Marco de Referencia Para la Gestión de Riesgos

SEC-GU-01 Versión 8

Dependencia

Dirección General- Comité Institucional de Coordinación de Control Interno

Objetivo

Establecer un esquema de identificación y evaluación de riesgos que aporte al logro de los objetivos del IDIGER fortaleciendo el enfoque preventivo, adaptando e integrando en los procesos el análisis de la incertidumbre como un factor que se puede mitigar a través controles y procedimientos para la toma de decisiones orientadas al cumplimiento de los objetivos estratégicos

Alcance

El presente marco de referencia aplica a todos los procesos y actividades del Instituto Distrital de Gestión de riesgos y Cambio Climático, contempla riesgos estratégicos, riesgos de proceso o de gestión, riesgos de corrupción, riesgos de seguridad digital, riesgos ambientales y de seguridad y seguridad en el trabajo a nivel estratégico.

Nota: Los riesgos ambientales y de seguridad y salud en el trabajo relacionados con las actividades ocupacionales, serán evaluados en las matrices definidas en los diferentes sistemas, estos serán gestionados de acuerdo a las metodologías adoptadas por los responsables de los procesos relacionados con el desarrollo de los sistemas de gestión de seguridad, salud en el trabajo y ambiente.

03/01/2019

1. POLITICA DE ADMINISTRACION DEL RIESGO

El Instituto Distrital de Gestión de Riesgos y Cambio Climático adopta las medidas descritas en el marco de referencia diseñado en la entidad, para administrar los riesgos de toda naturaleza (riesgos de proceso, corrupción, estratégicas, de seguridad digital y ambientales), valorados en los niveles "Medio", "Alto" y "Extremo", de tal forma que esta gestión contribuya con el logro de los objetivos estratégicos de la entidad y el desarrollo de su misionalidad.

Los riesgos de corrupción identificados tendrán la connotación de inaceptables y deberán incluir controles para eliminar las causas de ocurrencia, tal como lo establece la "Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas". Estos riesgos serán publicados en la página web de la entidad, en la sección particular de transparencia y acceso a la información pública de acuerdo al artículo 2.1.1.2.1.4 del Decreto 1081 de 2015, a más tardar el 31 de enero de cada año.

Teniendo en cuenta la estructura de los procesos, la gestión del riesgo y del cambio climático se concibe como una herramienta dinámica, por lo cual los instrumentos diseñados para tal fin son susceptibles de mejora y serán revisados permanentemente.

Para ello la entidad dispone los recursos necesarios y la participación del Nivel Directivo, mediante la definición de los instrumentos pertinentes, su estrategia de aplicación y los roles y responsabilidades de cada funcionario frente a los riesgos identificados, los cuales se establecen a partir de las líneas de defensa, relacionadas a continuación:

Tabla 1. Definición de Roles de acuerdo a las líneas de defensa

COMITÉ INSTITUCIONAL DE COORDINACION DE CONTROL INTERNO ALTA DIRECCIÓN		**DIRECTIVOS Y LIDERES DE PROCESO**	**SERVIDORES RESPONSABLES DE MONITOREO**	**OFICINA DE CONTROL INTERNO**
		OFICINA ASESORA DE PLANEACION		
LINEA ESTRATEGICA DE DEFENSA		PRIMERA LINEA DE DEFENSA Controles de Gerencia Operativa	SEGUNDA LINEA DE DEFENSA	TERCERA LINEA DE DEFENSA
RESPONSABILIDADES	Evalúa y define los lineamientos sobre la administración de los riesgos en la entidad	Identifica y valora los riesgos que pueden afectar el logro de los objetivos institucionales	Establecer un líder de la gestión de riesgos para coordinar las actividades Consolida los seguimientos a los mapas de riesgo	Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna
	Establece el marco general para el manejo de los riesgos valorados como altos y extremos	Establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección	**Oficina Asesora de Planeación** Realizar el Marco de referencia y de garantizar su pertinencia mediante revisión y actualización permanente	Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías

COMITÉ INSTITUCIONAL DE COORDINACION DE CONTROL INTERNO ALTA DIRECCIÓN		DIRECTIVOS Y LIDERES DE PROCESO	SERVIDORES RESPONSABLES DE MONITOREO	OFICINA DE CONTROL INTERNO
		OFICINA ASESORA DE PLANEACION		
	Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles.	Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos	Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada.	Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad
		Implementar procesos para identificar, disuadir y detectar fraudes.	Ayudar a la primera línea con evaluaciones del impacto de los cambios en el SCI	Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas
		Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos que afectan el cumplimiento de los objetivos institucionales y de sus procesos, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos.	Provee aseguramiento (evaluación) sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.
		Identifica y valora los riesgos que pueden afectar el logro de los objetivos institucionales	Consolida los seguimientos a los mapas de riesgo	Asesorar en metodologías para la identificación y administración de los riesgos
		Diseñar, implementar y monitorear los controles	Establecer un líder de la gestión de riesgos para coordinar las actividades	Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna
MONITOREO	Evalúa y define los lineamientos sobre la administración de los riesgos en la entidad	Establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección Diseñar, implementar y monitorear los controles	Ayudar a la primera línea con evaluaciones del impacto de los cambios en el SCI	Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías

2. GLOSARIO[1]

Riesgo de Gestión: Posibilidad que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencia.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

[1] **Departamento Administrativo de la función pública. (2018) Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades públicas. V1. P 7. 8**

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.

Gestión del Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de objetivos

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.

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

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impacta en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad

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

Riesgo Inherente: Es aquel al que enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto

Riesgo Residual: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo

Mapa de Riesgo: Documento con la información resultante de la gestión del riesgo

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.

Control: Medida que modifica al riesgo (Procesos, políticas, dispositivos)

Amenazas: Causa potencia de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

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

Disponibilidad: Propiedad de ser accesible y utilizable

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable

3. METODOLOGIA PARA LA ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES

El punto de partida para la administración de riesgos y oportunidades, es el conocimiento general de la entidad, del cual hace parte la planeación institucional, los objetivos estratégicos y el contexto de la organización.

Los objetivos estratégicos son el resultado que se espera para el cumplimiento de la misión y visión de la entidad, en el IDIGER, se establecieron 5 objetivos estratégicos orientados a:

1. Lograr colaboradores del IDIGER altamente motivados y competentes mediante la gestión del conocimiento, acciones de formación, bienestar y la provisión de bienes y servicios, para fortalecer la capacidad técnica, ejecutora y comunicativa de la entidad.
2. Generar y promover el conocimiento del riesgo y de los efectos del cambio climático mediante instrumentos y metodologías apropiadas y colaborativas para impulsar acciones de reducción, adaptación y dar soporte a las decisiones de desarrollo de la ciudad.
3. Lograr la apropiación de la reducción del riesgo, la respuesta a emergencias y la adaptación al cambio climático por parte de los sectores público, privado, y la comunidad, y ejecutar acciones para prevenir nuevas condiciones de riesgo, mitigar las existentes y contribuir al desarrollo sostenible de la ciudad.
4. Promover la ayuda mutua y solidaria entre los habitantes de la ciudad por medio del intercambio de experiencias y buenas prácticas, la educación, capacitación y comunicación, para reducir la vulnerabilidad de la población
5. Garantizar la efectiva respuesta a emergencias por medio de la coordinación de los ejecutores de los servicios de respuesta y de acciones de organización, capacitación, entrenamiento y equipamiento para salvaguardar la vida, los bienes y el ambiente, reducir el sufrimiento de las personas y mantener la gobernabilidad

El contexto de la organización se entiende como el entorno en el cual opera la entidad, es decir, las condiciones económicas, sociales, culturales, políticas, legales, ambientales o tecnológicas que inciden en la gestión de la entidad; contempla una dinámica interna y de los procesos que comprende la estructura institucional, cultura organizacional, objetivos del proceso, caracterizaciones, procedimientos relacionados, sistemas de información, recursos humanos y económicos con que cuenta la entidad, (cuando estos apliquen al proceso/proyecto)

Este contexto crea condiciones que afectan de manera positiva o negativa la gestión de la entidad en el desarrollo de su misionalidad, generando riesgos y oportunidades que, al identificarse y gestionarse de manera oportuna equilibran las acciones para asumir o prevenir la materialización de los riesgos, promoviendo la aplicación de controles y acciones que favorecen el cumplimiento de los objetivos estratégicos.

La administración del riesgo al ser un proceso dinámico, sistemático y lógico, se coordina desde la Oficina Asesora de Planeación, con asesoría y acompañamiento de la Oficina de Control Interno; se ejecuta en cada dependencias a partir de la identificación de riesgos estratégicos, de proceso, corrupción y de seguridad digital, y se monitorea a partir del seguimiento que periódicamente realizan los líderes de proceso y el monitoreo por la Oficina de Control Interno.

3.1. Descripción de metodología para la administración de riesgos y oportunidades.

El IDIGER tendrá en cuenta las orientaciones metodológicas establecidas en las guías o herramientas dispuestas para tal fin por el Departamento Administrativo de la Función Pública — DAFP, la Secretaría de Transparencia de la Presidencia de la República y las que puedan ser aplicables al tema de Administración de Riesgos, acorde a la dinámica y necesidades de la Entidad

La metodología de Administración de Riesgos que trata el presente numeral, se entiende implementada en la herramienta SEC-FT-13 Matriz *de riesgos y oportunidades,* en la cual cada dependencia registra los riesgos y oportunidades identificados teniendo en cuenta el contexto que da lugar a los mismos, establece las causas y consecuencias de los riesgos identificados, evalúa el nivel del riesgo mediante escalas de probabilidad e impacto y genera los controles para prevenir la materialización del riesgo inherente, de tal manera que los controles se orienten a disminuir la probabilidad o el impacto que generaría el riesgo.

De igual manera, mediante las casillas designadas para el seguimiento del control, los líderes y responsables de cada dependencia realizan monitoreo del estado de sus riesgos y finalmente la Oficina de Control Interno, realiza seguimiento a la administración de riesgos realizada por la dependencia y genera informes de seguimiento orientados a la mejora continua.

La estructura del documento se establece de la siguiente manera:

a. **Contexto Estratégico**: Contexto con el cual se relaciona el riesgo u oportunidad

b. **Proceso**: Proceso que identifica el riesgo

c. **Causas / Vulnerabilidad:** Causas y fuentes del riesgo basadas en el análisis de contexto para la entidad y el proceso, que pueden afectar el logro de los objetivos. A partir de los factores que se definan en el contexto es posible establecer las causas de los riesgos.
d. **Identificación del Riesgo y oportunidades:** La identificación del riesgo se realiza 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 u objetivos estratégicos. La identificación de riesgos supone un trabajo conjunto, en el cual por medio de lluvia de ideas, análisis de eventos o gestión del conocimiento, se podrá describir los riesgos que se relacionan al proceso o a la entidad.

Las preguntas claves para la identificación del riesgo permiten determinar:

- **¿Qué puede suceder?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **¿Cómo puede suceder?** Establecer las causas a partir de los factores determinados en el contexto
- **¿Cuándo puede suceder?** Determinar de acuerdo al desarrollo del proceso
- **¿Qué consecuencias tendría su materialización?** Determinar los posibles efectos por la materialización del riesgo La identificación de oportunidades De igual manera se identifican las oportunidades de los procesos.

Identificación de riesgos de corrupción: Para la identificación de riesgos de corrupción, es necesario responder las mismas preguntas definidas para riesgos de proceso o estratégicos, incluyendo en la descripción del riesgo los siguientes componentes en su definición, así: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Identificación de oportunidades: Para explicar la identificación de oportunidades, se parte de la base que el riesgo es un evento incierto que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos. Un riesgo puede tener una o más causas y, de materializarse, uno o más impactos. Una causa puede ser un requisito especificado o potencial, un supuesto, una restricción o una condición que crea la posibilidad de consecuencias tanto negativas como positivas. Los riesgos positivos son oportunidades, las cuales se dan al planificar adecuadamente una situación para que su resultado sea adecuado al cumplimiento de objetivos. Las preguntas para definir las oportunidades son las mismas que se hacen para identificar riesgos. Los riesgos positivos que ofrecen oportunidades dentro de los límites de la tolerancia al riesgo se pueden emprender a fin de generar un mayor valor.

El funcionario responsable de identificar las condiciones de riesgo y las oportunidades es el líder SIGD (Sistema integrado de Gestión Distrital), el responsable del proceso, quien valida la información y aprueba los riesgos identificados y la oficina Asesora de Planeación realiza el acompañamiento técnico a los procesos y estandariza la información para la administración de riesgos.

e. Valoración de Riesgos

La calidad y la credibilidad del análisis de riesgos requieren que se definan distintos niveles de probabilidad e impacto de los riesgos, específicos para el contexto del proceso. Cada riesgo se califica de acuerdo con su probabilidad de ocurrencia y con el impacto sobre un objetivo, en caso de que se materialice. Se debe determinar qué combinaciones de probabilidad e impacto dan lugar a una clasificación de riesgo alto, riesgo moderado y riesgo bajo

Probabilidad

Se analiza la posibilidad de ocurrencia del riesgo, la cual 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.

Tabla 2. Niveles de Probabilidad para riesgo de proceso, corrupción y seguridad Digital

Nivel	Descriptor	Frecuencia	Factibilidad
1	Improbable	No se ha presentado en los últimos 5 años	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)
2	Poco probable	Al menos 1 vez en los últimos 5 años	El evento puede ocurrir en algún momento
3	Probable	Al menos 1 vez en los últimos 2 años	El evento podrá ocurrir en algún momento
4	Posible	Al menos 1 vez en el último año.	Es viable que el evento ocurra en la mayoría de las circunstancias
5	Casi Seguro	Más de 1 vez al año.	Se espera que el evento ocurra en la mayoría de las circunstancias

Impacto

Se define como las consecuencias que puede tener la organización con la materialización de un riesgo.

A continuación se presentan las variables de evaluación, para impacto en riesgos de proceso, corrupción y de seguridad digital, en los tres casos la valoración se realiza teniendo en cuenta diferentes factores.

Impacto en riesgo de proceso

De acuerdo a la tabla definida a continuación, se evalúa el impacto que puede tener en la entidad la materialización del riesgo, la cual varía de acuerdo al tipo de riesgo identificado:

Tabla 3. Niveles de impacto para riesgo de proceso

Nivel	Descriptor	Impacto
1	Insignificante	• 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
2	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
3	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. • Reproceso de actividades y aumento de carga operativa
4	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. • Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.
5	Catastrófico	• Pérdida de cobertura en la prestación de los servicios de la entidad ≥50% • Impacto que afecte la ejecución presupuestal 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 • Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. • Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%

Impacto en riesgos de corrupción

El impacto en los riesgos de corrupción se evalúa, según respuesta a las preguntas que plantea la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades públicas. 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 si aplican para los demás riesgos.

Tabla 4. Preguntas que valoran el impacto para riesgos de corrupción

¿Afecta al grupo de funcionarios del proceso?	¿Genera intervención de los órganos de control, de la Fiscalía, u otro ente?
¿Afecta el cumplimiento de metas y objetivos de la dependencia?	¿Da lugar a procesos disciplinarios?
¿Afecta el cumplimiento de misión de la Entidad?	¿Da lugar a procesos fiscales?
¿Afecta el cumplimiento de la misión del sector al que pertenece la Entidad?	¿Da lugar a procesos penales?
¿Genera pérdida de confianza de la Entidad, afectando su reputación?	¿Genera pérdida de credibilidad del sector?
¿Genera pérdida de recursos económicos?	¿Ocasiona lesiones físicas o pérdida de vidas humanas?
¿Afecta la generación de los productos o la prestación de servicios?	¿Afecta la imagen regional?
¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?	¿Afecta la imagen nacional?
¿Genera pérdida de información de la Entidad?	¿Genera daño ambiental?

La valoración del impacto en los riesgos de seguridad digital se evalúa de acuerdo a los criterios definidos en el siguiente cuadro

Tabla 5. Niveles de impacto para riesgo de seguridad digital

Nivel	Descriptor	Impacto
1	Insignificante	Sin afectación de la integridad Sin afectación de la disponibilidad Sin afectación de la confidencialidad
2	Menor	Afectación leve de la integridad Afectación leve de la disponibilidad Afectación leve de la confidencialidad
3	Moderado	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
4	Mayor	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
5	Catastrófico	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 de la confidencialidad de la información debido al interés particular de los empleados y terceros

Una vez se valora la probabilidad e impacto, se genera la calificación automática en el formato *SEC-FT-13 Matriz de riesgos y oportunidades*, el cual mostrará el nivel de riesgo de acuerdo al cruce de probabilidad e impacto. Aquellos riesgos que debido a su naturaleza y/o impacto, se ubiquen en los espacios naranja, rojo y amarillo (Riesgo medio, alto y Extremo), requerirán de medidas de control que se orienten a prevenir y detectar la materialización de los riesgos.

Tabla 6 Valoración de riesgo

		IMPACTO				
		Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
FRECUENCIA	**Improbable**	Bajo	Bajo	Medio	Alto	Alto
	Poco probable	Bajo	Bajo	Medio	Alto	Extremo
	Probable	Bajo	Medio	Alto	Extremo	Extremo
	Posible	Medio	Alto	Alto	Extremo	Extremo
	Casi Seguro	Alto	Alto	Extremo	Extremo	Extremo

No aplica para riesgos de corrupción

Los controles a definir se deben orientar a políticas y procedimientos que contribuyan a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos de proceso y estratégicos.

f. **Valoración de los Controles Asociados al Riesgo**

Es necesario tener claridad sobre los puntos de control existentes en los procedimientos que conforman el proceso, los cuales permiten obtener la información necesaria para efectos de toma decisiones sobre las acciones que se desarrollarán con el fin de disminuir el nivel de riesgo.

Al definir las actividades de control por parte del proceso responsable, es importante considerar que los controles estén bien diseñados, es decir, que estos mitigan las causas que hacen que el riesgo se materialice, por lo cual para cada causa debe haber un control, que puede ser tan eficiente que ayude a mitigar varias causas.

Al momento de calificar el control, se responderán las preguntas que establecen si el diseño del control es adecuado, todas las respuestas deberán describir la justificación de la misma de tal manera que facilite el posterior monitoreo y seguimiento.

Pregunta 1: **¿Existe un responsable asignado a la ejecución del control? ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?**
El control debe iniciar con un cargo responsable o un sistema o aplicación, Evitar colocar áreas de manera general o nombres de personas, El control debe estar asignado a un cargo específico.

Pregunta 2. **¿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?**
Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control

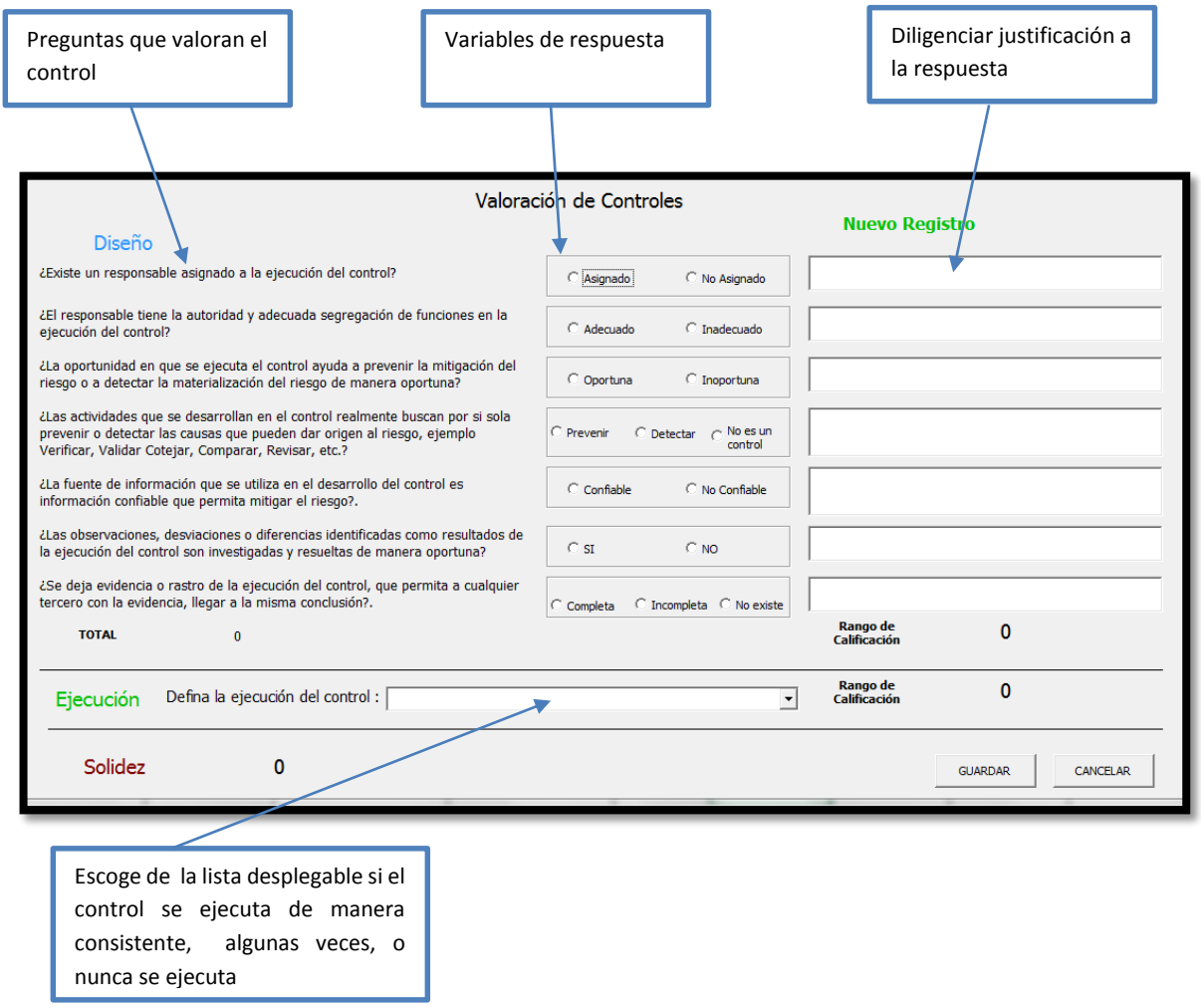
Pregunta 3: ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?
El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución.

Pregunta 4: ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?
Cuando estemos evaluando el control, debemos preguntarnos, si la fuente de información utilizada ¿es información confiable?, el cómo se realiza la actividad de control. Imaginémonos, la validación a un proveedor para saber que cumple con los requisitos de contratación, no la estemos realizando con una lista de chequeo, si no de memoria, porque los requisitos no los sabemos de memoria, o que la conciliación la realicemos con un extracto de Bancos que fue suministrado por la misma área de cartera o a través de un archivo en Excel

Pregunta 5: ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?
Al momento de evaluar si un control está bien diseñado para mitigar el riesgos, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumple, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debería gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones, el control tendría un problema en el diseño.

Pregunta 6: ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?
Hay controles que su evidencia queda en un flujo a través de una aplicación como un aprobado o revisado o que la evidencia cuando es un control automático es la configuración y programación de una aplicación.

.



Por cada respuesta afirmativa a las anteriores preguntas, el sistema asignará una puntuación la cual establece el rango de calificación de diseño del control y la solidez del control, de acuerdo a su ejecución.

Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

g. Tratamiento del Riesgo

Para la adecuada administración de los riesgos identificados se tendrán en cuenta, las siguientes directrices:

a. Aquellos riesgos que debido a su naturaleza y/o impacto relacionado, sobrepasen la capacidad del proceso en torno a la ejecución de medidas de tratamiento de los mismos, el Líder de Proceso los podrá presentar ante el Comité institucional de Coordinación de Control Interno para recibir orientación al respecto.

b. Cuando las condiciones externas y/o internas que originaron el riesgo, cambien o desaparezcan ocasionando la eliminación del riesgo, se documentará la situación en la *SEC-FT-13 matriz de riesgos y oportunidades,* donde quedará el registro hasta el inicio de la siguiente vigencia en aras de tener la trazabilidad de la situación presentada

c. Nivel de aceptación del riesgo: para el tratamiento de los riesgos residuales (después de la aplicación de controles), se tendrá en cuenta:

- Riesgos valorados como BAJO: no será necesario la formulación de planes de acción o de mitigación. Riesgos valorados como EXTREMO, ALTO y MODERADO: se deben formular planes de acción o mitigación para el tratamiento del riesgo
- En el caso de pasar a EXTREMO o ALTO se le dará el tratamiento indicado en el ítem anterior
- Los riesgos valorados como BAJO deberán mantenerse monitoreados en aras que se mantengan en dicho nivel.

d. El límite de tiempo para la ejecución de la acción será de un año a partir de la aprobación de la matriz de riesgos y oportunidades.

e. Tener en cuenta aspectos de viabilidad jurídica, técnica, institucional y financiera.

h. **Plan de Tratamiento:** El plan de tratamiento**,** describe el modo en que se estructurarán y se llevarán a cabo las actividades complementarias a los controles en la administración de riesgos. El plan de gestión de los riesgos incluye lo siguiente:

- Definición de la acción: Define las herramientas y las fuentes de datos que se utilizarán para llevar a cabo la gestión de riesgos en aras de mitigar el riesgo residual. Por lo cual adicional a los controles ya definidos, se deberán generan acciones adicionales para prevenir la materialización del riesgo.
- Roles y responsabilidades. Define el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del plan de gestión de los riesgos, y explica sus responsabilidades.
- Fecha inicio/fin. Define fecha de inicio y finalización de las acciones.
- Indicadores Relacionados: se formulan los indicadores clave de riesgo (que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (por riesgo identificado en los procesos).[2]

3.2. Seguimiento y revisión

[2] Consulte Guía para la construcción de indicadores de gestión
http://www.funcionpublica.gov.co/documents/418537/506911/1595.pdf/6c897f03-9b26-4e10-85a7-789c9e54f5a3

Es el control continuo que deben hacer los responsables de procesos del IDIGER para determinar cambios en las diferentes etapas de la Gestión del riesgo.
El seguimiento y la revisión deben:

- Garantizar que los controles son eficaces tanto en el diseño como en la operación
- Obtener información adicional para valorar el riesgo
- Analizar y aprender lecciones
- Verificar, atender e informar la materialización del riesgo

3.2.1. Reportes periódicos

El monitoreo y la revisión del riesgo y su materialización se efectuarán trimestralmente, en el Formato *SEC-FT-13 Matriz de riesgos y oportunidades*. El profesional de la Oficina Asesora de Planeación junto con el responsable del proceso, efectúan el análisis respectivo buscando que se adopten las medidas correctivas más adecuadas.

Los responsables deberán generar el seguimiento a la matriz de riesgos, trimestralmente dejando consignado en el formato *SEC-FT-13 Matriz de riesgos y oportunidades*. La entrega se realizará los primeros diez días siguientes al corte del trimestre.

Posterior a esta entrega los profesionales de la Oficina Asesora de Planeación, realizarán las revisiones respectivas de los riesgos teniendo en cuenta lo contemplado en este documento respecto a la segunda línea de defensa.

La Oficina de Control Interno, deberá monitorear y revisar de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos y entregará informe de acuerdo al programa de auditorías al Comité Institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno

3.2.2. Seguimiento a los riesgos de corrupción

En concordancia con la cultura del autocontrol al interior del IDIGER, los responsables de los procesos junto con su equipo realizarán anualmente la elaboración del mapa de riesgos de corrupción y son ellos quienes realizarán el monitoreo y evaluación permanente al mismo, en los plazos establecidos más adelante.

La Oficina Asesora de Planeación revisará que se cumpla con la presente metodología y liderará la consolidación de la información y su publicación. Para lo cual publicará el mapa de riesgos de corrupción anualmente antes del 31 de enero de cada año.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

* Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
* Seguimiento a la gestión del riesgo.
* Revisión de los riesgos y su evolución.
* Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

Para lo cual cumplirá con las siguientes fechas

Seguimiento	Fecha	Publicación
1er Seguimiento	Corte al 30 de abril	Dentro de los. diez (10) primeros días del mes de mayo
2do Seguimiento	Corte al 31 de agosto	Dentro de los diez (10) primeros días del mes de septiembre
3er Seguimiento	Corte al 31 de diciembre	Dentro de los diez (10) primeros días del mes de enero.

3.3. Materialización de los riesgos

Se deberá seguir el siguiente proceso en caso que un riesgo identificado o no identificado se materialice:

3.3.1. Materialización de riesgos de proceso

En caso de materializarse un riesgo, los responsables de la Segunda Línea de Defensa deberán implementar una acción correctiva de acuerdo al procedimiento SEC-PD-08 Plan de Mejoramiento (Acciones preventivas y correctivas).
Así mismo, a través de la segunda línea de defensa, informar al Comité Institucional de Coordinación de Control Interno para que desde allí se analice la situación y se den las orientaciones al respecto.

3.3.2. Materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:
1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
2) Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
3) Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
4) Realizar un monitoreo permanente.

3.4. Ajustes a la matriz de riesgos

Cuando el equipo responsable del proceso, producto del seguimiento y la revisión quisiera ajustar la redacción de un riesgo, incluir o eliminar algún riesgo identificado al inicio de la vigencia, el responsable del proceso deberá remitir un correo electrónico al jefe de la Oficina Asesora de Planeación con copia al profesional asignado, en el que se indique la justificación por la cual requiere que se realice la inclusión, modificación o eliminación del riesgo.
La Oficina Asesora de Planeación, realizará el análisis de esa información y generará sus observaciones, las cuales pueden ser aprobadas o no dependiendo de la justificación aportada. Si los ajustes proceden dará respuesta favorable al proceso vía correo electrónico y se ajustará la matriz de riesgos institucional.
.

3.5. Comunicación y Consulta

El consolidado de los mapas de riesgo debe publicarse en la página web de la entidad. La oficina Asesora de Planeación, consolida la información entregada por los procesos, y la Oficina de Tic´s publica la matriz de riesgos y oportunidades en la página web.

Se deberá realizar la socialización del mapa de riesgos de corrupción de la entidad a servidores públicos, contratistas y ciudadanía en general, de forma previa a su publicación, con el fin de recibir observaciones para su mejora.

Es responsabilidad de los líderes de proceso la socialización de los resultados obtenidos entre los miembros de su equipo y es responsabilidad de cada servidor público del IDIGER consultar permanentemente los riesgos documentados a fin de tener reconocimiento de las situaciones de riesgo existentes y de las nuevas condiciones.

4. Control de Cambios.

Versión	Fecha	Descripción de la Modificación	Aprobado por
1	21/07/2008	Creación de la Guía	Dirección General
2	05/10/2009	Actualización de acuerdo a lineamientos del Departamento Administrativo de la Función Pública	Dirección General
3	13/01/2012	Inclusión de elementos referentes al contexto estratégico y mapa de riesgos institucional	Dirección General
4	10/12/2013	Actualización de Guía por inclusión de elementos de la estrategia anticorrupción	Asesor de Planeación Estratégica
5	12/06/2015	Actualización de la guía por ajuste institucional	Jefe de Oficina Asesora de Planeación

6	31/07/2017	Se realiza actualización de la guía por definición de nuevos criterios para la valoración del riesgo	Jefe de Oficina Asesora de Planeación
7	26/11/2018	Se incluye lineamientos de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades públicas	Jefe de Oficina Asesora de Planeación
8	03/01/2019	Se tiene en cuenta observaciones del comité institucional de control interno, se especifica la identificación de riesgos, valoración de riesgos, se incluye monitoreo de riesgos y plan de gestión de riesgos	Jefe de Oficina Asesora de Planeación

5. Aprobación.

Elaborado por	Aprobado por
Ana Milena Álvarez Zabala. Profesional Oficina Asesora de planeación	**Jorge Andrés Castro** Jefe Oficina Asesora de Planeación

Nota: Para una mayor información referente a este documento comunicarse con la dependencia responsable.