TABLA DE CONTENIDO

1. OBJETIVOS

Definir los lineamientos generales de la administración de riesgos de la Unidad, que guíen el accionar de los funcionarios, en el tratamiento de los riesgos de gestión, corrupción y seguridad digital.

2. DESARROLLO

Política de Administración de Riesgos de la Unidad Administrativa Especial de Catastro Distrital

La Unidad Administrativa Especial de Catastro Distrital se compromete a dar tratamiento, manejo y seguimiento de los riesgos de gestión, de corrupción y de seguridad digital, que pueden afectar de manera negativa el alcance de los objetivos estratégicos y los objetivos de procesos de la cadena de valor. Para ello, define un documento de metodología y un procedimiento dentro del Proceso Direccionamiento Estratégico.

En el marco del cumplimiento de esta Política, se integran o adoptan los roles y responsabilidades sobre Gestión de los riesgos institucionales que establece el Modelo Integrado de Planeación y Gestión – MIPG.

2.1. Objetivos de la Política

La Política de Administración del Riesgo de la UAECD y sus objetivos descritos a continuación, brindan el marco general de actuación para gestionar los riesgos que afectan el logro de los objetivos estratégicos de la Unidad; así como, de los objetivos de los procesos de la cadena de valor.

Objetivos:

- Contribuir a la eficiencia operacional mediante la mitigación de probabilidad e impacto de eventos adversos.
- Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos organizacionales.
- Aportar información para tomar adecuadas decisiones estratégicas y operativas.
- Fortalecer la mejora continua en la gestión de los procesos y en general del Sistema de Control Interno.
- Brindar un marco en el que se identifiquen las amenazas y vulnerabilidades a las que puede estar expuesta la entidad desde la perspectiva de un entorno digital y se fortalezca el ambiente de control.
- Reprobar y combatir la corrupción por parte de cada uno de los servidores públicos que pertenecen a la Unidad, que afecte el logro de los objetivos de la entidad, socave el Estado de Derecho, distorsione el efecto de las políticas gubernamentales, quebrante la legitimidad del gobierno, desestimule la participación ciudadana y propicie escenarios de politización y de captura de la entidad por parte de intereses particulares.

2.2. Alcance

Esta política establece la intención general de la Unidad respecto al manejo de riesgos de gestión, corrupción y seguridad digital, con el fin que se realicen las actividades necesarias iniciando con la identificación de los factores externos e internos hasta realizar el tratamiento de los riesgos y seguimiento a las actividades de control definidas en cada uno de los procesos de la entidad. Es aplicable a todos los procesos de la entidad en materia de gestión de riesgos.

2.3. Componentes de la Gestión del Riesgo

Para lograr los objetivos precedentes, la UAECD ha elaborado un marco de referencia para la Gestión del Riesgo, el cual incluye:

2.3.1. Roles y responsabilidades

La definición de los roles y responsables de la gestión del riesgo en la entidad parten de lo definido por el Modelo Integrado de Planeación y Gestión – MIPG en su Manual Operativo[1] del cual se destacan:

Línea Estratégica – Alta dirección y Comité Institucional de Coordinación de Control Interno:

"Su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad."

Primera línea de defensa – Líderes de programas, procesos y proyectos y sus equipos de trabajo (en general servidores públicos en todos los niveles):

"Su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol"."

Segunda línea de defensa – Jefe de la Oficina Asesora de Planeación, coordinadores de equipos de trabajo que respondan de manera directa por el aseguramiento de la operación:

"Su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces; así mismo, consolidar y analizar información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión"."

Tercera línea de defensa – Jefe Oficina de Control Interno:

"A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces.

Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.

[1] Manual Operativo del Modelo Integrado de Planeación y Gestión. Versión 3. diciembre de 2019.

Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.

Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos."

Asimismo, el Anexo No 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas señala las responsabilidades del funcionario designado para Seguridad Digital, en concordancia con lo establecido por el Ministerio de Tecnologías de la información y las comunicaciones, la Unidad delegará la responsabilidad de gestionar los riesgos de seguridad digital al encargado de seguridad de la información con los siguientes compromisos:

"Responsable de Seguridad Digital:

- *Definir el procedimiento para la Identificación y Valoración de Activos.*
- *Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).*
- *Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.*
- *Apoyar en el seguimiento a los planes de tratamiento de riesgos definidos.*
- *Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital."*[2]

[2] Anexo No 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Ministerio de Tecnologías de la Información y las Comunicaciones.

2.3.2. Lineamientos para la gestión del riesgo

La implementación de la Gestión del Riesgo en la entidad cumple con las etapas de la Gestión del Riesgo a saber: Política de administración de riesgos, Identificación de riesgos, Valoración de riesgos, y comunicación y consulta (aspecto transversal).

Complementario a lo contenido en esta Política, el desarrollo de las etapas, los términos y definiciones aplicables y la estructura para la administración del riesgo se encuentran descritos en el Documento Técnico Metodología de riesgos y el Procedimiento Gestión de riesgos los cuales hacen parte del Proceso Direccionamiento Estratégico.

Los criterios para la valoración de los riesgos en relación con los niveles para calificar los aspectos de probabilidad e impacto serán los definidos en las tablas de valoración consignadas en el Documento Técnico de metodología.

El tratamiento de los riesgos de gestión y seguridad digital tendrá cuatro (4) escenarios posibles: eliminar, reducir, compartir y/o transferir y asumir. El tratamiento a los riesgos de corrupción sólo tendrá dos (2) escenarios posibles que corresponden a eliminar o reducir el riesgo.

El seguimiento de los Planes de Manejo de Riesgo – PMR que permiten dar tratamiento a los riesgos residuales se realizará con periodicidad trimestral.

En relación con los riesgos de corrupción, su formulación y seguimiento seguirán los lineamientos que sobre la materia establezcan el Gobierno Nacional y Distrital.

En el caso de los riesgos de seguridad digital, estos se gestionan siguiendo los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, basados en el Modelo de Seguridad y Privacidad de la Información, la Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno Nacional, territoriales y sector público y el Modelo de Gestión de Riesgos de Seguridad Digital, del Ministerio de Tecnologías de la Información y las Comunicaciones.

La materialización del riesgo de corrupción en la UAECD obliga a todos y cada uno de los servidores públicos y contratistas de la Unidad a:

- Comunicar a las autoridades competentes la ocurrencia del hecho.
- Comunicar al superior inmediato del servidor público y supervisor del contrato en caso de contratista, la ocurrencia del hecho.
- Implementar acciones correctivas inmediatas encaminadas a eliminar la causa raíz de la materialización del riesgo; tanto servidores públicos y contratistas, en el marco de su respectivo contrato.
- Monitorear permanentemente los riesgos a través de lo señalado en la metodología de riesgos y el procedimiento relacionado.

2.3.3. Niveles de aceptación del riesgo

La Unidad dará prioridad a los riesgos residuales ubicados en zonas de niveles: extremo, alto y moderado. Sobre los riesgos ubicados en zona baja pese a no generar Plan de Manejo del Riesgo – PMR, trimestralmente se deberá identificar si se presentó o no materialización e identificando si requiere realizar ajustes o mejora a la valoración definida.

Los riesgos de corrupción no admiten aceptación del riesgo, siempre debe conducir a realizar el tratamiento correspondiente.

2.3.4. Comunicación y consulta de la Política

Esta política es aprobada por la Alta dirección y el Comité Institucional de Coordinación de Control Interno y seguirá el trámite de gestión de documentos que establece el Manual del Sistema de Gestión Integral. Por esta razón, se encontrará disponible para consulta a través del Sistema de Gestión Integral – SGI-

3. DOCUMENTOS REFERENCIA

- Manual Operativo Sistema de Gestión MIPG, Modelo Integrado de Planeación y Gestión. Versión 3. diciembre de 2019.
- Guía para la gestión del riesgo y diseño de controles, en entidades públicas. DAFP. Febrero de 2018.
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018
- Modelo de Seguridad y Privacidad de la Información.
- Modelo de Gestión de Riesgos de Seguridad Digital.
- Guía de orientación para la gestión de riesgos de seguridad digital en el Gobierno nacional, territoriales y sector público.