Corporación Autónoma
Regional del Valle del Cauca

RESOLUCIÓN 0100 No. 0500- 0700 DE 2021
(04 OCT. 2021)

"POR MEDIO DE LA CUAL SE ACTUALIZA LA POLITICA DE ADMINISTRACIÓN DEL RIESGO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA-CVC"

El Director General de la Corporación Autónoma Regional del Valle del Cauca-CVC, en uso de sus facultades legales y estatutarias contenidas en la Ley 99 del 1993 y en el acuerdo AC No.003 de 26 de marzo de 2010, respectivamente, y

CONSIDERANDO:

Que la política de Administración del Riesgo de la CVC, se encuentra en concordancia con el Modelo Integrado de Planeación y Gestión -MIPG (Decreto 1499 de 2017) y el modelo Estándar de Control Interno, titulo 21, Capítulo 6 del Decreto Único Reglamentario del Sector de Función Pública-Decreto 1083 de 2015; teniendo como lineamientos, la Guía para la Administración del Riesgo del Departamento Administrativo de la Función Pública- DAFP V5 y el Decreto 124 de *2016 "Por el cual se sustituye el Titulo 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano"*, como mecanismo para identificar, medir valorar, monitorear, administrar y tratar los riesgos que puedan afectar de manera positiva o negativa el logro de los objetivos de la Corporación.

Que por medio de la Resolución 0100 No. 0340-0830 de fecha 25 de noviembre de 2008, se adoptó la Política de Administración del Riesgo de la Corporación Autónoma Regional del Valle del Cauca, la cual fue ajustada por la Resolución 0100 No. 0100-293 del 27 de abril de 2018.

Que el Departamento Administrativo de la Función Publica-DAFP, en octubre de 2018, publicó la versión 4 de la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Publicas.

Que por medio de la Resolución 100 No. 0100-0437 de fecha 11 de junio de 2019, se actualizó la Política de Administración del Riesgo de la Corporación Autónoma Regional del Valle del Cauca.

Que el Departamento Administrativo de la Función Pública en diciembre del 2020, actualizó y publicó la versión 5 de la Guía, denominada "*Guía para la administración del riesgo y el diseño de controles en entidades públicas*", conminando a realizar la actualización de las políticas de las entidades. Para el caso de la CVC, esto implicó cambios en el objetivo general, objetivos específicos, su alcance, modificaciones en términos y definiciones en la metodología; se amplía el alcance de la seguridad digital a la seguridad de la información, así como también la articulación de la institucionalidad de MIPG con la gestión del riesgo.

RESOLUCIÓN 0100 No. 0500- DE 2021
( )

"POR MEDIO DE LA CUAL SE ACTUALIZA LA POLITICA DE ADMINISTRACIÓN DEL RIESGO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA-CVC"

Que este ajuste hace parte de las metas establecidas en el Plan Anticorrupción y de la Atención al Ciudadano de la CVC, vigencia 2021, en el Subcomponente 1 - Política de Administración de Riesgos del componente 1 Gestión del riesgo de corrupción - mapa de riesgos de corrupción.

Que para la actualización de la Política se adelantaron reuniones técnicas con los profesionales de la Dirección de Planeación - Grupo de Gestión Ambiental y Calidad, de las cuales se encuentra registro en actas de comité de trabajo de fechas 8 de junio, 28 de junio, 20 de agosto del año 2021 y que hacen parte integral de la presente resolución y evidencian la revisión de la actualización de la Guía de riesgos formulados por DAFP frente a la versión que se encontraba vigente, identificando la necesidad de actualizar la Política de Administración de Riesgos de la Corporación.

Que, como resultado del ejercicio mencionado en el anterior considerando, la Dirección de Planeación, elaboró el documento de actualización de la "POLITICA DE ADMINISTRACION DEL RIESGO CVC", el cual habrá de adoptarse mediante la presente providencia.

Que el comité Institucional de Coordinación de Control Interno, en sesión del 6 de septiembre de 2021, aprobó por unanimidad la actualización de la Política de Administración del Riesgo de la Corporación.

Que de conformidad con el ordinal 5 del artículo 51 del Acuerdo AC No. 03 de 2010 por el cual se adoptaron los Estatutos Corporativos de la CVC, en concordancia con el ordinal 5 del articulo 29 de la ley 99 de 1993, es función del Director General, dictar los actos que se requieran para el normal funcionamiento y logro de los objetivos de la entidad.

En mérito de lo expuesto, el Director General de la Corporación Autónoma Regional del Valle del Cauca,

RESUELVE:

ARTICULO PRIMERO: Actualizar la Política de Administración del Riesgo de la Corporación Autónoma Regional del Valle del Cauca-CVC-, contenida en el

Corporación Autónoma
Regional del Valle del Cauca

RESOLUCIÓN 0100 No. 0500- 0700 DE 2021
( )

"POR MEDIO DE LA CUAL SE ACTUALIZA LA POLITICA DE ADMINISTRACIÓN DEL RIESGO PARA LA CORPORACIÓN AUTÓNOMA REGIONAL DEL VALLE DEL CAUCA-CVC"

Documento "POLITICA DE ADMINISTRACION DEL RIESGO CVC 2021", el cual hace parte integral de la presente Resolución

ARTICULO SEGUNDO: El presente acto administrativo deberá publicarse en el Diario Oficial y en la pagina web Corporativa.

ARTICULO TERCERO: La presente providencia rige a partir de su expedición y deroga expresamente la Resolución 100 No. 0100-437 de 11 de junio del 2019.

DADA EN SANTIAGO DE CALI, A LOS 04 OCT. 2021

PUBLÍQUESE Y CÚMPLASE

MARCO ANTONIO SUÁREZ GUTIÉRREZ
Director General

Proyectó/Elaboró: Juan Sebastián Rodríguez Acevedo – Abogado Contratista,Grupo Jurídico Ambiental, oficina Asesora Juridica
Reviso: Piedad Vargas Peña– Profesional Especializada Coordinadora Grupo Jurídico Ambiental, Oficina Asesora Jurídica
Jairo España Mosquera – Jefe Oficina Asesora Jurídica (C.)
Carolina Zúñiga Salguero – Coordinadora del Grupo de Gestión Ambiental y Calidad
Álvaro Hernán Roldan Álvarez- Director de Planeación (C.)
Oscar Marino Gómez García – Asesor Dirección General

CORPORACIÓN AUTÓNOMA REGIONAL
DEL VALLE DEL CAUCA

Corporación Autónoma
Regional del Valle del Cauca

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Santiago de Cali, septiembre de 2021

TABLA DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

1. INTRODUCCIÓN

El presente documento establece la política de administración del riesgo para la Corporación Autónoma Regional del Valle del Cauca – CVC, y contiene los lineamientos para la administración de los riesgos de gestión, corrupción y seguridad de la información , tomando como referencia las directrices indicadas en la *Guía para la administración de riesgos y el diseño de controles en entidades públicas*, el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (Anexo 4) emitidos por el Departamento Administrativo de la Función Pública y las pautas emitidas por el Ministerio de Tecnologías de la Información y Comunicaciones – MinTic

Teniendo como referente para la Corporación el Modelo Integrado de Planeación y Gestión - MIPG y buscando cumplir con la articulación del sistema de gestión con el Sistema de Control Interno, es importante resaltar que la administración de riesgos sienta sus bases en la dimensión 7 denominada 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 dimensión, se cumple el objetivo de MIPG "Desarrollar una cultura organizacional fundamentada en la información, el control y la evaluación, para la toma de decisiones y la mejora continua".[1]

[1] Marco General del Modelo Integrado de Planeación y Gestión. Departamento Administrativo de la Función pública DAFP. Versión 4. 2021

Corporación Autónoma
Regional del Valle del Cauca

2. POLITICA 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 identificación, valoración, tratamiento, monitoreo y seguimiento de los riesgos de gestión, corrupción y seguridad digital, que afectan el cumplimiento de la misión y de los objetivos estratégicos de la Corporación, ejerciendo un control efectivo para evitar o reducir la probabilidad de materialización de los mismos.
- Socializar las estrategias de mitigación o tratamiento de los riesgos.
- Establecer los mecanismos para dar a conocer la política de administración de riesgos en todos los niveles de la Corporación.

3. OBJETIVO

3.1 OBJETIVO GENERAL

Establecer un marco general de actuación de todos los servidores públicos y colaboradores 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.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Promover y fomentar la cultura para la administración de los riesgos en la Corporación, mediante acciones y estrategias encaminadas a un manejo adecuado de los mismos, por parte de los líderes de los procesos de la Entidad.
- ✓ Establecer la metodología para administración de los riesgos asociados a los procesos de la CVC.
- ✓ Identificar, gestionar y controlar los riesgos en los diferentes procesos, sensibilizando e involucrando a los diferentes servidores y colaboradores, en la búsqueda de acciones encaminadas a prevenir y administrar el riesgo en el cumplimiento de las actividades de su competencia.
- ✓ Definir estrategias de comunicación y divulgación adecuadas para la apropiación de la administración del riesgo en la Corporación.

El cumplimiento de estos objetivos será informado, antes del 31 de enero de cada vigencia, por la Dirección de Planeación mediante comunicación escrita a la Dirección General como líder del proceso de administración del riesgo en la CVC.

4. ALCANCE

La política de administración del riesgo es un elemento que contribuye al control del Sistema de Control interno de la entidad, fomentando la cultura del autocontrol al interior de los procesos y es de obligatorio cumplimiento. Es aplicable a:

- Los riesgos de gestión, los riesgos de corrupción y riesgos de seguridad de la información.
- Todos los procesos y proyectos que se adelanten en el área de jurisdicción de la Corporación.
- Los servidores públicos y colaboradores de la Corporación en el ejercicio de sus funciones.

La administración del riesgo en la Corporación tiene un carácter prioritario y estratégico, y está fundamentada en el modelo de gestión por procesos. En virtud de lo anterior, la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos se circunscribe a los objetivos de cada proceso, con lo cual se pretende el cumplimiento de los objetivos Corporativos.

5. TÉRMINOS Y DEFINICIONES

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

Alta Dirección: Persona o grupo de personas que dirige y controla una organización al más alto nivel. En la CVC es el Director General o los Comités de Dirección[3].

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.[4]

Causa Inmediata: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. [4]

Causa Raíz: causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.[4]

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.[5]

CICCI: Comité Institucional Coordinador de Control Interno.

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.[4]

---

[2] ICONTEC internacional. NTC ISO 31000 Gestión del riesgo – principios y directrices. 2018. P.1.
[3] Adaptada por el grupo gestión ambiental y calidad de la Dirección de Planeación. CVC.
[4] Guía para la administración del riesgo y diseño de controles en entidades públicas. Departamento Administrativo de la Función Pública; 2020. P.12.
[5] Ibid., P.13.

Control: medida que permite reducir o mitigar un riesgo. [4]

Factores de Riesgo: son las fuentes generadoras de riesgos. [4]

Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.[4]

Mapa de riesgos: documento con la información resultante de la administración o 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 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]

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.[5]

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. [4]

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. [4]

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). [4]

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. [4]

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.

Riesgo Residual: el resultado de aplicar la efectividad de los controles al riesgo inherente. [4]

Vulnerabilidad: representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas. [5]

6. METODOLOGÍA PARA LA GESTIÓN DE RIESGOS

A continuación, se describe la metodología apropiada por la CVC para la administración de riesgos, la cual se basa en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública – DAFP del año 2020.

6.1 IDENTIFICACIÓN DEL RIESGO

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Se aplican las siguientes fases:

6.1.1 Análisis de objetivos estratégicos y de los procesos.

Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Se plantea la necesidad de analizar su adecuada formulación, es decir, que contengan unos atributos mínimos, para lo cual puede hacer uso de las características *SMART*, cuya estructura se explica a continuación:

- **S: Especific (específico):** lo importante es resolver cuestiones como qué, cuándo, cómo, dónde, con qué, quién. Considerar el orden y lo necesario para el cumplimiento de la misión.
- **M: 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 ayuda 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.

6.1.2 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. Ejemplo: actividades de los procedimientos y analizar la cadena de valor.

6.1.3 Identificación de 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 áreas de factores de riesgo.

Son las fuentes generadoras de riesgos. En la *Tabla 1* se presenta un listado con ejemplos de factores de riesgo que puede tener una entidad.

Tabla 1. Factores de riesgos

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	Falta de procedimientos
		Errores internos en trámite de pagos
		Falta de capacitación
		Errores en autorización
Talento Humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Posibles comportamientos no éticos de los empleados
		Hurto de activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Fallas de software
		Caída de las redes
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Incendios
		Daños en instalaciones
Evento externo	Situaciones externas que afectan la entidad	Asalto en las instalaciones
		Atentados, vandalismo, orden público

Fuente: Adaptado de la guía para la administración del riesgo y el diseño de controles en entidades públicas, 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. La redacción inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

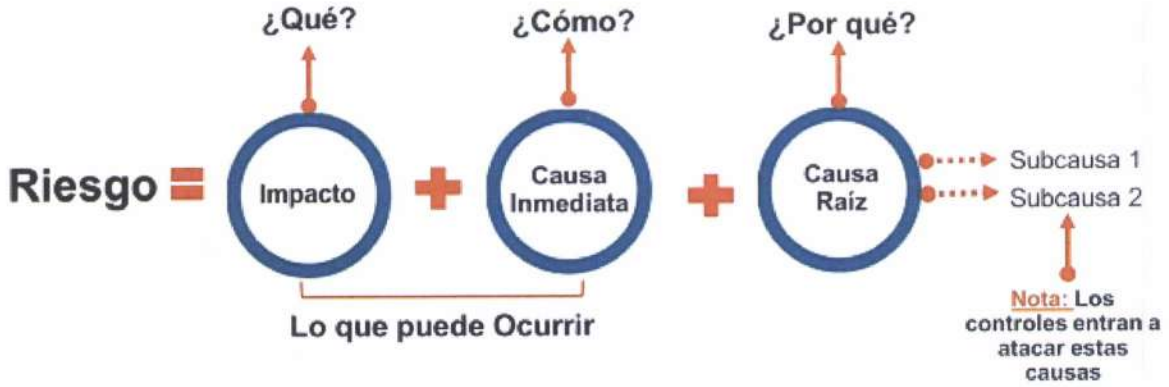


Figura 1. Estructura para la redacción del riesgo de gestión
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

- **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.

Ejemplo[6]:

Proceso: gestión de recursos físicos
Objetivo: mantener en operación óptima la infraestructura física, las condiciones de trabajo y los recursos para el normal funcionamiento de la Corporación.
Alcance: Aplica para el mantenimiento de insumos, elementos y servicios relacionados con la infraestructura física o condiciones de trabajo que se realicen para el funcionamiento de la Corporación.

[6] El ejemplo es tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Figura 2. Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo
Fuente: guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

6.1.6 Clasificación del riesgo.

Permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 2. Clasificación de riesgos

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	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	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	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

6.2 VALORACIÓN DEL RIESGO

Establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

6.2.1 Análisis de riesgos.

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

- **Determinar la probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo.

  La exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año. En la tabla 3 se establecen los criterios para definir el nivel de probabilidad.

Tabla 3. Criterios para definir el nivel de probabilidad de riesgos de gestión

	Frecuencia de la actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

- **Determinar el impacto**: Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

  Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles, se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

  En la siguiente tabla se establecen los criterios para definir el nivel de impacto:

Tabla 4. Criterios para definir el nivel de impacto en riesgos de gestión

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV*	El riesgo afecta alguna área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de consejo directivo y/o de proveedores
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a través de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel del país

*SMLMV: Salario mínimo legal vigente.

Fuente: Adaptado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

Ejemplo (continuación):

Proceso: gestión de recursos físicos
Objetivo: mantener en operación óptima la infraestructura física, las condiciones de trabajo y los recursos para el normal funcionamiento de la Corporación.
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.
N.º de veces que se ejecuta la actividad: la actividad de contratos se lleva a cabo 10 veces en el mes = 120 contratos en el año.
Cálculo afectación económica: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.

Aplicando las tablas de probabilidad e impacto, se tiene el siguiente resultado:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20 %
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40 %
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60 %
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces al año	80 %
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces al año	100 %

→ **La actividad se realiza 120 veces al año, la probabilidad de ocurrencia del riesgo es media**

	Afectación Económica	Reputacional
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores
Menor 60%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional con efecto sostenido a nivel país

La afectación económica se calcula en 500 SMLMV, el impacto del riesgo es **mayor**

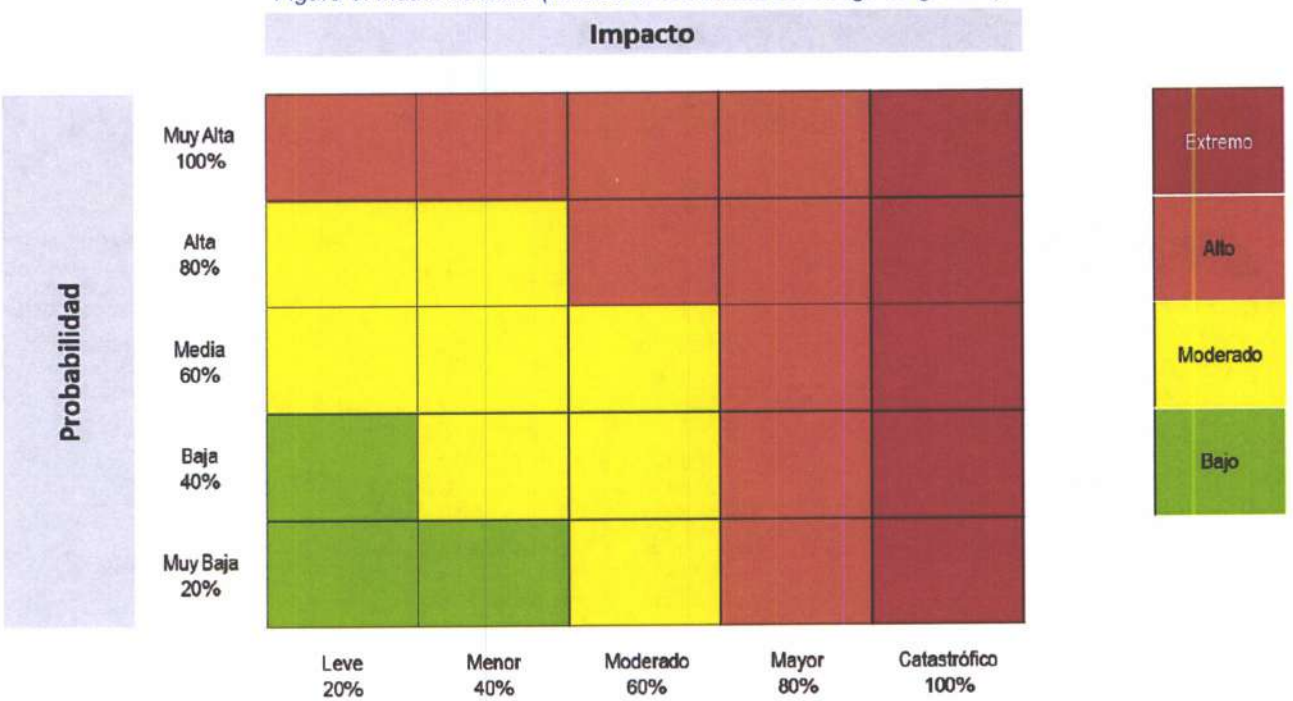
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

6.2.2 Evaluación de riesgos.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (riesgo inherente).

- **Análisis preliminar (riesgo inherente):** se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de color: extremo, alto, moderado y bajo, ver figura 3.

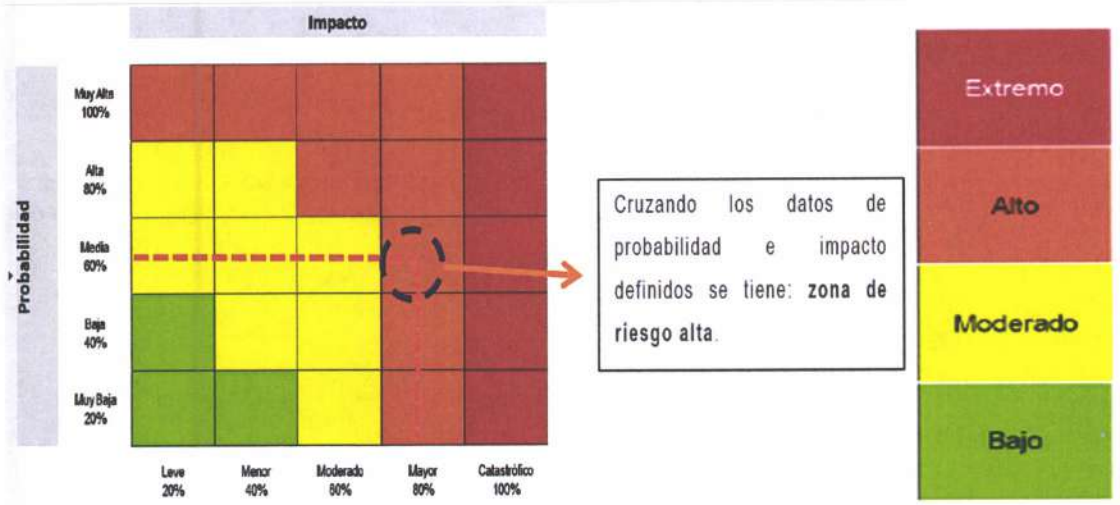
Figura 3. Matriz de calor (niveles de severidad del riesgo de gestión)



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 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 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%

Como resultado de aplicar la matriz de colores, se obtiene:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

- **Valoración de controles:** la valoración de controles se debe realizar a cada riesgo, por parte del líder proceso, aplicando el concepto de experto.

Estructura para la descripción del control (ver figura 4):

- **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.

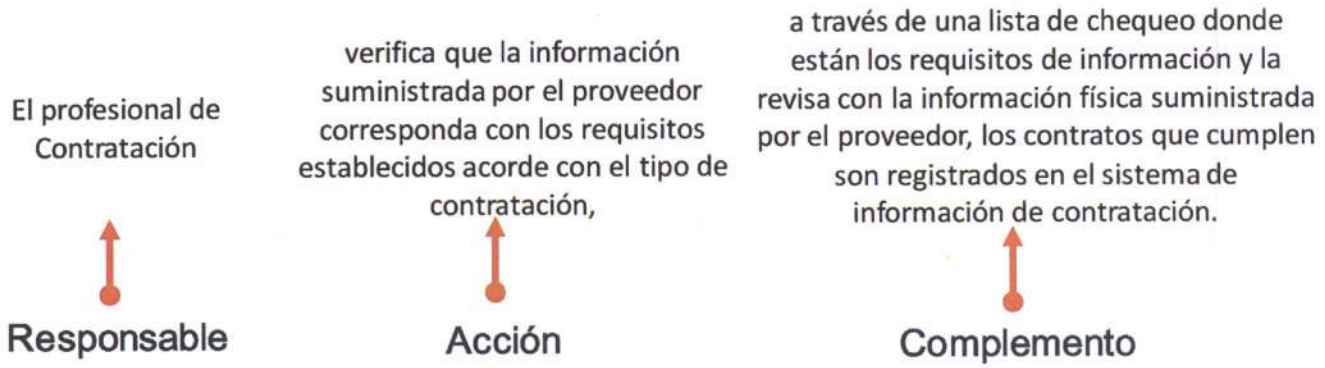


Figura 4. Ejemplo aplicado bajo la estructura propuesta para la redacción del control
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

Tipología de controles y los procesos:

Para los riesgos de gestión, se tienen las siguientes tipologías:

- **Control preventivo:** 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.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos y no aplican para riesgos de corrupción.

La forma como se ejecutan los controles:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

Para la implementación de acciones y controles se tendrá como referente la viabilidad jurídica, financiera y la disponibilidad de recurso humano y tecnológico, así como el análisis costo / beneficio para el manejo o la administración del riesgo.

Análisis y evaluación de los controles – Atributos: para la descripción y peso asociado a cada atributo, ver tabla 5:

Tabla 5. Atributos para el diseño de control

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	-

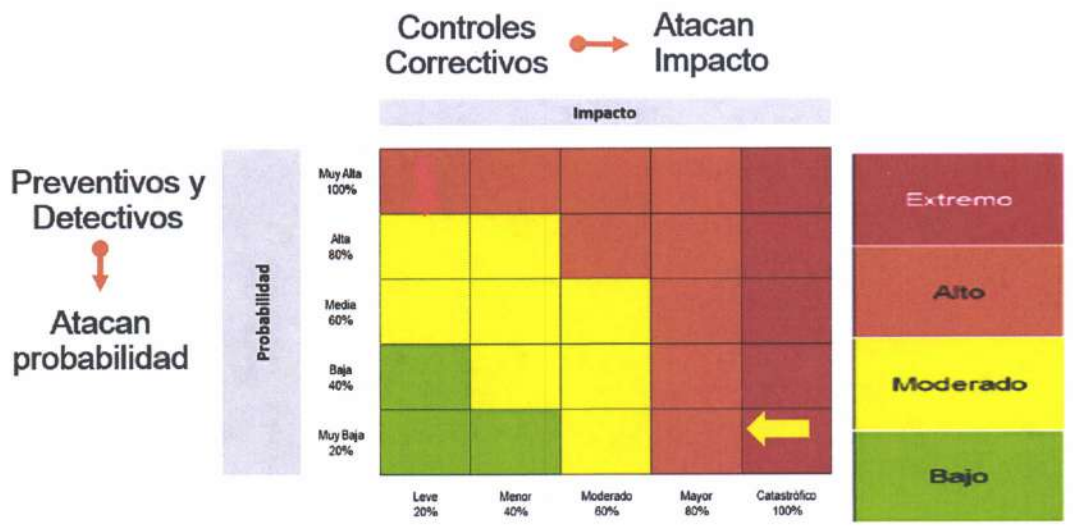
Características			Descripción	Peso
			cualquier otro documento propio del proceso.	
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza 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: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

***NOTA: Estos atributos no tienen incidencia en la efectividad del control**

Según los resultados obtenidos en los controles se dará movimiento en la matriz de calor en el eje de la probabilidad y en el eje de impacto de acuerdo a los siguientes controles:

Figura 5. Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

Ejemplo para aplicar este concepto (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 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 del 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 firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.

Tabla 6. Aplicación tabla de atributos para el diseño de controles a ejemplo propuesto

Características				Peso
Control 1 El profesional del 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. *Atributos informativos	Tipo	Preventivo	x	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
	Documentación	Documentado	x	-
		Sin documentar		-
	Frecuencia	Continua	x	-
		Aleatoria		-
	Evidencia	Con registro	x	-
		Sin registro		-
Total valoración control 1				**40%**
Control 2 El jefe de contratos verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias, devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
	Implementación	Automático		
		Manual	x	15%
	Documentación	Documentado		-
		Sin documentar		-
	Frecuencia	Continua	x	-
		Aleatoria		-
	Evidencia	Con registro	x	-
		Sin registro		-
Total valoración control 2				**30%**

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

- **Nivel de riesgo (riesgo residual):** es el resultado de aplicar la efectividad de los controles al riesgo inherente. En la tabla 7 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles y en la figura 6 se observa el movimiento en la matriz de calor:

Tabla 7. Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto		Datos de 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 requisitos normativos	Probabilidad inherente	60%	Valoración de control 1 preventivo	40%	60% * 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2° control	36%	Valoración ontrol 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
	Impacto Residual	**80%**			

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 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
Aunque el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

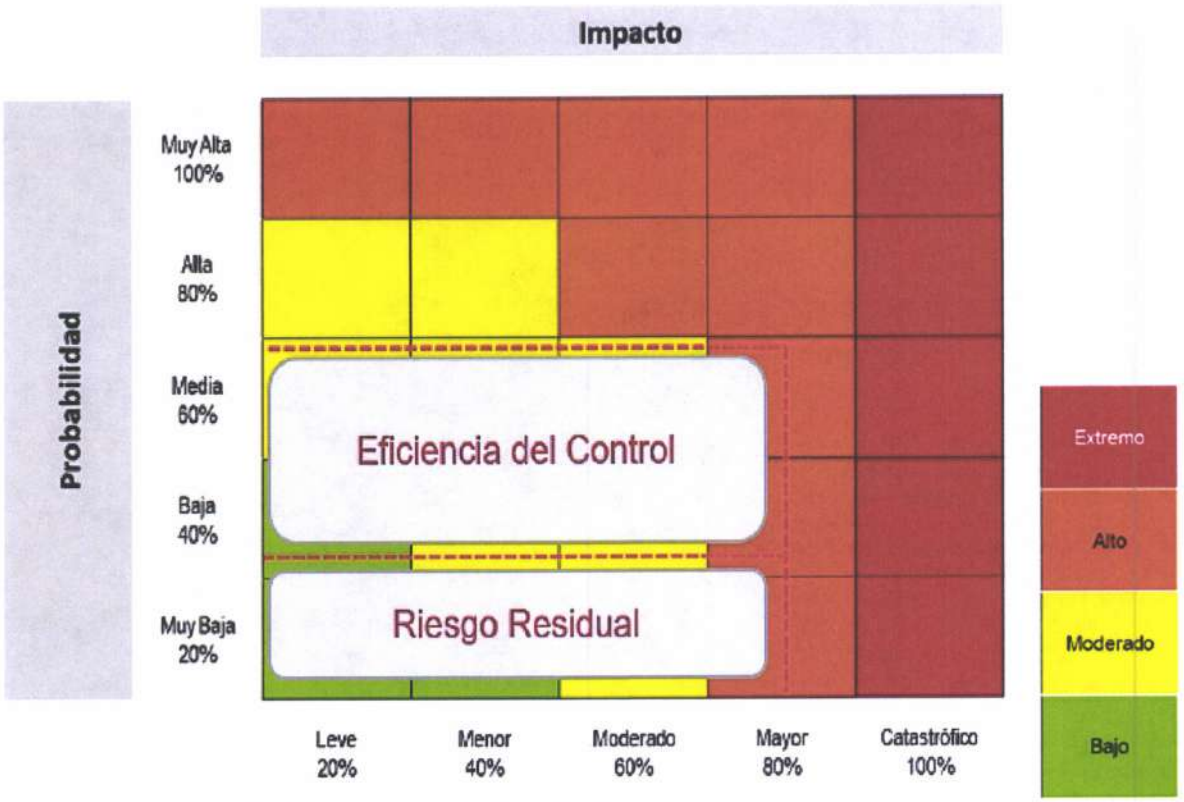


Figura 6. Movimiento en la matriz de calor con el ejemplo propuesto
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

6.2.3 Estrategias para combatir el riesgo.

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Ver figura 7.

Figura 7. Estrategias para combatir el riesgo
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

En la tabla 8 se muestra las estrategias para combatir los riesgos de gestión en la Corporación.

Tabla 8. Estrategias para combatir los riesgos de gestión en la Corporación

ZONA	COLOR	ESTRATEGIA	MANEJO
Extrema	Rojo	**EVITAR EL RIESGO O TRANSFERIR EL RIESGO**	• Establecer acciones o medidas que eviten la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. • Realizar monitoreo **mensual** a los controles y acciones.
Alta	Naranja	**REDUCIR EL RIESGO**	• Establecer acciones o medidas que mitiguen la materialización del riesgo y permitan reducir la probabilidad y/o el impacto. • Realizar monitoreo **bimensual** a los controles y acciones.
Moderada	Amarillo	**REDUCIR EL RIESGO**	• Establecer controles y acciones que permitan reducir la probabilidad y/o el impacto del riesgo. • Realizar monitoreo **trimestral** a los controles y acciones.
Baja	Verde	**ACEPTAR EL RIESGO**	• No se adoptan medidas que afecten la probabilidad o el impacto. • Realizar monitoreo **semestral** para que permanezcan en zona baja.

Fuente: adaptado de acuerdo con indicaciones en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

6.2.4 Herramientas para la Gestión del riesgo.

- **Mapas de riesgos**: La información sobre los riesgos de gestión debe ser registrada por proceso, en el formato mapa de riesgos (FT.0540.11).

  Cada riesgo debe ser identificado con un número, este número es irrepetible, esto con el fin de mantener la trazabilidad para cada uno. Esta información será administrada por el Grupo Gestión Ambiental y Calidad de la Dirección de Planeación.

  Estos mapas deben ser revisados por parte de los líderes de los procesos. La revisión de los mapas de riesgos no implica obligatoriamente su actualización, sin embargo, en los casos en que se identifique necesidad de ajustes, se debe solicitar su actualización a la Dirección de Planeación, de acuerdo con lo establecido en el procedimiento control de documentos (PT.0540.02).

  La necesidad de modificar o actualizar un mapa de riesgos de gestión, puede surgir de la actualización o eliminación de un procedimiento, por cambio de normativa, por ajuste del objetivo o alcance del proceso y debido a materialización de riesgos, entre otros.

- **Mapa de riesgos institucional:** La Dirección de Planeación coordinará la consolidación del mapa de riesgos institucional, como insumo para ello tomará, los mapas de riesgos por proceso, registrará en el formato denominado "Mapa de Riesgos Institucional" la información relacionada con aquellos riesgos cuya valoración se encuentran en "Zona de Riesgo Alta" y "Zona de Riesgo Extrema".

  La anterior información deberá quedar registrada de manera ordenada en el formato, dando prioridad a los mayores riesgos residuales. Consolidada la información, la Dirección de Planeación debe tramitar ante la Alta Dirección el mapa de riesgos para su revisión, análisis, aprobación y distribución. Los resultados de este ejercicio harán parte de la Planificación Estratégica de la Corporación.

- **Gestión de eventos:** "Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología establecida en este documento" *(Guía para la administración del riesgo y el diseño de controles en entidades públicas, pág. 58.)*.

  Una manera de identificar eventos es en el informe de PQRSD (peticiones, quejas, reclamos y denuncias.

6.2.5 Monitoreo y revisión de los mapas de riesgo

La Corporación asegura el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. A través de las líneas de defensa se establecen los roles y responsabilidad de todos los actores de la gestión del riesgo y control en la Corporación. (Ver figura 8).

Corporación Autónoma
Regional del Valle del Cauca

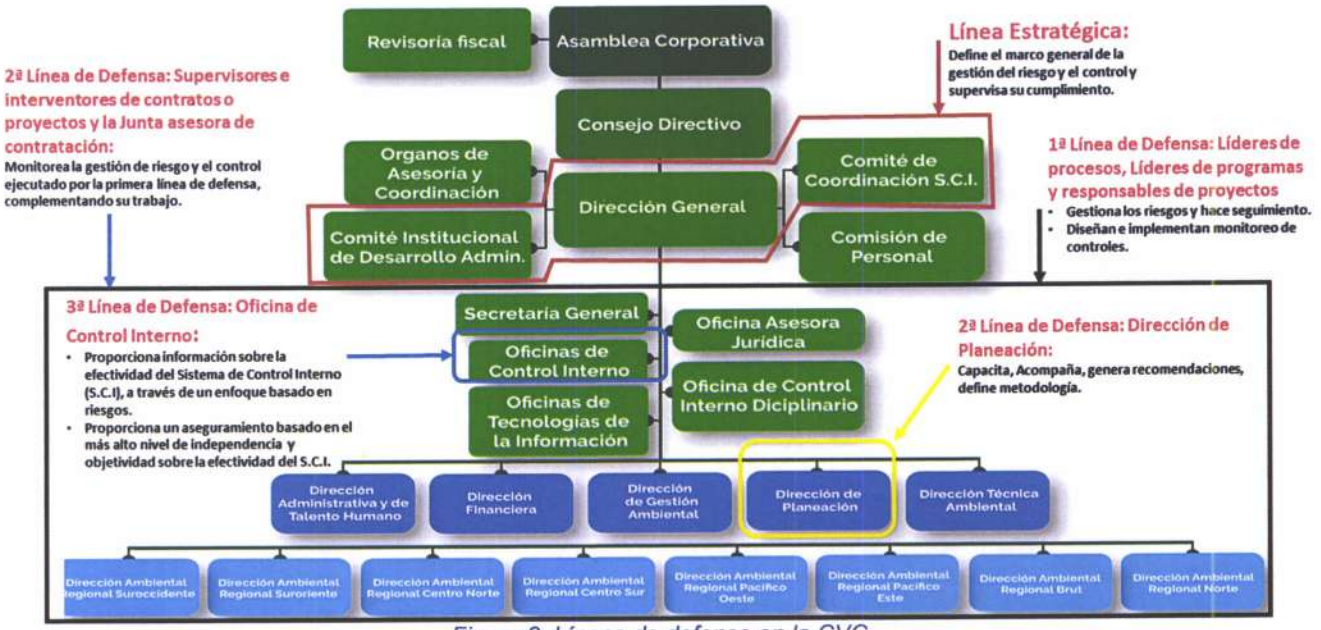


Figura 8. Líneas de defensa en la CVC
Fuente: Elaboración propia

7. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

7.1. IDENTIFICACIÓN DE RIESGOS DE CORRUPCIÓN

7.1.1 Definición de riesgos de corrupción

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Es necesario que en la descripción del riesgo concurran los **componentes de su definición**, así: **ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.**

En la siguiente matriz (ver tabla 10), se da un ejemplo de la descripción de un riesgo de corrupción, la X que aparece en cada casilla, quiere decir, que cumple con cada uno de los componentes de la definición.

Tabla 9. Matriz de definición del riesgo de corrupción

MATRIZ: DEFINICIÓN 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: Guía para la administración del riesgo, versión 4

Los riesgos de corrupción se establecen sobre procesos. Deben estar descritos de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Evitar iniciar con palabras negativas como: "No…", "Que no…", o con palabras que denoten un factor de riesgo (causa) tales como: "ausencia de", "falta de", "poco(a)", "escaso(a)", "insuficiente", "deficiente", "debilidades en…"

7.1.2 Generalidades acerca de los riesgos de corrupción

- Los riesgos de corrupción se gestionan anualmente por cada responsable de los procesos junto con su equipo de trabajo y deben ser registrados en el formato para mapas riesgos de corrupción (FT.0540.25)

- La publicación de los mapas de riesgos de corrupción se debe realizar en la página web de la Corporación, a más tardar el 31 de enero de cada año.

- Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación.

- **Ajustes y modificaciones**: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Monitoreo:** los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- **Seguimiento:** el jefe de control interno debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas de los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción. Se debe realizar tres seguimientos cada año, así:

  - ✓ **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.

  En especial deberá adelantar las siguientes actividades:

- **Acciones a seguir en caso de materialización de riesgos de corrupción**

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción.
2. Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
3. Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
4. Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe adelantar las siguientes acciones:

- ✓ Determinar la efectividad de 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.

7.2 VALORACIÓN DE RIESGOS DE CORRUPCIÓN

Esta valoración permite establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

7.2.1 Análisis de la probabilidad de riesgos de corrupción

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda. En la tabla 10 se describen los criterios para clasificar la **probabilidad** en los riesgos de corrupción.

Tabla 10. Criterios para calificar la probabilidad en los riesgos de corrupción

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Mas de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.

En caso de que el proceso no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, los integrantes del equipo de trabajo deben calificar el nivel de probabilidad en términos de factibilidad, de acuerdo con la experiencia de los funcionarios que desarrollan el proceso.

7.2.2 Análisis del impacto en riesgos de corrupción

El impacto se debe analizar y calificar a partir de las consecuencias identificadas. En la tabla 11 se describen los criterios para calificar el impacto en los riesgos de corrupción. Los criterios se aplicarán al siguiente riesgo, el cual se denominará en adelante **R1**:

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

Tabla 11. Criterios para calificar el impacto en riesgos de corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría:	Respuesta SI	Respuesta NO
1	¿Afecta al grupo de funcionarios del proceso?	X	
2	¿Afecta al cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar al cumplimiento de la misión de la Entidad?	X	
4	¿Afectar la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar perdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de los servicios?	X	
8	¿Dar lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien, servicio o recursos públicos?		X
9	¿Generar perdida de la información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
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.		**10**	

Nivel de impacto

Moderado	Genera a medianas consecuencias sobre la entidad
Mayor	Genera altas consecuencias sobre la entidad
Catastrófico	Genera consecuencias desastrosas para la entidad

Fuente: Adaptada de información tomada del departamento administrativo de la función pública

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles "moderado", "mayor" y "catastrófico", dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

7.2.3 Análisis preliminar del riesgo (riesgo inherente)

De acuerdo con la tabla 11, sobre criterios para calificar el impacto, el riesgo analizado (R1) tiene un nivel de impacto *Mayor*. Si como resultado del análisis de la probabilidad se obtuvo que el riesgo es *Probable*, al ubicar en el mapa de calor el punto de intersección resultante, para riesgo inherente se obtiene:

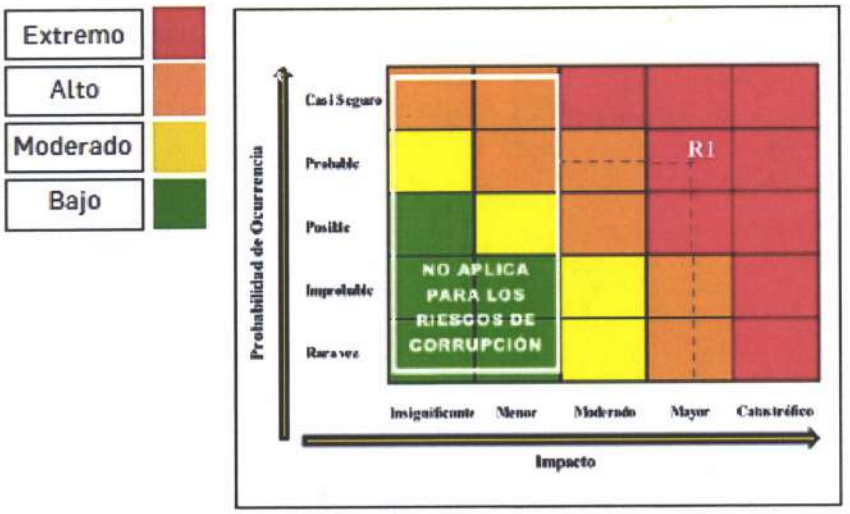


Figura 9.Mapa de calor para riesgos de corrupción
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018.

El nivel de riesgo inherente (sin controles), para R1 corresponde a EXTREMO.

7.2.4 Valoración de los controles – Diseño de controles

Para cada causa de riesgo, debe existir por lo menos un control. Se deben diseñar controles que mitiguen de manera adecuada el riesgo, para esto, se deben considerar, desde la redacción de los mismos, las siguientes variables:

1. **Debe tener definido el responsable de llevar a cabo la actividad de control:** el responsable es la persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso.

    - Cuando un control se hace de manera manual (ejecutado por personas) es importante establecer el cargo responsable de su realización, por ejemplo: Director o Jefe de Oficina, Profesional Especializado, Técnico Administrativo, etc..
    - Cuando el control es automático (lo hace un sistema o una aplicación), a través de un sistema programado, es importante establecer como responsable de ejecutar el control al sistema o aplicación, por ejemplo: El aplicativo de gestión documental, el aplicativo de contratación, etc..

2. **Debe tener una periodicidad definida para su ejecución:** el control debe tener una periodicidad específica (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo.

   Ejemplos:
   - El profesional especializado cada vez que se va a realizar un contrato con un proveedor de servicios.
   - El aplicativo de contratación cada vez que se realiza un pago.

3. **Debe indicar cuál es el propósito del control:** el control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo.

   Ejemplos:
   - El profesional especializado cada vez que se va a realizar un contrato con un proveedor de servicios, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación.
   - El aplicativo de contratación cada vez que se realiza un pago, valida que el proveedor al cual se le va a girar no esté reportado en listas restrictivas o de lavado de activos y financiación del terrorismo.

4. **Debe establecer el cómo se realiza la actividad de control**: permite evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.

   Ejemplo:
   - El profesional especializado cada vez que se va a realizar un contrato con un proveedor de servicios, 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 la información y la revisión con la información física suministrada por el proveedor.
   - El aplicativo de contratación cada vez que se realiza un pago, valida que el proveedor al cual se le va a girar no esté reportado en listas restrictivas, comparando el Número de Identificación Tributaria (NIT) o Cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo.

5. **Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control:** si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones.

   Ejemplo:
   - El profesional especializado cada vez que se va a realizar un contrato con un proveedor de servicios, 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 la información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo el suministro de la información y poder continuar con el proceso de contratación.

- El aplicativo de contratación cada vez que se realiza un pago, valida que el proveedor al cual se le va a girar no esté reportado en listas restrictivas, comparando el Número de Identificación Tributaria (NIT) o Cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo. En caso de encontrar coincidencias el sistema no permite realizar el pago.

6. **Debe dejar evidencia de la ejecución del control**: la evidencia ayuda a que se pueda revisar la misma información por un tercero y llegue a la misma conclusión de quien ejecutó el control.

   Ejemplo:

   - El profesional especializado cada vez que se va a realizar un contrato con un proveedor de servicios, 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 la información y la revisión con la información física suministrada por el proveedor. En caso de encontrar información faltante, requiere al proveedor a través de correo el suministro de la información y poder continuar con el proceso de contratación. Como evidencia deja lista de chequeo diligenciada con la información de la carpeta del cliente y correos solicitando la información faltante en los casos que aplique.

   - El aplicativo de contratación cada vez que se realiza un pago, valida que el proveedor al cual se le va a girar no esté reportado en listas restrictivas, comparando el Número de Identificación Tributaria (NIT) o Cédula con la información cargada en el aplicativo de las listas de clientes reportados en temas de lavado de activos y financiación del terrorismo. En caso de encontrar coincidencias el sistema no permite realizar el pago. Como evidencia queda la programación interna del aplicativo y el reporte de coincidencia con listas restrictivas.

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

En la tabla 12 se describe el peso o participación de cada variable en el diseño del control para la mitigación del riesgo de corrupción:

Tabla 12. Peso o participación de cada variable en el diseño del control para la mitigación del riesgo de corrupción

Criterio de evaluación	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del responsable	Asignado	15
	No asignado	0
1.2 Segregación y autoridad del responsable	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control	Confiable	15
	No confiable	0
5. Que pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan ni se resuelven oportunamente	0
6. Evidencia de la ejecución del control	Completa	15
	Incompleta	10
	No existe	0

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018

Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Tabla 13. Rango de calificación del diseño del control para riesgos de corrupción

Rango de calificación	Resultado – Peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018.

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

Resultados de la evaluación de la ejecución del control

Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe tener la confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna.

7.2.5 Nivel del riesgo (riesgo residual)

Una vez aplicados los controles a los riesgos, se debe tener en cuenta que, para los de corrupción, únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Resultados de los posibles desplazamientos de la probabilidad en riesgos de corrupción:

Si la calificación del control es "Fuerte", se disminuyen dos niveles en el eje de la probabilidad.
Si la calificación del control es "Moderado", se disminuye un nivel en el eje de la probabilidad.

Para el riesgo R1, se tiene el siguiente desplazamiento en el mapa de calor (ver figura 10):

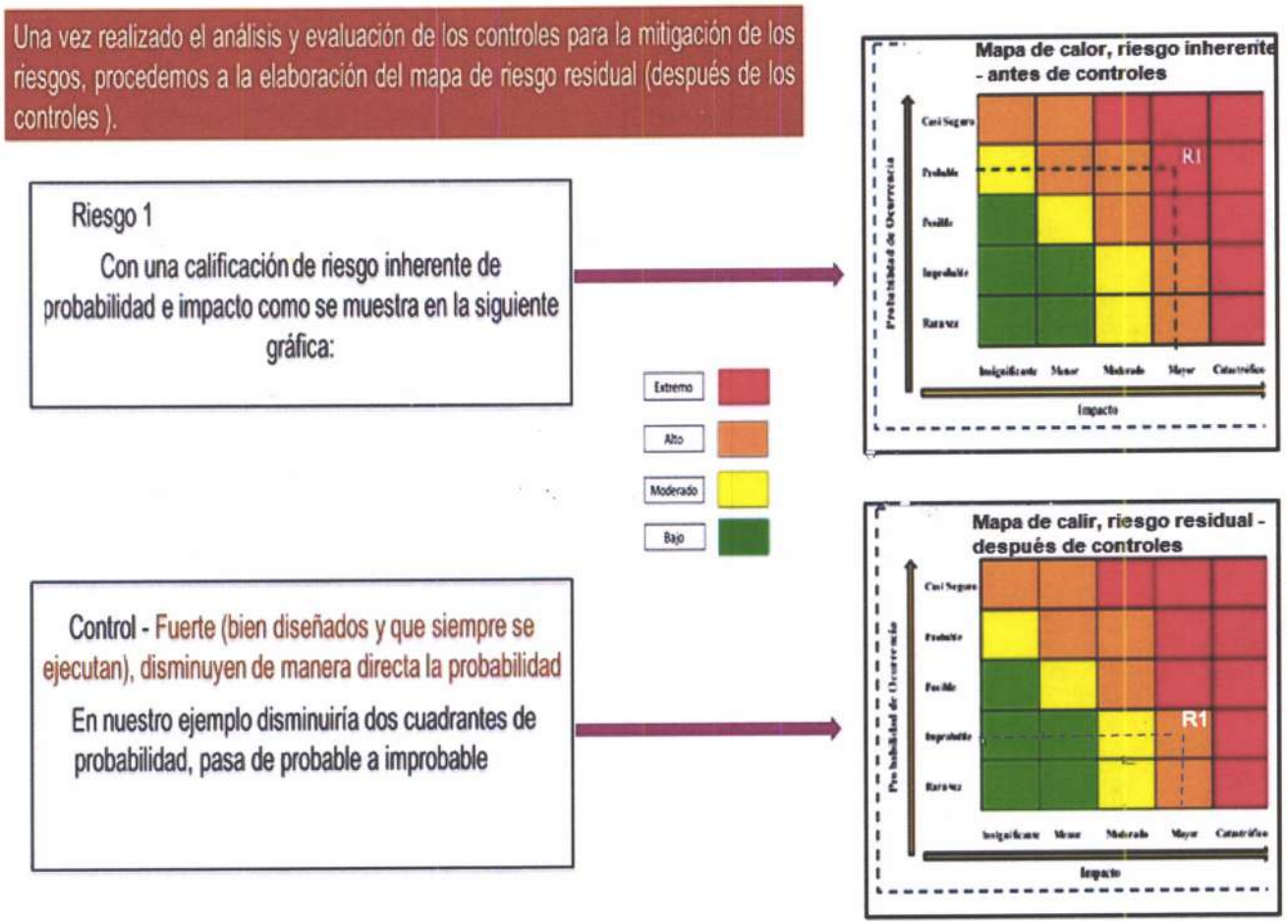


Figura 10. Resultado del mapa de calor - riesgo residual aplicado a R1
Fuente: adaptado de mapa de calor del departamento administrativo de la función pública

7.3 TRATAMIENTO PARA LOS RIESGOS DE CORRUPCIÓN

En todos los casos para los riesgos de corrupción, la respuesta en cuanto al tratamiento será **evitar, compartir o reducir** el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tabla 14. Estrategias para combatir los riesgos de corrupción en la Corporación

ZONA	COLOR	ESTRATEGIA	MANEJO
Extrema	Rojo	**EVITAR O COMPARTIR EL RIESGO**	• Establecer acciones o medidas que eviten la materialización del riesgo. • Compartir el riesgo. • Establecer controles y acciones que permitan reducir la probabilidad. • Realizar monitoreo **mensual o bimensual** a los controles y acciones.
Alta	Naranja		
Moderada	Amarillo	**REDUCIR EL RIESGO**	• Establecer controles y acciones que permitan reducir la probabilidad. • Realizar monitoreo mínimo **trimestral** a los controles y acciones.

Fuente: adaptado de acuerdo con indicaciones en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018

Corporación Autónoma
Regional del Valle del Cauca

8. LINEAMIENTOS SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

8.1 IDENTIFICACIÓN DE LOS ACTIVOS DE SEGURIDAD DE LA INFORMACIÓN

Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información de cada proceso. Con la identificación de los activos de seguridad de la información, la Corporación puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

¿Qué es un activo de información?

Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la corporación, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.

¿Cómo identificar los activos?

En la siguiente figura se describen los pasos para realizar la identificación de activos:

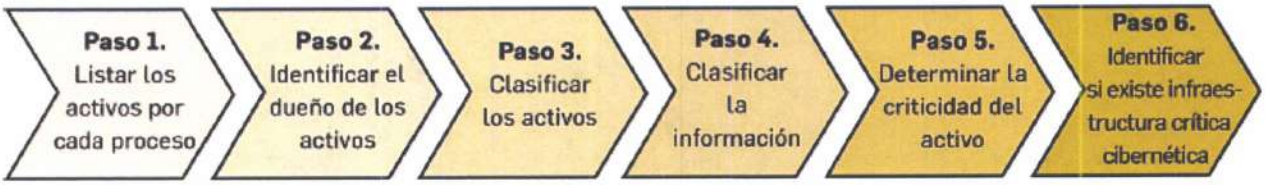


Figura 11. Pasos para la identificación de activos
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

Paso 1: Listar los activos por cada proceso:

En cada proceso, deberán listarse los activos, indicando algún consecutivo, nombre y descripción breve de cada uno. En la tabla 15 se describe un ejemplo de identificación de activos de un proceso:

Paso 2. Identificar el dueño de los activos:
Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.

Paso 3. Clasificar los activos:

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.

Paso 5. Determinar la criticidad del activo (Valoración del Activo):
Se debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICC-

Se debe identificar y reportar a las instancias y autoridades respectivas en el Gobierno nacional si la Corporación posee ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios.

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Con base a los seis (6) pasos vistos previamente, se generará información como el ejemplo que se describe en la siguiente tabla:

Tabla 15. Ejemplo de identificación de activos de un proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo de activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel del criticidad
Gestión Financiera	Base de datos nomina	Base de datos con información de nómina de la entidad	Director Financiero	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión Financiera	Aplicativo nómina	Servidor web que contiene el *front office* de la entidad	Director Financiero	Software	N/A	N/A	BAJA	BAJA	BAJA	BAJA
Gestión Financiera	Cuentas de cobro	Formatos de cobros diligenciados	Director Finanicero	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

8.2 IDENTIFICAR LOS RIESGOS INHERENTES DE SEGURIDAD DE LA INFORMACIÓN

se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida 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. Además, se debe identificar el **dueño del riesgo**, es decir, "*quien tiene que rendir cuentas sobre el riesgo o quien tiene la autoridad para gestionar el riesgo.*

8.2.1 Identificación de Amenazas:

Los siguientes listados de amenazas representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas:

- **Amenazas Comunes:** Deliberadas (D), fortuitas (F) o ambientales (A).

Tabla 16. Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
	Fallas del equipo	F

Tipo	Amenaza	Origen
Fallas técnicas	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (anexo 4 – Departamento Administrativo de la Función Pública)

- **Amenazas dirigidas por el hombre**: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Tabla 17. Amenazas dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	• Reto • Ego • Rebelión • Estatus • Dinero	• Piratería • Ingeniería Social • Intrusión, accesos forzados al sistema • Acceso no autorizado
Criminal de la computación	• Destrucción de la información • Divulgación ilegal de la información • Ganancia monetaria • Alteración no autorizada de los datos	• Crimen por computador • Acto fraudulento • Soborno de la información • Suplantación de identidad • Intrusión en el sistema
Terrorismo	• Chantaje • Destrucción • Explotación • Venganza • Ganancia política • Cubrimiento de los medios de comunicación	• Bomba/Terrorismo • Guerra de la información • Ataques contra el sistema DDoS • Penetración en el sistema • Manipulación en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	• Ventaja competitiva • Espionaje económico	• Ventaja de defensa • Ventaja política • Explotación económica • Hurto de información • Intrusión en privacidad personal • Ingeniería social

Fuente de amenaza	Motivación	Acciones amenazantes
		• Penetración en el sistema • Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	• Curiosidad • Ego • Intèligencia • Ganancia monetaria • Venganza • Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	• Asalto a un empleado • Chantaje • Observar información reservada • Uso inadecuado del computador • Fraude y hurto • Soborno de información • Ingreso de datos falsos o corruptos • Interceptación • Código malicioso • Venta de información personal • Errores en el sistema • Intrusión al sistema • Sabotaje del sistema • Acceso no autorizado al sistema.

Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (anexo 4 – Departamento Administrativo de la Función Pública)

8.2.2 Identificación de vulnerabilidades:

La CVC puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tabla 18. Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	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
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 envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección

Tipo	Vulnerabilidades
	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

Fuente: Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (anexo 4 – Departamento Administrativo de la Función Pública)

A continuación (ver figura 12), se muestra un ejemplo de la descripción de un riesgo de seguridad de la información:

Seleccionar las vulnerabilidades asociadas a la amenaza identificada

Riesgo	Activo	Descripción del riesgo	Amenaza	Tipo	Causas/vulnerabilidades	Consecuencias
Pérdida de la integridad	Base de datos de la nómina	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la perdida de la integridad de la base de datos de nómina	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza al ciudadano). Ejemplo: posible retraso en el pago de la nómina
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Figura 12. Ejemplo de descripción del riesgo de seguridad de la información
Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020

La identificación de riesgos, amenazas y vulnerabilidades puede ser realizada a través de diferentes metodologías. Como ejemplo, se citan las siguientes:

- **Lluvia de ideas:** mediante esta opción se busca animar a los participantes a que indiquen qué situaciones adversas asociadas al manejo de la información digital y los activos de información se pueden presentar o casos ocurridos que los participantes conozcan que se hayan dado en la Corporación o en el sector.

- **Juicio de expertos:** a través de este esquema se reúnen las personas con mayor conocimiento sobre la materia de análisis e indican cuáles aspectos negativos o riesgos de seguridad de la información se pueden presentar.
- **Análisis de escenarios:** en este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse.

- **Otras técnicas que pueden ser empleadas son**: entrevistas estructuradas, encuestas o listas de chequeo.

Posterior a la identificación de los riesgos de seguridad de la información con sus respectivas amenazas y vulnerabilidades enunciadas en este documento, se deberá continuar con el **Punto 6.2 Valoración del Riesgo, de esta política de administración del riesgo.**

8.3 CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se incluyen algunos ejemplos de controles:

Tabla 19.Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	**Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información**
Procedimientos de operación documentados	Control:Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten
Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información
Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, pruebas y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación
Protección contra códigos maliciosos	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información, estén protegidas contra códigos maliciosos
Copia de respaldo	Objetivo: Proteger la información contra perdida de datos
Respalo de información	Control: Se deberían hacer copias de respaldo de la información, del software y de las imágenes de los

Procedimientos operacionales y responsabilidades	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la información
	sistemas, ponerlas a prueba regularmente de acuerdo a la política de copias de respaldo aceptada

Fuente: Ministerio de Tecnología de la información y comunicaciones. Min Tic 2018

Proyectó: Grupo Gestión Ambiental y Calidad de la Dirección de Planeación
Revisó: Profesional especializado de la Oficina de Tecnologías de Información.
Director de Planeación (C)
Jefe Oficina de Tecnologías de la Información