CONTADURÍA
GENERAL DE LA NACIÓN
Cuentas Claras, Estado Transparente

Política de Administración del Riesgo

31 de agosto de 2020
GIT DE PLANEACIÓN

CONTENIDO

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO MAYO – 2019

1. INTRODUCCIÓN

La política de administración del riesgo de la Unidad Administrativa Especial Contaduría General de la Nación (CGN) denota el grado de compromiso de la entidad frente al cumplimiento de los objetivos estratégicos y del plan de acción institucional, direccionando a los procesos a asumir un pensamiento basado en riesgos, que permita anticiparse, disminuir y contrarrestar el impacto de eventos inesperados.

Es importante resaltar que esta política toma como base el Modelo Integrado de Planeación y Gestión MIPG v2, la Norma Técnica Colombiana NTC-ISO 31000:2018, el Decreto 2641 del 2012, y la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" v4, expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Función Pública.

2. ALCANCE

La Administración del Riesgo en la UAE Contaduría General de la Nación tendrá el siguiente alcance:

- Riesgos de Gestión y Corrupción: Todos los procesos de la CGN.
- Riesgos del Sistema de Gestión de Seguridad de la Información - Seguridad Digital: Los procesos que hacen parte del alcance del Sistema de Gestión de la Seguridad de la información (SGSI).

Esta política de administración del riesgo contribuye al control interno de la entidad, y fomenta la cultura del autocontrol al interior de los procesos.

3. OBJETIVOS

- Establecer los parámetros necesarios para una adecuada administración de los riesgos a través de los elementos: contexto estratégico; identificación de riesgos; análisis de riesgos; valoración de riesgos; políticas de administración del riesgo, su trazabilidad, registro y monitoreo.
- Orientar la toma de decisiones.
- Incentivar el pensamiento basado en riesgos dentro de la entidad.
- Buscar la mejora continua en cada uno de los procesos.

4. GLOSARIO

- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **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.
- **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 los 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 impactan 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 pueden ocasionar a la organización la materialización del riesgo.
- **Riesgo inherente:** Es aquel riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo permanente luego de tomar medidas de tratamiento del riesgo.
- **Mapa de Riesgos:** 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.
- **Confidencialidad**: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).
- **Vulnerabilidad:** es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Integridad:** propiedad de exactitud y completitud.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **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.
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

(Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, págs. 8,9)

5. CONTEXTO

Para la identificación de riesgos la entidad realiza un análisis de su entorno estratégico a partir de los siguientes factores internos y externos:

Contexto externo

- *Económicos y financieros:* Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
- *Políticos:* Cambio de Gobierno, legislación, políticas públicas, regulación.
- *Sociales:* Demografía, responsabilidad social, orden público.
- *Tecnológicos:* Avances en tecnología, acceso a sistemas de información externos, Gobierno en línea.
- *Ambientales:* Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
- *Legales y reglamentarios:* Normativa externa.

Contexto interno

- *Financieros:* Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
- *Personal:* Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
- *Procesos:* Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
- *Tecnología:* Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
- *Estratégicos:* Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- *Comunicación Interna:* Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

Contexto del proceso

- *Diseño del Proceso:* Claridad en la descripción del alcance y objetivo del proceso.
- Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
- *Transversalidad:* Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
- *Procedimientos Asociados:* Pertinencia en los procedimientos que desarrollan los procesos.

- *Responsables del Proceso:* Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
- *Comunicación entre los procesos:* Efectividad en los flujos de información determinados en la interacción de los procesos.

6. RIESGOS INSTITUCIONALES

El mapa de riesgos institucional se consolidará a partir de aquellos riesgos de gestión ubicados en la zona extrema y alta, a estos se les efectuará seguimiento continuo por parte de los líderes de proceso o responsables asignados para tal fin, quienes deberán garantizar que los controles se ejecuten en los tiempos estipulados, evitando con ello la materialización de los riesgos.

7. MAPA DE RIESGO INSTITUCIONAL

La información correspondiente a los riesgos ubicados en la zona extrema y alta se consolidará en el formato denominado "Mapa de riesgos institucional", el cual será presentado al Comité Institucional de Coordinación de Control Interno, para su respectiva revisión y aprobación.

8. METODOLOGÍA APLICADA

La metodología aplicada para la administración del riesgo será la contemplada en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" v4, expedida por la Presidencia de la República, Ministerio de Tecnologías de la Información y las Comunicaciones, y el Departamento Administrativo de la Función Pública.

9. PERIODICIDAD

La revisión de los mapas de riesgos de Gestión, Corrupción y Seguridad de la Información - Seguridad Digital de la UAE Contaduría General de la Nación, se realizará como mínimo dos veces al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en el contexto estratégico, cambios relevantes en los procesos y/o procedimientos, o cualquier hecho sobreviniente externo o interno que afecte la operación de la entidad.

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento a la gestión del riesgo de acuerdo con lo establecido en la "Guía rol de las unidades u oficinas de control interno, auditoría interna o quien haga sus veces", MIPG y "Estrategias para la Construcción del Plan Anticorrupción y de atención al ciudadano" ésta última define los siguientes cortes de seguimiento a los riegos de corrupción:

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

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

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

Adicionalmente se deberá presentar un informe cuatrimestral que contenga los resultados de los seguimientos a los riesgos de los procesos, con el fin de evidenciar la materialización, la creación, modificación o eliminación de alguno de ellos.

10. NIVELES DE RESPONSABILIDAD Y AUTORIDAD PARA EL MANEJO DE LOS RIESGOS

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Planeación y Gestión- **(MIPG)** en la dimensión siete (7) “Control Interno” desarrolla a través de la Línea Estratégica y las tres (3) Líneas de Defensa de responsabilidad de la gestión del riesgo y control.

LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección.

1ra LÍNEA DE DEFENSA

Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los líderes de cada uno de los procesos con el apoyo de sus colaboradores y el Integrante del Equipo Operativo.

2da LÍNEA DE DEFENSA

Asegura que los controles y los Procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

El GIT de Planeación tiene la responsabilidad de monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa y acompaña a los procesos en la administración de riesgos y elabora la consolidación de los mapas de riesgos de Gestión y Corrupción y Seguridad Digital, a su vez es el encargado de su publicación.

Para los riesgos de Seguridad de la Información - Seguridad Digital se debe tener el acompañamiento del GIT de Tecnologías de Información.

3ra LÍNEA DE DEFENSA

Proporciona información sobre la efectividad del **S.C.I**., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.

El **GIT** de Control Interno realiza el seguimiento y la medición de los avances de las acciones de respuesta y evaluación de la efectividad de las políticas.

(Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, pág. 76)

11. NIVELES DE ACEPTACIÓN DEL RIESGO

Para el caso de los riesgos de gestión y de seguridad de la información se consideran **ACEPTABLES** aquellos ubicados en nivel de riesgo bajo.

Los riesgos de corrupción **NO TIENEN** nivel de aceptación.

12. NIVELES PARA CALIFICAR EL IMPACTO

En los riesgos de gestión los niveles para calificar el impacto son:

NIVEL	VALOR DEL IMPACTO	CONSECUENCIAS CUALITATIVAS
INSIGNIFICANTE	**1**	• 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	**2**	• 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	**3**	• 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

NIVEL	VALOR DEL IMPACTO	CONSECUENCIAS CUALITATIVAS
MAYOR	**4**	• 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 por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
CATASTRÓFICO	**5**	• 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

(Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, págs. 40-41)

En los riesgos de Seguridad de la Información - Seguridad Digital, los niveles para calificar el impacto son:

NIVEL	VALOR DEL IMPACTO	CONSECUENCIAS CUALITATIVAS
INSIGNIFICANTE	**1**	• Sin afectación de la integridad. • Sin afectación de la disponibilidad. • Sin afectaciones de la confidencialidad.
MENOR	**2**	• Afectación leve de la integridad. • Afectación leve de la disponibilidad. • Afectaciones leves de la confidencialidad.
MODERADO	**3**	• 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 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 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.

(Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018, pág. 42)

En los riesgos de corrupción, los niveles para calificar el impacto son:

IMPACTO	DESCRIPTOR
MODERADO	Genera medianas consecuencias sobre la entidad.
MAYOR	Genera altas consecuencias sobre la entidad.
CATASTRÓFICO	Genera consecuencias muy graves para la entidad.

13. OPCIONES PARA TRATAMIENTO Y MANEJO DE RIESGOS

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción. En la CGN las opciones apuntarán a la toma de decisiones para:

- **Aceptar el riesgo:** Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo. No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción podrá ser aceptado)

- **Evitar el riesgo:** Cuando los escenarios de riesgo identificado se consideran demasiado extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.

- **Compartir el riesgo:** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

- **Reducir el riesgo:** El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se está logrando los objetivos estratégicos y de procesos de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control y esto implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales; por lo tanto, se deberá considerar para la implementación de acciones y controles, aspectos como: viabilidad jurídica, técnica, institucional, financiera o económica y análisis costo - beneficio.

14. RECURSOS

En cada uno de los pasos de la administración del riesgo se contemplarán los recursos necesarios para la definición, implementación y efectividad de las acciones que permitan un tratamiento

adecuado de los riesgos. Para ello se involucrarán a los procesos que tengan incidencia en el cálculo, aplicación o solicitud de los recursos: técnicos, financieros y talento humano.

15. DIVULGACIÓN

La Política de Administración del Riesgo, los Mapas de Riesgos: Institucional, Gestión y Corrupción, se divulgarán a través de la página web de la UAE Contaduría General de la Nación a fin de que todas las partes interesadas se informen de la gestión de riesgos realizada por los procesos.

16. CAPACITACIÓN

La administración del riesgo se considera un tema importante para la entidad, por ello se deberá realizar como mínimo una capacitación anual (interna o externa), que permita fortalecer las competencias de los servidores públicos, y así poder garantizar una gestión del riesgo coherente y adecuada, dentro de cada uno de los procesos.

17. ACOMPAÑAMIENTO DE PLANEACIÓN

- Brindar los lineamientos para implementar la Política de Administración del Riesgo y la metodología del DAFP en la identificación y tratamiento a los riesgos identificados por los procesos.
- Llevar a cabo las mesas de trabajo para la identificación/validación y seguimiento de la gestión de riesgos e indicadores del proceso.
- Dejar evidencia de los seguimientos realizados, por medio de las ayudas de memoria, en las cuales reposan punto por punto las actividades realizadas.
- Consolidar el mapa de riesgos (gestión, corrupción, seguridad digital).
- Presentar los mapas de riesgos consolidados para la socialización y aprobación al Comité Institucional de Coordinación de Control Interno CICCI.

18. ACCIONES PARA SEGUIR EN CASO DE MATERIALIZACIÓN DEL RIESGO

En caso de presentarse la materialización de un riesgo, el líder de proceso realizará los análisis de causas y ajustes necesarios a los mapas del proceso.
De igual manera se deberán tomar las siguientes medidas dependiendo del tipo de riesgo materializado:

Riesgo de corrupción:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.

- Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
- Realizar un monitoreo permanente.

Para los riesgos de corrupción, su materialización puede derivar en acciones legales y pérdida de imagen para la entidad; estas acciones disciplinarias no solo recaen sobre las personas directamente implicadas, sino también sobre los líderes de procesos.

Riesgos de gestión y Seguridad digital:

Es necesario realizar acciones de mejoramiento ejecutando actividades, tales como:

- Hacer una descripción detallada de lo ocurrido y del impacto generado en el proceso.
- Revisar el mapa de Riesgos del proceso en particular las causas, riesgos y controles. Se debe tener en cuenta que en el análisis del riesgo varia la probabilidad.
- Tomar acciones para evitar el que se repita la materialización del riesgo detectado y actualizar el Mapa de riesgos y sus acciones de seguimiento contempladas.
- Realizar un monitoreo permanente.

Los procesos deben Informar al GIT de Planeación la materialización de sus riesgos, quien a su vez comunicará al ***COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO***.