RESOLUCIÓN No. 001109 DE 13 MAY 2019

"POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO - CRQ"

El Director General de la Corporación Autónoma Regional del Quindío - CRQ, en uso de sus facultades constitucionales y legales, en especial las conferidas por el artículo 29 de la Ley 99 de 1993, el decreto 1083 de 2015 modificado por los decretos 648 y 1499 de 2017 y en concordancia con el artículo 51 de la resolución No. 988 del 22 de julio de 2005 por la cual se aprueban los estatutos de la entidad, el acuerdo del consejo directivo 09 del 06 de agosto de 2018, y

CONSIDERANDO:

Que el artículo 209 de la Constitución Política de Colombia de 1991 establece que *"La administración pública, en todos sus órdenes, tendrá un control interno que se ejercerá en los términos que señale la ley"*, y el artículo 269 preceptúa que *"en las entidades públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno, de conformidad con lo que disponga la ley"*.

Que los literales a) y f) del artículo 2º de la ley 87 de 1993 establecieron que el diseño y desarrollo del Sistema de Control Interno se orientará, entre otros, al logro de los siguientes objetivos fundamentales: *"a. proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que lo afecten; (...) f. definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y puedan afectar el logro de sus objetivos"*

Que el Decreto 2641 de 2012 en su artículo primero señala como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento *"Estrategias para la construcción del plan anticorrupción y de atención al ciudadano"*

Que el artículo 2.2.21.3.1 Sistema institucional de control interno del decreto 1083 de 2015 sector de función pública se establece que el *"El Sistema Institucional de Control Interno estará integrado por el esquema de controles de la organización, la gestión de riesgos, la administración de la información y de los recursos y por el conjunto de planes, métodos, principios, normas, procedimientos, y mecanismos de verificación y evaluación adoptados por la entidad, dentro de las políticas trazadas por la dirección y en atención a las metas, resultados u objetivos de la entidad."*

Que el artículo 2.2.21.5.4 Administración de ri sgos, del decreto 1083 de 2015 sector de función pública establece que *"Como parte int gral del fortalecimiento de los sistemas de control interno en las entidades públicas las a toridades correspondientes establecerán y aplicarán políticas de a dministración del riesgo."*

Calle 19 norte # 19-55 B./ Mercedes del Norte
Tel. (57) (6) 746 06 00 / F x. (57) (6) 749 80 21
www.crq.gov.co / e-mc l: crq@crq.gov.co
Armenia - Quind Colombia

RESOLUCIÓN No. 001109 **DE** 13 MAY 2019

"POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO - CRQ"

Que el Decreto 648 de 2017 modificó y adicionó el Decreto 1083 de 2015, Reglamentario Único del sector de la función pública y en su artículo 17 modificó el artículo 2.2.21.5.3. De las oficinas de control interno donde estableció que "*las Unidades de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control.*"

Que el decreto 1499 de 2017 estableció en su artículo 2.2.22.3.1 actualización del modelo integrado de planeación y gestión *"Para el funcionamiento del Sistema de Gestión y su articulación con el Sistema de Control Interno, se adopta la versión actualizada del Modelo Integrado de Planeación y Gestión –MIPG.* " y que en su artículo 2.2.22.3.2 Definición del Modelo Integrado de Planeación y Gestión – MIPG, se establece que *"El Modelo Integrado de Planeación y Gestión – MIPG es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio."*

Que el Departamento Administrativo de la Función Pública expidió la *Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión corrupción y seguridad digital,* donde plantea los lineamientos para la gestión del riesgo.

Que por medio de la resolución 471 del 05 de marzo de 2019, la Corporación Autónoma Regional del Quindío – CRQ, adoptó el Modelo Integrado de Planeación y Gestión MIPG.

Que la Oficina Asesora de Planeación, con la asesoría de la Oficina Asesora de Control Interno, elaboró la política de administración del riesgo para la Corporación Autónoma Regional del Quindío en virtud de la normatividad en cita, para lo cual el Director General en uso de sus facultades legales decide presentarla para su revisión y aprobación ante el Comité Institucional de Coordinación de Control Interno.

Que el día 11 de mayo de 2019 se reunió el Comité Institucional de Coordinación de Control Interno y aprobó de manera unánime la Política de Administración del Riesgo presentada.

En virtud de lo anterior

CRQ Corporación Autónoma Regional del Quindío Protegiendo el futuro
Calle 19 norte # 19-55 B./ Mercedes del Norte
Tel. (57) (6) 746 06 00 / Fax. (57) (6) 749 80 21
www.crq.gov.co / e-mail: crq@crq.gov.co
Armenia - Quindío, Colombia
QUINDÍO VERDE, UN PLAN AMBIENTAL PARA LA PAZ

RESOLUCIÓN No. 001109 **DE** 13 MAY 2019

"POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE LA CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO - CRQ"

RESUELVE:

Artículo 1: Adoptar la Política de administración del riesgo para la Corporación Autónoma Regional del Quindío – CRQ (Ver anexo 1)

Artículo 2: Socialización. La política de administración del riesgo adoptada en la presente resolución será puesta en conocimiento de todos los servidores públicos de la Corporación Autónoma Regional del Quindío – CRQ, a través de los medios internos con que cuenta la entidad para tal fin.

Artículo 3: Vigencia y derogatoria. La presente resolución empezará a regir a partir de su fecha de aprobación y publicación y deroga las demás normas y documentos que le sean contrarias.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dado en Armenia (Quindío) a los 13 MAY 2019

JOSÉ MANUEL CORTÉS OROZCO
Director General

Elaboró:
Jhon Fredy Roncancio López/Profesional Especializado
Carlos Eduardo Mejía Salazar/Contratista/Contratista
Revisó:
César Augusto Montes Quintero/Contratista DACI.
Revisión Jurídica:
Jhoan Sebastián Palacio Gómez/Jefe Oficina Asesora Jurídica
Reviso/Aprobó:
Víctor Hugo González Giraldo /Jefe Oficina Asesora de Planeación

Calle 19 norte # 19-55 B./ Mercedes del Norte
Tel. (57) (6) 746 06 00 / Fax. (57) (6) 749 80 21
www.crq.gov.co / e-mail: crq@crq.gov.co
Armenia - Quindío Colombia

ANEXO No. 1

CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDIO

C.R.Q.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Armenia-Quindío

ANEXO No. 1

Contenido

1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Corporación Autónoma Regional del Quindío declara su compromiso con la correcta administración de los riesgos que puedan afectar el cumplimiento de la normatividad, los objetivos estratégicos de la Entidad y de los procesos internos, a través de la definición de la presente política de Administración del Riesgo como guía para identificar y valorar los riesgos y establecer los controles para su tratamiento.

Siendo así, la Corporación Autónoma Regional del Quindío diligenciará las matrices de riesgos por proceso, los cuales incluirán los riesgos de corrupción, riesgos de gestión y riesgos de seguridad digital.

La Corporación Autónoma Regional del Quindío declara que aceptará, una vez valorados, aquellos riesgos que se ubiquen en zona de riesgo inferior y bajo. Por lo tanto, no es necesario el establecimiento de controles para su tratamiento, sin embargo, el responsable de la ejecución del proceso podrá establecer controles con el objetivo de disminuir el riesgo de materialización.

No obstante, los riesgos clasificados como Riesgos de Corrupción no tienen nivel de aceptación, lo que implica que deberá establecerse controles para los riesgos ubicados en todas las zonas de riesgo.

2. OBJETIVO DE LA POLÍTICA

Establecer parámetros para una adecuada administración de los riesgos a través de los siguientes elementos:

Contexto estratégico, identificación del riesgo, análisis de riesgos, valoración de riesgos, su trazabilidad, registro y monitoreo en los procesos de la Corporación Autónoma Regional del Quindío, así como el diseño de los controles para su tratamiento.

3. ALCANCE

La administración del riesgo en la **CORPORACIÓN AUTÓNOMA REGIONAL DEL QUINDÍO** será de carácter prioritario y estratégico, fundamentada en el modelo de operación por procesos, por tal razón la identificación, análisis y valoración de los riesgos e implementación de controles se alinearán a los objetivos de los procesos, lo que permitirá la identificación del riesgo estratégico y los demás riesgos asociados a cada proceso.

4. DEFINICIONES

4.1. Actitud hacia el riesgo: enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo.

4.2. Apetito al riesgo: Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener

4.3. Causa: falla u origen de un riesgo

4.4. Control: medida tomada para la mitigación, eliminación de un riesgo.

4.5. Contexto Externo: ambiente externo el cual la empresa quiere alcanzar sus objetivos. Puede incluir el ambiente social, económica, legal, ambiental.

4.6. Contexto Interno: ambiente interno de la empresa. Puede incluir estructura orgánica, políticas, sistemas implementados, estrategias, documentación existente, entre otros.

4.7. Efecto: es una desviación de aquello que se espera, sea positivo, negativo o ambos

4.8. Evento: presencia o cambio de un conjunto particular de circunstancias.

4.9. Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

4.10. Impacto: efecto o consecuencia que puede ocasionar a la organización del riesgo.

4.11. Matriz de riesgos: herramienta implementada que contiene la información resultante de la gestión del riesgo.

4.12. Probabilidad: posibilidad que un evento se materialice.

4.13. Propietario del riesgo: persona con la responsabilidad de rendir cuentas y la capacidad de ejercer control para gestionar un riesgo.

4.14. Riesgo: efecto de la incertidumbre sobre los objetivos

4.15. Riesgo inherente: es la evaluación preliminar del riesgo con la cual la organización quiere conocer el nivel de exposición al mismo, sin tener en cuenta las medidas de mitigación o los controles.

4.16. Riesgo residual: riesgo que subsiste, después de haber implementado controles.

4.17. Tolerancia del riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Para el riesgo de corrupción la tolerancia es inaceptable.

4.18. Riesgo Estratégico: se define como el impacto actual y futuro en los ingresos y el capital que podría surgir de las decisiones adversas de la Corporación, la aplicación indebida de las decisiones, o la falta de capacidad de respuesta a los cambios del contexto.

5. NORMATIVIDAD

5.1. LEY 1474 DE 2011 *"por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública."*

5.2. ISO 31000 Gestión del riesgo. Principios y directrices

5.3. Decreto 648 de 2017: por el cual se modifica y adiciona el decreto 1083 de 2015, Reglamento único del sector de la función pública.

5.4. Decreto 1499 de 2017 "*Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*"

5.5. Guía para la administración del riesgo y diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital Versión 4 del Departamento Administrativo de Función Pública.

6. RESPONSABILIDAD

Líneas de defensa	**Responsable**	**Responsabilidad frente al riesgo**
Estratégica	Director General y Comité Institucional de Coordinación de Control Interno	*Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento. *Establecer y aprobar la política general de la administración del riesgo, la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención de riesgos de corrupción, seguridad digital y de gestión. *Definir los niveles de aceptación de riesgo de la Entidad. *Hacer seguimiento a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas. *Analizar los cambios en los contextos internos y externos que puedan tener un impacto en la Entidad y en la administración de los riesgos. *Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.
Primera línea de defensa	Responsables de ejecución del proceso	*Identificar y valorar los riesgos que puedan afectar los objetivos de sus procesos. *Establecer y hacer seguimiento a los controles para mitigar los riesgos identificados. *Informar a la segunda línea de defensa sobre la materialización de los riesgos. *Supervisar la ejecución de los controles propuestos, determinar las deficiencias y establecer las acciones de mejoramiento correspondientes. *Realizar ejercicios de autoevaluación para establecer la eficacia y efectividad de los controles

Segunda línea de defensa	Jefe Oficina Asesora de Planeación	*Asesorar a la línea estratégica en el análisis del contexto interno y externo, establecimiento de la política del riesgo, aceptación de niveles de aceptación del riesgo *Consolidar el mapa de riesgos, y presentarlo ante el Comité Institucional de Coordinación de Control Interno para su análisis. *Acompañar a los responsables de actividades y procesos en la identificación, valoración de riesgos y establecimiento de controles. *Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno. *Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia. *Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los responsables de ejecución del proceso. *Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos, se encuentren documentadas y actualizadas en los procedimientos *Presentar informe de seguimiento a la eficacia y efectividad de los controles en los diferentes procesos de la entidad al Comité institucional de Coordinación de Control Interno. *Promover ejercicios de autoevaluación para establecer la eficacia y efectividad de los controles.
	Supervisores e interventores de contratos o proyectos	Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Reportar a la Oficina de Planeación el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejoramiento correspondiente. Supervisar que la primera línea de defensa identifique, evalué y gestione los riesgos en los temas de su competencia e implementar los controles correspondientes.
Tercera línea de defensa	Oficina asesora de control interno	*Verificar la eficacia de la gestión del riesgo y control, con énfasis en la idoneidad de los controles establecidos y generar recomendaciones. *Asesorar a la línea estratégica en el establecimiento de la política de administración del riesgo y modificaciones

		*Asesorar a la primera y segunda línea de defensa en la identificación, valoración de riesgos y establecimiento de los controles. *Realizar seguimiento a los riesgos establecidos en las matrices de riesgos. *Recomendar mejoras en la metodología para la administración de los riesgos de la Entidad, así como en la herramienta de matriz de riesgos y la política general de la administración del riesgo. * Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se puedan actualizar las matrices de riesgos por parte de los responsables. * Revisar que se hayan identificado los riesgos significativos que afectan el cumplimiento de los objetivos de los procesos incluyendo riesgos de corrupción. * Revisar el perfil del riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil del riesgo de la entidad o que su calificación de impacto y probabilidad del riesgo no es coherente con el resultado de las auditorias. * Hacer seguimiento a que las actividades de control establecidos para la mitigación de los riesgos se encuentren documentados y se realicen de manera oportuna.

NOTA: La entidad designará como mínimo a un funcionario de planta que hará las veces de gestor del riesgo, que conozca acerca de la gestión del riesgo y de la entidad. En caso de no contar con conocimiento sobre riesgos, la Oficina Asesora de Planeación y la Oficina Asesora de Control Interno capacitarán al personal delegado.

7. ANÁLISIS DEL CONTEXTO

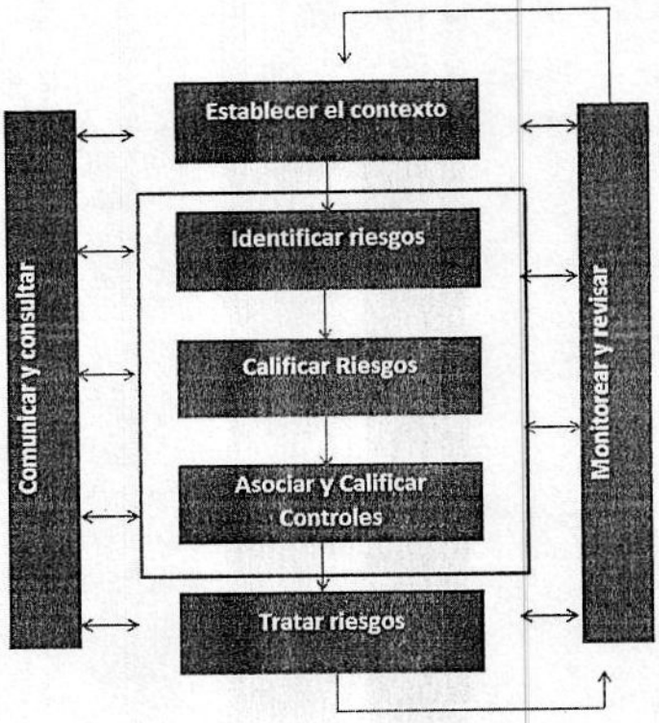
La alta dirección definirá la metodología para realizar el análisis del contexto externo e interno, una de las metodologías recomendadas es la matriz DOFA. Una vez se obtengan los resultados, la alta dirección debe socializar los resultados a los funcionarios de la corporación.

Debilidades		**Oportunidades**
Fortalezas		**Amenazas**

8. CONDICIONES Y DIRECTRICES

Con el fin de dar cumplimiento a la normatividad aplicable a la Corporación referente a la gestión de los riesgos y con el propósito de prevenir o evitar la materialización de eventos que puedan afectar el normal desarrollo de los procesos y el cumplimiento de los objetivos estratégicos, la Corporación Autónoma Regional del Quindío establece la presente política, basado en la guía para la administración del riesgo y diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo de la Función Pública y la norma internacional ISO 31000, para que sea utilizado como orientación para la correcta implementación de la administración del riesgo en la Entidad.

8.1. La Metodología para la Gestión del riesgo adoptada por la Corporación Autónoma Regional del Quindío comprende:



8.2. El responsable de ejecución de cada proceso será el responsable de reportar la información en la herramienta establecida para el control de los riesgos: matriz de riesgos. Se realizará una revisión semestral por parte de la oficina de control interno y se presentará informe de la gestión del riesgo del periodo a la Dirección General y al jefe de la oficina asesora de planeación, para que este último realice un análisis de la información, y una revisión, por lo menos, cada 4 meses por parte de cada uno de los responsables de ejecución de los procesos internos de la entidad, elaborando informe dirigido al jefe de la oficina asesora de planeación.

8.3 Uso de la herramienta de gestión del riesgo: Matriz de riesgo:

La corporación definió una matriz para la gestión del riesgo, la cual permite priorizar los riesgos, identificar controles y elaborar los mapas de calor, lo que permite consolidar la información para ser presentada a la alta dirección y al comité de coordinación de control interno.
La herramienta de matriz de riesgos debe ser diligenciada de izquierda a derecha, siguiendo sus ítems para la identificación, valoración y gestión del riesgo.

9. CÓDIGO DEL RIESGO

Código único otorgado a un riesgo. La estructura del código deberá ser R YY 00, siendo:

YY: código del proceso. A continuación, se presentan los procesos y códigos correspondientes determinados por la Entidad:

CODIGOS POR PROCESO Y ACTIVIDAD		
PROCESO	ACTIVIDAD	CODIGO
Direccionamiento Estratégico	Planificación Institucional	D-PI
	Actualización o ajuste del Plan de Gestión Ambiental Regional, PGAR	D-PG
	Actualización o ajuste del Plan de Ordenación y Manejo de la Cuenca del Río La Vieja	D-RV
	Asesoría y acompañamiento en la planificación ambiental departamental y municipal	D-PD
	Planeación ambiental regional	D-PL
	Coordinación de planes ambientales	D-CP
	Asesoría procesos de licencias y permisos ambientales	D-AL
	Información y administración tecnológica	D-AT
	Administrar el Sistema Integrado de Gestión de Calidad	D-GC
Ejecución de Políticas Ambientales	Gestión Integral del Recurso Hídrico	P-GH
	Gestión Integral de la Biodiversidad y sus servicios Ecosistémicos	P-GB

	Gestión Ambiental Productiva	P-GA
	Gestión Integral de Residuos Sólidos	P-GS
	Gestión de Riesgos y Cambio Climático	P-GR
	Educación Ambiental y Participación Comunitaria	P-EA
Control y Seguimiento Ambiental	Regulación Ambiental	C-RA
	Control y Seguimiento	C-CS
	Monitoreo y Conocimiento Ambiental	C-MC
	Instrumentos económicos	C-IE
Servicio al Cliente	Comunicación con el Cliente	S-CC
	Administración Documental y Bibliográfica	S-DB
Gestión Operativa y del Talento Humano	Administración de Personal	O-AP
	Administración de Recursos Físicos y materiales	O-RF
Financiero	Gestión Presupuestal	F-GP
	Gestión Contable	F-GC
	Gestión de Tesorería	F-GT
	Gestión de Ingresos	F-GI
Jurídico	Representación Judicial	J-RJ
	Contratación Estatal	J-CE
	Cobro Coactivo	J-CC
	Secretaria Asamblea Corporativa y del Consejo Directivo	J-SA
	Participación Activa en la Conformación de Comités y Grupos	J-PC
	Conceptos jurídicos y revisión jurídica de actos administrativos	J-CJ
Laboratorio de Aguas	Gestión Administrativa	L-GA
	Operativas de Carácter Técnico	L-OT
	Auditorías de Calidad	E-AC

Evaluación y Control de la Gestión	Seguimiento y Verificación de Informes	E-SC
Comunicaciones	Comunicación Corporativa	CO-CC
	Comunicación interna	CO-CI
	comunicación externa	CO-CE
	comunicación digital	CO-CD
Sancionatorio Ambiental	Sancionatorio Ambiental	SA-SA
Disciplinario	Disciplinario Interno	DI-DI

- **00:** número consecutivo del riesgo.

Ejemplo: primer riesgo operativo del proceso Direccionamiento Estratégico; código: R-D-PI-01. (R: Riesgo-D: Direccionamiento-PI (Planeación Institucional)-01 (Consecutivo).

El funcionario que asigna el código es el responsable de ejecución del proceso.

9.1. Identificación y descripción del riesgo

Para efectuar la identificación de los riesgos, se deberá realizar primero el estudio del contexto, externo e interno, del proceso. En cuanto al contexto macro, se tendrá en cuenta los resultados de acuerdo a la metodología definida por la alta dirección según el numeral 7 del presente documento, por su parte, el contexto interno se soportará según las características de cada proceso, cuya principal herramienta será la caracterización de los procesos internos y la matriz DOFA. A partir del estudio de los parámetros de los contextos, se podrán establecer causas de los riesgos a identificar.

Fuente: *Guía para la administración del riesgo y diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital Versión 4*

Una vez realizado el estudio del contexto del proceso, se procederá a la identificación de los riesgos respondiendo las siguientes preguntas:

¿Qué puede suceder?

¿Cómo puede suceder?

¿Cuándo puede suceder?

Finalmente, la redacción del riesgo identificado debe permitir al lector comprender con facilidad cómo se vería afectada la empresa en caso de su materialización y debe ir enfocado a la amenaza que supone para el objetivo de su proceso.

9.3. Descripción de las causas

Con base en el análisis de contexto interno y externo expuesto según el numeral 9.2, se identificarán las causas de los riesgos redactados en la matriz de riesgos del proceso. Para cada riesgo se podrán registrar hasta cinco (5) razones o eventos principales que originan el riesgo descrito con anterioridad.

En caso de identificar más causas a un riesgo, se deberán priorizar cinco (5), esto debido a que tratar más de 5 causas a través de controles puede derivar en burocratizar procedimientos o implementación de puntos de control innecesarios. Se recomienda usar la metodología de análisis de causa que se encuentra en el formato plan de mejoramiento FO-D-GC-03.

9.4. Descripción de las consecuencias

Para identificar las consecuencias de los riesgos debe responderse a la pregunta ¿Qué consecuencias tendría su materialización? Se podrá incluir en la matriz de riesgos hasta cinco (5) consecuencias identificadas.

9.5. Probabilidad

Lista de valores con los cuales se califica la probabilidad de ocurrencia del evento de riesgo con base en una escala determinada de la siguiente manera:

Escala cualitativa	Escala cuantitativa	Color asignado
Inferior	1	
Baja	2	
Media	3	
Alta	4	
Muy Alta	5	

Los criterios utilizados para calificar la probabilidad de ocurrencia son subjetivos, en cuanto dependen de la experiencia y pericia de quien (es) identifica (n) y/o conoce (n) el riesgo; sin embargo, se podrá tener en cuenta la tabla de probabilidad de ocurrencia que se muestra a continuación para su calificación:

TABLA PROBABILIDAD DE OCURRENCIA	
INFERIOR	El evento no se ha presentado en los últimos cinco (5) años en la entidad o en otras entidades.
BAJA	El evento se ha presentado por lo menos una vez en la entidad o en otras entidades en los últimos cinco (5) años
MEDIA	El evento se presentó por lo menos una vez en los últimos dos (2) años. o en otras entidades.
ALTA	El evento se presentó una vez en el último año. o en otras entidades.
MUY ALTA	El evento se presentó más de una vez en el último año. o en otras entidades.

Nota (1): Los valores anteriores son mutuamente excluyentes.

9.6. Impacto

Corresponde a una lista de valores con los cuales se califica el nivel de impacto del evento de riesgo en caso de materializarse, con base en una escala determinada de la siguiente manera:

Escala cualitativa	Escala cuantitativa	Color Asignado
Insignificante	1	
Tolerable	2	
Moderado	3	
Alto	4	
Crítico	5	

Nota: Los valores anteriores son mutuamente excluyentes.

Los criterios utilizados para calificar el impacto dependen de la experiencia y pericia de quien (es) identifica (ı) y/o conoce (n) el riesgo; sin embargo, se podrá tener en cuenta la tabla de impacto que se muestra a continuación para su calificación:

Los criterios utilizados para calificar el impacto son los siguientes:

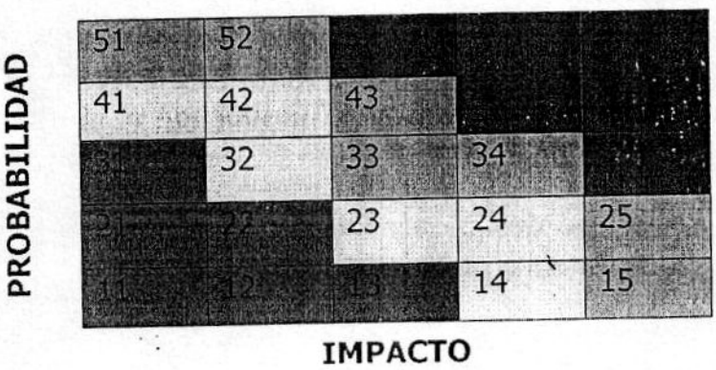
Variables / Nivel Criticidad	Impacto Financiero Pérdida de utilidades operativas (%)	Impacto Económico Pérdida económica por retrasos en la entrega de servicios	Impacto Operacional Suspensión o detención de procesos y/o actividades vitales	Impacto en la imagen Costos de Recuperación de imagen	Impacto legal Incumplimiento obligaciones legales	Impacto en la Confidencialidad Fuga de información/ seguridad de información	Impacto en seguridad y salud Peligro en las personas
[illegible]	mayor a 3%	Pérdida superior al 50% de los clientes o usuarios. Las pérdidas económicas no se recuperan	Produce la interrupción inmediata de operaciones criticas	Pérdida de la confianza y daños a la imagen de la corporación Campaña continuada en los medios nacionales	Se generan multas o sanciones que pueden ocasionar alguno de las siguientes situaciones: pérdidas financieras, intervención por parte de entes de control, destitución del representante legal. El impacto tiene una gran extensión, afectando varios componentes de las obligaciones legales o a varios grupos de interes (proveedores, ususarios, visitantes comunidad, colaboradores, consejo directivo, comité direccion, entes de control, contratistas, entre otros). La alteración generada sobre un componente o grupo(s) de interes es irrecuperable	Divulgación de información de tipo confidencial en redes públicas	Seguridad. Muerte de una persona o incapacidad permanente, pérdida de un órgano o alguna parte del cuerpo
Alto	de 2 a 2,9%	Pérdida del 20 al 50% de los clientes o usuarios. Las pérdidas económicas no se recuperan	Produce retrasos graves en operaciones criticas	Pérdida de confianza en los trámites y servicios o en varios procesos de la organización. Comentarios adversos en los medios nacionales.	La situación/evento produce una sanción económica (de cobertura legal) de mayor cuantía. La incidencia es alta en (por lo menos) un componente de las obligaciones legales o a un grupo de interes El impacto tiene efecto fuera de los límites de la sede, sin afectar infraestructura comunitaria. La alteración generada sobre un componente o sobre los grupos de interes es mitigable o compensable en el largo plazo.	Divulgación de la información confidencial a partes externas no previamente autorizadas	Lesión o enfermedad sin incapacidad permanente, requiere atención medica
Moderado	de 1 a 1,9%	Pérdida inferior al 20% de los clientes o usuarios. Las pérdidas económicas no se recuperan	Produce retrasos leves en operaciones criticas	Pérdida de confianza en un tramite o servicio especifico o en una parte de la organización. Comentarios adversos en medios locales.	La situación/evento produce una sanción económica de menor cuantía. La incidencia es media en (por lo menos) un componente de las obligaciones legales o a un grupo de interes El impacto se manifiesta en un espacio reducido dentro de los limites de la sede, sin exceder los limites del área, sin embargo hay ó puede haber afectacion a alguna parte interesada o grupo de interes La alteración generada es recuperable en el mediano plazo.	Divulgación de la información de tipo confidencial al interior de la organizacion hacia colaboradores no autorizados	Lesión o sintomatologia leve, con reacción alérgica, sin incapacidad
Tolerable	de 0,6% a 0,9% No calculado	Produce una interrupción leve en el suministro de servicios con leve impacto en la operación. La pérdida económica se recupera parcialmente al reanudar la actividad	Produce retrasos en operaciones NO criticas No produce retrasos en operaciones o actividades vitales	Conocido solamente por algunos clientes. Aun no conocido por los clientes No conocimiento por parte de medios locales	La situación/evento produce una amonestación o podria generarla La incidencia es baja en (por lo menos) un componente de las obligaciones legales o a un grupo de interes El impacto se manifiesta en un espacio reducido dentro de los limites de la sede, sin exceder los limites del área, sin embargo hay ó puede haber contacto directo con algún recurso natural y/ó alcanza a ser percibido por la comunidad. La recuperación del recurso se puede hacer en el corto plazo	Divulgación no autorizada de la información no confidencial y no pública al interior de la organización Manejo no adecuado de informacion que pone en riesgo las politicas de seguridad	Incumplimiento requisitos seguridad, salud , sin lesiones a las personas Deteccion incumplimiento puntos criticos de control sin lesiones a personas
INSIGNIFICANTE	DE 0,1% a 0,599%	Produce una interrupción mínima en el suministro de servicios sin impacto en la operación. La pérdida económica no se ve impactada	Produce retrasos mínimos que no impactan la operación	Afectación mínima en la imagen, poca difusión del impacto en medios	Se generan incumplimientos normativos que no impiden el normal desarrollo de la operación y funcionamiento de la entidad	Fugas de infromacion no confidencial sin afectacion a la operación	Incumplimiento a un requisito normativo de bajo impacto

9.7. Riesgo inherente

El riesgo inherente es calculado teniendo en cuenta la probabilidad de ocurrencia e impacto anteriormente determinado; la escala establecida para el riesgo, tanto inherente como residual, se muestra a continuación:

Escala cualitativa	Escala cuantitativa	Color asignado
Inferior	Entre 0 y 1.99	
Bajo	Entre 2 y 2.99	
Medio	Entre 3 y 3.99	
Alto	Entre 4 y 5	

El riesgo inherente determina el nivel de riesgo asociado al evento por el cual se puede materializar el riesgo. El cálculo se realiza al combinar los valores de la escala cuantitativa de la probabilidad y el impacto del riesgo como se muestra a continuación:



9.8. Tipo del riesgo

Tipo de riesgo	**Descripción**
Riesgo estratégico	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos.
Riesgo Gerencial	Posibilidad de ocurrencia de eventos que afecte los procesos gerenciales y/o a la alta dirección.

Riesgo operacional	Aquel que puede provocar pérdidas debido a errores humanos, procesos internos inadecuados o defectuosos, fallas en sistemas.
Riesgo legal	Posibilidad de ocurrencia de eventos que afecten al cumplimiento normativo y legal por parte de la entidad.
Riesgo imagen	Es la perdida de la confianza por parte de la ciudadanía hacia la institución.
Riesgo de defensa jurídica	Pérdidas debido a transacciones no documentadas, reclamos o acciones legales, protección legal defectuosa de los derechos o activos, desconocimiento normativo y/o cambios en la ley.
Riesgo de contratación	Posibilidad de que la entidad pueda sufrir afectación como consecuencia de una acción de contratación ejecutada.
Riesgo tecnológico	Posibilidad de ocurrencia de fallas o vulneraciones a la capacidad tecnológica disponible.
Riesgo Seguridad digital	Eventos que generen amenaza a la Entidad como consecuencia de fallas en la seguridad digital establecida en la Entidad.
Riesgo de corrupción	Se generan por realización de actividades ilegitimas e ilegales que buscan beneficios personales y que afectan la transparencia de la institución. El riesgo de corrupción no tiene nivel de aceptación del riesgo. Para conocer si un riesgo es de corrupción, deberá responderse las siguientes preguntas: ¿Es causado por acción u omisión?, ¿Es derivado del abuso del poder?, ¿Busca desviar la gestión de lo público?, ¿Busca el beneficio privado?
Riesgo ambiental	Posibilidad de que por forma natural o por acción humana se produzca daño en el medio ambiente
Riesgo financiero	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad.

10. CONTROLES:

10.1. Descripción del control: propósito + ejecución + acciones de desviación

Espacio para describir el control que se establecerá para mitigar, eliminar o transferir el riesgo en mención; se podrán establecer hasta cinco (5) controles para cada riesgo.

El control deberá tener un propósito que indique la razón por la cual se ejecuta y cómo conlleva a la mitigación de cada una de las causas identificadas con anterioridad.

Ejecución: deberá establecer claramente cómo se ejecuta correctamente, qué información necesita o herramientas.

Desviaciones: deberá establecer en caso de no contar con la información requerida o herramientas, qué acciones deben realizarse. Ejemplo: *en caso de no contar con la información, el responsable deberá dejar constancia a través de correo electrónico, indicando la información faltante.*

10.2. Propósito del control

Es una lista de valores que permite seleccionar si el propósito del control es:

- Prevenir: acciones orientadas a prevenir que el riesgo se materialice.
- Detectar: acciones orientadas a detectar cuando ya se ha materializado un riesgo y en búsqueda de evitar que el riesgo tenga un impacto mayor en la organización.
- No es un control: No cumple con las condiciones para ser considerado un control.

10.3. Desviaciones:

En caso de encontrar desviaciones, seleccionar si estas se investigan y resuelven por el responsable.

10.4. Frecuencia de aplicación del control

Lista que permite registrar la frecuencia de implantación del control correspondiente:

. Permanente: es un control implementado para que siempre esté presente en la operación.
a. Periódica: el control se realiza cada cierto período de tiempo; puede ser diario, semanal, semestral...
a. Ocasional: control que se ejecuta esporádicamente, ya sea por su naturaleza (Auditorías...) o por decisión del responsable del proceso.

10.5. Evidencia del control

Establecer si el control posee evidencia de su ejecución (Completa o Incompleta).

10.6. Responsable

Persona responsable de la ejecución del control correspondiente.

Estado: Evalúa automáticamente el estado del control antes de su calificación por parte del propietario del riesgo; se tienen en cuenta los ítems propósito de control, Frecuencia, Evidencia. La escala de calificación se muestra a continuación:

Escala cualitativa
Muy Débil
Débil
Aceptable
Fuerte
Muy Fuerte

10.7. Confiabilidad de control

Es la valoración que da el propietario del riesgo a cada control o auditor designado, teniendo en cuenta la efectividad que ha tenido hasta el momento su implantación o la efectividad que espera tenga el control; la calificación del control depende de la experiencia y pericia del personal calificador. Puede ser modificado por autoevaluación, autogestión o auditorías.

10.8. Solidez grupal

Es la mediana de la valoración de cada uno de los controles, y el cual demuestra la solidez de los controles establecidos para la administración del riesgo.

11 RIESGO RESIDUAL

Calcula automáticamente el riesgo que subsiste después de la aplicación de los controles al riesgo inherente. Su escala de valoración es igual al Riesgo inherente.

12. INDICADOR

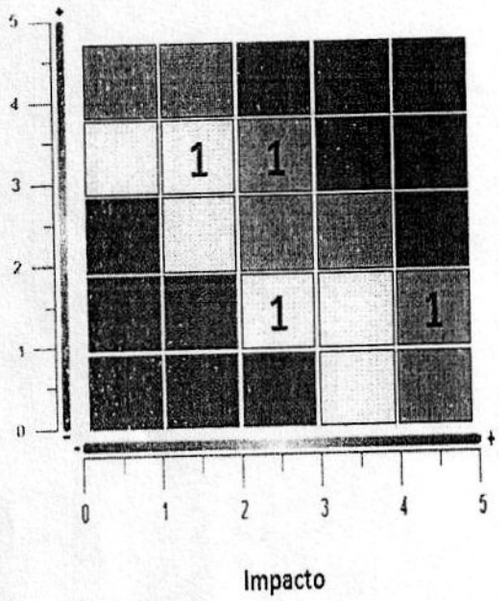
Es el valor que indica la materialización del riesgo en un periodo de tiempo determinado.

13. MAPA DE CALOR DE LOS RIESGOS: RIESGO INHERENTE Y RIESGO RESIDUAL

Es una gráfica que permite observar la cantidad y ubicación de los riesgos inherentes y riesgos residuales de cada proceso evaluado. Las matrices son 5 x 5 y grafican la probabilidad vs el impacto y segmenta la información por colores, según lo establecido en el numeral 5.5.7 Riesgo Inherente:

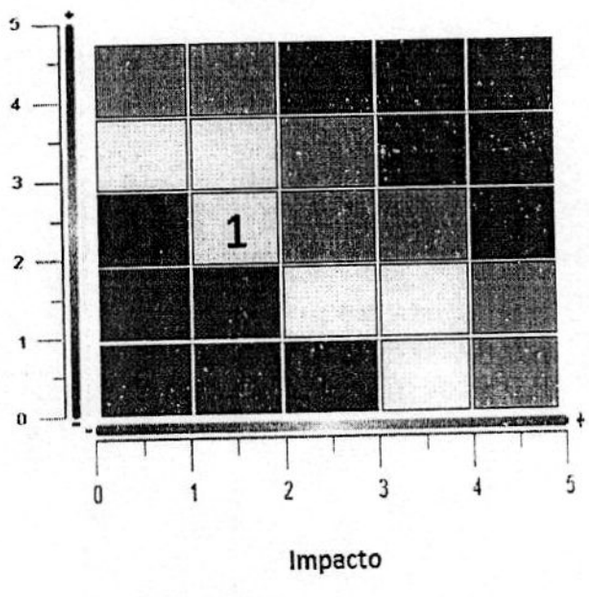
Escala cualitativa	Color asignado
Inferior	
Bajo	
Medio	
Alto	

Riesgo Inherente



Frecuencia

Riesgo Residual



Riesgo Inherente	Riesgo residual
En el gráfico anterior se evidencian siete (7) riesgos, antes de aplicar los controles, ubicados de la siguiente manera: Alto: 3 Medio: 2 Bajo: 2	En el gráfico se evidencia que una vez se aplican los controles los riesgos quedaron distribuidos de la siguiente manera: Bajo: 1 Inferior: 6

14. DOCUMENTOS Y FORMATOS

Herramienta matriz de riesgos

Formato plan de mejoramiento FO-D-GC-03

15. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de Cambios
1	01/04/2019	Formalización del documento y Ajuste a la metodología del DAFP, versión 4 de octubre de 2018.

Elaboró:	Revisó:	Aprobó:
Jhon Fredy Roncancio López	Víctor H. González Jefe Oficina Asesora de Planeación.	Comité Institucional de Coordinación de Control Interno