Política Institucional de Administración de Riesgos Administrativos, de Corrupción, Tecnológicos y Fiscales.

ADELI

EMPRESA INDUSTRIAL Y COMERCIAL DEL ESTADO

Versión 3 Aprobada mediante acta No.2 del Comité Institucional de Coordinación de Control Interno, del 12 de septiembre de 2024.

Tabla de contenido

1. INTRODUCCIÓN

La Política de Administración de Riesgos es un compromiso desde la Alta Dirección de la Agencia de Desarrollo Local de Itagüí-ADELI, frente a la identificación, tratamiento y control de riesgos, a través de un análisis de las estrategias, formulación de objetivos y la gestión de la entidad, con la finalidad de establecer acciones que permitan que permitan evitar la materialización de aquellos sucesos que puedan afectar el cumplimiento de las metas institucionales, manteniendo un enfoque preventivo que permita proteger los recursos, mejorar los resultados y la prestación de los servicios, siempre fomentando la generación de valor público.

A través de la presente política se adopta la metodología presentada por el Departamento Administrativo de la Función Pública, mediante la "Guía para la Administración del riesgo y diseño de controles en entidades públicas" versión 6 de 2022, en donde se asocia un capítulo para el análisis de los riesgos fiscales adaptada a la realidad de la Agencia de Desarrollo Local de Itagüí-ADELI- y se aborda de forma más clara lo referente a riesgos de seguridad, por tanto, integra en su funcionamiento las directrices del Modelo Integrado de Planeación y Gestión-MIPG-; así mismo se continua con los lineamientos de identificación, gestión y tratamiento de las demás tipologías de riesgos que sean aplicables a la entidad.

2. DEFINICIONES

A continuación, se desarrollan algunos conceptos que permiten establecer claridad frente a algunas disposiciones presentadas en la presente política de administración de riegos, dichas definiciones son tomadas de la "Guía para la administración de riesgos y el diseño de controles en entidades públicas", versión No.6 de 2022, emitida por el Departamento Administrativo de la Función Pública:

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
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.
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 Fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como

recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública.

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

a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional.
Ejemplos: Las calles, plazas, puentes, vías, parques etc.
b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.
Activo de Información: Cualquier tipo de elemento que tenga valor para la organización.
Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el 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.
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. OBJETIVO

Establecer lineamientos generales frente a la identificación y valoración de riesgos dentro de la Agencia de Desarrollo Local de Itagüí-ADELI.

4. ALCANCE

La política de administración de riesgos es aplicable a todos los procesos, políticas institucionales y actividades que se desarrollen al interior de la Agencia de Desarrollo Local de Itagüí-ADELI, por parte de cada uno de sus funcionarios, en virtud de sus responsabilidades, los cuales deberán tener en cuenta los lineamientos que aquí se presentan.

5. ROLES Y RESPONSABILIDADES

El Modelo Integrado de Planeación (MIPG) opera a través de siete (7) dimensiones y diecinueve (19) políticas de gestión y desempeño institucional, que trabajan de forma articulada para su funcionamiento y dando paso a un clico de mejora continua, en su séptima dimensión, denominada Control Interno, desarrolla un esquema de líneas de defensa con el fin de identificar los roles y responsabilidades frente a la gestión y control de riesgos a nivel institucional, que se sintetizan a continuación:

Línea Estratégica: Conformada por la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

- ✓ Definen y aprueban el marco general (lineamientos) para la gestión de riesgos, verificando y monitoreando el cumplimiento de las directrices establecidas, así mismo, constituyen las instancias en donde se dirimen cambios al respecto.
- ✓ Instancia para verificar y establecer acciones frente a las desviaciones presentadas en la gestión de riesgos.
- ✓ Sirve como línea de reporte ante la gestión de riesgos.

Primera Línea de Defensa: Conformada por todos los servidores de la Agencia, independiente de su forma de vinculación.

- ✓ Como principales actores durante el desarrollo e implementación de los procesos, son los encargados del análisis del contexto, de la identificación, gestión y tratamiento de riesgos. Así mismo, hacen parte integral en el monitoreo y establecimiento de las acciones de mejora correspondientes.

Segunda Línea de Defensa: Conformada por el Director de Planeación y jefes de área de procesos transversales como la Dirección Administrativa y Financiera, Dirección Jurídica y Operativa y de Proyectos. En general, en adelante todos aquellos cargos que evalúen la gestión de la primera línea se incorporarán a esta línea y que pertenezcan a la media o alta gerencia.

- ✓ Aseguran que los controles, acciones y el proceso de gestión de riesgos identificados e implementados por la primera línea de defensa sean apropiados y funcionen de forma correcta. Así mismo, tienen a su cargo el acompañamiento, asesoría metodológica y monitoreo en la gestión de los riesgos, así como la consolidación de estos para que sean evaluados por la tercera línea de defensa y publicados en el caso de los requerimientos de ley.

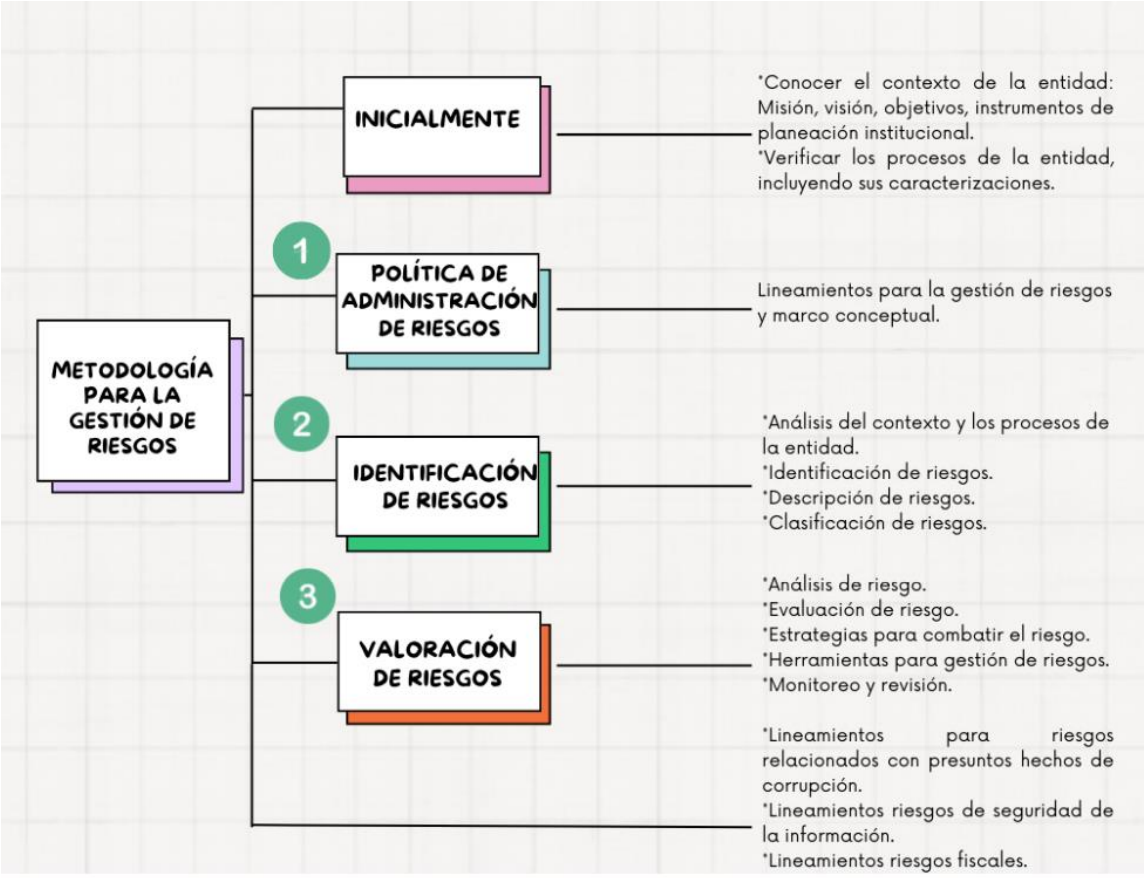
Tercera Línea de Defensa: A cargo de la Oficina de Control Interno o quien haga sus veces, tiene dentro de sus responsabilidades:

- ✓ Evalúa y hace seguimiento a la efectividad en la gestión de los riesgos (identificación, gestión, monitoreo y seguimiento), así mismo, proporciona información que permita establecer el funcionamiento y aplicación del Sistema de Control Interno, mediante un enfoque basado en riesgos en el cual se incluya la operación efectuada desde la primera y segunda línea de defensa.
- ✓ Posee un rol de asesoría técnica frente a la gestión de riesgos, y junto a la Dirección de Planeación proporcionan condiciones en la materia para ayudar al logro de los objetivos institucionales.
- ✓ Realiza las recomendaciones respecto a la gestión de los riesgos, puesto que posee un carácter evaluador, incluyendo proactividad en el asesoramiento de la Alta Dirección.

6. GESTIÓN DE RIESGOS

Para la gestión de riesgos de la ADELI, se establece como metodología la propuesta a través de la “Guía de Administración del Riesgos y el diseño de controles en entidades públicas” en su versión 6, y la cual se representa en la figura 1:

Figura 1 Metodología de administración de riesgos



Fuente: Elaboración propia con datos de la “Guía para la Administración del riesgo y diseño de controles en entidades públicas”, en su versión 6 de 2022.

En ella se define como paso previo e inicial, el conocimiento y reconocimiento del contexto institucional y aquello que la compone: misión, visión, objetivos estratégicos, planes e instrumentos que permiten alcanzar las metas trazadas; así mismo, su estructura y forma de operación. Posteriormente, y partiendo de este insumo inicial, se desarrollan una serie de pasos para la valoración de riesgos, y finalmente se establecen condiciones para el análisis de relacionados con presuntos hechos de corrupción, seguridad de la información y como nueva incorporación, lo referente a riesgos de tipo fiscal.

6.1. Paso 1: Política de Administración de riesgos

La Agencia de Desarrollo Local de Itagüí-ADELI, a través de la Alta Dirección genera un compromiso con el cumplimiento de los objetivos estratégicos, para ello define una serie de lineamientos con carácter preventivo, que cobija a todos los niveles de operación y cada uno de los procesos.

A partir del análisis respectivo se establece una metodología para la gestión integral de riesgos en materia de:

- Operación de procesos, que puedan afectar el cumplimiento de objetivos y metas institucionales.
- Riesgos frente a posibles hechos de corrupción, que bajo el carácter del servicio público se considera inadmisible.
- Riesgos en materia de seguridad de la información, con una gestión que procure la protección de la información derivada de la operación de procesos institucionales.
- Riesgos fiscales, que procuren la protección del recurso público.

Su revisión y actualización dependerá de los lineamientos que en la materia emita el Departamento Administrativo de la Función Pública.

6.2. Paso 2: Identificación

De forma inicial se debe efectuar una identificación de los riesgos que estén asociados a la entidad, para lo cual se debe tener claridad frente al contexto estratégico en el que opera, los procesos establecidos para el cumplimiento de sus objetivos y la caracterización de estos. Dentro del análisis del contexto se deben tener presente todos aquellos factores internos y externos que puedan generar alguna desviación o incumplimiento a alguno de los objetivos organizacionales.
Algunos elementos adicionales a tener en cuentan durante el proceso de identificación son los siguientes:

- ✓ Análisis de los objetivos estratégicos y de los procesos.
- ✓ Identificación de puntos críticos dentro de la operación de los procesos.
- ✓ Identificar áreas de impacto (económica o reputacional) en caso de materialización de algún riesgo.
- ✓ Identificar áreas generadoras de riesgos: procesos, infraestructura, talento humano, todo evento externo (obras).

Para los riesgos de corrupción también se debe hacer la identificación a aquellos procesos, procedimientos o actividades susceptibles a ellos.

Las identificaciones para los riesgos de seguridad de la información deberán partir del análisis de los activos de información: Aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de la información TI o tecnologías de operación que utilice la entidad. Para ello se requerirá de un inventario que facilite el proceso. Así mismo, su riesgo inherente estará asociado a:

- Pérdida de confidencialidad.
- Perdida de integridad de la información.
- Perdida de la disponibilidad de la información.

Cada riesgo deberá estar asociado a un activo de información, con la finalidad de analizar las amenazas o vulnerabilidades que lo rodea tal y como se presenta el ejemplo la tabla 1.

Tabla 1 Amenazas y vulnerabilidades según activo de información

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso

Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

La gestión respecto al tipo de riesgo de seguridad de la información incluirá o solo lo correspondiente a la lo determinado en la política institucional, si no, lo correspondiente a los lineamientos determinados a través del *Modelo nacional de gestión de riesgos de la seguridad de la información,* y estarán asociados en el *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.*

En cuanto a los riesgos de tipo fiscal se requiere establecer los puntos de riesgos fiscal, que corresponden a las actividades que potencialmente pueden originarlos. Estas pueden corresponder a administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, adjudicación, gasto, inversión y disposición de bienes de recursos públicos. Dentro de estos pueden incluirse todas aquellas actividades para las cuales exista alguna alerta, hallazgo o fallo de responsabilidad fiscal.

Así mismo, para el riesgo fiscal se hace necesario identificar las causas inmediatas, que al igual que en análisis para los otros tipos de riesgo, se asocia a la razón por

la cual se desarrolla el riesgo.

6.2.1. Descripción del riesgo

Debe contener elementos que permitan detallar claramente y que sean comprensibles para cualquier persona que pertenezca al proceso como aquellos que no. El DAFT a partir de una adaptación del curso operativo de la Universidad del Rosario (2020), propone una estructura para su redacción, que contiene los siguientes aspectos:

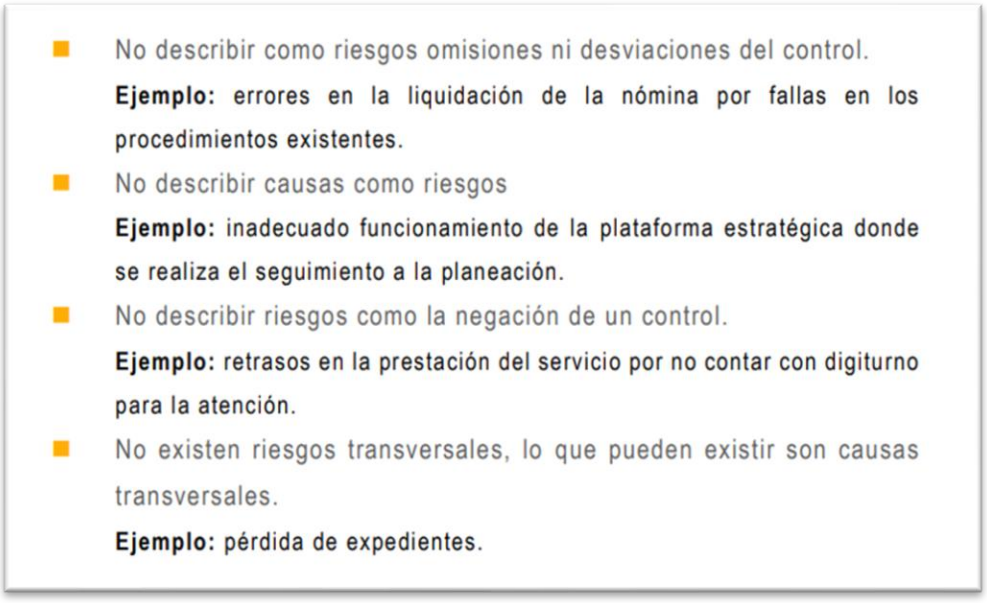
RIESGO= IMPACTO+CAUSA INMEDIATA+CAUSA RAÍZ

En esta ecuación:

- El impacto determina el ¿qué?, y señala las consecuencias que puede ocasionar para la entidad la materialización del riesgo.
- La causa inmediata el ¿cómo?, que no es más que las situaciones más evidentes sobre las cuales se presenta el riesgo detectado. No representa precisamente la causa raíz. La causa raíz corresponde al ¿por qué?, y, corresponde la causa principal o razón por la cual se presenta el riesgo identificado, justamente los controles que se establezcan entran a atacarla. Y pueden corresponder a más de una.

Al respecto pueden existir algunas premisas, definidas en la figura 2, que pueden ayudar a definir y describir riesgos con mayor precisión.

Figura 2 Premisas sobre riesgos



Fuente: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

Respecto a los riesgos de corrupción dentro de su descripción se deben tener presentes los componentes de su definición: ACCIÓN U OMISIÓN+USO DE PODER+DESVIACIÓN DE LA GESTIÓN PÚBLICA+EL BENEFICIO PRIVADO.

En materia de riesgos fiscales, se continua el análisis de los tres elementos para la descripción de un riesgo, teniendo en cuenta que, el efecto dañoso será sobre bienes públicos, recursos públicos o intereses patrimoniales de naturaleza pública, conceptos que se desarrollan en el punto 2 del presente documento, así mismo, se debe tener en presente:

- Iniciar la oración con: Posibilidad de.
- El impacto hace referencia al efecto dañoso3 sobre el bien público, recurso público o interés patrimonial de naturaleza pública.
- La circunstancia inmediata corresponde a la situación que origina el riesgo.
- La causa raíz corresponde al hecho generador del riesgo, si este hecho no se produce, el daño no se genera. Es la acción u omisión que de presentarse provocaría la pérdida o detrimento.

6.2.2. Clasificación de riesgos

Con la finalidad de facilitar la agrupación de diversos riesgos identificados según su

fuente, el DAFP propone una serie de categorías que se relacionan a continuación:

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: Elaboración propia con datos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

6.3. Paso 3: Valoración de Riesgos

La valoración de riesgos corresponde a un proceso posterior a la identificación de estos; consiste en el establecimiento de la probabilidad de ocurrencia y su impacto o consecuencias iniciales, en caso de su materialización y sin ningún tipo de tratamiento (riesgo inherente), y posteriormente, luego de un análisis se definen una serie de controles que permiten mitigar alguno de los dos aspectos y obtener un estado de riesgo final (riesgo residual).

Al respecto, se desarrollan a detalle cada uno de los elementos constitutivos de la

valoración de riesgos:

6.3.1. Probabilidad:

En este punto se desea establecer la probabilidad de ocurrencia del riesgo identificado, que no es más que la posibilidad de que se materialice.

Para efectos prácticos la probabilidad estará asociada a la exposición del riesgo que tiene la actividad o hecho que se está analizando. Así, la probabilidad inherente será el número de veces que se efectúe la actividad dentro de un periodo de tiempo. De esta forma, las actividades o acciones que se ejecutan de forma constante, tendrán un riesgo mayor, frente a aquellas con una frecuencia menor.

Bajo el análisis y ejecución de los procesos de la entidad, se presentan los criterios para definir la probabilidad dentro de ADELI:

Tabla 3 Análisis de probabilidad.

	Frecuencia de la Actividad	Nivel	Probabilidad
Muy baja	La actividad que origina el riesgo se ejecuta 1 vez al año.	1	20%
Baja	La actividad que origina el riesgo se ejecuta como máximo 2 veces al año	2	40%
Media	La actividad que origina el riesgo se ejecuta entre 12 y 24 veces al año.	3	60%
Alta	La actividad que origina el riesgo se ejecuta entre 24 y 240 veces en un año (o al menos 1 vez en un día hábil).	4	80%
Muy Alta	La actividad que origina el riesgo se ejecuta más de 240 veces en el año.	5	100%

Fuente: Elaboración propia

Para los riesgos de corrupción se hace necesario aplicar un análisis respecto a la frecuencia y la posibilidad de ocurrencia en alguno de los procesos, tal y como se muestra en la figura 3.

Figura 3 Criterios para calificar probabilidad en riesgos de corrupción

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más 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: Tomado de la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6.

6.3.2. Impacto:

Así mismo, se deben establecer las consecuencias en caso de ocurrencia de alguno de los riesgos identificados, haciendo énfasis en el impacto económico y reputacional como variables principales. Cuando de la evaluación se estime que puede ocurrir tanto el impacto económico como el reputacional, se selecciona aquel cuyo nivel sea mayor en el mapa de calor.

Tabla 4 Análisis de impacto.

Nivel	Afectación Económica	Reputacional
Leve	Afectación menor a 100 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general interno, de junta directiva y/proveedores.

Nivel	Afectación Económica	Reputacional
Moderado	Entre 500 y 2.000 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor	Entre 2.000 y 4.000 SMLMV	El riesgo afecta la imagen de la entidad con el efecto publicitario sostenido a nivel de sector administrativo o municipal.
Catastrófico	Mayor a 4.000 SMLMV	El riesgo afecta la imagen de la entidad a nivel departamental o nacional, con efecto publicitario sostenido a nivel país.

Fuente: Elaboración propia

Cuando se trata de evaluar los riesgos de tipo fiscales, es necesario tener presente que siempre tendrán un impacto económico, toda vez que, existe un efecto dañoso sobre un bien, recurso o interés patrimonial de naturaleza pública.

6.3.3 Impacto en riesgos de corrupción:

Para el caso específico de los riesgos asociados a presuntos actos de corrupción es necesario efectuar la medición del impacto por medio de una serie de criterios diferenciales, a través de una serie de interrogantes que se desarrollan en la figura 4. Aclarando que, en temas de probabilidad se utiliza el mismo análisis descrito en el punto 6.3.1.

Figura 4 Criterios calificación de impacto riesgos de corrupción.

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de 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 pregunta(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	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas V6.2022.

De allí, se evalúa el número de preguntas y sus respuestas, se contabilizan, y según los resultados se determina el nivel de impacto, de acuerdo con la escala que se presenta en la figura anterior.

En el contexto de los riesgos de corrupción no existe impacto leve ni menor, su materialización siempre tendrá consecuencias desde la escala MODERADO,

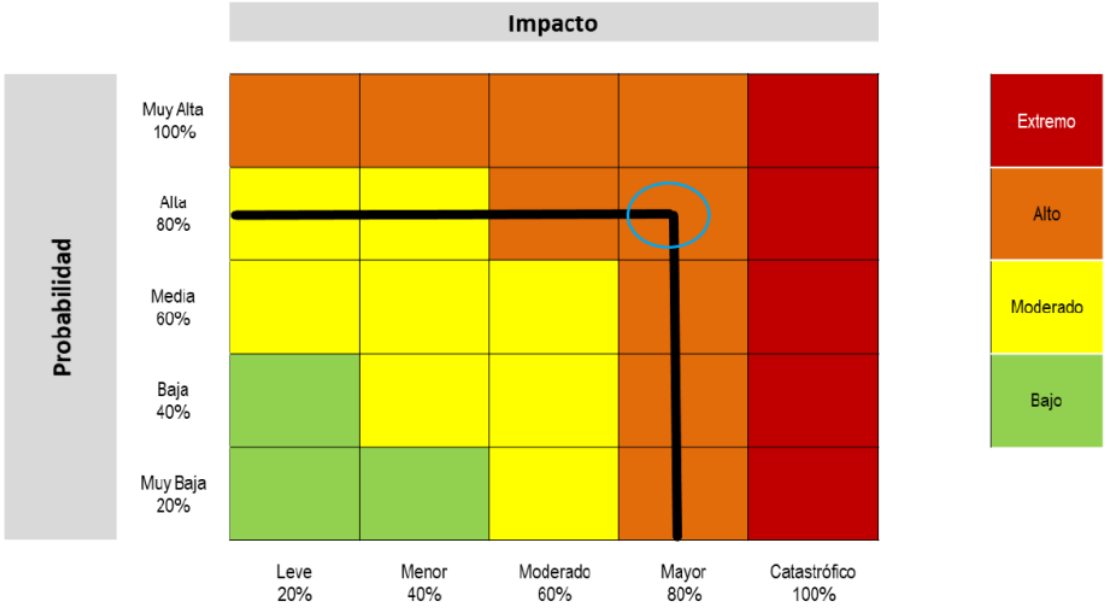
MAYOR Y CATASTRÓFICO.

Así mismo, debe anotarse que, en caso de que la respuesta a la pregunta 16 del análisis del impacto sea positiva, inmediatamente se cuenta con consecuencias CATASTRÓFICAS para la entidad.

6.3.4. Evaluación de riesgos:

La evaluación corresponde a la identificación de la zona inicial dentro del matriz de calor (riesgo inherente), que no es más que el primer análisis del riesgo. Se trata de combinar un nivel de probabilidad e impacto, que cruzadas establecen una de las cuatro zonas dentro de dicha matriz, representada a continuación:

Figura 5 Matriz de calor

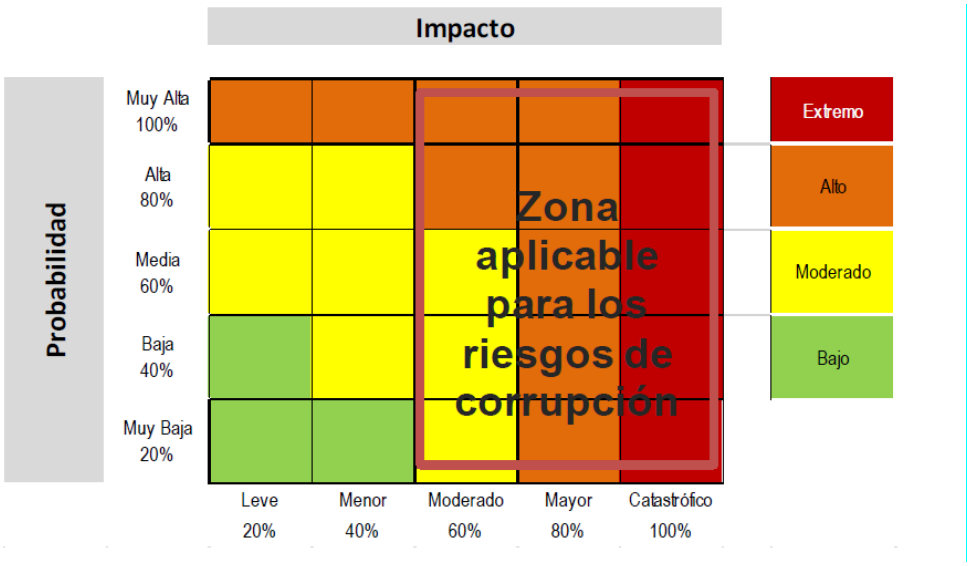


Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 de 2022.

En la figura 5 se muestra la relación de un análisis de riesgo cuya probabilidad es del 80% (alta), y un impacto mayor, del 80%, ambos de forma inicial, lo que genera que su intercepción se ubique en una zona dentro de la matriz de calor alta.

Cabe anotar que, como se mencionó en el apartado 6.3.3, existen restricciones para la valoración del impacto para aquellos riesgos identificados como de presuntos hechos de corrupción, creando zonas dentro de la matriz de calor mucho más reducidas, tal y como se muestra en la figura 6.

Figura 6 Matriz de calor riesgos de corrupción.



Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 6 de 2022.

6.3.5. Definición de controles:

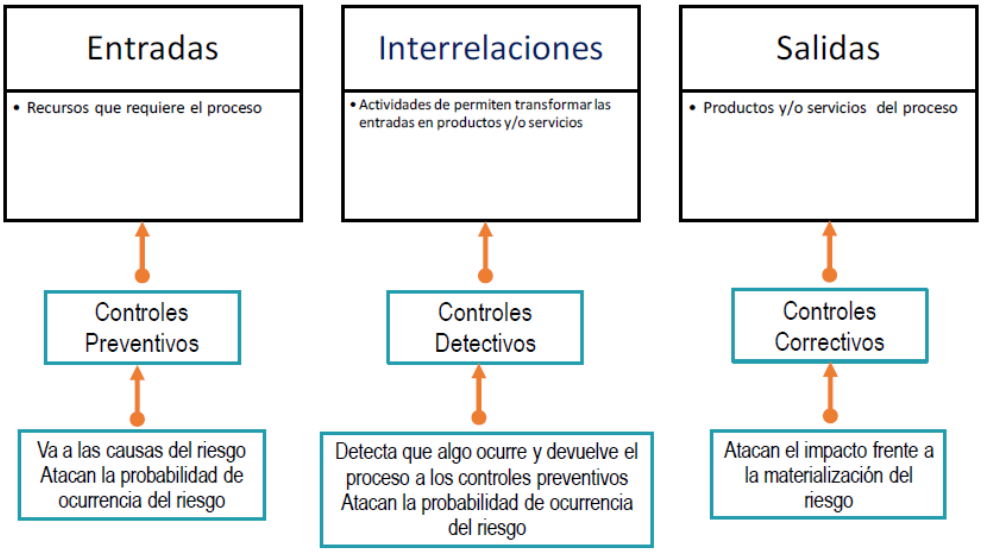
Definido como las medidas que se adoptan y que permiten reducir o mitigar el riesgo. Para su valoración es necesario revisar y realizar su construcción con cada uno de los líderes de procesos y servidores en general (Guía administración del riesgo V6, 2022, pag.45).

Para la descripción de los controles se sugiere que, en su estructura se identifique el responsable de ejecutarlo, la acción a realizar y un complemento que dé coherencia y su objeto.

6.3.5.1. Tipos de controles

Teniendo en cuenta el ciclo de los procesos es posible determinar cuándo se activa y establecer su tipología.

Figura 7 Tipología de controles



Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas V6, 2022.

En la figura 7 se muestra cada una de las tipologías partido de las etapas del ciclo de un proceso. En esta se pueden observar tres tipos: preventivos, detectivos y correctivos.

- Los preventivos se relacionan a las entradas del proceso y están asociados a establecer condiciones antes de que se realice la actividad asociada al origen del riesgo, por su naturaleza atacan la probabilidad que asegure un resultado final.
- Los detectivos son relacionados a las interrelaciones que se desarrollan al interior de los procesos y que permiten transformas en servicios y/o productos. En vista que se asocian a la ocurrencia durante la ejecución, atacan la probabilidad y generan reprocesos al llevar a controles preventivos.
- Los controles de tipo correctivo se asocian a las salidas, es decir, a los productos y/o servicios, y se refieren a aquellos accionados una vez materializado el riesgo, por tanto, no atacan probabilidad sino impacto.

Así mismo, estos controles pueden estar clasificados según la forma de ejecución en:

- Manuales si son ejecutados por personas
- Automáticos si los ejecuta un sistema.

6.3.5.2. Análisis y evaluación de controles

Para generar el análisis de los controles se establecen una serie de atributos que permiten su definición, relacionados su eficiencia, que se desarrollan en la tabla 5.

Tabla 5 atributos para el diseño de controles

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

Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas V6, 2022.

Respecto a los atributos informativos tienen solo la finalidad de dar formalidad y conocimiento respecto al entorno del control, y no tienen incidencia directa sobre su

efectividad.

A partir de la valoración que se le hace al control con el uso de dichos atributos, se puede generar un desplazamiento a través de la matriz de calor, lo ideal sería una reducción en la probabilidad de ocurrencia y/o el impacto, dependiendo del tipo aplicado.

6.3.6 Riesgo Residual:

El riesgo residual es el resultante de la aplicación de los controles, y puede trabajar de forma acumulativa; es decir, en caso que se establezcan varios el resultado de la evaluación de uno será la base para el análisis del siguiente, con ello, entre más controles mayor reducción en la matriz de calor se tendrá.

Para calcularlo se hace necesario el uso de la siguientes formulas:

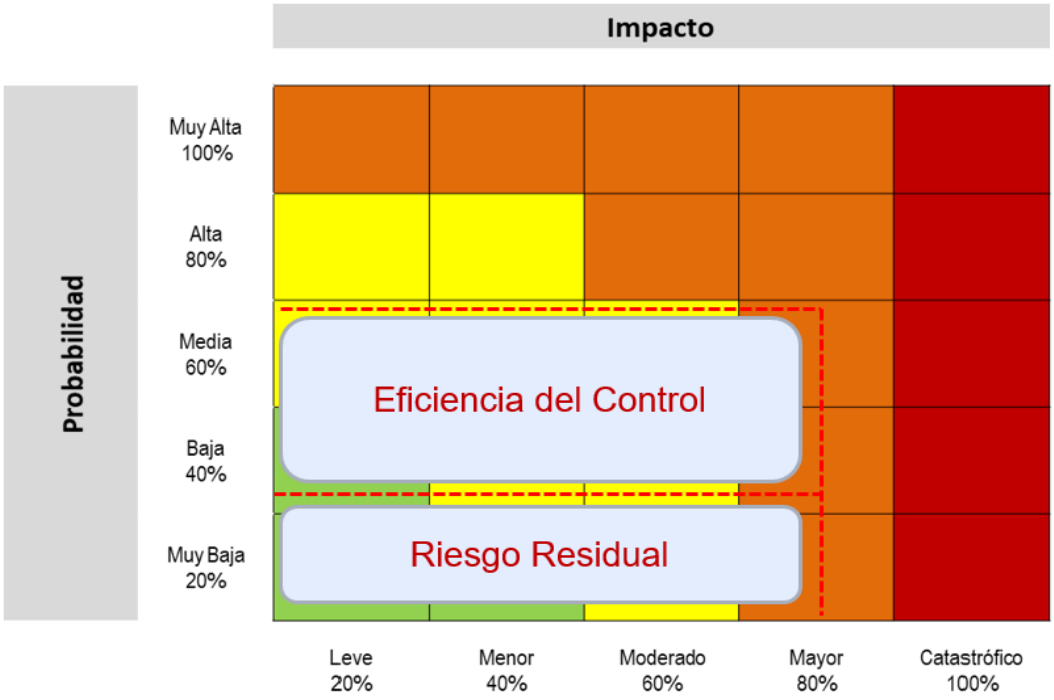
1.	Eficiencia del control=Probabilidad (impacto) inherente (%) *valoración del control (%).
2.	Probabilidad (impacto)residual=Probabilidad(impacto) inherente-Eficiencia del control.

Se debe aclara que:

- Para el tipo de control preventivo y detectivo solo se realiza movimiento sobre la probabilidad, dejando constante el impacto inherente.
- Para el tipo de control correctivo se hace movimientos sobre el impacto dejando constante la probabilidad inherente.
- Las dos aclaraciones anteriores solo pueden ser falsas cuando se combinen controles que ataquen tanto probabilidad como impacto, en cuyo caso habría movimiento en ambos ejes sobre la matriz de calor.
  - De forma inicial se calcula la fórmula 1) y con los resultados obtenidos se procede a utilizar la 2).

Este proceso se puede evidenciar de forma gráfica, a través de la matriz de calor, tal como se aprecia en la figura 8.

Figura 8 Movimiento matriz de calor luego de controles.



Fuente: Tomado de Guía para la administración del riesgo y el diseño de controles en entidades públicas V6.2022.

En esta se puede observar que la eficiencia del control no es más que la reducción en la probabilidad o impacto, causada por la aplicación del control o los controles establecidos, dando como resultado una zona residual. Entre más controles, mayor será la zona de eficiencia.

7. NIVELES DE TRATAMIENTO

De acuerdo con la zona en la que se ubiquen los riesgos después de la aplicación de controles (riesgo residual), se puede llevar a cabo una estrategia para combatirlo, que va desde su reducción a través del traslado del riesgo, por ejemplo, desde una tercerización del proceso, o la mitigación a través de acciones adicionales, pasando por la aceptación del mismo e incluso tomar la decisión de evitar la actividad que lo genera.

Existen varias formas de tratamiento del riesgo residual:

- ACEPTAR EL RIESGO: No Se adopta ninguna medida frente a la probabilidad o impacto residual.

- REDUCIR EL RIESGO: Se adoptan controles para reducir la probabilidad o impacto residual, o ambas.
- EVITAR EL RIESGO: Se abandonan las actividades que originan el riesgo.
- COMPARTI EL RIESGO: Se transfiere o comparte parte del riesgo. Por lo general, se comparte el riesgo, pero no la responsabilidad.

A partir de lo anterior, se establece unos niveles de aceptación general para la Agencia, descritos en la tabla 6:

Tabla 6 Aceptación del riesgo

NIVEL	NIVEL DE ACEPTACIÓN	SEGUIMIENTO
EXTREMO	No se acepta	Cuatrimestral
ALTO		Cuatrimestral
MODERADO		Cuatrimestral
BAJO	Aceptable	Cuatrimestral

Fuente: Elaboración propia

Nivel de riesgo BAJO: Sí posterior al establecimiento de controles el valor residual se ubica en zona baja, se puede contemplar el ACEPTAR el riesgo, siempre que medie un análisis al respecto, por tanto, no requerirá acciones adicionales.

Nivel de riesgo MODERADO, ALTO o EXTREMO: Para los casos en los cuales luego de la aplicación de controles la zona residual este entre MODERADO A EXTREMO, se deberá procurar combatir a través de estrategias de EVITAR, REDUCIR O COMPARTIE, prevaleciendo la segunda. Solo en casos de un análisis profundo y bajo acuerdos con la alta dirección podrá asumirse evitar la actividad riesgosa. En el caso de tomar como decisión la de REDUCIR EL RIESGO, se deberán establecer acciones adicionales.

Respecto a los riesgos asociados a posibles hechos de corrupción no es admisible la opción de ACEPTAR.

8. SEGUIMIENTO

La periodicidad de seguimiento será cuatrimestral, excepto que por argumento significativo se deba hacer lo contrario, este se llevará a cabo según las disposiciones y responsabilidades de cada línea de defensa.

Todos los riesgos deben ser incluidos en la matriz de riesgos, independiente de su valoración, efectuando el seguimiento respectivo. Anualmente el mapa de riesgos

de la entidad (consolidado de matrices de riesgos por área) debe ser revisado y en caso de requerir actualizado.

Para los riesgos de corrupción los seguimientos realizados por la Oficina de Control Interno de Gestión de forma cuatrimestral deberán ser publicados en la sede electrónica institucional en las siguientes fechas: el primero con corte al 30 de abril se publicará durante los diez (10) primeros días del mes de mayo; el segundo con corte al 31 de agosto durante los diez (10) primeros días del mes de septiembre; el tercero con corte al 31 de diciembre se publica durante los diez (10) primero días del mes de enero.

En caso de materialización de alguno de los riesgos identificados:

- Generar reporte a la Dirección de Planeación y Oficina de Control Interno.
- Revisar y analizar los controles y acciones establecidas, con el fin de verificar su pertinencia y generar las modificaciones necesarias, así como los efectos de su materialización.
- Establecer acciones de mejora que permitan una respuesta rápida y eficaz, con la finalidad de que nuevamente no se materialice.
- Si se refiere a un hecho de corrupción, deberá ser informado a la Alta Dirección; en caso de proceder llevarlo ante la Red Interinstitucional de Transparencia y Lucha Contra la Corrupción-RITA para que determine si amerita escalar a ente competente.

9. COMUNICACIÓN

La política de administración de riesgos debe ser socializada con todos los niveles de la organización, incluyendo el instrumento mediante el cual se generará todo su procesamiento: matriz de riesgos.

La matriz correspondiente debe ser publicada en el sitio web de la entidad, al igual que los seguimientos respectivos a los riesgos de corrupción, según lo estipule los términos de ley o las entidades competentes.

10. CONTROL DE CAMBIOS

Versión	Observación
Versión 01 de febrero de 2018.	Creación del documento
Versión 2 de mayo	Se incorporan elementos para la identificación de

de 2021	riesgos. Se genera un cambio en la metodología de la valoración de los riesgos. Se incorporan elementos detallados sobre el tipo de controles y los niveles de tratamiento de los riesgos. Se incorporan elementos para el monitoreo según las líneas de defensa. Se incorporan nuevas tipologías de riesgos.
Versión 3 de abril de 2024.	Se incorporan nuevos conceptos respecto a riesgos de seguridad digital y fiscales. Se cambia el objetivo de la política institucional. Se incorporan cambios frente a la identificación de riesgos, incluyendo los relacionados con seguridad digital y riesgos fiscales. Se especifican las tipologías de riesgos. Se agrega la gestión de riesgos fiscales y se hacen aclaraciones frente a riesgos de seguridad de la información. Se modifica los niveles para la valoración de probabilidad.

11. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6. https://www.funcionpublica.gov.co/.