las responsabilidades para la gestión de riesgos en la Corporación, se establece a través de las siguientes líneas de defensa:

Tabla 1. Responsabilidades de la línea estratégica de defensa

LINEA ESTRATÉGICA DE DEFENSA: está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno [Adaptada del manual operativo MIPG, dimensión de control interno].	
RESPONSABLES	**FUNCIONES**

LINEA ESTRATÉGICA DE DEFENSA: está conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno [Adaptada del manual operativo MIPG, dimensión de control interno].	
RESPONSABLES	**FUNCIONES**
Comité Institucional de Coordinación de Control Interno.	▪ Aprobar la política de administración del riesgo previamente estructurada por parte de la Dirección de Planeación. ▪ Revisar la política de administración del riesgo por lo menos una vez al año para su actualización, mejora y supervisar el cumplimiento de la misma. ▪ Realizar seguimiento a los riesgos en zona residual extrema, haciendo uso de la información suministrada por la 1ª línea y reportada por las instancias de 2ª linea identificadas y la 3ª linea por lo menos dos veces al año. ▪ Tomar las acciones necesarias para intervenir situaciones detectadas como incumplimientos o retrasos evitando consecuencias graves para la Corporación.

Tabla 2. Responsabilidades de la primera línea de defensa

PRIMERA LÍNEA DE DEFENSA: esta línea de defensa le corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad.[manual operativo MIPG, dimensión de control interno]	
RESPONSABLES	**FUNCIONES**
Líderes de proceso. Líderes de proyectos. Directores de las Direcciones Ambientales Regionales.	• Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo” la política y metodologías que han sido aprobadas. • Identificar, valorar y actualizar por lo menos una vez al año, los riesgos que pueden afectar los objetivos de los procesos y realizar seguimiento al mapa de riesgo de su proceso o de proyectos. • Registrar los riesgos en el aplicativo. • Realizar el seguimiento, y socialización de los riesgos a su grupo de trabajo. • Reportar en el aplicativo los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración y tratamiento del riesgo. • En caso de la materialización de un riesgo no identificado, este debe ser registrado en el aplicativo y ser incluido en el mapa de riesgos institucional. • El Director de Planeación es el responsable de elaborar y actualizar un manual en donde se describa la metodología para los riesgos de gestión, riesgos de corrupción y riesgos fiscales. • El Jefe de la Oficina Asesora Jurídica es el responsable de la identificación, valoración y tratamiento de los riesgos asociados a su gestión con enfoque en la prevención del daño anti-jurídico. • El Director Administrativo y del Talento Humano, es el responsable de liderar la Identificación, valoración y tratamiento de los riesgos de seguridad y salud en el trabajo, con el objetivo de prevenir accidentes y enfermedades laborales. • El Jefe de la Oficina de Tecnologías de la Información es el responsable de liderar la Identificación, valoración y tratamiento de los riesgos de seguridad de la Información, así como de elaborar y actualizar el manual que describe la metodología para este tipo de riesgos.

PRIMERA LÍNEA DE DEFENSA: esta línea de defensa le corresponde a los servidores en sus diferentes niveles, quienes aplican las medidas de control interno en las operaciones del día a día de la entidad.[manual operativo MIPG, dimensión de control interno]	
RESPONSABLES	**FUNCIONES**
Funcionarios y personal de apoyo en general.	• Identificar riesgos e informarlos al líder del proceso para gestionar la evaluación. • Apoyar en la identificación, valoración y tratamiento de los riesgos de acuerdo a la asignación realizada por el líder del proceso. • Conocer los riesgos relacionados a su proceso. • Participar en el diseño de los controles. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes.

Tabla 3. Responsabilidades de la segunda línea de defensa

SEGUNDA LÍNEA DE DEFENSA: esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor, quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. [manual operativo MIPG, dimensión de control interno]	
RESPONSABLES	**FUNCIONES**
Director de Planeación	• Publicar la información de los riesgos de gestión, riesgos de corrupción y riesgos fiscales de cada proceso. • Consolidar y publicar el mapa de riesgos institucional y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno, por lo menos dos veces al año. • Acompañar, orientar y entrenar a los líderes de procesos en la elaboración del análisis del contexto, necesidades y expectativas de las partes interesadas, identificación, análisis, valoración y evaluación del riesgo. • Capacitar a los grupos de trabajo de cada dependencia en el aplicativo para la gestión del riesgo. • Asesorar a la línea estratégica en la definición de la política de administración del riesgo. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados. • Realizar seguimiento al avance de la implementación de los controles y acciones reportadas a riesgos de gestión, riesgos de corrupción y riesgos fiscales. • Evaluar que la gestión de los riesgos este acorde con la presente política.
Líder del proceso Asesoría y Representación Jurídica.	• Monitorear los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico y presentar informe al Comité Institucional de Coordinación de Control Interno. • Capacitar al personal de la Corporación, con responsabilidad en trámites de contratación en la identificación de riesgos en las diferentes contrataciones.
Líder del proceso Gestión de Tecnologías de Información.	• Monitorear los riesgos de seguridad de la información en los procesos de la Corporación. • Presentar informes de seguimiento a los riesgos de seguridad de la información al Comité Institucional de Coordinación de Control Interno.

SEGUNDA LÍNEA DE DEFENSA: esta línea de defensa está conformada por servidores que ocupan cargos del nivel directivo o asesor, quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección. [manual operativo MIPG, dimensión de control interno]	
RESPONSABLES	**FUNCIONES**
Líder del proceso Gestión de Talento Humano.	• Monitorear los riesgos de seguridad y salud en el trabajo en los procesos de la Corporación. • Presentar informes de seguimiento a los riesgos de seguridad y salud en el trabajo al Comité Institucional de Coordinación de Control Interno.

Tabla 4. Responsabilidades de la tercera línea de defensa

TERCERA LÍNEA DE DEFENSA: lleva a cabo una evaluación independiente de la gestión de riesgos, de forma coordinada con la 2ª Línea de Defensa.	
RESPONSABLES	**FUNCIONES**
Jefe de la Oficina de Control Interno.	• Monitorear la exposición de la Corporación al riesgo y realizar recomendaciones con alcance preventivo. • Establecer a través de auditorias internas, la efectividad de los controles para evitar la materialización de los riesgos. • Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. • Formar a la Alta Dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. • Informar los hallazgos y proporcionar recomendaciones de forma independiente. • Adelantar seguimiento a todos los tipos de riesgos, verificando la efectividad de los controles. En cuanto a los riesgos de corrupción debe realizar tres seguimientos al año, como se indica a continuación : - Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo. - Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre. - Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero. El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. En especial deberá adelantar las siguientes actividades: - Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la Corporación. - Proponer esquemas de asesoría y acompañamiento a la entidad, en la gestión de los riesgos, actividad que debe coordinar con la Dirección de Planeación.

4.4 METODOLOGÍAS PARA LA ADMINISTRACIÓN DEL RIESGO

- ANÁLISIS DE CONTEXTO

Se debe realizar un análisis de contexto de cada proceso a partir de los siguientes factores internos y externos:

FACTORES INTERNOS DE RIESGO [6]
De estos factores se debe analizar las fortalezasy debilidades.

Procesos: capacidad, diseño, claridad en la descripción del alcance y el objetivo, ejecución, proveedores, entradas, salidas, gestión del conocimiento, falta de procedimientos, errores de grabación, autorización, errores en cálculos para pagos internos y externos, falta de capacitación, interacciones con otros procesos o relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios, o clientes, pertinencia en los procedimientos que desarrollan los procesos, efectividad en los flujos de información determinados en la interacción de los procesos.

Talento Humano: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. Se analiza posible dolo e intención frente a la corrupción, hurto activos, posibles comportamientos no éticos de los empleados y fraude interno (corrupción, soborno).

Infraestructura: eventos relacionados con la infraestructura física de la Corporación.

Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, daño de equipos, caída de aplicaciones, caída de redes y errores en programas.

Financieros: Presupuesto de funcionamiento, recursos de inversión,

Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

FACTORES EXTERNOS DE RIESGO[6]

De estos factores se debe analizar las oportunidades y amenazas.

Políticos: cambio de gobierno, legislación, políticas públicas y regulación.

Económicos: disponibilidad de capital.

Sociales: responsabilidad social y orden público.

Tecnológicos: avances en tecnología, acceso a sistemas de información externos y gobierno en línea.

Legales: normativa externa.

Ambientales: emisiones y residuos, energía, catástrofes naturales y desarrollo sostenible.

Pandemia: crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

Proveedores y contratistas: disponibilidad, competencia, suministro de información solicitada.

Ademas del análisis de estos factores se requiere tener una comprensión de las necesidades y expectativas de los grupos de valor de cada proceso, es decir, identificar las partes interesadas del proceso, cuáles son sus necesidades, expectativas y los riesgos en el relacionamiento con estas partes interesadas.

[6] Definiciones adaptadas de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, versión 6. 2022.

- IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

La metodología a aplicar para los riesgos de gestión, riesgos de corrupción, riesgos fiscales y riesgos de seguridad de la información será descrita con base en la guía para la administración del riesgo y el diseño de controles en Entidades Públicas, versión vigente, emitida por el Departamento Administrativo de Función Pública - DAFP. Para el caso de los riesgos de seguridad y salud en el trabajo se implementará lo establecido en la guía para la identificación de los peligros y la valoración de los riesgos en seguridad y salud ocupacional, GTC 45 del Icontec.

4.5 ACCIONES A IMPLEMENTAR ANTE LA MATERIALIZACIÓN DE CUALQUIER TIPO DE RIESGO EN LA CORPORACIÓN

En la siguiente Tabla se definen las acciones a implementar en caso de la materialización de un riesgo:

Tabla 5. Acciones a implementar ante la materialización de un riesgo

TIPO DE RIESGO	RESPONSABLE	ACCIÓN
Riesgos de Gestión y Riesgos Fiscales	Líderes de procesos	• Informar a la Dirección de Planeación como segunda línea de defensa, el evento o materialización de un riesgo.
	Dirección de Planeación	• Dar acompañamiento al líder del proceso para analizar la causa de la materialización y de ser necesario actualizar controles de riesgos.
Riesgos de Seguridad de la Información	Líderes de procesos	• Informar a la Oficina de Tecnologías de la Información como segunda línea de defensa, el evento o materialización de un riesgo.
	Líder proceso gestión de tecnologías de la Información	• Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar el plan de mejoramiento.
Riesgos de Gestión, Riesgos Fiscales y Riesgos de Seguridad de la Información	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho encontrado. • Informar a la segunda línea de defensa con el fin de dar acompañamiento al líder del proceso, para revisar los riesgos del proceso. • Verificar que se tomen las acciones y se actualicen los datos del riesgo en el aplicativo. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento respectivo.
Riesgos de Corrupción	Líderes de procesos	• Informar a las autoridades de la ocurrencia del hecho de corrupción. • Revisar los riesgos de corrupción, en particular, las causas, riesgos y controles. • Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción. • Llevar a cabo un monitoreo permanente.

	Oficina de Control Interno	• Determinar la efectividad de los controles. • Mejorar la valoración de los riesgos. • Mejorar los controles. • Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción. • Determinar si se adelantaron acciones de monitoreo. • Revisar las acciones del monitoreo.

4.6 MECANISMOS DE COMUNICACIÓN UTILIZADOS PARA DAR A CONOCER LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO EN TODOS LOS NIVELES DE LA CORPORACIÓN.

Los lineamientos, metodologías y responsabilidades frente a la administración del riesgo es comunicada y consultada a través de los siguientes medios:

- Correo Institucional y aplicativo.
- Actividades de capacitaciones presenciales o virtuales, de obligatoria asistencia.
- Mesas de trabajo por procesos y por tipo de riesgo.
- Informes sobre la gestión del riesgo presentados al Comité Institucional de Coordinación de Control Interno.
- Consultas en el aplicativo y Portales de la Corporación.

5. ANEXOS

No aplica.