CONGRESO DE LA REPÚBLICA DE COLOMBIA SENADO DE LA REPÚBLICA	Gestión de Calidad	**CÓDIGO:** GC-Gi01
	Guía para la administración del riesgo	**VERSIÓN:** 002
	SENADO DE LA REPÚBLICA	**FECHA DE APROBACIÓN:** 2023-05-29

Guía para la administración del riesgo

SISTEMA GESTIÓN DE CALIDAD

Senado de la República

TABLA DE CONTENIDO

INTRODUCCIÓN

1. OBJETIVO

2. ALCANCE

3. TÉRMINOS Y DEFINICIONES

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

5. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

5.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

5.2. IDENTIFICACIÓN DE LOS RIESGOS

5.3. DESCRIPCIÓN DEL RIESGO

5.4 CLASIFICACIÓN DEL RIESGO

6. VALORACIÓN DEL RIESGO

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

8. LINEAMIENTOS SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

9. MONITOREO DE LOS RIESGOS

10. MAPA DE RIESGO

11. ANEXOS

12. FORMATOS

13. DOCUMENTOS RELACIONADOS

14. CONTROL DE CAMBIOS

INTRODUCCIÓN

El Senado de la República con el propósito de garantizar la misión, visión y los objetivos estratégicos, busca Identificar, analizar, valorar y comunicar los riesgos asociados a la gestión de la entidad, con el fin de prevenir o detectar oportunamente desviaciones en el cumplimiento de los objetivos institucionales, establece la Política GC-Pi02 Política de Administración del Riesgo la gestión de los procesos y la satisfacción de los grupos de interés.

La administración del riesgo es una herramienta de tipo preventivo la cual se encarga de cuantificar la probabilidad de ocurrencia de los riesgos, a través del análisis de los diferentes escenarios que pueden afectar sus operaciones críticas y sus servicios. La entidad tiene el objetivo de evaluar la administración de riesgos y facilitar su ejecución

Los principales beneficios para la identificación de los riesgos en 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
- Mejoramiento en la calidad de procesos y servicios
- Fortalecimiento de la cultura de control de la organización
- Incremento en la capacidad de la entidad, para alcanzar sus objetivos
- Dota a la entidad en herramientas y controles, para hacer una administración más eficaz y eficiente

1. OBJETIVO

Establecer los lineamientos y criterios metodológicos para una adecuada gestión del riesgo en el Senado de la República, con el fin de minimizar los efectos adversos que se puedan ocasionar, permitiendo la orientación de la toma de decisiones referida a la formulación de acciones efectivas que garanticen el mejoramiento continuo en la entidad.

2. ALCANCE

La gestión de los riesgos en el Senado de la República, tendrá un carácter prioritario y estratégico, fundamentada en el modelo de operación por procesos, conforme a los parámetros del Modelo Integrado de Planeación y Gestión -MIPG- impartido por el departamento de la Función Pública, para lo cual se tendrán en cuenta los procesos estratégicos, misionales, de apoyo y de evaluación. Por tal razón, la identificación, análisis y valoración de los riesgos y controles, se circunscribe a los objetivos de cada proceso.

3. TÉRMINOS Y DEFINICIONES

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.

Administración del riesgo: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

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 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 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.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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 correctivo: Acción o conjunto de acciones que atacan el impacto frente a la materialización del riesgo

Control detectivo: Acción o conjunto de acciones que están orientados a detectar que algo ocurre atacan la probabilidad de ocurrencia del riesgo.

Control preventivo: Acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Control: Medida que permite reducir o mitigar un riesgo.

Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado o particular.

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

Factores de Riesgo: Son las fuentes generadoras de riesgo

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

Integridad: Propiedad de exactitud y completitud.

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 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 un (1) año.

Riesgo de Corrupción: Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo 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; nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

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.

Sistema de Administración de Riesgo: conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.

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 ser explotada por una o más amenazas.

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 los siguientes términos:

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.

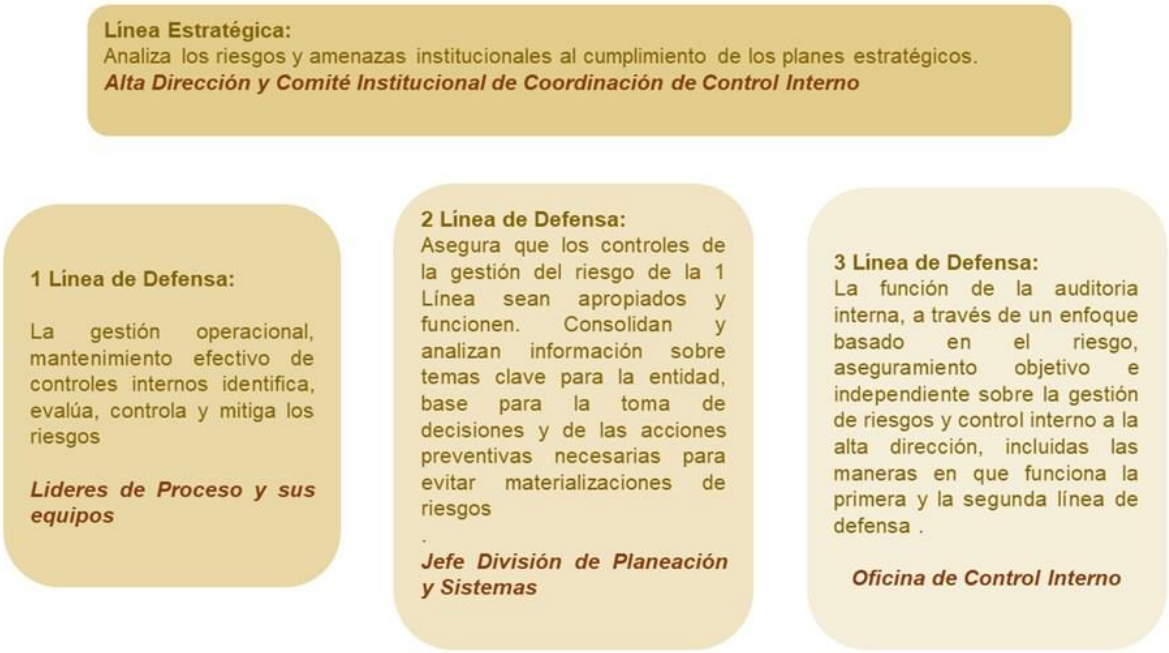
Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

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.

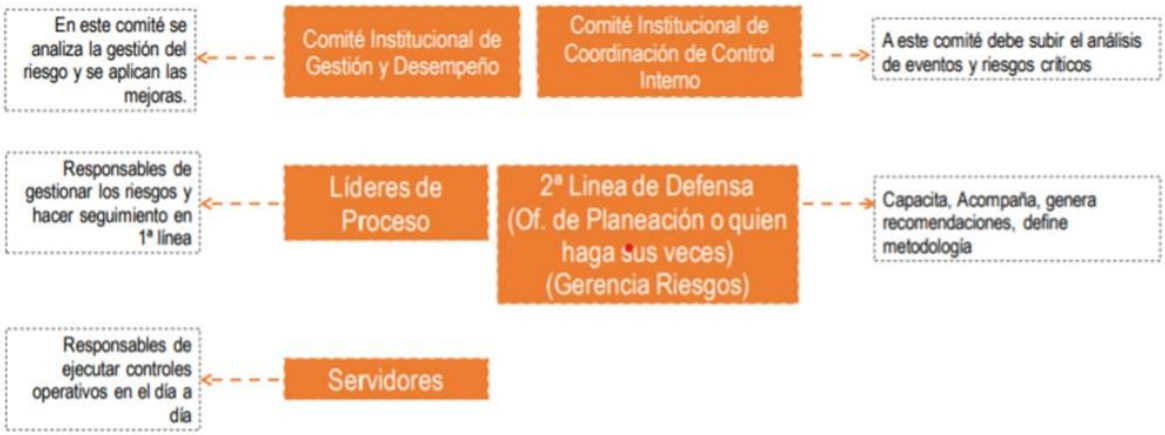
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

Es preciso identificar los actores que intervienen en la administración del riesgo, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión MIPG, las líneas de defensa son el eje articulador donde se definen las responsabilidades frente al control, el cual proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.



La operatividad institucional para la adecuada administración de la gestión del riesgo es la siguiente:



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

De igual manera, la División de Planeación y Sistemas lleva a cabo las siguientes acciones:

- Socializar anualmente la metodología de riesgos.
- Liderar las mesas de trabajo de identificación del riesgo
- Socializar y publicar el mapa de riesgos de gestión y de corrupción.

Jefe División de Planeación y Sistemas: responsable de coordinar la revisión y actualización de los mapas de riesgo de cada proceso.

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración del riesgo”, la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

.

- Delegar, por parte del líder del proceso, el profesional que se encargará del monitoreo, reporte y socialización de los riesgos asociados.

Coordinador Oficina Coordinadora del Control Interno: responsable de realizar el seguimiento a los controles establecidos en los mapas de riesgo y su efectividad.

La gestión del riesgo es un proceso efectuado por la alta dirección del Senado de la República y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

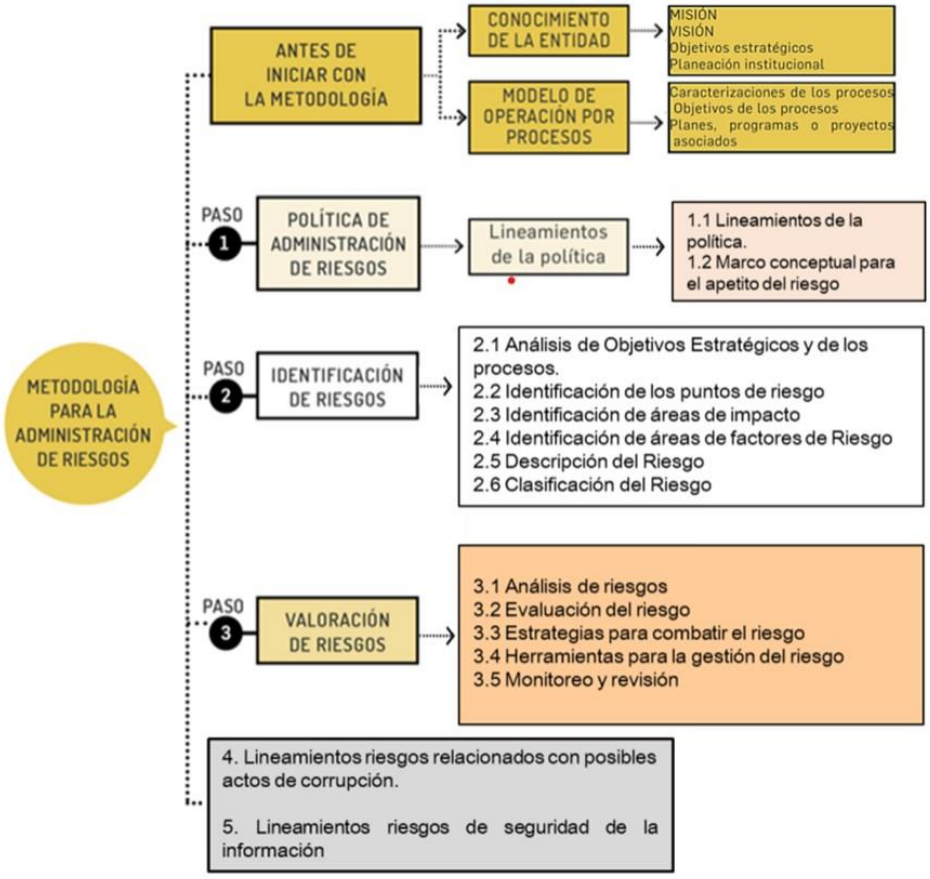
Valores

El Senado de la República, ha adoptado 5 valores institucionales, los cuales promueven y fortalecen su cumplimiento por parte de todos los servidores públicos (funcionarios y contratistas) de la entidad en el desarrollo de sus funciones. Estos valores son:

- Diligencia: Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera pon imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación.

5. METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

La metodología para la administración del riesgo requiere un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad y desde un punto de vista estratégico de la aplicación de los tres pasos básicos para su desarrollo (Política de administración de riesgos, identificación de riesgos y valoración de riesgos). A continuación, se muestra la estructura completa:



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

Los siguientes numerales presentan cada una de las etapas a desarrollar, esta guía establece que para la administración del riesgo al interior del Senado de La República se tendrá en cuenta los lineamientos de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión vigente.

5.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Política de Administración del Riesgo GC-Pi02 es una declaración de la Dirección General Administrativa y las intenciones generales de la entidad con respecto a la gestión del riesgo donde se establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos, tiene en cuenta objetivos estratégicos de la entidad y niveles de responsabilidad frente al manejo de riesgos de acuerdo con las responsabilidades establecidas en las líneas de defensa.

5.2. IDENTIFICACIÓN DE LOS RIESGOS

Determinación de la capacidad del riesgo

El Senado de La República debe aplicar los valores de probabilidad e impacto contenidos en esta guía, 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 los requisitos del marco legal aplicable, puede ser aceptado por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina “capacidad del riesgo”.

La capacidad institucional de riesgo, es el máximo valor de nivel de riesgo que una entidad puede soportar y a partir de la cual se considera que no sería posible el logro de los objetivos de la entidad.

Determinación del apetito del riesgo

El apetito del riesgo es el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del MIPG en la entidad, este valor se denomina, dado que equivale al nivel de riesgo que la entidad puede aceptar.

Tolerancia del riesgo

Es el valor de la máxima desviación admisible de nivel de riesgo con respecto al valor del apetito del riesgo, para determinar la tolerancia del riesgo se debe definir un valor que es igual o superior al apetito del riesgo y menor o igual a la capacidad 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, la caracterización de cada proceso contemplando su objetivo y alcance, adicionalmente el análisis frente a los factores internos y externos que pueden generar riesgos que afectan el cumplimiento de los objetivos.

La identificación de riesgos se realiza por procesos identificando el contexto estratégico y el alcance de los factores internos y externos.

Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

Esta actividad dentro del flujo, puede estar relacionada con un procedimiento, un lineamiento o un activo de seguridad de la información.

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/o reputacional.

Identificación de áreas de factores de riesgo

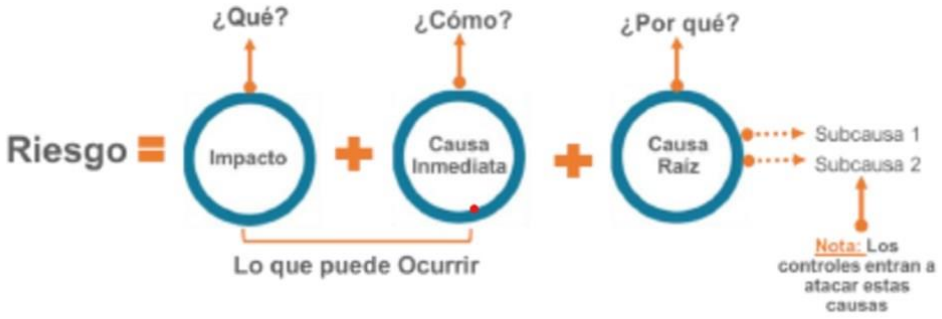
Los factores de riesgo los podemos clasificar según la siguiente tabla:

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	Hurtos 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 los programas
EVENTO EXTERNO	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
		Daños a activos físicos
EVENTO EXTERNO	Situaciones externas que afectan la entidad	Suplantación
		Asalto de la oficina
		Atentados, vandalismo, orden público

Fuente: Adaptado del curso Riesgo Operativo de la Universidad del Rosario por la Dirección de la Gestión y Desempeño institucional de Función Pública, 2020

5.1. DESCRIPCIÓN DEL RIESGO

La descripción del riesgo debe contener todos los elementos que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone la siguiente estructura que facilita su redacción y claridad que inicia con la frase ***POSIBILIDAD DE*** y se analizan los siguientes aspectos:



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

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

Desglosando los términos de la estructura 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 las 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

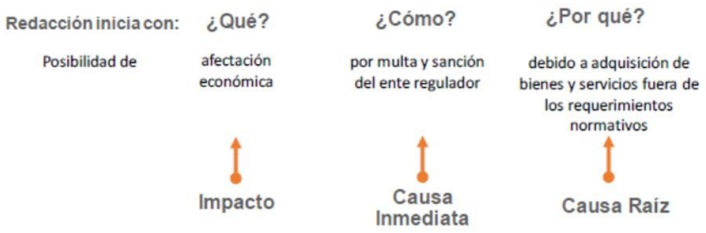
Ejemplo:

Proceso: Gestión de Bienes e Infraestructura

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 necesidad 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.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:



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 riesgo 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 atención

- ***No existen riesgos transversales, lo que puede 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.

5.4 CLASIFICACIÓN DEL RIESGO

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

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos
Fraude externo	Pérdida derivada de actos de Fraude por personas ajenas a la organización (no participa personal de la entidad)
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos
Relaciones laborales	Perdidas que surgen de acciones contrarias a las leyes o acuerdos de

	empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos
Daños a activos fijos / eventos externos	Pérdida por daño 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

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

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

6. VALORACIÓN DEL RIESGO

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

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

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; bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos.

La valoración del riesgo que ocasionalmente también se llama gestión del riesgo es el segundo componente del sistema de control interno (SCI). Se asociará la tabla de probabilidad e impacto:

	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%

Determinación del impacto:

Entendiendo que el impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

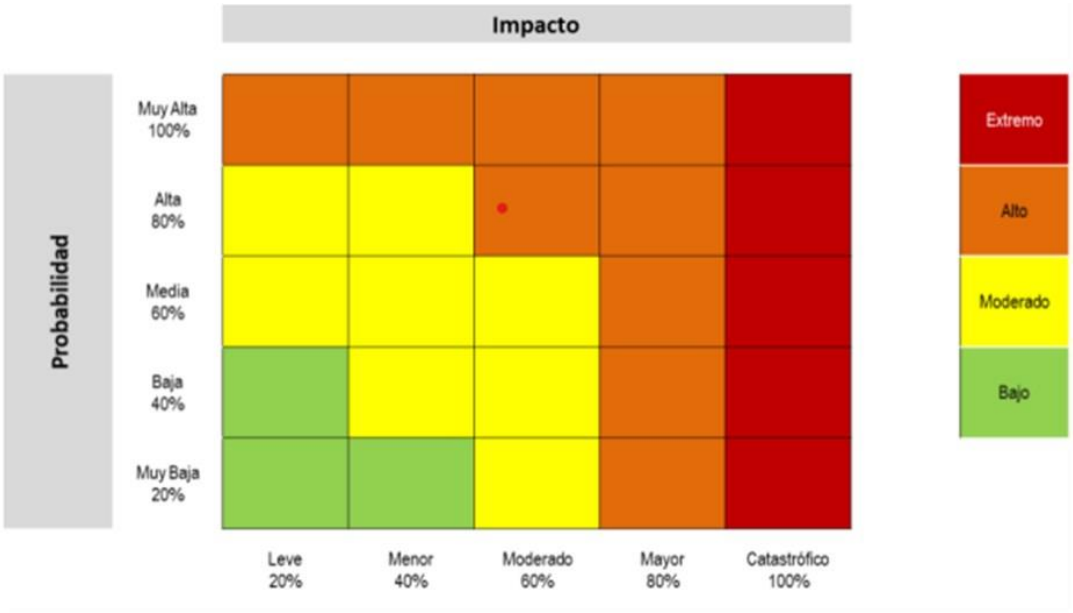
	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
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

Análisis del riesgo:

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

Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la siguiente matriz de calor:



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

Ejemplo:

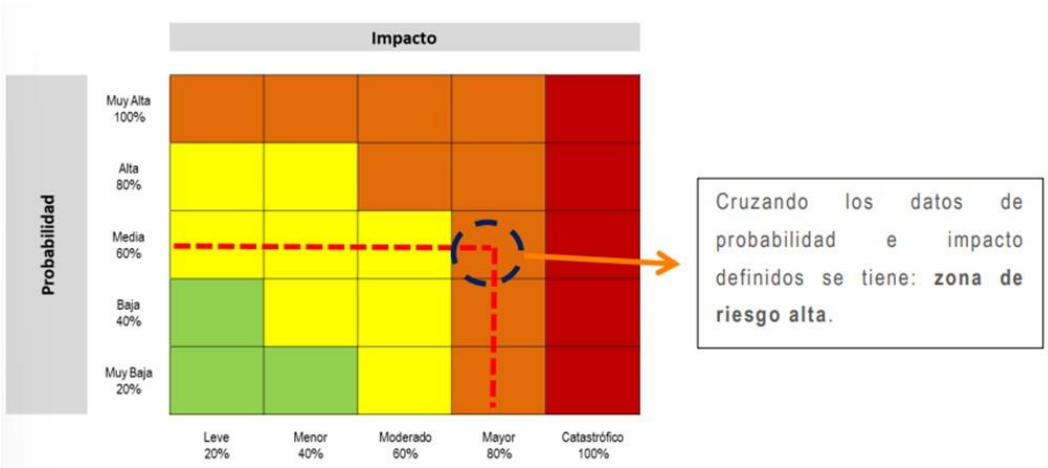
Proceso: gestión de recursos

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 **Probabilidad Inherente:** moderada 60%

Impacto Inherente: mayor 80%

Aplicando en la matriz de calor se tiene



Valoración de controles:

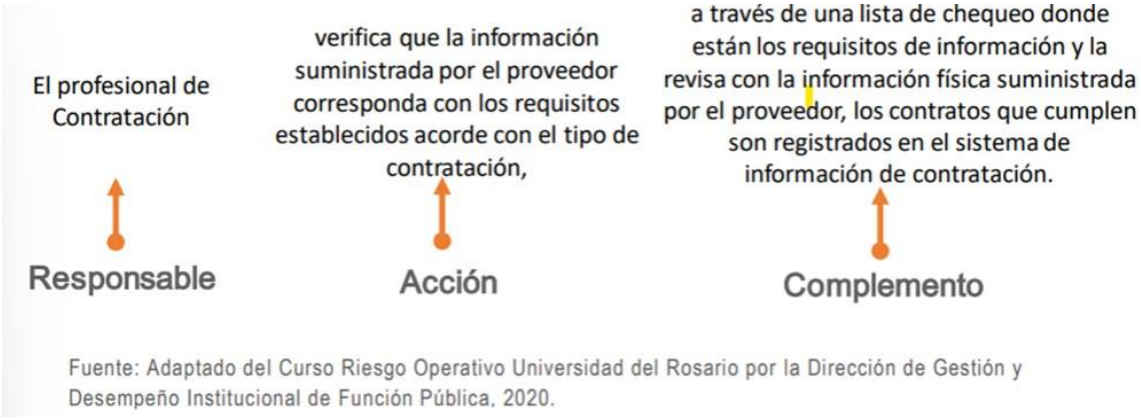
Un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través del trabajo en equipo con los líderes del proceso y su equipo de trabajo.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo

El Mecanismo de Autocontrol, como uno de los fundamentos del Modelo Estándar de Control Interno, busca que los servidores públicos tengan la capacidad de detectar las desviaciones del quehacer diario y tomar por iniciativa propia, los correctivos necesarios para lograr el cumplimiento de nuestras metas individuales.

Para ejercer el autocontrol, se requiere como primer paso, el convencimiento personal de que, al aplicar el autocontrol, se logra mejorar las labores diarias y, por ende, se contribuye al cumplimiento de los objetivos de la institución; esto, obviamente, nos lleva a contribuir para lograr una mejor Administración Pública.

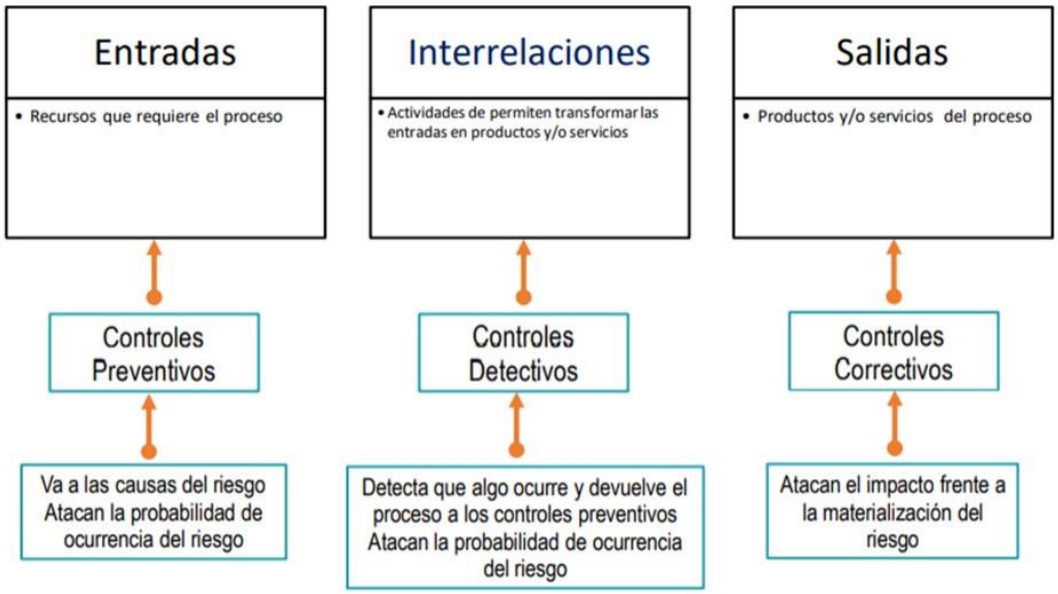
Ejemplo bajo esta estructura:



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

Tipología de controles y los procesos:

A través del ciclo de los procesos es posible establecer cuándo 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:



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.

Análisis y evaluación de los controles – Atributos:

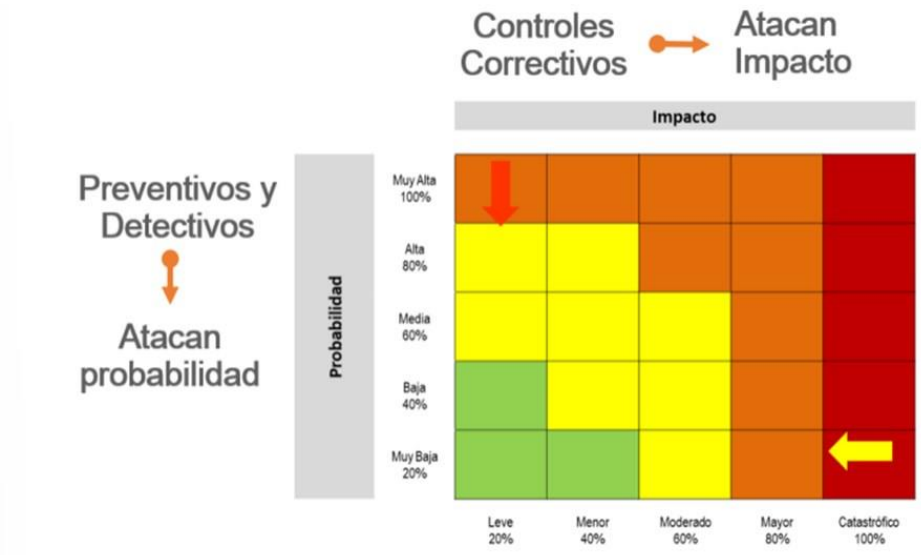
A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

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 e n su implementación	10%
	implementación	automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o	25%

			aplicativo de manera automática sin la intervención de personas para su realización	
		manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos informativos	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo	-
		aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	evidencia	con registro	El control deja un registro permite evidenciar 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.

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.



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 siguiente tabla se observan los cálculos requeridos para la aplicación de los controles.

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

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

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 pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

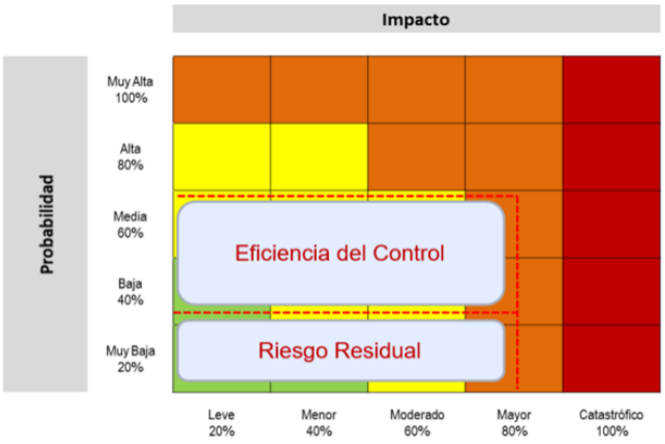
Probabilidad residual: baja 26.8%

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 siguiente figura se observa el movimiento en la matriz de calor:



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

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

Disposiciones generales En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. Es importante recordar que el desarrollo de este componente se articula con los demás establecidos para el desarrollo del plan, ya que se trata de una acción integral en la lucha contra la corrupción. En materia de riesgos asociados a posibles actos de corrupción, para la presente guía se consideran los siguientes aspectos:

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, a continuación, se transcriben algunas de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018, que reiterando sigue vigente.

Por otra parte, es de resaltar que la Secretaría de Transparencia, en la actualidad está analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción.

Por otra parte, es de resaltar que la Secretaría de Transparencia, en la actualidad está analizando la posibilidad de actualizar la metodología para la gestión de riesgos de corrupción.

Identificación de riesgos - técnicas para la identificación de riesgos RIESGO DE CORRUPCIÓN

Definición:

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 concurran 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 los 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:

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.

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 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 Criterios para calificar la probabilidad.

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

Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo Criterios para calificar el impacto en riesgos de corrupción

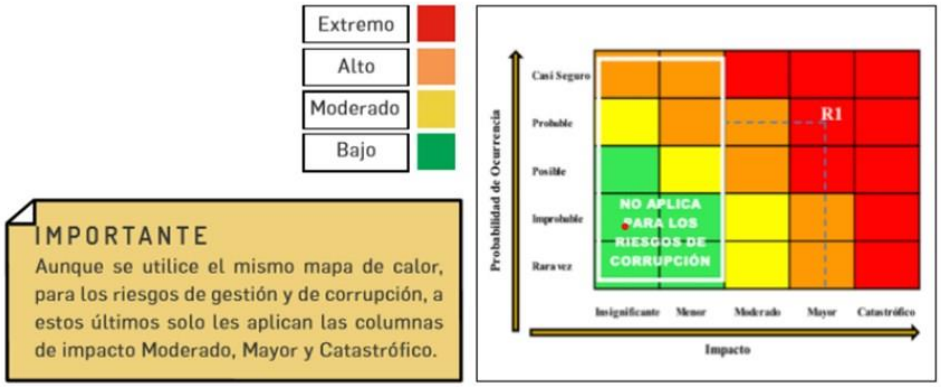
Tabla valoración riesgos de corrupción:

No.	Pregunta: Si el riesgo de corrupción se materializa podría.....	RIESGO 1 Respuesta SI	RIESGO 1 Respuesta NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad?		
5	¿Generar perdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar perdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios de los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía, u otros entes?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad en el sector?		
16	¿Ocasiona lesiones físicas o pérdida de vidas humanas? ***Si la respuesta a esta pregunta es afirmativa, el riesgo se considera automáticamente como CATASTRÓFICO***		
17	¿Afecta la imagen regional?		
18	¿Afecta la imagen nacional?		
19	¿Genera daño ambiental?		
	TOTAL	0	0

MODERADO	**Responder afirmativamente de 1 a 5 preguntas**
MAYOR	**Responder afirmativamente de 6 a 11 preguntas**
CATASTROFICO	**Responder afirmativamente de 12 a 18 preguntas**

Análisis del impacto en riesgos de corrupción

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

8. LINEAMIENTOS SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

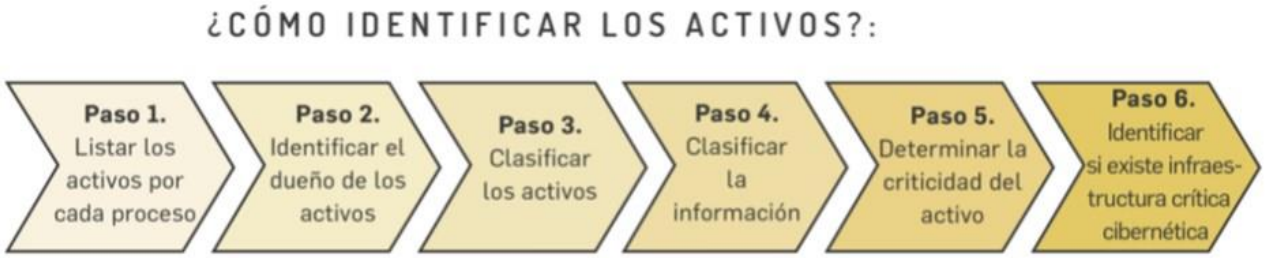
En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) [3], el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno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

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.

¿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 **qué es lo más importante que cada entidad y sus procesos poseen** (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 **qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano**, aumentando así su confianza en el uso del entorno digital

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

Pasos para la identificación de activos



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

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.

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

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar las siguientes tablas:

- Tabla de amenazas comunes
- Tabla de amenazas dirigida por el hombre

- Tabla de vulnerabilidades comunes

Identificación de Amenazas: Se plantean los siguientes listados de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos. A manera de ejemplo se citan las siguientes amenazas: Deliberadas (D), fortuito (F) o ambientales (A).

Tabla amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Fuente: ISO/IEC 27005:2009

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

Tabla de amenazas dirigida por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDoS Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de información
Intrusos (empleados con	Curiosidad	Asalto a un empleado

Fuente de amenaza	Motivación	Acciones amenazantes
entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Ganancia monetaria	Chantaje

Fuente: ISO/IEC 27005:2009

Identificación de vulnerabilidades: la entidad pública puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tabla de vulnerabilidades comunes

VULNERABILIDADES	
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla

Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización Ausencia de procedimiento de registro/retiro de usuarios	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para
	muchas actividades que la entidad no tenga documentadas y formalizadas como
	uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

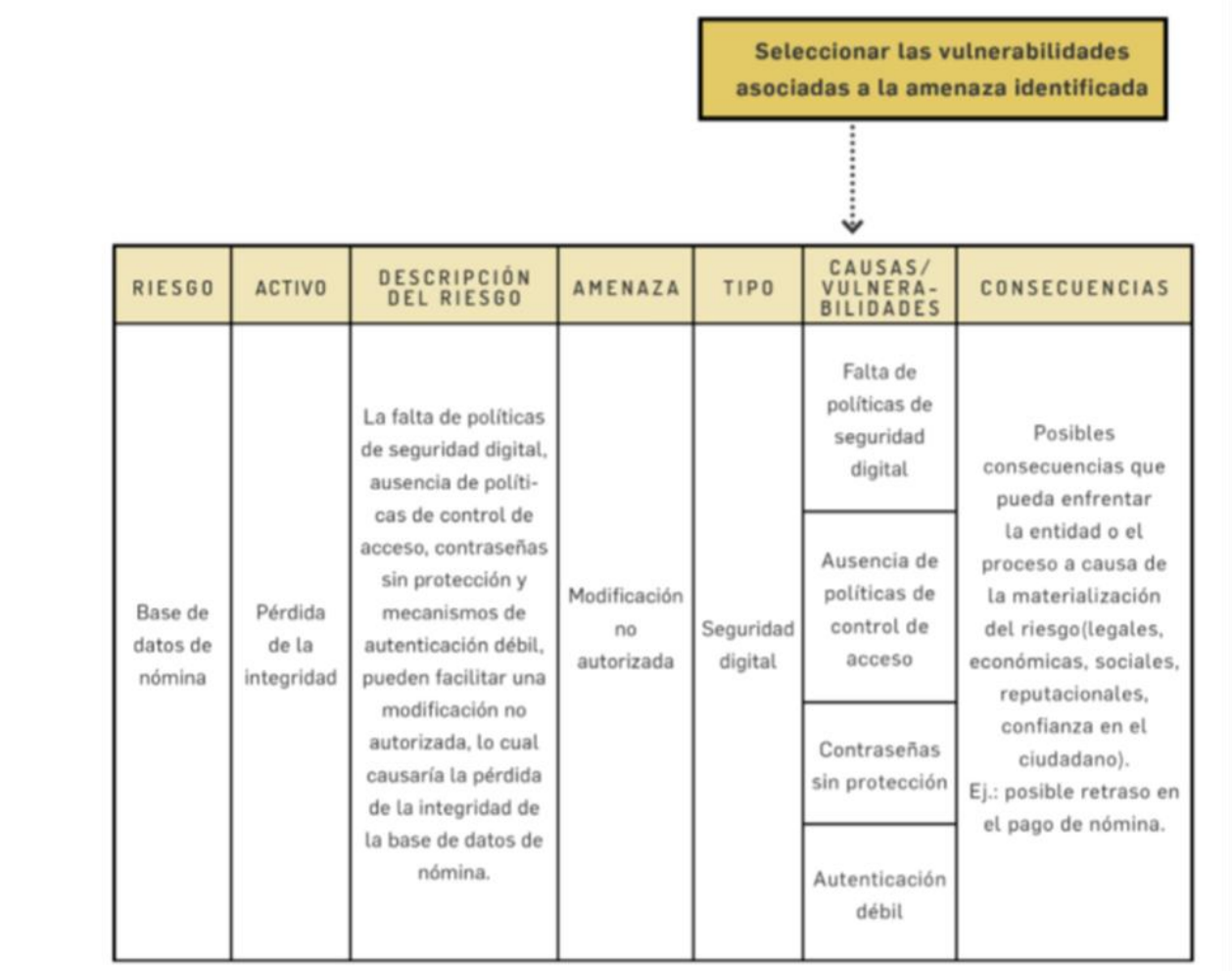
Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no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

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

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

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

A continuación, se observa un ejemplo de identificación del riesgo sobre un activo como es la base de datos de nómina.



RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas 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	

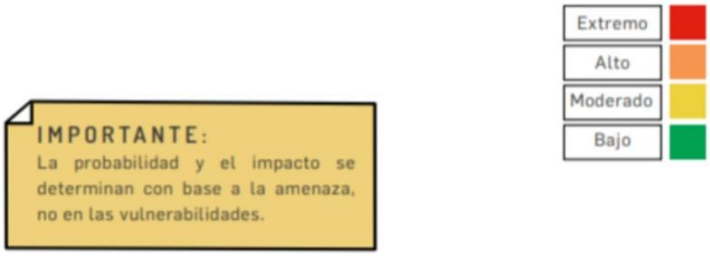
Importante existirán tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

Valoración del riesgo: Para esta etapa se asociaron las tablas de probabilidad e impacto definidas en la primera parte de la presente guía.

Valoración del riesgo en seguridad de la información

RIESGO	ACTIVO	AMENAZA	VULNERABILI-DAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confiden-cialidad	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.



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

9. MONITOREO DE LOS RIESGOS

La entidad monitorea y revisa anualmente la gestión de los riesgos, de acuerdo con lo establecido en la Política de Administración el riesgo.

Los líderes de los procesos con el apoyo de su equipo de trabajo, presentan informe periódicamente, en el Formato GC-Fr27 Informe Análisis de Gestión del Riesgo y Efectividad de los Controles sobre su gestión a la Dirección General Administrativa, cuyo fin es brindar apoyo en el seguimiento al cumplimiento de la gestión llevada a cabo por la primera y segunda línea de defensa. Con ello, la línea estratégica genera recomendaciones y/o acciones de mejora, retroalimenta al Comité de Gestión del Desempeño Institucional sobre los ajustes que se deban hacer frente a la gestión del riesgo.

10. MAPA DE RIESGO

El mapa de riesgos estará disponible para la consulta de todos los servidores, en https://www.senado.gov.co/ . Los líderes de procesos y sus equipos de trabajo deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser tramitada con la División de Planeación y Sistemas.

Será la Oficina Asesora de Planeación la responsable de la publicación del mapa de riesgos de corrupción en la página web de la Entidad; esta publicación se realizará cada vez que se realicen ajustes a la información registrada por los procesos.

11. ANEXOS

Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5. DAFP

12. FORMATOS

- GC- Fr08 Formato Mapa de Riesgos
- GC-Fr27 Informe Análisis de Gestión del Riesgo y Efectividad de los Controles

13. DOCUMENTOS RELACIONADOS

- GC-Pi02 Política de Administración del Riesgo

14. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 002// Rev. 1// FV. 29 de mayo de 2023

  Cambios:

  - Se solicita la modificación a la "Guía para la administración del riesgo", con el fin de complementar la información en la Identificación de los puntos de riesgo, ya que aquellos pueden estar relacionados con los procedimientos, sus lineamientos o a un activo de seguridad de la información.
  - En el apartado nro. 9. Monitoreo de Riesgos se incluye la información para presentación del Informe semestral sobre la gestión del riesgo y la efectividad de los controles a la Dirección General Administrativa.
  - Se incluye el Formato: GC-Fr27 Informe Análisis de Gestión del Riesgo y Efectividad de los Controles.

Justificación: Modificación

Responsable: Oscar Ernesto Luquez Ardila

Fecha: 2023-06-09

- Ver. 001// Rev. 1// FV. 26 de mayo de 2022

Cambios:

Se crea el documento con el fin de establecer los lineamientos y criterios metodológicos para una adecuada gestión del riesgo en el Senado de la República.

Justificación: Creación

Responsable: Lina Marcela Piñeros Lopez

Fecha: 2022-07-11

ELABORÓ	REVISÓ	APROBÓ
Nombre: Mary Rodríguez / Claudia Guerrero Tavera	Nombre: Pablo Eduardo Alzate Pérez	Nombre: Comité Institucional de Gestión y Desempeño del Senado de la República
Cargo: Profesional Universitaria / Contratista Div. Planeación y Sistemas	Cargo: Jefe División de Planeación y Sistemas.	No. Acta 23.05 y Fecha 29 de Mayo de 2023

Maria Fernanda Cardona Suarez @ 2023-06-09, 19:04:06