



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026

Versión: 1

Fecha de elaboración: 05/11/2020

Fecha de revisión:

Página: Página 1 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

# POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

## RED SALUD ARMENIA ESE

### 2021



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026
Versión: 1
Fecha de elaboración: 05/11/2020
Fecha de revisión:
Página: <b>Página 2 de 72</b>

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

## Contenido

INTRODUCCIÓN.....	4
JUSTIFICACIÓN.....	4
OBJETIVO DE LA POLÍTICA .....	5
ALCANCE .....	5
GLOSARIO .....	5
FUNCIONALIDAD DE LA ADMINISTRACIÓN DEL RIESGO .....	8
METODOLOGÍA.....	8
PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS.....	10
LINEAMIENTOS DE LA POLÍTICA DE RIESGOS: .....	10
1.2 MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO: .....	11
1.3 DETERMINACIÓN DEL APETITO DE RIESGO .....	13
1.4 TOLERANCIA DE RIESGO .....	13
PASO 2: IDENTIFICACIÓN DEL RIESGO .....	13
2.1 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS: .....	14
2.2 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGO: .....	14
2.3 IDENTIFICACIÓN DE ÁREAS DE IMPACTO:.....	15
2.4 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO:.....	15
2.5 DESCRIPCIÓN DEL RIESGO: .....	17
2.5.1 Estructura propuesta para la redacción del riesgo.....	17
2.6 CLASIFICACIÓN DEL RIESGO:.....	20
PASO 3: VALORACIÓN DEL RIESGO .....	21
3.1 ANÁLISIS DE RIESGOS: .....	22
Tabla de Criterios para definir el nivel de impacto.....	25
3.2 EVALUACIÓN DE RIESGOS: .....	27
3.2.1 Análisis preliminar (riesgo inherente):.....	27
Matriz de calor (niveles de severidad del riesgo) .....	28
3.2.2 Valoración de controles: .....	29
3.2.2.2 Tipología de controles y los procesos: .....	30
Figura Ciclo del proceso y las tipologías de controles .....	31
<b>3.2.2.3 Análisis y evaluación de los controles – Atributos:</b> .....	32
Tabla de Atributos de para el diseño del control.....	32
Controles identificados:.....	35
Tabla de Aplicación tabla atributos a ejemplo propuesto .....	36

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 3 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

3.2.3 Nivel de riesgo (riesgo residual): .....	37
PARTE 2 VALORACIÓN DEL RIESGO: .....	40
PARTE 3 PLANES DE ACCIÓN (PARA LA OPCIÓN DE TRATAMIENTO REDUCIR):.....	41
3.3 Estrategias para combatir el riesgo:.....	41
Figura de Estrategias para combatir el riesgo .....	42
<b>3.4.2 Indicadores clave de riesgo:</b> .....	43
Tabla de Ejemplos indicadores clave de riesgo .....	44
3.5 MONITOREO Y REVISIÓN: .....	45
4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN .....	46
GESTIÓN RIESGOS DE CORRUPCIÓN .....	58
5. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN .....	59
Figura Conceptualización activos de información.....	60
5.2. IDENTIFICACIÓN DEL RIESGO:.....	61
5.3. VALORACIÓN DEL RIESGO: .....	64
5.4 CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN .....	68
BIBLIOGRAFÍA.....	71
ANEXOS.....	72

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 4 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## INTRODUCCIÓN

Red Salud Armenia ESE, actualiza la política de administración del riesgo, tomando como base los parámetros establecidos en el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema Obligatorio de Garantía de la Calidad y la adopción de la “Guía para la administración del riesgo y el diseño de controles en entidades públicas” de la Función Pública, versión 5 de 2020.

Por lo anteriormente descrito, Red Salud Armenia ESE, se acoge a la metodología de la Función Pública para la administración del riesgo y diseño de controles, estableciendo lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos identificados.

### INTENCIÓN DE LA DIRECCIÓN CON ESTA POLÍTICA

Mediante una adecuada administración de los riesgos, la Alta Dirección pretende alcanzar los mejores niveles de conocimiento respecto a la gestión de estos en la entidad, elevar la productividad y garantizar la eficiencia y la eficacia de los procesos organizacionales.

## JUSTIFICACIÓN

Con la entrada en vigencia del Modelo Integrado de Planeación y Gestión, (MIPG), que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el sistema de control interno, por lo cual, se hace evidente la importancia de aplicar controles que permitan, a través de las herramientas disponibles por la Función Pública y el Ministerio de Salud y Protección Social, tanto para el manejo de los riesgos, como para su control en todos los niveles de la organización, brindar una seguridad razonable frente al logro de los objetivos, utilizando para ello un enfoque preventivo que permita la identificación y tratamiento de cada uno de los riesgos.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 5 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## OBJETIVO DE LA POLÍTICA

Orientar a la Alta Dirección en la toma de decisiones oportunas al interior de la ESE, mediante la aplicación de acciones y controles orientados a la reducción de la probabilidad de la ocurrencia del riesgo o a la mitigación del impacto negativo del evento, al interior de cada uno de los procesos y subprocesos de Red Salud Armenia ESE.

## ALCANCE

La Política de Administración del Riesgo y Diseño de los Controles Institucionales es aplicable a todos los procesos, subprocesos y proyectos de la ESE y a todas las acciones ejecutadas por los servidores públicos, contratistas y trabajadores en misión durante el ejercicio de sus funciones, en representación de la Entidad y/o actividades a cargo. Red Salud Armenia ESE mantiene los canales de información apropiados para garantizar un adecuado conocimiento y gestión de los riesgos.

## GLOSARIO<sup>1</sup>

**Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

**Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

**Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede

<sup>1</sup> Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 6 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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.

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

**Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

**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.

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

**Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

**Factores de Riesgo:** Son las fuentes generadoras de riesgos.

**Integridad:** Propiedad de exactitud y completitud.

**Impacto:** las consecuencias que puede ocasionar a la organización la materialización 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 poder ser Probabilidad \* Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 7 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

**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.

**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.

**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.

**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.

**Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

**Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 8 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

ser explotada por una o más amenazas.

## FUNCIONALIDAD DE LA ADMINISTRACIÓN DEL RIESGO

La administración del riesgo es un proceso dinámico interactivo continuo, lógico y sistemático desarrollado en cada proceso en coordinación con el área de Planeación y el acompañamiento y asesoría de la oficina de Control Interno. Los riesgos de gestión y de corrupción identificados en los mapas de riesgos por proceso y en el mapa de riesgos de corrupción se consolidarán anualmente y se publicarán en la página web de la ESE para su consulta permanente.

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- ✓ Apoyo a la toma de decisiones.
- ✓ Garantizar la operación normal de la organización.
- ✓ Minimizar la probabilidad e impacto de los riesgos.
- ✓ Fortalecimiento de la cultura de control de la organización.
- ✓ Incrementar la capacidad de la entidad para alcanzar sus objetivos.
- ✓ Dotar a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente.

## METODOLOGÍA

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, el conocimiento de esta desde un punto de vista estratégico de la aplicación de pasos básicos para su desarrollo y de la definición e implantación de estrategias de comunicación transversales a toda la entidad, para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 9 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

- Paso 1, Política de Administración del Riesgo, mantiene los lineamientos, teniendo en cuenta que se trata de un paso esencial en cabeza de la alta dirección de la entidad, en tanto se constituye en la base para la gestión del riesgo en todos los niveles organizacionales.

- Paso 2, Identificación del riesgo, se propone una estructura para la redacción adecuada del riesgo, lo que facilita el análisis de la causa raíz y se proponen una serie de premisas básicas para evitar errores o generalizaciones del riesgo que dificultan la aplicación de los pasos siguientes definidos en la metodología. En este mismo apartado se precisan los factores de riesgo y su relación con las tipologías de riesgo.

- En el paso 3, valoración del riesgo, se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad, en este apartado se propone la tabla para el análisis de probabilidad con un enfoque en la exposición al riesgo, análisis que le permite a los líderes de proceso contar con elementos objetivos para su definición; en cuanto a la tabla de impacto, se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos, en tal sentido, se ajusta la matriz de calor de acuerdo con la escala de severidad definida en 5 zonas (baja, moderada, alta y extrema), elementos que, en su conjunto, plantean un análisis más ácido, es decir de mayor profundidad y estricto, teniendo en cuenta el entorno cambiante en el cual se desenvuelven las entidades públicas del país.

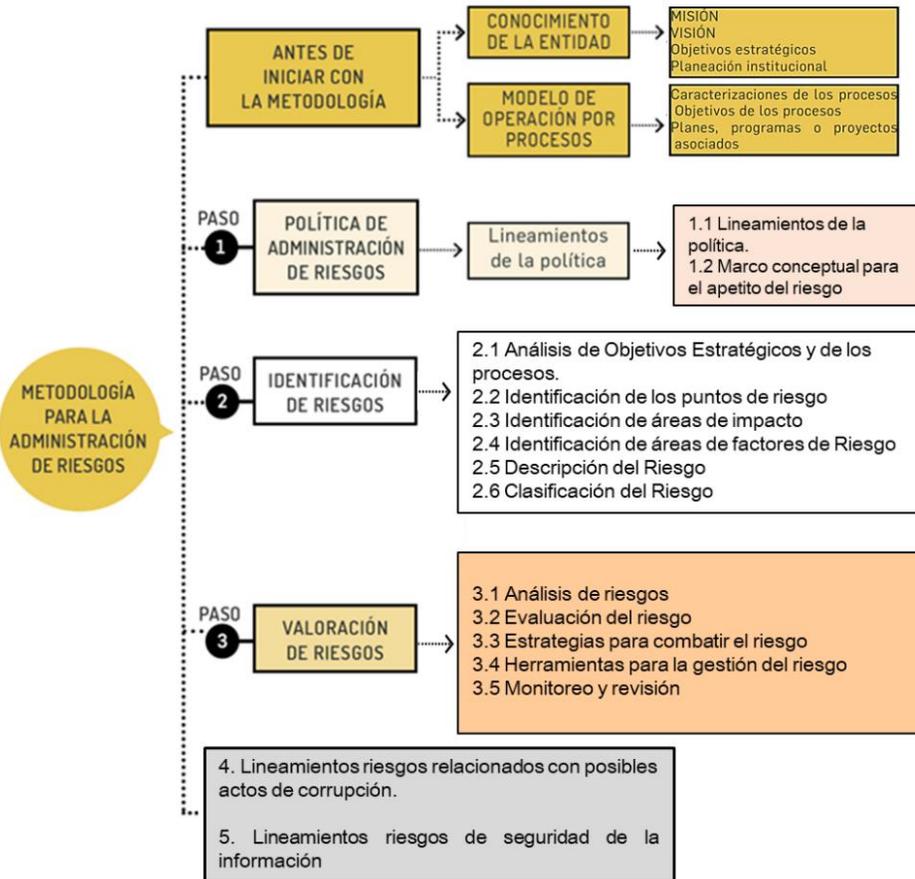
Se incluye al final, en los anexos una matriz propuesta para la construcción del mapa de riesgos, se actualiza el Anexo 4: Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas del Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) y se mantiene 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.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: Página 10 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

## PASO 1: POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

### LINEAMIENTOS DE LA POLÍTICA DE RIESGOS:

Estructuración de la política de administración de riesgos



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026
Versión: 1
Fecha de elaboración: 05/11/2020
Fecha de revisión:
Página: <b>Página 11 de 72</b>

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

**¿QUÉ ES?**

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

**¿QUIÉN LA ESTABLECE?**

La Alta Dirección de la entidad  
Con el liderazgo del representante legal  
Con la participación del Comité Institucional de Coordinación de Control Interno

**POLÍTICA DE ADMINISTRACIÓN DE RIESGOS**

**¿QUÉ SE DEBE TENER EN CUENTA?**

Objetivos estratégicos de la entidad  
Niveles de responsabilidad frente al manejo de riesgos  
Mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad

**¿QUÉ DEBE CONTENER?**

<b>Objetivo:</b>	Se debe establecer su alineación con los objetivos estratégicos de la entidad y gestionar los riesgos a un nivel aceptable.
<b>Alcance:</b>	La administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información (ver caja de herramientas)
<b>Niveles de aceptación al riesgo:</b>	Decisión informada de tomar un riesgo particular (NTC GTC137, Numeral 3.7.1.6). Para riesgo de corrupción es inaceptable.
<b>Niveles para calificar el impacto:</b>	Esta tabla de análisis variará de acuerdo con la complejidad de cada entidad, será necesario considerar el sector al que pertenece (riesgo de la operación, los recursos humanos y físicos con los que cuenta, su capacidad financiera, usuarios a los que atiende, entre otros aspectos).
<b>Tratamiento de riesgos:</b>	Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1.).
Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual.	

Los lineamientos son la declaración de la Gerencia y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

**1.2 MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO:**

Teniendo en cuenta que dentro de los lineamientos para la política de administración del riesgo se debe considerar el apetito del riesgo, a continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis en cada una de las entidades, iniciando con las siguientes definiciones:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>12</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

- ✓ 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.
- ✓ Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- ✓ Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- ✓ Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Determinación de la capacidad de riesgo.

La entidad aplica los valores de probabilidad e impacto y debe determinar, con la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

- a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la entidad, puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos.

Este valor se denomina “capacidad de riesgo”. De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>13</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### 1.3 DETERMINACIÓN DEL APETITO DE RIESGO

Luego de determinada la capacidad de riesgo por parte de la alta dirección, estas mismas instancias deben determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Este valor se denomina “apetito de riesgo”, dado que equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

### 1.4 TOLERANCIA DE RIESGO

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo. El límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

### PASO 2: 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:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>14</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## 2.1 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.

Análisis de objetivos estratégicos	Análisis de los objetivos de proceso
<p>La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.</p> <p>Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).</p>	<p>Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.</p> <p>A continuación encontrará un ejemplo de análisis en el proceso de contratación:</p> <p>La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.</p>

Fuente: Comité of Sponsoring Organizations of the Treadway Commission COSO Marco Integrado, Componente Evaluación de Riesgos, Principio. p. 73. 2013.

La ESE debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desglose hacia los objetivos de los procesos.

## 2.2 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.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>15</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## CADENA DE VALOR PÚBLICO



### 2.3 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.

### 2.4 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO:

Son las fuentes generadoras de riesgos. Se anexa un listado con ejemplo de factores de riesgo que puede tener una entidad.

A continuación, se presenta un formato con la identificación de factores de riesgo. La ESE analizará los que considere pertinente con su complejidad y otros aspectos que puedan permitir el análisis del contexto, e incluirlos como temas clave dentro de los lineamientos de la política de administración del riesgo.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: Página **16** de **72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 17 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

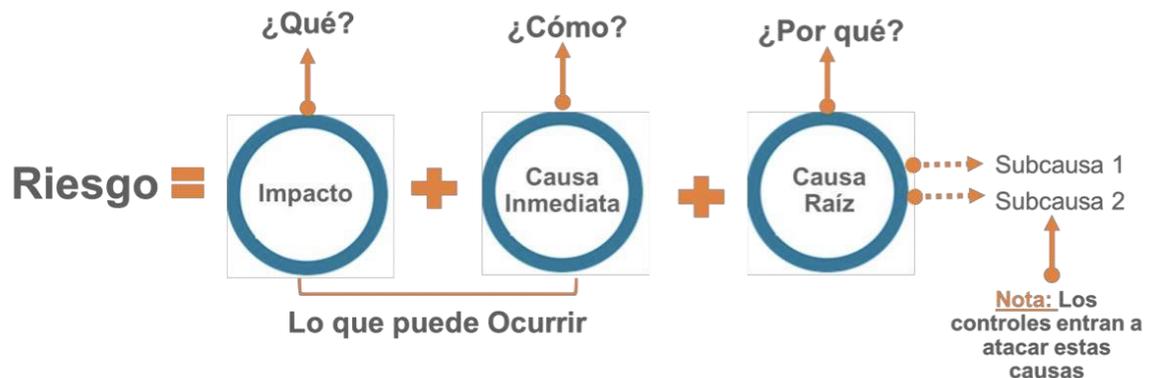
Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

## 2.5 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. Se presenta una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

### 2.5.1 Estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>18</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **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:**

**Proceso:**

Gestión de recursos

**Objetivo:** adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.

**Alcance:** inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquirentes) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, se tiene:

Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>19</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### Redacción inicia con:

Posibilidad de

¿Qué?

afectación económica

**Impacto**

¿Cómo?

por multa y sanción del ente regulador

**Causa Inmediata**

¿Por qué?

debido a adquisición de bienes y servicios fuera de los requerimientos normativos

**Causa Raíz**

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**Premisas para una adecuada redacción del riesgo**

No describir como riesgos omisiones ni desviaciones del control. **Ejemplo:** errores en la liquidación de la nómina por fallas en los procedimientos existentes.

No describir causas como riesgos

**Ejemplo:** inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

No describir riesgos como la negación de un control. **Ejemplo:** retrasos en la prestación del servicio por no contar con digiturno para la

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>20</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

atención.

No existen riesgos transversales, lo que pueden existir son causas transversales.

**Ejemplo:** pérdida de expedientes.

Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes.

## 2.6 CLASIFICACIÓN DEL RIESGO:

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

<b>Ejecución y administración de procesos</b>	Pérdidas derivadas de errores en la ejecución y administración de procesos.
<b>Fraude externo</b>	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
<b>Fraude interno</b>	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.
<b>Fallas tecnológicas</b>	Errores en <i>hardware</i> , <i>software</i> , telecomunicaciones, interrupción de servicios básicos.
<b>Relaciones laborales</b>	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.
<b>Usuarios, productos y prácticas</b>	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
<b>Daños a activos fijos/ eventos externos</b>	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 21 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Teniendo en cuenta que se definieron una serie de factores generadores de riesgo, para poder definir la clasificación de riesgos, su interrelación es la siguiente:

Relación ente factores de riesgo y clasificación del riesgo

<b>Clasificación Factores de Riesgo</b>	
<b>Ejecución y Administración de Procesos</b>	<b>Procesos</b>
<b>Fraude externo</b>	<b>Evento externo</b>
<b>Fraude interno</b>	<b>Talento humano</b>
<b>Fallas tecnológicas</b>	<b>Tecnología</b>
<b>Relaciones laborales</b>	
<b>Usuarios, productos y practicas</b>	
<b>Daños a activos fijos</b>	<b>Infraestructura</b>
	<b>Evento externo</b>

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

### **PASO 3: VALORACIÓN DEL RIESGO**

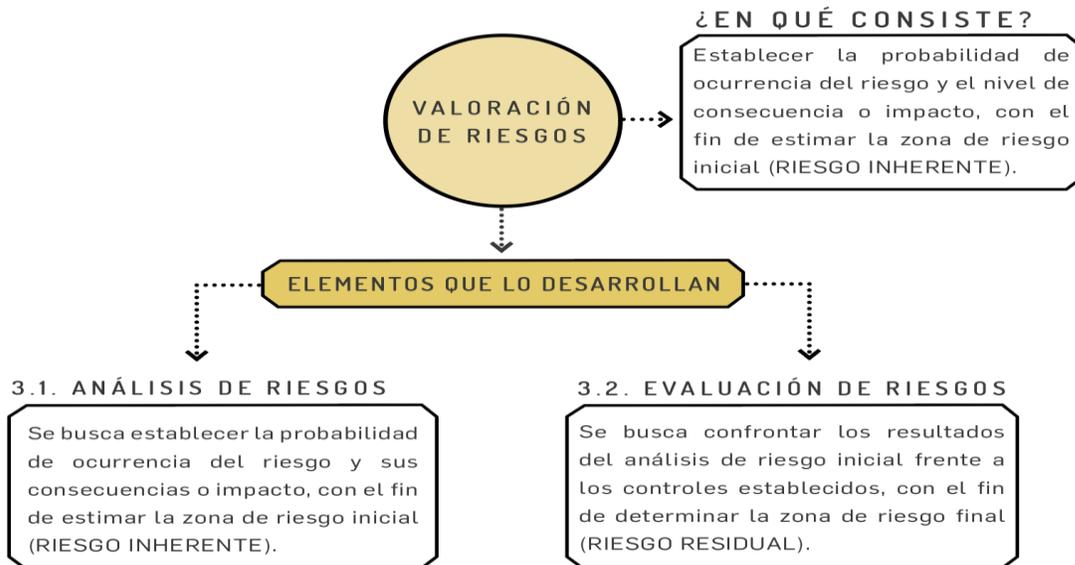
Estructura para el desarrollo de la valoración del riesgo



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
Versión: 1  
Fecha de elaboración: 05/11/2020  
Fecha de revisión:  
Página: Página 22 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018

### 3.1 ANÁLISIS DE RIESGOS:

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

#### 3.1.1 Determinar la probabilidad:

Se entiende como la posibilidad de ocurrencia del riesgo.

Para efectos de este análisis, 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.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos,

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 23 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de las entidades públicas colombianas.

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Tabla de Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
<p><b>*Tecnología (incluye disponibilidad de aplicativos), tesorería</b></p> <p><b>*Nota:</b> En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez.</p> <p>Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.</p>	Diaria	Muy alta

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>24</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, 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 4 se establecen los criterios para definir el nivel de probabilidad.

### Tabla de Criterios para definir el nivel de probabilidad

	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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

#### 3.1.2 Determinar el impacto:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacional 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

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>25</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

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

### Tabla de Criterios para definir el nivel de impacto

	Afectación Económica	Reputacional
Leve 20%	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.
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 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 publicitario sostenido a nivel país

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>26</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### IMPORTANTE:

Frente al análisis de probabilidad e impacto **no se utiliza criterio experto**, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuantas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

Ejemplo:

**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.

No. 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:



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: **Página 27 de 72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

	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%

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

	Afectación Económica	Reputacional
Leve 20%	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.
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 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 publicitario sostenido a nivel país

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

**Probabilidad inherente= media 60%, Impacto inherente: mayor 80%**

### 3.2 EVALUACIÓN DE RIESGOS:

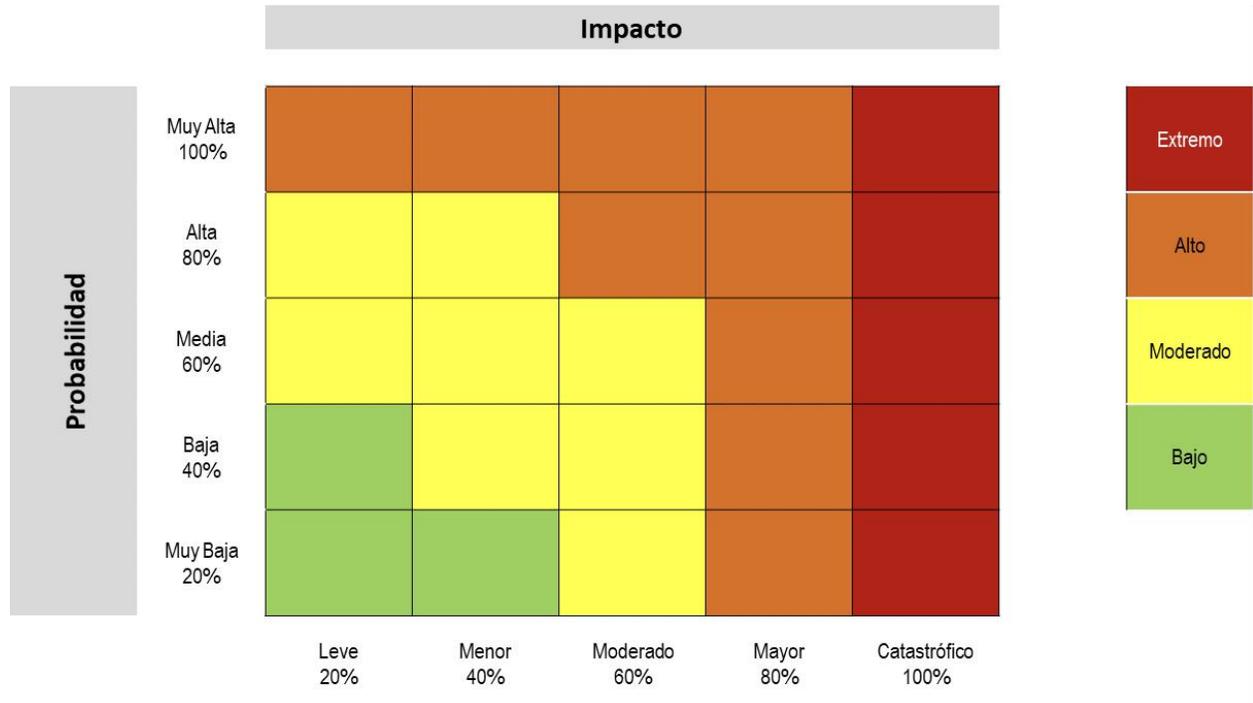
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

#### 3.2.1 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 calor.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 28 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### Matriz de calor (niveles de severidad del riesgo)



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 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%

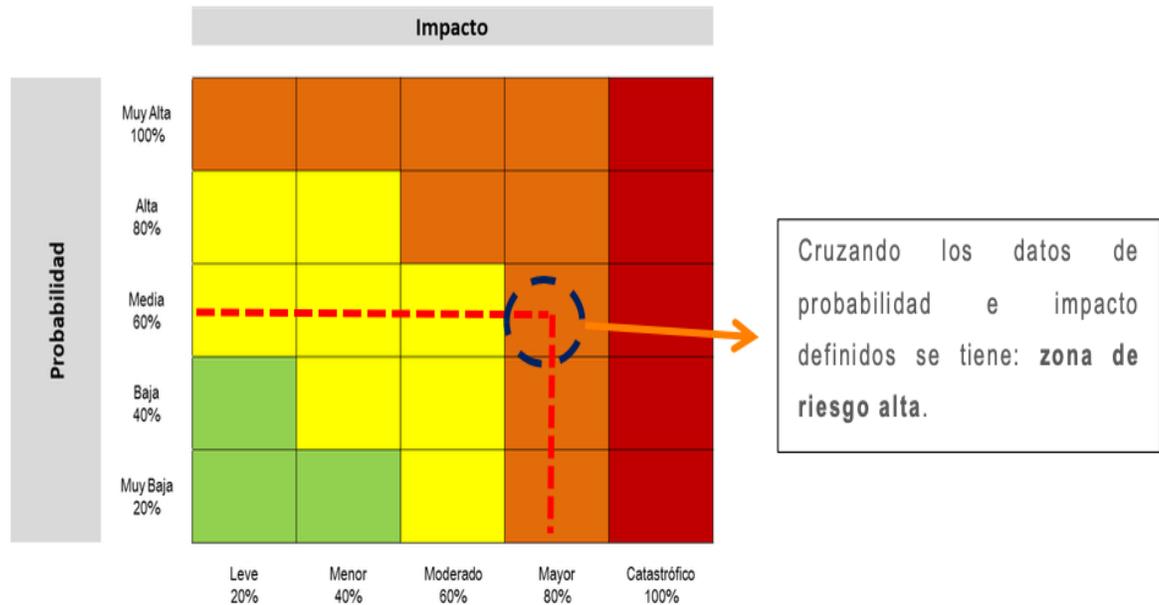
Aplicando la matriz de calor se tiene:



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
Versión: 1  
Fecha de elaboración: 05/11/2020  
Fecha de revisión:  
Página: Página 29 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------



### 3.2.2 Valoración de controles:

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

**3.2.2.1 Estructura para la descripción del control:** para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

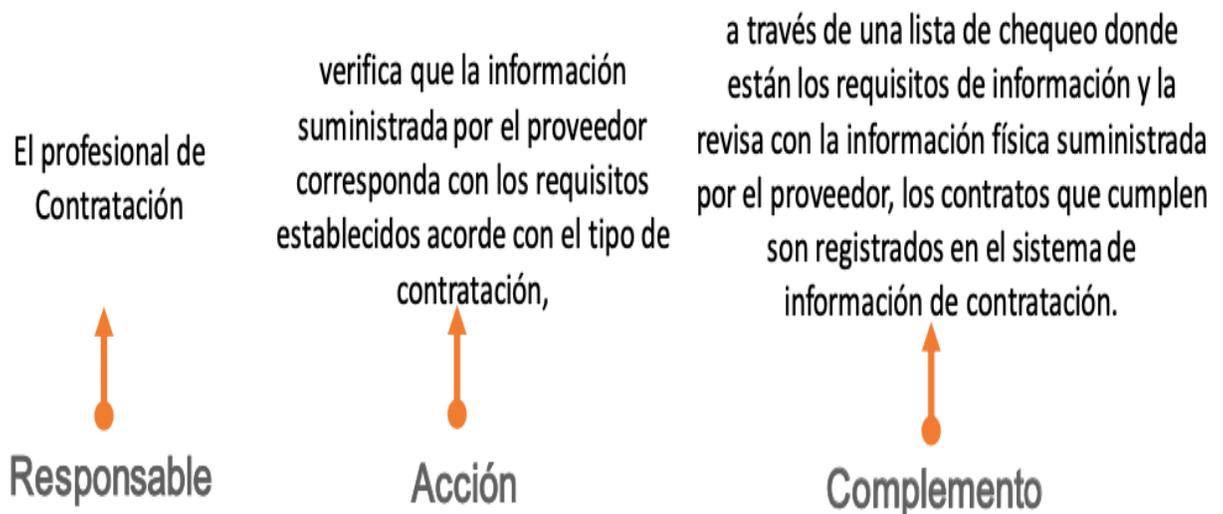
- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>30</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

- **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.

Cruzando los datos de probabilidad e impacto definidos se tiene: **zona de riesgo alta.**

Ejemplo aplicado bajo la estructura propuesta para la redacción del control



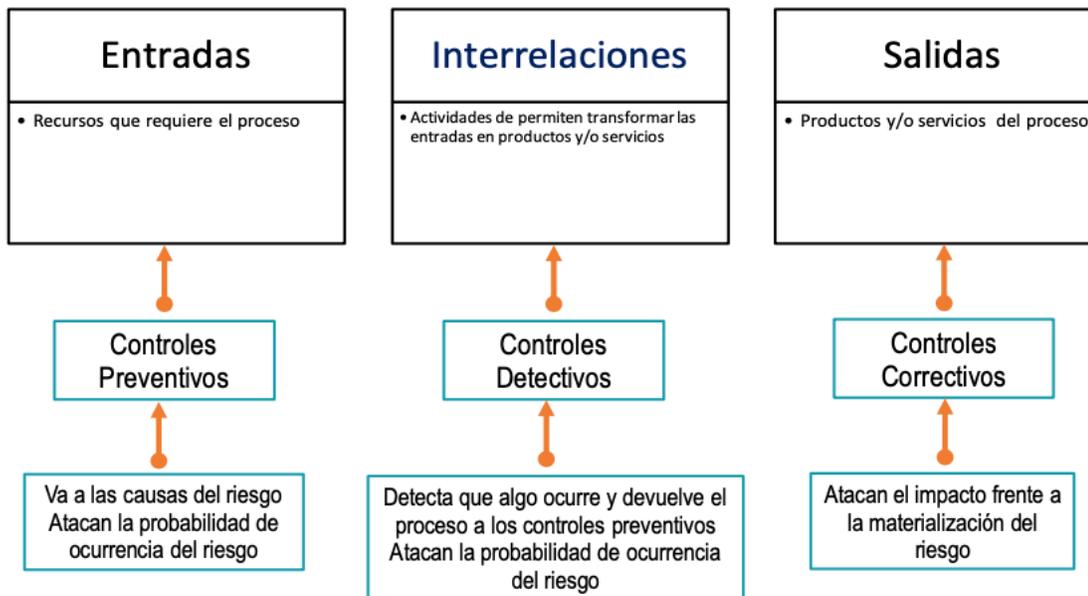
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

### 3.2.2.2 Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuando se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura 15 se consideran 3 fases globales del ciclo de un proceso así:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>31</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### Figura Ciclo del proceso y las tipologías de controles



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **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.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:  
**Control manual:** controles que son ejecutados por personas.

**Control automático:** son ejecutados por un sistema.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 32 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### 3.2.2.3 Análisis y evaluación de los controles – Atributos:

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:

**Tabla de Atributos de para el diseño del 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	25%



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: Página 33 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

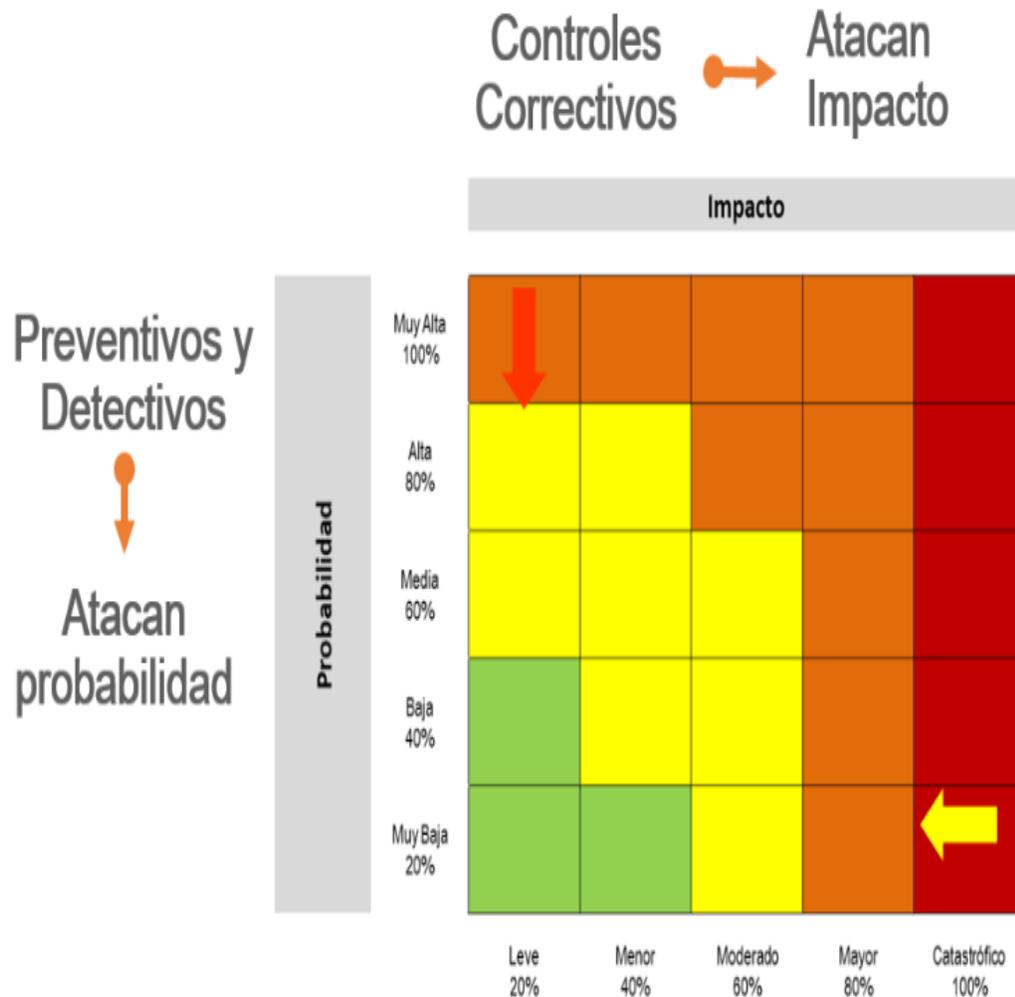
Características		Descripción	Peso	
*Atributos informativos			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

**\*Nota:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>34</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la siguiente figura, 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: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>35</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### 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%

**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.

En la siguiente tabla se observa la aplicación de la tabla de atributos, esta le servirá como ejemplo para el análisis y valoración de los dos controles propuestos.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>36</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### Tabla de Aplicación tabla atributos a ejemplo propuesto

Controles y sus características			Peso	
<b>Control 1</b> 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.	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			-	
<b>Total valoración control 1</b>				<b>40%</b>
<b>Control 2</b> 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	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-

Controles y sus características			Peso	
inconsistencias, devuelve el proceso al profesional de contratos asignado.	Evidencia	Con registro	X	-
		Sin registro		-
<b>Total valoración control 2</b>				<b>30%</b>

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>37</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### 3.2.3 Nivel de riesgo (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.

Para mayor claridad, en la tabla 8 se da continuación al ejemplo propuesto, donde se observan los cálculos requeridos para la aplicación de los controles.

### Tabla de Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
	Probabilidad inherente		Valoración control 1 preventivo		
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 control 1 preventivo	40%	$60\% * 40\% = 24\%$ $60\% - 24\% = \mathbf{36\%}$
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	$36\% * 30\% = 10,8\%$ $36\% - 10,8\% = \mathbf{25,2\%}$
	<b>Probabilidad Residual</b>	<b>25,2%</b>			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	<b>Impacto Residual</b>	<b>80%</b>			

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 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.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>38</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

**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%

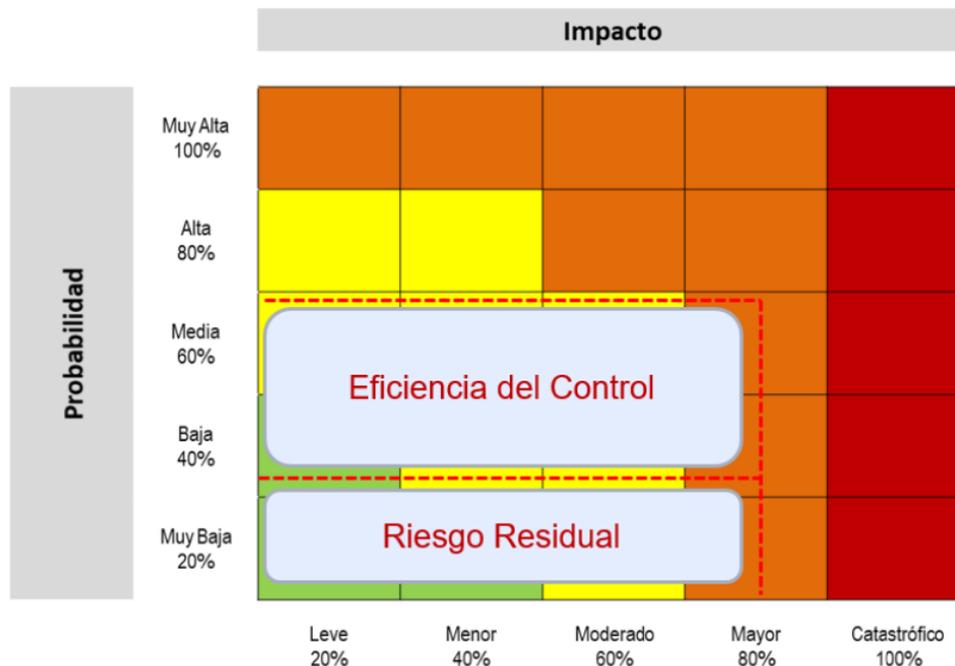
**Impacto Residual:** mayor 80%

**Zona de riesgo residual:** alta

Para este caso, si bien el riesgo se mantiene en zona alta, se bajó el nivel de probabilidad de ocurrencia del riesgo.

En la próxima figura se observa el movimiento en la matriz de calor.

**Figura de Movimiento en la matriz de calor con el ejemplo propuesto**



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026
Versión: 1
Fecha de elaboración: 05/11/2020
Fecha de revisión:
Página: Página <b>39</b> de <b>72</b>

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

**Nota:** En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

A continuación, se podrá observar el formato propuesto para el mapa de riesgos, este incluye la matriz de calor correspondiente.

### Formato mapa de riesgos

#### Parte 1 identificación del riesgo:

#### Tabla de Ejemplo mapa de riesgos acorde con el ejemplo propuesto

<b>Proceso:</b>		Gestión de recursos										
<b>Objetivo:</b>		Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación										
<b>Alcance:</b>		Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas										
*Referencia	Impacto	Causa inmediata	Causa raíz	Descripción del riesgo	Clasificación riesgo	Frecuencia	Probabilidad inherente	%	Impacto inherente	%	Zona de riesgo inherente	
1	Afectación económica	Multa y sanción del organismo de control	Incumplimiento de los requisitos para contratación	Posibilidad de afectación económica por multa y sanciones del organismo de control debido la adquisición de bienes y servicios fuera de los requerimientos normativos.	Ejecución y administración de procesos	120	Moderada	60%	Mayor	80%	Alta	

**\*Nota:** La columna referencia se sugiere para mantener el consecutivo de riesgos, así el riesgo salga del mapa no existirá otro riesgo con el mismo número. Una entidad puede ir en el riesgo 150, pero tener 70 riesgos, lo que permite llevar una traza de los riesgos. Esta información la debe administrar la oficina asesora de planeación o gerencia de riesgos.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: Página **40** de **72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

## PARTE 2 VALORACIÓN DEL RIESGO:

Parte 2 Valoración del riesgo:

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
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.	X		Preventivo	Manual	40%	Documentado	Continua	Registro material	36%	Baja	25,2%	Mayor	80%	Alta	Reducir

No. control	Descripción del control	Afectación		Atributos						Probabilidad residual (2 controles)	Probabilidad residual final	%	Impacto residual final	%	Zona de riesgo final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
2	El jefe de 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.	X		Detectivo	Manual	30%	Documentado	Continua	Con registro	25,2%						

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 41 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### PARTE 3 PLANES DE ACCIÓN (PARA LA OPCIÓN DE TRATAMIENTO REDUCIR):

Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado
Automatizar la lista de chequeo que utiliza el profesional de contratación, a fin de reducir la posibilidad de error humano y elevar la productividad del proceso.	Oficina de TIC	30/11/2020	30/06/2020	Se han adelantado las actividades de levantamiento de requerimientos funcionales para la automatización de la lista de chequeo.	En curso

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

### 3.3 Estrategias para combatir el riesgo:

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la próxima figura se observan las tres opciones mencionadas y su relación con la

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 42 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

### Figura de Estrategias para combatir el riesgo



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la Gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

**Nota:** El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio<sup>2</sup> y se consideraría un control

<sup>2</sup> De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>43</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

correctivo.

**3.4 Herramientas para la Gestión del riesgo:** como producto de la aplicación de la metodología se contará con los mapas de riesgo.

Además de esta herramienta, se tienen las siguientes:

3.4.1 **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.

Algunas fuentes para establecer una base histórica de eventos pueden ser:

- ✓ Mesa de ayuda.
- ✓ Las PQRD (peticiones, quejas, reclamos, denuncias)
- ✓ Oficina jurídica
- ✓ Líneas internas de denuncia.

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

**Desempeño del control=**

# eventos / frecuencia del riesgo (# veces que se hace la actividad)

**3.4.2 Indicadores clave de riesgo:**

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o

organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>44</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (*Key Risk Indicators*), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos. En la tabla 9 se muestran algunos ejemplos de estos indicadores.

### Tabla de Ejemplos indicadores clave de riesgo

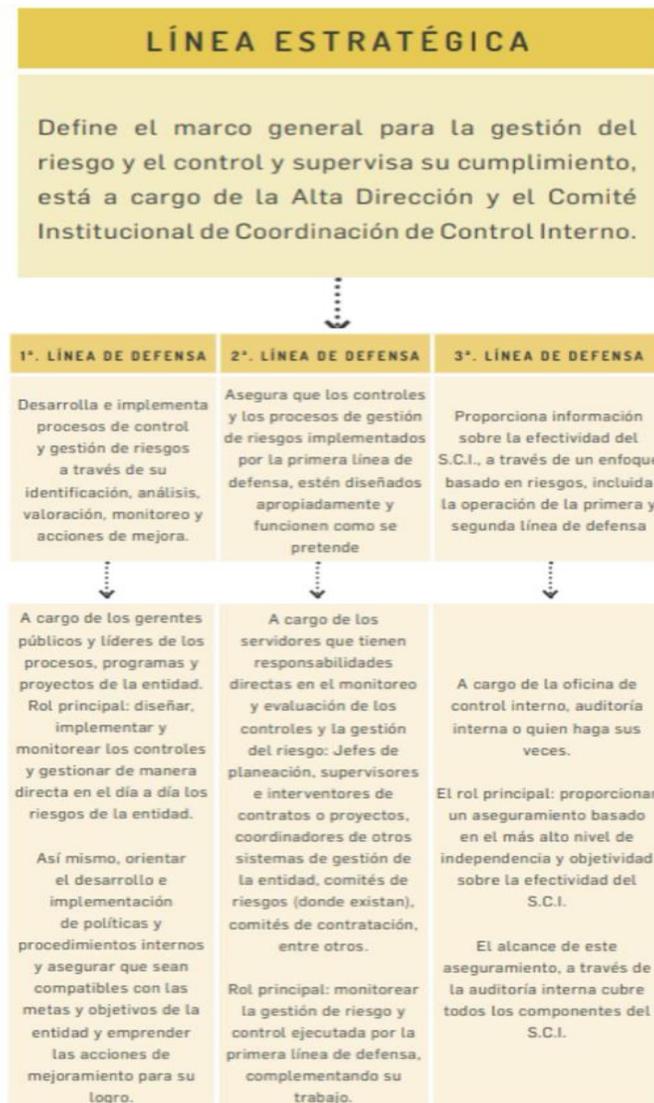
PROCESO ASOCIADO	INDICADOR	MÉTRICA
TIC	Tiempo de interrupción de aplicativos críticos en el mes	Número de horas de interrupción de aplicativos críticos al mes
FINANCIERA	Reportes emitidos al regulador fuera del tiempo establecido	Número de reportes mensuales remitidos fuera de términos
ATENCIÓN AL USUARIO	Reclamos de usuarios por incumplimiento a términos de ley o reiteraciones de solicitudes por conceptos no adecuados	% solicitudes mensuales fuera de términos % solicitudes reiteradas por tema
ADMINISTRATIVO Y FINANCIERA	Errores en transacciones y su impacto en la gestión presupuestal	Volumen de transacciones al mes sobre la capacidad disponible
TALENTO HUMANO	Rotación de personal	% de nuevos empleados que abandonan el puesto dentro de los primeros 6 meses

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>45</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

### 3.5 MONITOREO Y REVISIÓN:

El modelo integrado de Planeación y Gestión (MIPG) desarrolla en la dimensión 7 *control interno* las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad como sigue:

#### Tabla de Esquema de líneas de defensa



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>46</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Se deben considerar los siguientes aspectos de acuerdo con los pasos de la metodología así:

1. En el paso *política de administración del riesgo* se deben incluir los lineamientos requeridos para el manejo de estas tipologías de riesgo.

Para el caso de los riesgos sobre seguridad de la información, se debe incorporar el modelo nacional de gestión de riesgo de seguridad de la información donde los responsables analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes.

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, las entidades deben incluir las matrices relacionadas con la redacción de este tipo de riesgos, las preguntas para la definición del nivel de impacto y la matriz de calor correspondiente, donde se precisan las zonas de severidad aplicables. Para esta tipología de riesgos se incluye 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.

2. En la etapa de identificación del riesgo se enmarcan en los procesos, lo que exige el análisis frente a los objetivos, cadena de valor, factores generadores de riesgo (explicados en los primeros apartes de la presente guía). Estos lineamientos son aplicables a ambas tipologías de riesgos.

3. En la etapa de valoración del riesgo se asocian las tablas para el análisis de probabilidad, impacto niveles de severidad, así como para el diseño y evaluación de los controles identificados. En este caso, para los riesgos de corrupción se precisan algunas herramientas para la definición del impacto y las zonas de riesgo aplicables. En cuanto a los riesgos de seguridad de la información se incorporan las tablas de probabilidad, impacto y matriz de calor definidas en la metodología general.

#### **4. LINEAMIENTOS SOBRE LOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN**

Para la Gestión de riesgos de corrupción es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. A continuación, se

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>47</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, que sigue vigente.

Identificación de riesgos - técnicas para la identificación de riesgos

## RIESGO DE CORRUPCIÓN

### Definición de riesgo 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.

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurren los componentes de su definición así:

### ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Los riesgos de corrupción se establecen sobre **procesos**. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de Gestión y uno de corrupción, se sugiere la utilización de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 48 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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: Secretaría de Transparencia de la Presidencia de la República.

### Generalidades acerca de los riesgos de corrupción

Se elabora anualmente por cada responsable de los procesos al interior de las entidades junto con su equipo.

Consolidación: la Oficina de Planeación o quien haga sus veces, o a la dependencia encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>49</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

de 2014.

En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

Recuerde que las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

**Socialización:** Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de Planeación o quien haga sus veces, o la de Gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos de corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

**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:** en concordancia con la cultura del autocontrol al interior de la entidad, 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 o quien haga sus veces 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, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

## **EJEMPLO Información Anonimizada**



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
Versión: 1  
Fecha de elaboración: 05/11/2020  
Fecha de revisión:  
Página: Página **50** de **72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

N.º	Riesgo	Clasificación	Causa	Probabilidad	Impacto	Riesgo Residual	Opción de Manejo	Actividad de Control
1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o para terceros...	Corrupción	Falta de...	Probable	Catastrófico	Catastrófico	Evitar	

Información  
anonimizada

**IMPORTANTE**

Tenga en cuenta que la información clasificada o reservada la señala la ley, un decreto con fuerza de ley o convenio internacional ratificado por el Congreso o en la Constitución.

Una resolución no puede calificar la información como clasificada o reservada.

**IMPORTANTE**

Los riesgos de corrupción, siempre deben gestionarse.

**IMPORTANTE**

En la descripción de los riesgos de corrupción deben concurrir **TODOS** los componentes de su definición:

**Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.**

Fuente: Secretaría de Transparencia de la Presidencia de la República

**Valoración de riesgos**

**Cálculo de la probabilidad e impacto Análisis de la probabilidad**

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, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>51</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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

### Crterios para calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	<b>Casi seguro</b>	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	<b>Probable</b>	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	<b>Posible</b>	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	<b>Improbable</b>	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	<b>Rara vez</b>	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

### Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Crterios para calificar el impacto en riesgos de corrupción:



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: Página 52 de 72

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

Tabla 16 Criterios para calificar el impacto en riesgos de corrupción

N.º	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.		<b>10</b>	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

**Nivel de impacto MAYOR**

Fuente: Secretaría de Transparencia de la Presidencia de la República.

**IMPORTANTE**

Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.  
 Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

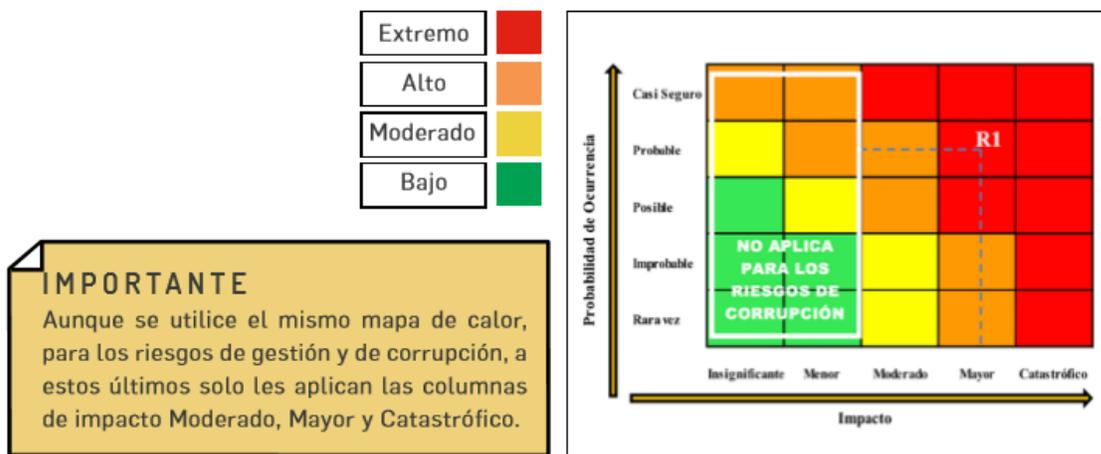
**Análisis del impacto en riesgos de corrupción**

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>53</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.



Fuente: Secretaría de Transparencia de la Presidencia de la República.

## Valoración de los controles – diseño de controles

Tenga en cuenta para el diseño de controles, los parámetros señalados en la **versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes**, por lo tanto, se sugiere remitirse a dicho documento.

### Nivel del riesgo (riesgo residual)

### Desplazamiento del riesgo inherente para calcular el riesgo residual

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>54</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

**IMPORTANTE**  
 Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

## Tratamiento del riesgo

### ¿Qué es tratamiento del riesgo?

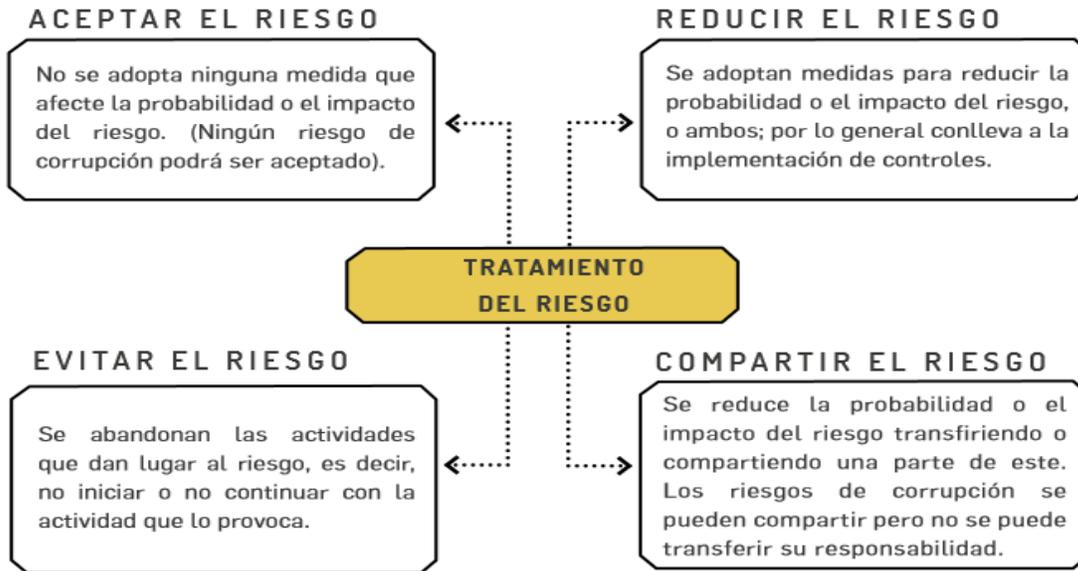
Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración 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 de este 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. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

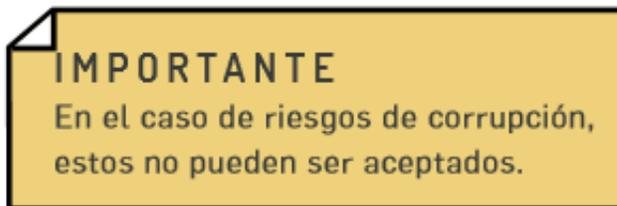
Código: ES – PL – FO - 026  
Versión: 1  
Fecha de elaboración: 05/11/2020  
Fecha de revisión:  
Página: Página **55** de **72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------



Fuente: DAFP

## ACEPTAR EL RIESGO



## 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.

Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>56</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

## 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.

## 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.

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

### Tratamiento del riesgo – rol de la primera línea de defensa

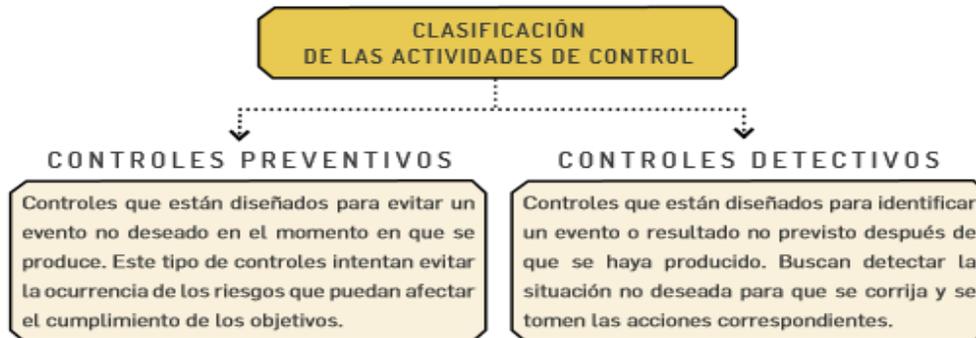
Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
Versión: 1  
Fecha de elaboración: 05/11/2020  
Fecha de revisión:  
Página: Página **57** de **72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------



(Fuente DAFP)

### **Monitoreo de riesgos de corrupción**

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la Gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa). Le corresponde, igualmente, a la oficina de Planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la Gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

### **Reporte de la Gestión del riesgo de corrupción**

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado

### **Seguimiento de riesgos de corrupción**

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 58 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## GESTIÓN RIESGOS DE CORRUPCIÓN

\* Seguimiento: El Jefe de Control Interno, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la Gestión del riesgo, verificando la efectividad de los controles.

\* Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

\* Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

\* Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano. (Ver anexo 6. matriz de seguimiento a los riesgos de corrupción)

En especial deberá adelantar las siguientes actividades:

\* Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.

\* Seguimiento a la Gestión del riesgo.

\* Revisión de los riesgos y su evolución.

\* Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

### 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.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>59</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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 asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

Determinar la efectividad de los controles.

Mejorar la valoración de los riesgos.

Mejorar los controles.

Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.

Determinar si se adelantaron acciones de monitoreo.

Revisar las acciones del monitoreo.

## 5. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)<sup>3</sup>, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad

<sup>3</sup> Tomado de: <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>60</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

de la información, arquitectura, servicios ciudadanos digitales.

### 5.1. 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 del proceso.

#### Figura Conceptualización activos de información

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar <b>qué es lo más importante que cada entidad y sus procesos poseen</b> (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

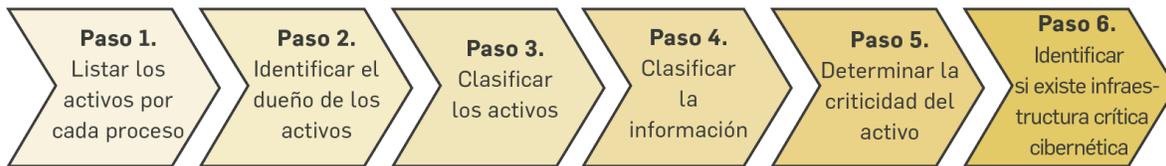
¿Qué son los activos?	¿Por qué identificar los activos?
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber <b>qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano</b> , aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>61</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## Figura Pasos para la identificación de activos

### ¿CÓMO IDENTIFICAR LOS ACTIVOS?:



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

### Tabla Ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del 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 de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el front office de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

## 5.2. IDENTIFICACIÓN DEL RIESGO:

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

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>62</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

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. Para este efecto, es necesario consultar el Anexo 4 *Modelo nacional de Gestión de riesgos de seguridad de la información para entidades públicas* donde se encuentran las siguientes tablas necesarias para este análisis:

Tabla 5. Tabla de amenazas comunes

Tabla 6. Tabla de amenazas dirigida por el hombre

Tabla 7. Tabla de vulnerabilidades comunes

**Nota:** La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

#### Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

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

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página 63 de 72
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

### Ejemplo Formato de descripción del riesgo de seguridad de la información

Seleccionar las vulnerabilidades asociadas a la amenaza identificada



RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	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 pérdida 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 en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 64 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

**IMPORTANTE**

- \* Existirían tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.
- \* Los catálogos de amenazas y vulnerabilidades comunes se encuentran en la sección 4.1.7. del **anexo “Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas”**, el cual hace parte de la presente guía.
- \* **NOTA 1:** tener en cuenta que la agrupación de activos debe ser del mismo tipo, por ejemplo, analizar conjuntamente activos tipo hardware, software, información, entre otros, para determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.
- \* **NOTA 2:** las entidades públicas deben incluir como mínimo los procesos y procedimientos establecidos en esta guía. Aquellas entidades que ya estén adelantando procesos relacionados con la gestión de este tipo de riesgo y que incorporen al menos lo dispuesto en estas guías podrán continuar bajo sus procedimientos. Si alguno de los aspectos contenidos en esta guía no está contemplado, deberá ser agregado a los que manejan actualmente.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

### 5.3. VALORACIÓN DEL RIESGO:

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

En este sentido, se debe considerar para este análisis la tabla definida en el aparte 3.1.1, la cual se retoma a continuación:

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>65</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

	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%

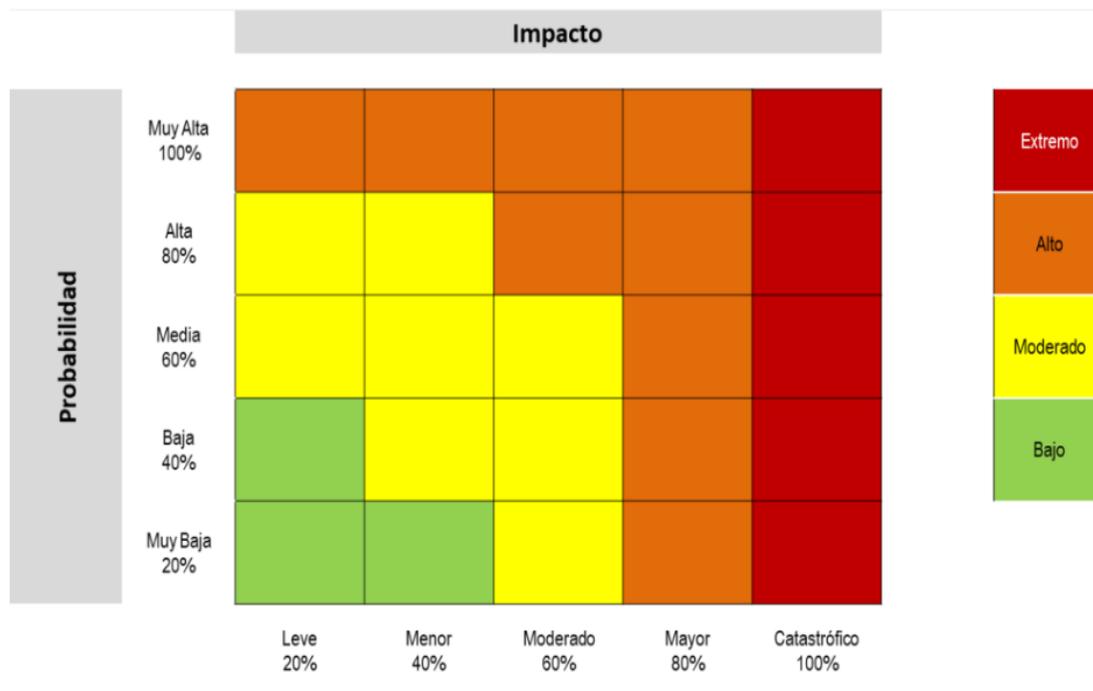
La determinación del impacto se debe llevar a cabo de acuerdo con lo establecido en el aparte 3.1.2 del presente documento entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

En este sentido, se debe considerar para este análisis la tabla definida en el aparte 3.1.2, que se retoma a continuación:

	Afectación Económica	Reputacional
Leve 20%	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.
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 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 publicitario sostenido a nivel país

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>66</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 3.2.1, que se retoma a continuación:



En la figura siguiente se observa un ejemplo aplicando la etapa de valoración del riesgo sobre un activo como es la base de datos de nómina.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 67 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## Figura Valoración del riesgo en seguridad de la información

### IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.  
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.

La variable presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026  
 Versión: 1  
 Fecha de elaboración: 05/11/2020  
 Fecha de revisión:  
 Página: **Página 68 de 72**

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo	
Alto	
Moderado	
Bajo	

**IMPORTANTE:**

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

## 5.4 CONTROLES ASOCIADOS A LA SEGURIDAD DE LA INFORMACIÓN

Las ESE podrá mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> <b>NIT. 801001440-8</b>		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: Página <b>69</b> de <b>72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en el documento maestro del modelo de seguridad y privacidad de la información (MSPI):

### Tabla de 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 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, prueba 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.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del <i>software</i> y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.



**EMPRESA SOCIAL DEL ESTADO  
ARMENIA QUINDÍO  
NIT. 801001440-8**

Código: ES – PL – FO - 026
Versión: 1
Fecha de elaboración: 05/11/2020
Fecha de revisión:
Página: Página <b>70</b> de <b>72</b>

<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional
------------------------------	-----------------------	-------------------------------	--------------------------------------------

### Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	<b>Pérdida de la integridad</b>	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	<b>Probable</b>	<b>Menor</b>	<b>Moderado</b>	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	<b>EFICACIA:</b> Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100  <b>EFFECTIVIDAD:</b> Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
				Contraseñas sin protección	Reducir				A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018		
				Ausencia de mecanismos de identificación y autenticación de usuarios	Reducir				A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018		
				"Ausencia de bloqueo	Reducir				A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018		

\*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 71 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## BIBLIOGRAFÍA

FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Diciembre 2020. Versión 5.

Referencias Celis, Ó. B. (2012). Gestión Integral de Riesgos. Bogotá D.C.: Consorcio Gráfico Ltda. COSO Committee of Sponsoring Organizations of the Treadway Commission. (2017). Enterprise Risk Management. Integrating with Strategy and Performance. Durham: Association of International Certified Professional Accountants. ICONTEC Internacional. (2011).

NORMA TÉCNICA COLOMBIANA GTC 137. GESTIÓN DEL RIESGO. VOCABULARIO. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). ICONTEC Internacional. (2011).

NORMA TÉCNICA COLOMBIANA NTC ISO 31000. GESTIÓN DEL RIESGO. PRINCIPIOS Y DIRECTRICES. Bogotá D.C.: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).

Instituto de Auditores Internos de Colombia. (2017). MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA. Bogotá D.C. <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-deSeguridad/>

TIPOLOGÍAS DE CORRUPCIÓN. Oficina de las Naciones Unidas contra la Droga y el Delito –UNODC– y la Alcaldía Mayor de Bogotá – 2015. <https://www.icbf.gov.co/cuales-son-los-delitos-que-tienen-relacion-con-hechosde-corrupcion>

	<b>EMPRESA SOCIAL DEL ESTADO ARMENIA QUINDÍO</b> NIT. 801001440-8		Código: ES – PL – FO - 026
			Versión: 1
			Fecha de elaboración: 05/11/2020
			Fecha de revisión:
			Página: <b>Página 72 de 72</b>
<b>Nombre del Documento:</b>	Formato institucional	<b>Unidad Administrativa:</b>	Subgerencia de planificación institucional

## ANEXOS

A continuación, se relacionan las herramientas y documentos complementarios, los cuales podrá descargar en el siguiente link: <https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>, ingresa a la Dimensión Control Interno, en la pestaña Herramientas e Instrumentos Técnicos.

- 
 1. Formato mapa de riesgos parametrizado
- 
 2. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas
- 
 3. Protocolo Identificación Riesgos corrupción en Tramites.
- 
 4. Documentos Buenas prácticas para el análisis de riesgos de fraude y corrupción
- 
 5. Lineamientos identificación y análisis de riesgos en entidades pequeñas.
- 
 6. Matriz de seguimiento a riesgos de corrupción.