RAP PACÍFICO Una región de oportunidades Región Administrativa y de Planificación	**PROCESO: GESTIÓN DEL MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN**	**Código:** POL-01-GM
		Versión: 01
	Política: Política de Administración de Riesgos	**Fecha Aprobación**: 26/08/2021

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

RAP PACÍFICO
Una región de oportunidades
Región Administrativa y de Planificación

RAP PACÍFICO

ELABORÓ	REVISÓ	APROBÓ
Jocelyn Danna Carrillo Área de Planeación **Angélica María Ortíz Marín** Practicante Área de Planeación	**Laura Loreto Arias Medina** Coordinadora área jurídica y administrativa	**Comité Institucional de coordinación de control interno** **Camilo Ernesto Lloreda Becerra** Gerente General RAP

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4

2. OBJETIVO: 5

3. ALCANCE 5

4. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO 5

5. TÉRMINOS Y DEFINICIONES 5

6. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO: 7

6.1 Metodología a Utilizar 7

7. ETAPAS DE LA ADMINISTRACIÓN DE RIESGOS 7

8. LINEAMIENTOS: 9

8.1 Zona de riesgo y tratamiento: 11

8.2 Probabilidad 12

8.3 Impacto: 13

8.4 Mapa de calor 13

8.5 Valoración de controles 14

8.6 Análisis y evaluación de los controles 14

8.7 Nivel de Riesgo (Riesgo Residual). 16

9. COMUNICACIÓN Y CONSULTA 17

1. INTRODUCCIÓN

La administración del Riesgo comprende el conjunto de Elementos de Control y sus Interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos institucionales; contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de Autocontrol y autoevaluación al interior de la misma.

Teniendo en cuenta que la administración de riesgos es estratégica para el logro de los objetivos institucionales y de procesos, en este manual se enuncia la política marco de acción que permitirá tomar decisiones relativas a la administración del riesgo, el cual está alineado y armonizado con el Modelo Integrado de Planeación y Gestión MIPG, la Guía para la Gestión del Riesgo establecida por el Departamento Administrativo de la Función Pública

La tendencia más común es la valoración del riesgo como una amenaza; en este sentido, los esfuerzos institucionales se dirigen a reducir, mitigar o eliminar su ocurrencia. No obstante, el riesgo como oportunidad, implica que su gestión está dirigida a optimizar los resultados que este genera.

En tal sentido, LA RAP PACÍFICO*,* no es inmune al riesgo, es más, los riesgos de la Entidad cambian constantemente y la naturaleza y las consecuencias potenciales que se enfrentan son cada vez más complejas y sustanciales. La rapidez del cambio, la creciente complejidad de la economía mundial, las expectativas más exigentes de la comunidad, los requerimientos del estado colombiano, el impacto de una posible falla en los controles, los rápidos cambios en las tecnologías y un sinnúmero de otros factores pueden afectar la Entidad, de manera tal que se requiere de una alta y oportuna capacidad, así como de una estructura organizacional preparada.

2. OBJETIVO:

Definir la metodología para la gestión adecuada de los riesgos, a través de la identificación de acciones de control, respuestas oportunas y estrategias institucionales, con el propósito de atacar las causas potenciales, las amenazas, las vulnerabilidades y minimizar los impactos ante una eventual materialización que puedan afectar la misionalidad, las estrategias y objetivos Institucionales.

3. ALCANCE

La política de administración de riesgos es aplicable a todos los procesos de la Entidad y a las acciones ejecutadas por los servidores y/o contratistas durante el ejercicio de sus funciones.

En el caso de los riesgos de seguridad digital debe ser extensible y aplicable a los procesos de la entidad que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

4. NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO

Ningún riesgo de corrupción podrá ser aceptado

Los riesgos de gestión y de seguridad digital identificados en zona de riesgo BAJA, Se ACEPTARÁ el riesgo y se administrará por medio de las actividades propias del proceso o procedimiento asociado.

5. TÉRMINOS Y DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos

externos.

- **Riesgo de 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).

- **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.

- **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.

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

- **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

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

- **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.

- **Control:** Medida que permite reducir o mitigar un riesgo.

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

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

- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad de exactitud y completitud.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

6. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO:

6.1 Metodología a Utilizar

Se utilizará la metodología vigente publicada por el Departamento Administrativo de la Función Pública DAFP para la administración de los Riesgos de Gestión, Corrupción y Seguridad Digital.

Se utilizará la metodología vigente por Colombia Compra Eficiente, para la administración de riesgos para el proceso de contratación dirigido a los partícipes del sistema de compras y contratación pública.

7. ETAPAS DE LA ADMINISTRACIÓN DE RIESGOS

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad. Con el fin de asegurar dicho manejo, en LA RAP PACÍFICO, se establecieron las siguientes etapas que aseguran la mitigación de los riesgos:

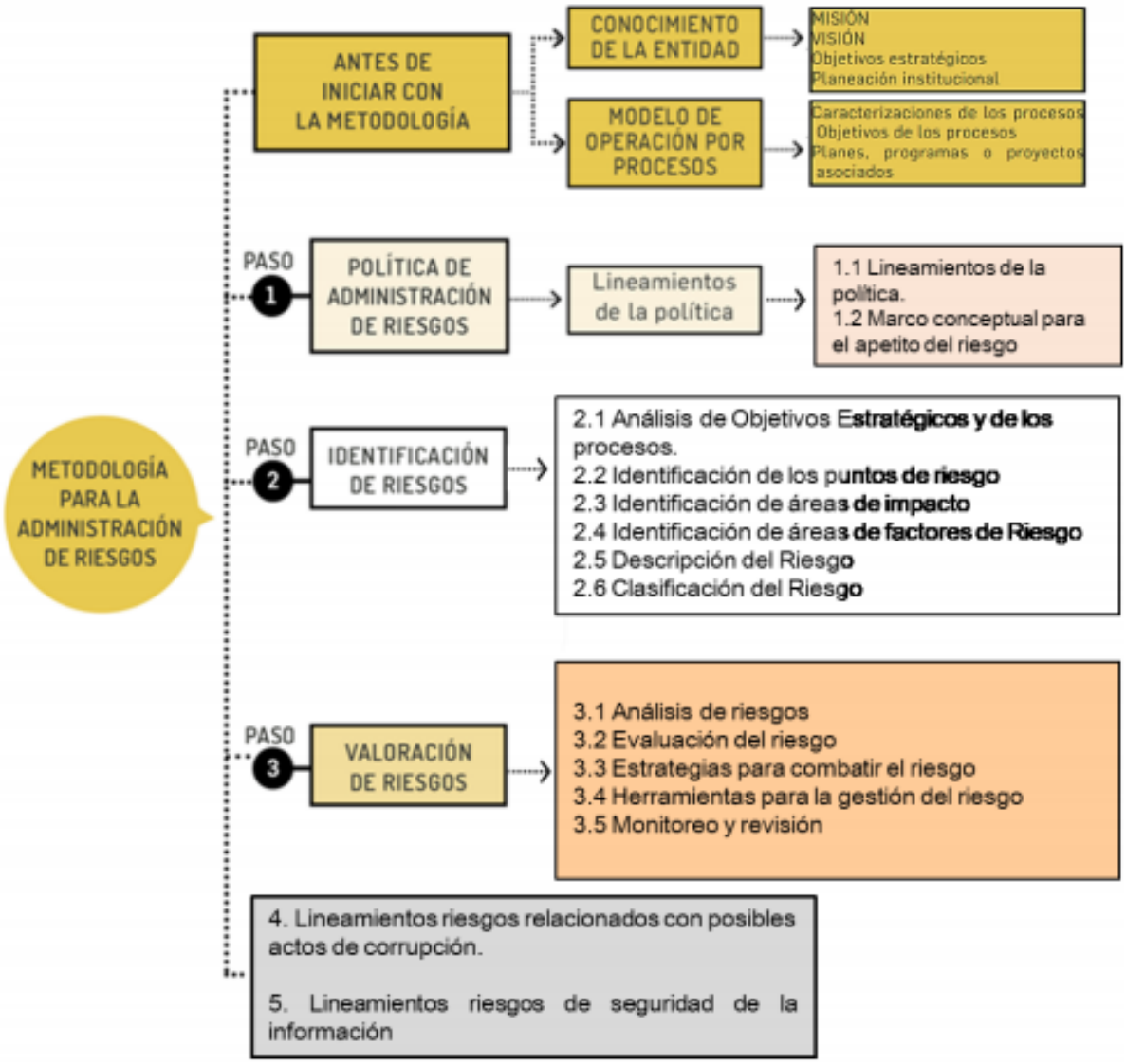


Ilustración 1. Metodología para la administración del riesgo
Tomado de: guía de administración del riesgo y el diseño de controles en entidades públicas

8. LINEAMIENTOS:

Para la correcta interpretación de esta política, se deben tener en cuenta los siguientes lineamientos:

- Los riesgos siempre deben asociarse a los objetivos o estrategias definidas en la ***RAP PACÍFICO***, objetivos de los procesos o proyectos. Un pre-requisito indispensable para trabajar en la identificación de riesgos consiste en el entendimiento uniforme y completo de los objetivos y estrategias que se establezcan en la Entidad, en el marco de su contexto estratégico.

- Se mantiene el protocolo para la identificación de riesgos de corrupción, asociados a la prestación de trámites y servicios, en el marco de la política de racionalización de trámites, liderado por la dirección de participación, transparencia y servicio al ciudadano de Función Pública.

- Para los riesgos de seguridad digital se debe implementar el anexo 4 de la Guía para la administración de riesgos y el diseño de controles en entidades públicas, bajo el lineamiento del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC).

El tratamiento de riesgos, es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo.

Opción para el manejo del riesgo	Descripción
Evitar el riesgo	Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Se abandonan las actividades que dan lugar al riesgos, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo	Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo. Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.
Reducir el riesgo	El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este. Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Aceptar el riesgo	No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. **Importante:** Ningún riesgo de corrupción debe ser acetado.

8.1 Zona de riesgo y tratamiento:

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
Riesgos de Gestión y seguridad digital	**Baja**	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias del proceso o procedimiento asociado y se realiza en el reporte bimensual de su desempeño.
	Moderada	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace monitoreo bimestral y se registran sus avances en la matriz establecida para tal fin.
	Alta y Extrema	Se adoptan medidas para **REDUCIR O COMPARTIR** la probabilidad o el impacto del riesgo, o ambos; esto conlleva a la implementación de controles. Periodicidad bimestral.
Riesgos de Corrupción	**Moderada**	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los procesos.
	Alta y Extrema	Se adoptan medidas para: **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **EVITAR** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
		TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad bimestral de monitoreo para evitar a toda costa su materialización por parte de los

Tipo de riesgo	Zona de riesgo	Nivel de aceptación
		procesos a cargo de los mismos y se registra en el Módulo de Riesgos – SGI.

8.2 Probabilidad

Se entiende por probabilidad como la posibilidad de ocurrencia del riesgo. La probabilidad de ocurrencia estará asociada a la **exposición al riesgo** del proceso o actividad que se esté analizando.

De este modo, la probabilidad inherente será el **número de veces que se pasa por el punto de riesgo en el periodo de 1 año.**

Para su determinación se utiliza la tabla de probabilidad (ver Tabla 4 - Criterios para definir el nivel de probabilidad. Guía DAFP versión 5)

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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 de riesgos y el diseño de controles en entidades públicas.

8.3 Impacto:

Se adopta la siguiente tabla con los criterios para calificar el Impacto – riesgos de gestión

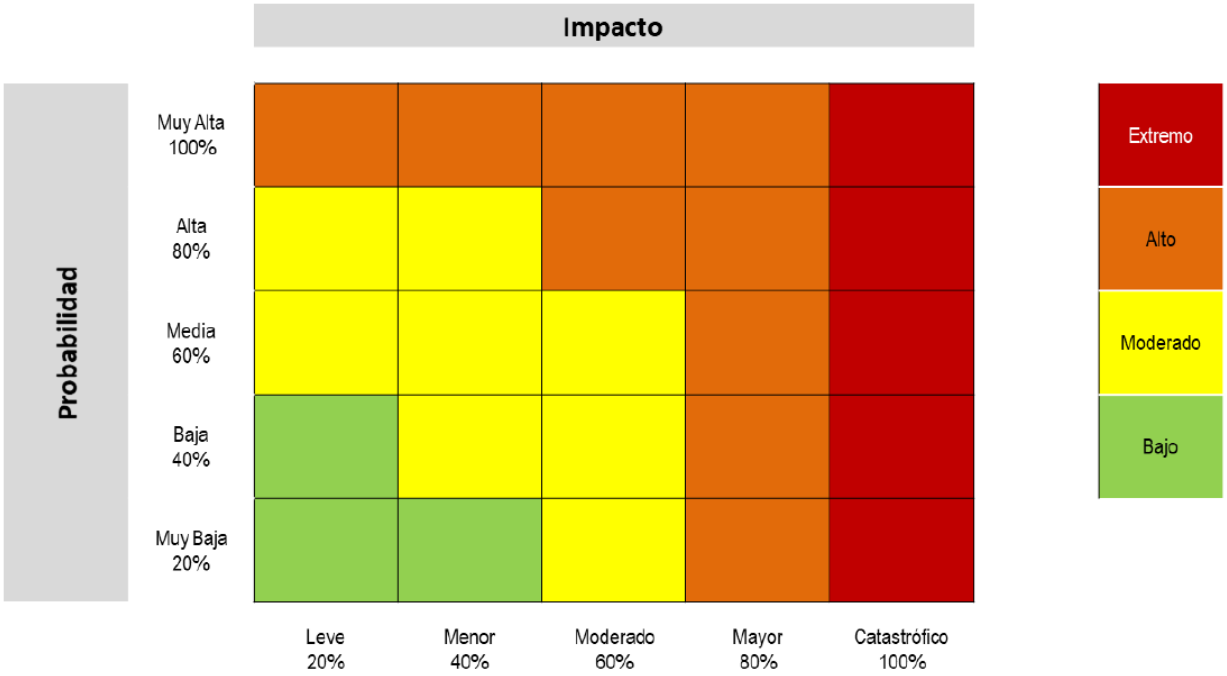
Tabla De Impacto

Nivel	Afectación Económica	Impacto (consecuencias) Reputacional
Leve 20%	Afectación menor a 5 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 5 y 10 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 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 50 y 100 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 100 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.5.

8.4 Mapa de calor

Para poder identificar la zona de riesgo y los niveles de severidad, se utilizará el siguiente mapa de calor a través de la combinación de la probabilidad y el impacto determinados tanto para los riesgos inherentes como para los residuales.



Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.5.

8.5 Valoración de controles

Un control se define como la medida que permite reducir o mitigar el riesgo.

Nota: La valoración de controles se ha establecido conforme la metodología establecida en la pagina 43 de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.5.

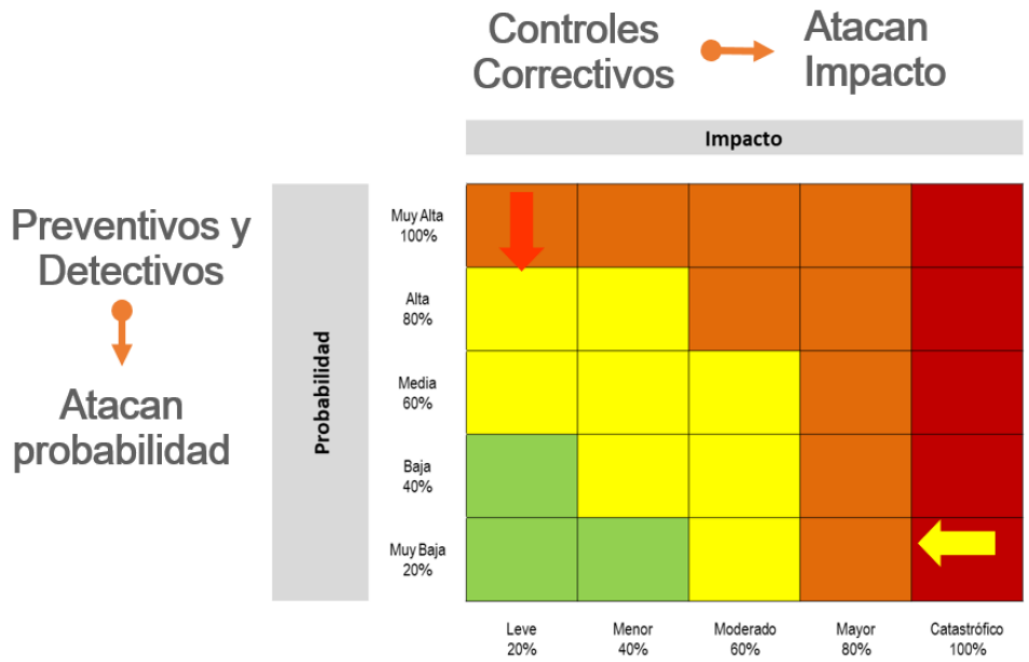
8.6 Análisis y evaluación de los controles

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así.

Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio 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.	-

Características			Descripción	Peso
		Sin registro	El control no deja registro de la ejecución del control.	-

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



Fuente: Tomado de la Guía para la administración de riesgos y el diseño de controles en entidades públicas V.5.

8.7 Nivel de Riesgo (Riesgo Residual).

El riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control ***(Ver. Guía para la administración de riesgos y el diseño de controles en entidades públicas V.5. Apartado 3.2.3.)***

9. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas tanto internas como externas debe desarrollarse durante todas las etapas del proceso para la gestión del riesgo.

Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

Así mismo es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.