Al contestar por favor cite estos datos:
Radicado No. 20181500560823
Fecha: 18-12-2018

Cód. 150
Bogotá D.C

MEMORANDO

PARA: **Dr. JUAN MIGUEL DURÁN PRIETO**
Secretario Distrital de Gobierno

SEBASTIAN CASTRO GAONA
Jefe Oficina Asesora de Planeación

DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: Informe comparativo para el Manual de gestión del riesgo de la Secretaria Distrital de Gobierno frente a los lineamientos emitidos por el Departamento Administrativo de la Función Pública.

Respetados Doctores,

La Oficina de Control Interno Realizó un ejercicio comparativo entre el Manual de riesgos institucional y los lineamientos emitidos por el Departamento Administrativo de la Función Pública. De acuerdo con lo anterior, se remite el informe correspondiente con el fin de contribuir en el mejoramiento de la gestión de riesgos en la Entidad.

Cordial Saludo,

LADY JOHANA MEDINA MURILLO

Anexos:

- Informe comparativo para el Manual de gestión del riesgo de la Secretaria Distrital de Gobierno frente a los lineamientos emitidos por el Departamento Administrativo de la Función Pública.

Elaboró: Daissy Tatiana Santos Yate
Aprobó: Lady Johanna Medina M.

Informe comparativo para el Manual de gestión del riesgo de la Secretaria Distrital de Gobierno frente a los lineamientos emitidos por el Departamento Administrativo de la Función Pública

Contenido

1. Introducción

El Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y Comunicaciones presentaron la Versión No 4 “Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital”, como una herramienta con enfoque preventivo, vanguardista y proactivo que permitirá el manejo del riesgo, así como el control en todos los niveles de la entidad pública, brindando seguridad razonable frente al logro de sus objetivos.

De acuerdo lo anterior, se verificará y validará el Manual de Gestión del Riesgo de la Secretaria Distrital de Gobierno – SDG, con la versión del 11 de octubre de 2018; teniendo en cuenta que la justificación de esta actualización determina que el documento es ajustado según lo establecidos en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, en los roles y responsabilidades se realiza el ajuste de acuerdo con las líneas de defensa establecidas por el MIPG, se cambian las instancias frente a la administración del riesgo en cuanto al cumplimiento de los lineamientos y criterios contemplados en la Guía del DAFP.

2. Objetivo de la verificación

Realizar un ejercicio comparativo entre el Manual de riesgos institucional y los lineamientos emitidos por el Departamento Administrativo de la Función Pública, con el fin de identificar oportunidades de mejora para la gestión de riesgos en la Entidad.

Nota: las recomendaciones que se presentan en el informe son oportunidades de mejora y no se configuran como incumplimientos en la gestión de riesgos de la Entidad.

3. Verificación de Criterios

2.1. Alcance

El alcance definido en el manual institucional se encuentra definido de la siguiente manera:

"Este manual presenta la metodología desarrollada por la SDG para la administración y gestión de los riesgos establecidos en los procesos de la entidad; define las etapas que permiten la definición del contexto del riesgo, la identificación de los riesgos, su análisis, evaluación, tratamiento, monitoreo, seguimiento y revisión por el comité institucional de gestión y desempeño".

De acuerdo con lo anterior, y teniendo en cuenta que en el numeral 9.2.1 Tipología de riesgos; se establecen los tipos de riesgos a administrar por la entidad con los lineamientos establecidos en el manual, se recomienda replantear el alcance, incluyendo la aplicación para las diferentes tipologías de riesgo definidas en la entidad dentro del alcance del manual.

2.2. Paso 1. Política de Administración del Riesgo

La política de Administración del Riesgo es una declaración establecida por la Alta Dirección de la entidad con el liderazgo del representante legal y la participación del Comité Institucional de Coordinación de Control Interno, de 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.

La política de administración del riesgo puede adoptar la forma de un manual o guía de riesgos, donde se deben incluir mínimo los siguientes aspectos:

- Objetivo
- Alcance
- Niveles de Aceptación del Riesgo o Tolerancia al Riesgo
- Términos y Definiciones
- Estructura para la Gestión del Riesgo

Se verifica que la Política de Administración del Riesgo en la SDG se contempla en el Documento PLE-PIN-M001 "Manual de Gestión del Riesgo" en su Versión No 03 con vigencia desde el 11 de octubre de 2018. En cuanto a los aspectos mínimos se da cumplimiento de la siguiente manera:

- 1.Objetivo
- 1.1.Objetivos Específicos
- 2. Alcance
- 9.5 Nivel de tolerancia al riesgo
- 9.6 Perfil de riesgo
- 3. Términos y Definiciones
- 9. Política de Administración del Riesgo

2.3. Paso 2: identificación de riesgos

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

Los elementos que componen este paso son:

- 2.1. Establecimiento del contexto
- 2.2. Identificación del Riesgo.

2.3.1. Establecimiento del contexto

El establecimiento del contexto consiste en la definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar. Se establece el establecimiento del contexto a partir de:

- 2.1.1. Establecimiento del contexto externo
- 2.1.2. Establecimiento del contexto interno
- 2.1.3. Establecimiento del contexto del proceso

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.1 Contexto del Riesgo

El objetivo de esta etapa es identificar e incorporar el contexto del riesgo en la administración de riesgos de la Entidad. El resultado esperado consiste en un análisis DOFA institucional y por proceso/Situaciones preliminares negativas que pueden reflejarse en alguno de los elementos de un riesgo (Evento, fuente de riesgo, causas, área de impacto, consecuencia) del proceso objeto de análisis en la etapa de identificación del riesgo.

El apartado 9.1 Contexto del Riesgo está compuesto de los siguientes subapartados:

- 9.1.1. Descripción
- 9.1.2. Propósito
- 9.1.3. Método para generar el contexto del riesgo
- 9.1.4. Periodicidad
- 9.1.5. Resultado y articulación con la matriz de riesgos de proceso

Frente a la información presentada en el Manual de la Entidad; no existe claridad sobre cómo se da cubrimiento al contexto del proceso, definido en los lineamientos emitidos por el Departamento Administrativo de la Función Pública DAFP.

Respecto a seguridad de la información, en el contexto, se recomienda incluir la Identificación de activos de seguridad de la información, lo anterior, teniendo en cuenta que en el apartado 9.2.1.2 Riesgos de seguridad de la información ni en el contexto, se define la metodología para la identificación de los activos.

2.3.2. Identificación de riesgos – técnicas para la identificación de riesgos de Gestión y de Corrupción

La identificación del Riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.2 Identificación del Riesgo

El objetivo de esta etapa es identificar y desarrollar los elementos que componen la etapa de identificación del riesgo. El resultado esperado consiste en la elaboración de la Matriz de Riesgos con evento, fuente de riesgo, causa, área de impacto, consecuencia y nivel del riesgo registrados.

El apartado 9.2 Identificación del Riesgo está compuesto de los siguientes subapartados:

- 9.2.1. Tipología de riesgos

En el marco de los sistemas de gestión de la SDG, existen diferentes tipos de riesgo que deben identificarse y controlarse: Riesgos de Calidad, Riesgos de Seguridad de la Información, Riesgos de seguridad y salud en el trabajo, Riesgos ambientales, Riesgos de credibilidad, buen nombre y reputación y Riesgos de corrupción.

- 9.2.2 Estructura del Riesgo

La identificación de los riesgos comprende el establecimiento de cuatro aspectos fundamentales:

1. Evento
2. Causa
3. Consecuencia
4. Nivel organizacional

Con el fin de complementar las orientaciones que deben atender los procesos para la identificación de los riesgos, se recomienda revisar los siguientes aspectos:

- *Los eventos de los riesgos de corrupción deberán contener los siguientes elementos: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.*
- *Para determinar las causas de los riesgos de corrupción se recomienda el análisis de hechos de corrupción -si los hay- presentados en los últimos años en la entidad, las quejas, denuncias e investigaciones adelantadas; así como los actos de corrupción presentados en entidades similares*
- *Las consecuencias de los riesgos de corrupción deberán adicionalmente contener explícitamente el incumplimiento o afectación negativa a los principios de la función pública en la gestión de la Entidad, a los usuarios o a la relación de la Entidad con la ciudadanía.*
- *Dentro de los riesgos de Seguridad de la Información, un evento se asocia a la noción de incidente, que corresponde a la presencia identificada de una condición del activo de información que tiene una probabilidad significativa de comprometer la prestación de los servicios, e indica una posible violación de la seguridad de la información (confidencialidad, integridad y/o disponibilidad).*

2.4. Paso 3. Valoración de Riesgos

Esta etapa consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE) para luego confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

Los elementos que componen este paso son:

- 3.1. Análisis de Riesgos
- 3.2. Evaluación de Riesgos
- 3.3. Monitoreo y Revisión
- 3.4. Seguimiento Riesgos de Corrupción

2.4.1. Análisis de Riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE). El análisis de Riesgos se consigue a partir de:

- 3.1.1. Análisis de Causas
- 3.1.2. Análisis de la probabilidad
- 3.1.3. Análisis del impacto

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.3 Análisis del riesgo

El objetivo de esta etapa es calcular la evaluación del riesgo inherente a partir de su probabilidad e impacto. El resultado esperado es la elaboración de la Matriz de Riesgos con cálculo de probabilidad, impacto y riesgo inherente registrado.

- 9.2.2.2. Causas

La identificación de las causas debe involucrar el análisis y definición de los siguientes elementos: Fuente de riesgo y Definición de las causas (Falta, ausencia, inexistencia, debilidad + controles asociados al evento (acto y fuente)

- 9.3.1 Probabilidad

La probabilidad del riesgo se cataloga en cinco niveles que son: raro, improbable, posible, probable y casi seguro, de acuerdo con los siguientes criterios:

PROBABILIDAD	RARO 1	Se estima o se cuenta con información precisa que da cuenta de que, dadas las circunstancias, el riesgo puede ocurrir en menos del 5% de las ocasiones en las que se realiza la actividad asociada a éste.
	IMPROBABLE 2	Se estima o se cuenta con información precisa que da cuenta de que, dadas las circunstancias, el riesgo puede ocurrir entre el 5% y 15% de las ocasiones en las que se realiza la actividad asociada a éste.
	POSIBLE 3	Se estima o se cuenta con información precisa que da cuenta de que, dadas las circunstancias, el riesgo puede ocurrir entre el 15% y 30% de las ocasiones en las que se realiza la actividad asociada a éste.
	PROBABLE 4	Se estima o se cuenta con información precisa que da cuenta de que, dadas las circunstancias, el riesgo puede ocurrir entre el 30% y 50% de las ocasiones en las que se realiza la actividad asociada a éste.
	CASI SEGURO 5	Se estima o se cuenta con información precisa que da cuenta de que, dadas las circunstancias, el riesgo puede ocurrir en más del 50% de las ocasiones en las que se realiza la actividad asociada a éste.

La probabilidad de los riesgos de seguridad y salud en el trabajo se analiza y evalúa con base en los siguientes niveles:

Nivel de Probabilidad (NP)	Valor NP	Significado
Muy alto (MA)	Entre 40 y 24	Situación deficiente con exposición continua, o muy deficiente con exposición frecuente. Normalmente la materialización del riego ocurre con frecuencia
Alto (A)	Entre 20 y 10	Situación deficiente con exposición frecuente u ocasional, o bien situación muy deficiente con exposición ocasional o esporádica. La materialización del riego es posible que suceda varias veces en la vida laboral.
Medio (M)	Entre 8 y 6	Situación deficiente con exposición esporádica, o bien situación mejorable con exposición continuada o frecuente. Es posible que suceda el daño alguna vez.
Bajo (B)	Entre 4 y 2	Situación mejorable con exposición ocasional o esporádica, o situación sin anomalía destacable con cualquier nivel de exposición. No es esperable que se materialice el riesgo, aunque puede ser concebible.

En los casos que no se cuente con información suficiente para definir la probabilidad del evento, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de los factores internos y externos.

Se recomienda que los integrantes del equipo de trabajo implementen la tabla de priorización de probabilidad:

Tabla 9. Priorización de probabilidad

N°	RIESGO	P1	P2	P3	PROMEDIO

- 9.3.2. Impacto del Riesgo

La calificación del impacto se realiza de acuerdo con el área de impacto establecida según la consecuencia del riesgo objeto de análisis, definida en la etapa previa de identificación del riesgo. El impacto se cataloga en cinco niveles que son: mínimo, menor, moderado, mayor o catastrófico.

ÁREA DE IMPACTO	IMPACTO	CUANTITATIVO	CUALITATIVO
Calidad	Mínimo	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5%del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.
	Menor	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1%del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
	Moderado	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
	Mayor	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional
	Catastrófico	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018

El impacto del riesgo de seguridad de la información depende del valor del activo o conjunto de activos de información afectados por dicho riesgo.

ÁREA DE IMPACTO	NIVEL	VALOR DEL IMPACTO	IMPACTO CUANTITATIVO	IMPACTO CUALITATIVO
Seguridad de la Información	Mínimo	1	Afectación ≥X% de la **población** Afectación ≥X% del **presupuesto** anual de la entidad No hay **Afectación medioambiental**	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad
	Menor	2	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación leve del Medio Ambiente requiere de ≥X días de recuperación	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
	Moderado	3	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación leve del Medio Ambiente requiere de ≥X semanas de recuperación	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros
	Mayor	4	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación importante del Medio Ambiente que requiere de ≥X meses de recuperación	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
	Catastrófico	5	Afectación ≥X% de la población Afectación ≥X% del presupuesto anual de la entidad Afectación muy grave del Medio Ambiente que requiere de ≥X años de recuperación	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros Afectación muy grave confidencialidad de la información debido al interés particular de los empleados y terceros

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018

El impacto de los riesgos de corrupción se calificará de acuerdo con el puntaje obtenido de la siguiente tabla:

Tabla 10: Criterios para calificar el impacto- Riesgos de Corrupción

N°	PREGUNTA: Si el riesgo de corrupción se materializa podría	RESPUESTA	
		Si	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 pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida 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 o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente?		
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 del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen distrital?		
18	¿Generar daño ambiental?		

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018. Adaptado de Secretaría de Transparencia de la presidencia de la república.

- Responder afirmativamente de UNO 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.**

Para los criterios de definición del impacto del riesgo de corrupción, se recomienda ajustar de acuerdo con la actualización realizada por el Departamento Administrativo de la Función Pública – DAFP.

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Nivel de impacto MAYOR

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

El nivel de riesgo INHERENTE se calcula a partir del resultado de multiplicar el valor asignado a cada nivel tanto de probabilidad como de impacto en la matriz de riesgos:

PROBABILIDAD	IMPACTO: MÍNIMO	MENOR	MODERADO	MAYOR	CATASTRÓFICO
RARO	Aceptable	Aceptable	Tolerable	Tolerable	Tolerable
IMPROBABLE	Aceptable	Tolerable	Moderado	Moderado	Importante
POSIBLE	Tolerable	Moderado	Moderado	Importante	Importante
PROBABLE	Tolerable	Moderado	Importante	Inaceptable	Inaceptable
CASI SEGURO	Tolerable	Importante	Importante	Inaceptable	Inaceptable

ZONA DE RIESGO INHERENTE

ZONA DE RIESGO INHERENTE

El mapa calor para los riesgos de corrupción no tendrá en cuenta las columnas de impacto: mínimo y menor, dado que estos riesgos son significativos

2.4.2. Evaluación de Riesgos

En este punto se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL). La evaluación de riesgos se consigue a partir de:

- 3.2.1. Riesgo Inherente
- 3.2.2. Diseño y Valoración de Controles
- 3.2.3. Riesgo Residual
- Tratamiento del Riesgo
- Actividades de Control

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.4 Evaluación del riesgo

El objetivo de esta etapa es determinar la existencia de controles y su calificación a partir de la valoración de sus características, para luego hallar el riesgo residual. El resultado esperado consiste en la elaboración de la Matriz de Riesgos con controles existentes identificados, calificados y valor de riesgo residual individual.

- 9.4.1 Calificación de los controles

Los mecanismos de manejo de los riesgos son los controles, los cuales son acciones permanentes orientadas a reducir la probabilidad de ocurrencia y/o el impacto. En las matrices de riesgos por proceso se deberá registrar el control, teniendo en cuenta los siguientes pasos:

Tabla 11: para el diseño de controles

PASOS	DESCRIPCIÓN
1	Debe tener definido el responsable de realizar la actividad de control.
2	Debe tener una periodicidad definida para su ejecución.
3	Debe indicar cuál es el propósito del control.
4	Debe establecer el cómo se realiza la actividad de control.
5	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
6	Debe dejar evidencia de la ejecución del control.

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018

La evaluación de la efectividad del control se realizará con base en los siguientes criterios:

Tabla 12: evaluación de controles

Criterio de evaluación	Aspecto por evaluar en el diseño del control	Respuesta	Calificación
1.Responsable	¿Existe un responsable asignado a la ejecución del control?	Aginado	15
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	No Aginado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3.Propósito	Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0
5.Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6.Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?	Completa	15
		Incompleta	10
		No existe	0

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública.

- 9.4.2 Resultados de la evaluación del diseño del control

El resultado de la sumatoria obtenida en la evaluación del control definirá el rango de calificación del diseño del control:

Rango de calificación del diseño	Resultado - peso en la evaluación del diseño del control
Fuerte	Entre 96 y 100
Moderado	Entre 86 y 95
Débil	Entre 0 y 85

Sí la calificación del diseño del control es débil, la segunda línea de defensa (Oficina Asesora de Planeación) deberá informar al líder del proceso, para que este establezca las acciones a las que haya lugar para aumentar la calificación a nivel moderado o fuerte.

- 9.4.3 Resultado de la evaluación de la ejecución del control

Aunque un control este bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. Es responsabilidad de la primera línea de defensa asegurar la implementación de los controles, reportar el monitoreo y materialización de los riesgos, para ello deberá hacer uso la siguiente tabla:

Peso individual del diseño (DISEÑO)	El control se ejecuta de manera consistente por los responsables (EJECUCIÓN)	**Solidez individual** de cada control fuerte:100; moderado: 50; débil:0	Debe informar al líder de proceso la necesidad de fortalecer el control
Fuerte calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + fuerte = fuerte	NO
	Moderado (algunas veces)	Fuerte + moderado= moderado	NO
	Débil (no se ejecuta)	Fuerte + débil= débil	SI
Moderado Calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado + fuerte = moderado	NO
	Moderado (algunas veces)	Moderado + moderado = moderado	NO
	Débil (no se ejecuta)	Moderado + débil = débil	SI
Débil Entre 0 y 85	Fuerte (siempre se ejecuta)	Débil + Fuerte = débil	SI
	Moderado (algunas veces)	Débil + moderado = débil	SI
	Débil (no se ejecuta)	Débil + débil = débil	SI

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018

- 9.4.4 Solidez del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas y a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo, para esto se utiliza la solidez del conjunto de controles para cada uno de los riesgos, este se obtiene calculando el promedio aritmético simple de los controles por cada riesgo.

- 9.4.5 Valoración del riesgo residual

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Tabla 13. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos

Solidez del conjunto de controles	Los controles ayudan a disminuir la probabilidad	Los controles ayudan a disminuir el impacto	# Columnas en la matriz que se desplaza en el eje de la probabilidad	# Columnas en la matriz que se desplaza en el eje del impacto
Fuerte	Directamente	Directamente	2	2
	Directamente	Indirectamente	2	1
	Directamente	No disminuye	2	0
	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
	Directamente	Indirectamente	1	0
	Directamente	No disminuye	1	0
	No disminuye	directamente	0	1

Fuente: Guía de Administración del Riesgo Departamento Administrativo de la Función Pública. Versión 1.2018

Es importe tener en cuenta que:

Si la solidez de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

Si se está analizando un riesgo de corrupción. Únicamente se realizará disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

- 9.7 Tratamiento

El objetivo de esta etapa es establecer los planes de tratamiento o mejora de acuerdo con los criterios definidos según el nivel de riesgo residual individual. El resultado esperado consiste en la elaboración de la Matriz de Riesgos con planes de mejora formulados, registrados y asociados a cada riesgo de acuerdo a los criterios definidos.

De acuerdo con su propósito, las principales alternativas de acciones de tratamiento son:

ALTERNATIVAS DE TRATAMIENTO DE LOS RIESGOS		
TIPO DE ACCIÓN	DESCRIPCIÓN DE LA ACCIÓN	ZONA DE RIESGO RESIDUAL EN LA QUE ES APLICABLE
ASUMIR EL RIESGO	Hace referencia a la aceptación del riesgo y las pérdidas que pueden quedar después de la aplicación del control. Esta alternativa no implica el desarrollo de ninguna acción concreta que deba ser incluida en el plan de mejoramiento del proceso.	ACEPTABLE
EVITAR/ EL RIESGO	Previene la materialización del riesgo, mediante la incorporación o fortalecimiento de controles al interior de los procesos, orientados a disminuir la probabilidad de ocurrencia o el impacto	MODERADA INACEPTABLE
COMPARTIR / TRANSFERIR EL RIESGO	Formulación y desarrollo de acciones preventivas y/o correctivas en asocio con otros agentes al interior de la entidad. Cuando la acción necesaria a implementar para mitigar el riesgo excede los recursos o la capacidad del proceso, ésta se deberá escalar de manera oportuna al proceso o dependencia que corresponda. Ejemplo: contratos de riesgo compartido, pólizas de amparo, gestión conjunta con otras dependencias de acuerdo a sus competencias.	MODERADA INACEPTABLE

En el caso de los riesgos de corrupción no admiten aceptación del riesgo, por lo cual siempre debe conducir a un tratamiento en donde la redacción deberá ser precedida además por la sigla del proceso correspondiente.

Una vez identificado el nivel de riesgo residual, es necesario adelantar acciones de tratamiento frente a ellos, orientadas a fortalecer los controles existentes o institucionalizar uno nuevo, para asegurar que se reduzca la probabilidad de ocurrencia del riesgo (control preventivo), o se fortalezca la capacidad de respuesta de la entidad ante su materialización (control correctivo).

Tratamiento del riesgo = Acción preventiva

⇩

Fortalecimiento o institucionalización de un control

2.4.3. Monitoreo y Revisión

El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión del MIPG de "Control interno", que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad.

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.8 Monitoreo y/o seguimiento de los riesgos

El objetivo de esta etapa es monitorear el comportamiento de los riesgos y la efectividad de su tratamiento. El resultado esperado consiste, en primera instancia se registra en la matriz de riesgos en el campo en el cual se relaciona la manera de identificar cómo se comportó el/los riesgo/s, en términos de qué insumo de debe tener en cuenta, qué indagar y/o qué revisar y cómo reportar la materialización bajo esos criterios. En segunda instancia, el segundo resultado esperado es el reporte del monitoreo permanente y periódico por parte de los servidores públicos de la Entidad según sus roles y responsabilidades a través de los mecanismos dispuestos para tal fin.

Se determina la responsabilidad de cada una de las líneas de defensa frente al monitoreo y seguimiento de los riesgos.

- 9.8.1 Monitoreo al tratamiento

El líder del proceso - con el acompañamiento del promotor de mejora local o central y el referente ambiental (en el caso de las alcaldías locales)-, efectuará seguimiento al avance de las acciones de tratamiento a los riesgos, con base en las evidencias que carguen los responsables de tales acciones en el Aplicativo Gestión para la Mejora vigente en la entidad, con la oportunidad que allí se establezca

La periodicidad del monitoreo del tratamiento de los riesgos de corrupción será, como mínimo, la establecida en las disposiciones normativas que regulan dicha materia, es decir, cuatrimestral.

- 9.8.2 Monitoreo al comportamiento de los riesgos

Monitoreo periódico: Con una periodicidad trimestral, los líderes de los procesos, -con el acompañamiento del promotor de mejora local o central y el referente ambiental (en el caso de las alcaldías locales)-, realizarán un reporte de los resultados del monitoreo y análisis constante de la totalidad de los riesgos identificados, materializados y potenciales de sus procesos; así como de la aplicación y efectividad de los controles establecidos para su gestión.

Los resultados de dicho análisis deben ser reportados a la OAP por los promotores de mejora local o central y/o el ambiental según corresponda, a través del mecanismo dispuesto para tal fin. Una vez se reciba el reporte, será responsabilidad de cada analista de proceso, la alimentación de la base de datos de consolidación del monitoreo de los riesgos de la entidad.

El reporte de la existencia o materialización de los riesgos de corrupción por parte de los promotores de mejora de proceso no se efectuará a través del mismo mecanismo o herramienta del monitoreo de riesgos permanente. En tal caso, se deberá reportar a las instancias o autoridades competentes, mediante los canales formalmente establecidos.

Se presenta incumplimiento del criterio Indicadores de Gestión del Riesgo, en la manera en que no se precisa en el Manual la metodología para el diseño y evaluación de los indicadores de gestión del riesgo (Eficacia y Efectividad).

2.4.4. Seguimiento Riesgos de Corrupción

El Jefe de Control Interno o quien haga sus veces, 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.

Se verifica cumplimiento de este punto en los apartados del Manual de Gestión del Riesgo de la SDG de la siguiente manera:

- 9.8 Monitoreo y/o seguimiento de los riesgos

En el caso de los riesgos de corrupción, la OAP consolidará la información del comportamiento de tales riesgos que reporten los líderes de cada proceso en las sesiones de seguimiento al comportamiento y tratamiento de los riesgos.

La periodicidad del monitoreo del tratamiento de los riesgos de corrupción será, como mínimo, la establecida en las disposiciones normativas que regulan dicha materia, es decir, cuatrimestral.

- *Para el seguimiento a los riesgos de corrupción, se recomienda puntualizar en el numeral correspondiente, la función que ejerce la Oficina de Control Interno.*

- *Respecto a las etapas de administración de riesgo, en el manual institucional se establece la etapa de comunicación y consulta; la cual no se refleja en el desarrollo del documento; al respecto, se recomienda tener en cuenta: que no se precisa la metodología para el análisis de la comunicación y consulta con las partes involucradas, tanto internas como externas. Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.*

4. Verificación de cumplimiento a las herramientas “Formato matriz de riesgos PLE-PIN-F001” y “Formato matriz de riesgos de corrupción PLE-PIN-F002”

El formato Mapa y plan de tratamiento de riesgos para los riesgos de gestión y corrupción presenta los siguientes campos mínimos:

- No.
- Riesgo.
- Clasificación
- Causas
- Probabilidad
- Impacto
- Riesgo residual
- Opción de manejo
- Actividad de control
- Soporte
- Responsable

- Tiempo
- Indicador

N.	RIESGO	CLASIFICACIÓN	CAUSAS	PROBABILIDAD	IMPACTO	RIESGO RESIDUA	OPCIÓN MANEJO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR

El formato Mapa y plan de tratamiento de riesgos para los riesgos de seguridad digital presenta los siguientes campos mínimos:

- No.
- Riesgo
- Activo
- Tipo
- Amenazas
- Causas
- Probabilidad
- Impacto
- Riesgo residual
- Actividad de control
- Soporte
- Responsable
- Tiempo
- Indicador

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR

Se verifica la herramienta **Formato matriz de riesgos PLE-PIN-F001** y se validan los criterios de cumplimiento de la siguiente manera:

- El formato cumple con los siguientes campos mínimos de la siguiente manera:

DAFP	SDG
No.	No
Riesgo.	Evento
Clasificación	
Causas	Causa

Probabilidad	Probabilidad
Impacto	Impacto
Riesgo residual	Zona de Riesgo residual
Opción de manejo	
Actividad de control	Control
Soporte	Normatividad / Documento de la Entidad
Responsable	
Tiempo	
Indicador	

Se recomienda ajustar los formatos de mapas de riesgos de acuerdo con la actualización realizada al manual, teniendo en cuenta que, al realizar la verificación, se deben incluir nuevos campos, especialmente, en la definición de los controles.

Se verifica la herramienta **Formato matriz de riesgos de corrupción PLE-PIN-F002** y se validan los criterios de cumplimiento de la siguiente manera, teniendo en cuenta los campos mínimos de la Matriz de Seguimiento Mapa de Riesgos de Corrupción del DAFP:

- El formato cumple con los siguientes campos mínimos de la siguiente manera:

DAFP	SDG
No.	No.
Riesgo de Corrupción	Evento
Proceso	Procesos en los que tiene lugar
Causa	Causa
Análisis de los controles (Si o No)	Características de los controles
Efectividad de los controles (Si o No)	
Responsable de los controles (Si o No)	
Periodicidad de los controles (Si o No)	Periodicidad
Evidencias de los controles (Si o No)	Normatividad / Documento de la Entidad
Acciones de mejora (Si o No)	Acciones
Mejora de los controles (Si o No)	
Alertas tempranas (Si o No)	
Implementación de correctivos (Si o No)	
Alertas convertidas en denuncias	
Observaciones	

Se recomienda ajustar el formato para el mapa de riesgos de corrupción en cuanto a la escala de Impacto debido a que en el mapa de calor para los riesgos de corrupción no se tendrá en cuenta las escalas mínimo y menor, dado que estos riesgos son significativos. Además, no se tienen en cuenta los criterios para calificar el impacto en Riesgos de Corrupción.

5. Correspondencia entre la Guía de Riesgos – DAFP y el Manual de Gestión del Riesgo – SDG

Guía para la administración del riesgo y el diseño de controles en entidades públicas -DAFP	Manual de Gestión del Riesgo - SDG	Nivel de Cumplimiento
Paso 1. Política de Administración del Riesgo		
Objetivo	1.Objetivo 1.1.Objetivos Específicos	100
Alcance	2. Alcance	100
Niveles de Aceptación del Riesgo o Tolerancia al Riesgo	9.5 Nivel de tolerancia al riesgo 9.6 Perfil de riesgo	100
Términos y Definiciones	3. Términos y Definiciones	100
Estructura para la Gestión del Riesgo	9. Política de Administración del Riesgo	100
Paso 2: identificación de riesgos		
2.1. Establecimiento del contexto	9.1 Contexto del Riesgo	100
2.1.1. Establecimiento del contexto externo	9.1.1. Descripción	100
2.1.2. Establecimiento del contexto interno	9.1.1. Descripción	100
2.1.3. Establecimiento del contexto del proceso	9.1.3. Método para generar el contexto del riesgo	100
2.1.4. Identificación de activos de seguridad de la información	9.2.1.2 Riesgos de seguridad de la información	50
2.2. Identificación de riesgos - técnicas para la identificación de riesgos de Gestión y de Corrupción	9.2 Identificación del Riesgo 9.2.2 Estructura del Riesgo	100
2.2.2. Tipología de riesgos	9.2.1. Tipología de riesgos	100
Paso 3. Valoración de Riesgos		
3.1. Análisis de Riesgos	9.3 Análisis del Riesgo	100
3.1.1. Análisis de Causas	9.2.2.2. Causas	100
3.1.2. Análisis de la probabilidad	9.3.1 Probabilidad	100
3.1.3. Análisis del impacto	9.3.2. Impacto del Riesgo	100
3.2. Evaluación de Riesgos	9.4 Evaluación del riesgo	100
3.2.1. Riesgo Inherente	9.3.3. Determinación de la zona de riesgo inherente	100
3.2.2. Diseño y Valoración de Controles	9.4.1 Calificación de los controles 9.4.2 Resultados de la evaluación del diseño del control 9.4.3 Resultado de la evaluación de la ejecución del control 9.4.4 Solidez del conjunto de controles para la adecuada mitigación del riesgo	100
3.2.3. Riesgo Residual	9.4.5 Valoración del riesgo residual	100
Tratamiento del Riesgo	9.7 Tratamiento	100
Actividades de Control	9.7 Tratamiento	100
3.3. Monitoreo y Revisión	9.8 Monitoreo y/o seguimiento de los riesgos 9.8.1 Monitoreo al tratamiento	100
Mapa y Plan de Tratamiento de Riesgos	9.8.2 Monitoreo al comportamiento de los riesgos 9.8.3 Actualización de las matrices de riesgos	100
Indicadores de Gestión del Riesgo		0
3.4. Seguimiento Riesgos de Corrupción	9.8 Monitoreo y/o seguimiento de los riesgos	100
Comunicación y Consulta		0
Información, Comunicación y Reporte	9.8.1 Monitoreo al tratamiento 9.8.2 Monitoreo al comportamiento de los riesgos 9.8.3 Actualización de las matrices de riesgos	100

De acuerdo con la matriz anterior, el porcentaje de correspondencia del Manual institucional frente a los lineamientos del Departamento Administrativo de la Función Pública para el tema, se ubica en 91%.

6. Aspectos generales identificados sobre la metodología de riesgos institucional:

- Para asegurar el éxito e impacto positivo en la administración de riesgos de la Entidad a partir de los ajustes metodológicos realizados, se recomienda adelantar acciones de armonización del manual con las herramientas de mapas de riesgos; actualmente existen diferencias entre los lineamientos y las herramientas utilizadas.

- Respecto al proceso de actualización de las herramientas que se realiza actualmente, se recomienda tener en cuenta para su diseño aspectos como claridad en las orientaciones para el diligenciamiento, estructura clara del archivo, facilidad para el diligenciamiento de la información, funcionalidad de la herramienta, entre otros aspectos orientados a facilitar su adecuado uso por parte de los procesos al momento de realizar actualización o modificaciones a los riesgos.

- Se recomienda generar nuevas herramientas y ayudas metodológicas que le permitan a los servidores públicos y contratistas, adelantar la gestión adecuada de los riesgos identificados, como guías rápidas, tutoriales, presentaciones, entre otras ayudas que faciliten el manejo y apropiación del tema en la Entidad.

- Desarrollar espacios de socialización y capacitación en los ajustes metodológicos definidos en el manual vigente de la Entidad, mediante jornadas de capacitación presenciales y virtuales, espacios de sensibilización, talleres prácticos, entre otros.