Política de Administración del Riesgo

25 de septiembre de 2019

POLITICA DE ADMINISTRACIÓN DL RIESGO SEPTIEMBRE 2019

1. INTRODUCCIÓN

La política de la administración del riesgo del Instituto de la Cultura, el Turismo, el Deporte y Recreación de Moniquirá (ICUTUDER) vela por el grado de compromiso frente al cumplimiento de los objetivos estratégicos propuestos como para el desarrollo del Plan de Acción de la Entidad se cumplan sin que en ninguna actividad que se realice se generen contratiempos con la materialización de algunos de los riesgos que se podrían presentar, por el contrario permita anticiparse, mitigar y contrarrestar el impacto en caso que se presente alguno.

Para esta política es importante que se ha articulado con el Modelo Integrado de Planeación y de Gestión MIPG, el Decreto 2641 del 2012, la Norma Técnica Colombiana NTC-ISO 31000:2018 Y "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 ICUTUDER el alcance será en la identificación, análisis, valoración y establecer controles que permitan monitorear periódicamente su eficacia para todos los procesos estratégicos, misionales y de apoyo.

3. OBJETIVOS.

- Establecer 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 a cada uno de los dirigentes y coordinadores de la entidad.
- Buscar estrategias de mejoramiento continuo en cada uno de los procesos.
- Velar porque se implementan acciones preventivas efectivas en cada uno de los procesos de la entidad y hacer periódicamente su respectivo seguimiento.

4. CONCEPTOS BASICOS RELACIONADOS CON EL RIESGO

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

Riesgo de seguridad 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.

Riesgo inherente: es aquel al que se 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 sus correspondientes medidas de tratamiento.

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.

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.

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

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

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

5. CONTEXTO

Para la identificación de los riesgos se realiza un análisis dentro de los diferentes contextos

CONTEXTO EXTERNO:

- Económicos y Financieros: disponibilidad de capital, liquidez, desempleo
- 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 y entre otros.
- Ambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
- Legales y reglamentarios: normatividad externa.

CONTEXTO INTERNO

- Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura y capacidad instalada de los diferentes escenarios.
- Personal: competencia del personal, disponibilidad del personal, prebendas, Seguridad y Salud en el Trabajo.
- Procesos: gestión del conocimiento, diseño, ejecución, proveedores, capacidad, entradas, salidas.
- Tecnología: disponibilidad e integridad de datos, sistemas, desarrollo, producción y mantenimiento de los sistemas de información.
- Estratégicos: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
- Comunicación Interna: Canales de comunicación 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 de cada proceso de la Entidad.
- Interacción con otras entidades: Suministro de información, soporte, apoyo en la gestión estructural y organizacional:
- Procesos transversales: Todos los procesos que determinan los lineamientos y que son inherentes al cumplimiento de la misión institucional.
- Procedimientos asociados: el sentido de pertinencia en los procedimientos que desarrollan los procesos.
- Responsables de los procesos: grado de responsabilidad, autonomía, autoridad de los funcionarios frente a la ejecución de los diferentes procesos de la Entidad.
- Comunicación interna entre los procesos: medios de comunicación, efectividad en el flujo de la información de los procesos que interactúan entre sí.

6. RIEGOS INSTITUCIONALES

En el mapa de riesgos se evaluarán todos los procesos para la identificación de los riesgos, pero los que estén en una extrema o Alta posición se creara una metodología para mejorar y se efectuara control y seguimiento con mayor periodicidad por parte de los Coordinadores de cada proceso quienes serán los responsables de implementar acciones de intervención para cada riesgo identificado los cuales también deberán garantizar que los controles se ejecuten en los tiempos estipulados evitando a futuro la materialización de los riesgos.

7. MAPA DE RIESGOS INSTITUCIONAL

La información correspondiente que se consolidara en la matriz de riesgos lo cual es en base al previo análisis de los procesos documentados frente a su ejecución y se dará a conocer al Director de la Entidad para su 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. SEGUIMIENTO

La periodicidad que se le dará intervención al mapa de riesgos es semestralmente, pero en caso que se presente algún evento inesperado por algún riesgo se debe realizar de inmediato plan de acción correctivo y preventivo, 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:

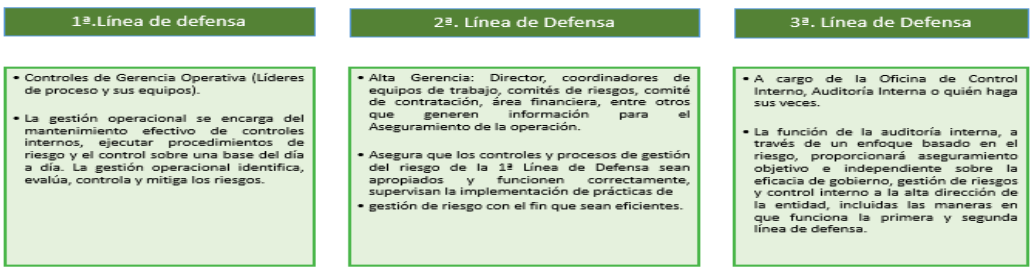
- **Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- **Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- **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 si en algún momento se presentó la materialización, creación, modificación o eliminación de alguno de ellos.

10. Nivel de Jerarquía para el manejo de los riesgos

ICUTUDER 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.

La línea estratégica define el marco general para la gestión del riesgo, ejerce el control y vigila su cumplimiento la cual está a cargo de la alta dirección.



(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** pero única y exclusivamente los que se encuentran en nivel bajo.

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

12. NIVELES PARA CALIFICAR EL IMPACTO

En los riesgos de gestión para calificar el impacto se tuvieron en cuenta los siguientes:

- Moderado
- Mayor
- Catastrófico

En el siguiente ítem se relacionan las características de los niveles de riesgo que califican el impacto para los riesgos de Seguridad de la Información – Seguridad Digital son los siguientes:

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. Afectación moderada de la **confidencialidad** de la información debido al interés particular de los empleados y tercero.

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. El ICUTUDER tomara acciones pertinentes para la toma de decisiones según su criterio:

• **Aceptar el riesgo:** Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario implementar 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 cumplimiento de los objetivos, la entidad implementara actividades de control orientadas a prevenir la materialización de los riegos, la efectividad de los controles depende de que tanto se están logrando los objetivos estratégicos y de procesos de la entidad.

como según se había indicado con las líneas de defensa en este caso le corresponde a la primera línea de defensa lo cual su tratamiento es gerencial el establecer actividades de control y esto también implica equilibrar los costos y el talento humano capacitado para su implementación y los aspectos importantes que se deben tener en cuenta para llevar a cabo este trabajo son: la 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 del ICUTUDER 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).

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.

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 ICUTUDER de Planeación la materialización de sus riesgos, quien a su vez comunicará al Comité Institucional de Coordinación de Control Interno.

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.

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.

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.

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.