1. OBJETIVO

Establecer los parámetros para la administración del riesgo, los cuales incluyen su identificación, análisis, evaluación, tratamiento y monitoreo, con el fin de proporcionar al Instituto Colombiano de Antropología e Historia – ICANH un aseguramiento razonable con respecto al logro de los objetivos institucionales.

2. ALCANCE

La administración del riesgo inicia con la definición y aprobación de los lineamientos para la administración del riesgo de la entidad y termina con el seguimiento a las etapas de la administración de riesgo de la entidad.

3. ENTRADAS

- Contexto institucional.
- Resultados de evaluaciones o auditorías internas y/o externas.
- Catálogo de Productos y Servicios.
- Salidas no conformes.
- Implementación y estado de requisitos (componentes) de los modelos de gestión adoptados por la entidad que apliquen al proceso.
- Normograma de la entidad.
- Documentación de la caracterización de procesos de la entidad.
- Peticiones, quejas, reclamos.
- Información relevante de grupos de valor e interés.
- Monitoreo de riesgos de gestión, corrupción y seguridad de la información.
- Resultados de indicadores.
- Resultados del (IDI) y Plan de trabajo asociado al cumplimiento del MIPG.
- Necesidades de mejora identificadas internamente (sugerencias de los servidores).
- Activos de información.
- Mapa de Aseguramiento.
- Líneas de Defensa.

4. LINEAMIENTOS DE OPERACIÓN

- La administración de riesgos se desarrolla siguiendo los lineamientos establecidos en la metodología emitida por el DAFP a través de la guía para la administración del riesgo y el diseño de controles en entidades públicas, así como en la normatividad legal y técnica vigente que regule la materia.

- El contexto estratégico institucional se formula para el período correspondiente a la ejecución del plan estratégico de la entidad, y se revisa anualmente para su actualización, lo anterior es fuente principal de información para la construcción de los mapas de riesgos de la entidad.

- El Comité Institucional de Coordinación de Control Interno o quien haga sus veces es el responsable de aprobar los lineamientos para la administración del riesgo de la entidad.

- La entidad identifica los riesgos de gestión y corrupción enfocados al objetivo de los procesos y los riesgos de seguridad de la información enfocados a los activos identificados igualmente por proceso.

- Los líderes de proceso deben identificar y documentar los riesgos teniendo en cuenta las diferentes fuentes de información (entradas de este documento y otras que se consideren pertinentes).

- La revisión y/o actualización anual de los riesgos de corrupción es obligatoria. Los riesgos de gestión y de seguridad de la información se actualizan cada vez que se requiera.

- Las líneas de defensa para la administración del riesgo en la entidad están compuestas por:

  a) **La línea estratégica** conformada por la alta dirección a través del comité institucional de coordinación de control interno quien define el marco general para la gestión del riesgo y supervisa su cumplimiento.
  b) **La primera línea de defensa** a cargo de los líderes de procesos quienes con el apoyo de la Oficina Asesora de Planeación y la Oficina de Tecnología de Información definen los riesgos, el tratamiento para la mitigación de éstos, incluyendo aquellos relacionados con la corrupción y el monitoreo permanente a la ejecución de los controles.
  c) **La segunda línea de defensa** a cargo de la Oficina Asesora de Planeación para los riesgos de gestión y corrupción y el área funcional de Tecnología y Sistemas de Información para los riesgos de seguridad de la información, quienes monitorean la gestión del riesgo y complementan lo realizado por la primera línea.
  d) **La tercera línea de defensa** a cargo de la Oficina de Control Interno quien revisa la efectividad de los controles establecidos y en general realiza el seguimiento a la administración de los riesgos de la entidad.

- La Oficina Asesora de Planeación es la encargada de consolidar el mapa de riesgos de corrupción y de gestión. La consolidación de los riesgos de seguridad de la información está a cargo del área el área funcional de tecnología y sistemas de información.

- Para la descripción de los riesgos de corrupción la entidad garantiza que concurran los componentes de su definición, así: ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

- Los riesgos de seguridad de la información se mitigan o tratan empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”.

- Para los riesgos de corrupción, el análisis de impacto se realiza teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre son significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

- La Oficina Asesora de Planeación debe publicar una versión consolidada de los riesgos de corrupción a más tardar el 31 de enero de cada año (de acuerdo con lo establecido en artículo 2.1.4.8. Publicación del Plan Anticorrupción y de Atención al Ciudadano y Mapa de riesgos de corrupción - Decreto 1081 de 2015); esta versión debe haberse sometido con antelación a la consulta de la ciudadanía a través de la sede electrónica u otro medio, junto con el Plan Anticorrupción y de Atención al Ciudadano; cada vez que surjan cambios en este consolidado, deben publicarse con las actualizaciones pertinentes.

- En caso de que algunos de los elementos constitutivos de los mapas de riesgo contengan información que se considere clasificada (en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014), se debe anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.

- Para los riesgos de corrupción las fechas para el monitoreo se realizan de forma cuatrimestral y el resultado del monitoreo de éstos se deben reportar a la segunda línea de defensa para que la Oficina Asesora de Planeación realice la revisión, el seguimiento respectivo y la publicación en la sede electrónica dentro del mes siguiente al corte del cuatrimestre.

- Para los riesgos de gestión y seguridad de la información las fechas para cada monitoreo se realizan de forma semestral y el resultado del monitoreo de los riesgos se debe reportar a la segunda línea de defensa (Oficina

Asesora de Planeación o al área funcional de Tecnología y Sistemas de Información) dentro del mes siguiente al corte del semestre.

- Los funcionarios y contratistas del ICANH deben conocer los mapas de riesgos de gestión, corrupción y seguridad de la información antes de su publicación. Para lograr este propósito la Oficina Asesora de Planeación y el área funcional de Tecnología y Sistemas de Información, ponen en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.

- La Oficina de Control Interno debe realizar seguimiento al cumplimiento de la administración de riesgos conforme con los lineamientos establecidos para la administración de riesgos y la normatividad legal y técnica vigente que regule la materia.

5. DEFINICIONES[1]

- **Activo:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).
- **Anonimización**: Proceso técnico consiste en transformar los datos individuales de las unidades de observación, de tal modo que no sea posible identificar sujetos o características individuales de la fuente de información, preservando así las propiedades estadísticas en los resultados (Departamento Administrativo Nacional de Estadística – DANE).
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la entidad
- **Causa**: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Control:** Medida que permite reducir o mitigar 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.
- **DAFP**: Departamento Administrativo de la Función Pública es la entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la

[1] Definiciones extractadas de: Metodología emitida por el Departamento Administrativo de la Función Pública – DAFP a través de la guía para la administración del riesgo y el diseño de controles en entidades públicas, Modelo Integrado de Planeación y Gestión MIPG / Glosario / Versión 7, NTC ISO 31000:2018, ISO/IEC 27001:2013 y DANE https://www.dane.gov.co/index.php/sistema-estadistico-nacional-sen/normas-yestandares/sistema-de-consulta.

gestión de los servidores públicos y las instituciones en todo el territorio nacional. El DAFP hace parte de los 24 sectores que componen la Rama Ejecutiva Nacional, siendo cabeza del sector Función Pública.

- **Disponibilidad**: propiedad de ser accesible y utilizable a demanda por una entidad. (DAFP 2018).
- **Factores de riesgo**: Son las fuentes generadoras de riesgos.
- **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.
- **IDI:** Índice de Desempeño Institucional establecido por el DAFP refleja el grado de orientación del grupo de entidades de la Rama Ejecutiva del Orden Nacional y Territorial hacía la eficacia (la medida en que se logran los resultados institucionales), eficiencia (la medida en que los recursos e insumos son utilizados para alcanzar los resultados) y calidad (la medida en la que se asegura que el producto y/o prestación del servicio responde a atender las necesidades y problemas de sus grupos de valor.
- **Impacto**: se entiende como las consecuencias que puede ocasionar la materialización del riesgo. (DAFP 2018).
- **Impacto Inherente**: Calificación final del impacto de acuerdo con el criterio seleccionado.
- **Integridad**: propiedad de exactitud y completitud.
- **Líneas de defensa**: Manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados. (IIA 2013:2).
- **MIPG:** Es un marco de referencia establecido por el DAFP para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, según dispone el Decreto 1083 de 2015.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **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
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
- **Probabilidad inherente:** número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. (DAFP 2018).
- **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. (DAFP 2018).
- **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. (DAFP 2018).
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC27000:2016).
- **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. (DAFP 2018).
- **Riesgo inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad

- **Riesgo residual**: El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Tolerancia del riesgo**: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Vulnerabilidad**: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
1.	Planificar los lineamientos para la administración del riesgo.	Establecer los lineamientos y el marco general de la administración de riesgos de gestión, de corrupción y de seguridad de la información para la entidad.	Jefe y Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información, Líder Área funcional de Tecnologías y Sistemas de Información.	Lineamientos y metodología.	Verificar que los lineamientos contengan todos los elementos requeridos en la normatividad vigente que rige la materia.
2.	Incluir tema en la agenda del Comité Institucional de Coordinación de Control Interno.	Se incluye dentro de la agenda de la siguiente reunión, la socialización y aprobación de la metodología para la administración del riesgo en la entidad.	Jefe Oficina Control Interno.	Agenda del comité	
3.	Aprobar lineamientos y para la administración del riesgo de la entidad.	Como línea de defensa estratégica el comité revisa y aprueba la metodología para la administración del riesgo en la entidad solicitando, si es el caso, los ajustes que considere pertinente.	Comité Institucional de Coordinación de Control Interno.	Acta de reunión.	Según lo solicitado por el comité se debe ajustar la metodología de riesgos de la entidad.
4.	Establecer el Contexto.	Establecer el contexto externo e interno en que opera la entidad, lo anterior se hace con el objeto de identificar las fuentes potenciales de riesgos para la entidad para tenerlas en cuenta en el proceso, el proyecto o servicio analizado. Para el caso del contexto externo se determinan características o factores como: políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios. Para el caso del contexto interno se deben considerar factores como: Procesos, estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y conocimientos con que se cuenta (personas, procesos, sistemas, tecnología), relaciones con las partes involucradas (grupos de valor e interés) y cultura organizacional.	Jefe y Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Documento de contexto	
5.	Identificar y clasificar el riesgo o los activos de información.	Identificar las variables para considerar en la identificación del riesgo tales como: • Análisis de objetivos estratégicos y del proceso.	Líderes de Procesos y equipo asignado, Profesional de la Oficina Asesora de	Mapa de riesgos de corrupción, gestión y de seguridad de la	

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		• Identificación de las causas raíz e inmediata de riesgo. • Identificación y descripción del riesgo. • Clasificación del riesgo **(Ver Anexo 1).** • Identificación de activos de información (solo para riesgos de seguridad de la información). **NOTA: Para los riesgos de seguridad de la información documentar en el formato respectivo.**	Planeación, Oficial de Seguridad de la Información.	información por proceso.	
6.	Registrar el riesgo identificado.	Definir de acuerdo con el objetivo del proceso o los activos identificados el riesgo inherente o propio de la actividad. Determinar nivel de probabilidad (posibilidad de ocurrencia del riesgo) de conformidad con la tabla de probabilidad **(Ver anexo 2).** Indicar nivel de impacto (consecuencias) según lo establecido en el anexo adjunto. **(Ver anexo 3).** Establecer el nivel del riesgo inicial en la matriz de calor residual. **(Ver anexo 4)**. Finalmente determinar la Zona de Riesgo Inherente (Nivel de Severidad). **NOTA: Para los riesgos de seguridad de la información documentar en el formato respectivo.**	Líderes de Procesos y equipo asignado, Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Mapa de riesgos de corrupción, gestión y seguridad de la información por proceso.	
7.	Definir controles	Analizar la naturaleza del control con el fin de determinar si están documentados, si son automáticos o manuales y si se están aplicando en la actualidad, mediante la aplicación de la tabla de atributos para el diseño del control **(Ver anexo 5).** Asimismo, definir claramente aspectos como: a) Nombre del control b) Propósito del control c) Descripción detallada de la operación del control d) Frecuencia del control e) Responsable del control f) Manejo de las desviaciones del control g) Evidencia del control **NOTA: Para los riesgos de seguridad de la información documentar en el formato respectivo.**	Líderes de Procesos y equipo asignado, Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Mapa de riesgos de corrupción, gestión y seguridad de la información por proceso.	Verificar que los controles se encuentren establecidos en la documentación aplicable al proceso.
8.	Dar tratamiento a los riesgos	Determinar el riesgo residual, comparando los resultados del análisis de riesgo inherente frente a los controles establecidos. La formulación de controles debe contribuir a eliminar las causas generadoras del riesgo y	Líderes de Procesos y equipo asignado, Profesional de la Oficina Asesora de	Mapa de riesgos de corrupción, gestión y seguridad de la	

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable (Cargo y/o Grupo responsable / Dependencia)	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		deben hacer que el riesgo inherente baje su calificación uno o más niveles de acuerdo con la solidez del control. Igualmente, asociado a lo anterior se debe establecer el tratamiento que se da al riesgo, es decir asumir o aceptar, evitar, reducir, transferir o compartir de acuerdo con la tabla de criterios establecidos. **(Ver anexo 6).** **NOTA: Para los riesgos de seguridad de la información documentar en el formato respectivo.**	Planeación, Oficial de Seguridad de la Información.	información por proceso.	
9.	Consolidar el mapa de riesgos institucional	Recopilar, analizar y consolidar la información suministrada por los responsables de los procesos.	Profesional Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Mapa de riesgos de gestión, corrupción y seguridad de la información consolidado	
10.	Socializar el mapa de riesgos	Socializar los riesgos a quienes intervienen o participan en el proceso, especialmente a los encargados de ejecutar los controles.	Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Mapa de riesgos de gestión, corrupción y seguridad de la información consolidado	
11.	Monitorear los riesgos por parte de la primera línea de defensa.	La primera línea de defensa conformada por los líderes de los procesos junto con su equipo de trabajo debe realizar monitoreo y evaluación permanente los riesgos de gestión y seguridad de la información, para lo cual semestral o cuatrimestralmente en las fechas estipuladas dentro de los lineamientos de este documento según el tipo de riesgo, debe verificar la ejecución de los controles a través de la evidencia establecida, considerando aspectos como: a. Que las amenazas y vulnerabilidades que generan los riesgos siguen controladas. b. Que la ejecución y efectividad de los controles es apropiada. c. Verificar la posibilidad de nuevos riesgos emergentes para reportarlos y formalizarlos. d. Si existió la materialización de alguno de los riesgos.	Líder de Procesos y equipo asignado	Mapa de riesgos de corrupción, gestión y seguridad de la información por proceso.	Verificar que se estén ejecutando los controles definidos y que las evidencias correspondan a lo identificado en el mapa de riesgos y a las acciones establecidas en los planes de tratamiento (cuando aplique).
12.	Reportar materialización de riesgos.	La primera línea de defensa debe revisar si existe materialización de riesgos de gestión, corrupción o seguridad de la información y debe reportar al correo de la Oficina Asesora de Planeación planeación@icanh.gov.co, o al correo de TI areati@icanh.gov.co para los riesgos de seguridad de la información, indicando el proceso al que pertenece el riesgo materializado o el activo afectado, la fecha, la descripción del evento y demás información relevante (quién, cómo, cuándo,	Líder de Procesos y equipo asignado		Verificar frente a la descripción del riesgo y los eventos sucedidos si existe materialización del mismo.

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		dónde, por qué) que permita entender la situación y posteriormente pasar a la siguiente actividad, si no existe materialización de riesgos se debe pasar a la actividad No. 14.			
13.	Formular plan de mejoramiento.	En caso de que en el monitoreo de los riesgos de la primera o segunda línea de defensa se evidencie materialización de algún(os) riesgo(s) se debe formular un plan de mejoramiento con acciones tendientes a evitar que vuelva a ocurrir. Si el riesgo materializado es de corrupción, además de la formulación del plan de mejoramiento, el hecho debe ponerse en conocimiento del superior inmediato y de la Oficina de Control Interno Disciplinario. La Oficina Asesora de Planeación y el Oficial de Seguridad de la Información asesoran de forma proactiva estas actividades. Siempre que ocurra una materialización de riesgos se debe analizar si se requiere una nueva evaluación de riesgo o la definición de nuevos controles, un plan de tratamiento especial o cualquier otra actividad, además de la formulación del plan de mejora, con el fin de mantenerlo controlado, para lo anterior se debe iniciar el análisis respectivo en la actividad No.5 del presente documento.	Líder de proceso, Jefe y Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Plan de Mejoramiento	Verificar que la suscripción de los planes de mejoramiento se realice de conformidad con lo establecido en el procedimiento de la Oficina de Control Interno y que las actividades propuestas subsanen la causa raíz del problema identificado.
14.	Monitorear los riesgos por parte de la segunda línea de defensa.	La segunda línea conformada por la Oficina Asesora de Planeación y el Oficial de Seguridad de la Información revisa lo realizado por la primera línea de defensa y elabora los reportes semestrales para presentar, el resultado del monitoreo de los riesgos a la línea estratégica y a la tercera línea de defensa. Igualmente, a dichas línea se debe presentar el reporte de cualquier evidencia de materialización reportada por los líderes de proceso o identificada por la segunda línea de defensa. Este seguimiento se debe publicar en la sede electrónica el siguiente mes finalizado el semestre o cuatrimestre para los riesgos de gestión y seguridad de la información o corrupción respectivamente. En caso de evidenciar materialización de riesgos que no haya sido reportada por la primera línea de defensa se debe informar por correo al líder del proceso para que realice el reporte oficial y el diligenciamiento del plan de mejoramiento respectivo (ver actividades 12 y 13).	Profesional de la Oficina Asesora de Planeación, Oficial de Seguridad de la Información.	Monitoreo al mapa de riesgos de gestión, corrupción y seguridad de la información.	Seguimiento a al monitoreo de la primera línea en cuanto a la ejecución de los controles y posibles materializaciones.
15.	Monitorear los riesgos por parte de la tercera línea de defensa.	La tercera línea de defensa conformada por la Oficina de Control Interno revisa el reporte cargado en la sede electrónica el cual contiene el monitoreo de la primera y segunda línea de defensa, y realiza la respectiva evaluación de	Oficina de Control Interno	Informe de riesgos de la entidad	

6. DESCRIPCIÓN DE ACTIVIDADES

No	Actividad	Descripción	Responsable Cargo y/o Grupo responsable / Dependencia	Registro (Documento que se deja como evidencia de ejecución)	Punto de Control
		cumplimiento de los riesgos reportados, el resultado debe ser presentado ante el Comité Institucional de Coordinación de Control Interno.			
16.	Realizar seguimiento a las etapas de la administración de riesgo de la entidad.	Realizar actividades de monitoreo y revisión a las etapas de la administración de riesgos, con el fin de presentar recomendaciones relacionadas con: Cambios en el direccionamiento estratégico o en el contexto y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. La identificación de riesgos significativos que afectan el cumplimiento de los objetivos de los procesos. El adecuado diseño y ejecución de los controles para la mitigación de los riesgos establecidos por parte de la primera línea de defensa (es decir, que se encuentren documentados y actualizados en los procedimientos) y realizar recomendaciones y seguimiento para el fortalecimiento de estos. El perfil de riesgos inherente y residual. Cualquier riesgo que se encuentre por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas. Seguimiento al cumplimiento de los planes de tratamiento o mejoramiento relacionados con la administración del riesgo. De lo anterior se debe elaborar los informes para la Línea estratégica relacionados con lo evidenciado en este seguimiento.	Oficina de Control Interno	Informe	Revisión del mapa de riesgos de gestión, corrupción y seguridad de la información frente a la normatividad vigente, a la materialización de riesgos y al perfil de riesgo de la entidad.

7. DIAGRAMA DE FLUJO

N.A.

8. REGISTROS

Nombre	Almacenamiento
Mapa de Riesgos de gestión y corrupción consolidado.	Carpeta compartida por la Oficina Asesora de Planeación/riesgos/ vigencia.
Monitoreo de Riesgos de Gestión por Proceso.	Carpeta compartida por la Oficina Asesora de Planeación/riesgos/ vigencia.
Monitoreo de Riesgos de Corrupción por Proceso.	Carpeta compartida por la Oficina Asesora de Planeación/riesgos/ vigencia.

Evidencias de ejecución de controles por proceso riesgos de gestión y corrupción.	Carpeta compartida por la Oficina Asesora de Planeación/riesgos/ vigencia.
Mapa de riesgos de seguridad de la información Consolidado.	Unidad compartida del Área Funcional de Tecnologías y Sistemas de Información/vigencia.
Monitoreo de riesgos de seguridad de la información por proceso.	Unidad compartida del Área Funcional de Tecnologías y Sistemas de Información/vigencia.
Evidencias de ejecución de controles por proceso riesgos de seguridad de la información.	Unidad compartida del Área Funcional de Tecnologías y Sistemas de Información/vigencia.
Acta de reunión.	Unidad compartida del Área Funcional de Tecnologías y Sistemas de Información/ Oficina Asesora de Planeación /vigencia.

1. ANEXOS

- Formato mapa de riesgos de gestión y corrupción.
- Formato mapa de riesgos de seguridad de la información.
- Formato plan de mejoramiento.

2. CONTROL DE CAMBIOS

Versión	Fecha	Descripción general del cambio
01	2022-11-21	Creación del documento dada la necesidad de contar con directrices, actividades y responsabilidades claras en la administración del riesgo para la entidad.

ELABORÓ	REVISÓ	APROBÓ
Cargo: Profesional de la Oficina Asesora de Planeación.	**Cargo:** Profesional especializado de la Oficina Asesora de Planeación. Oficial de Seguridad de la Información. Profesional Oficina de Control Interno.	**Cargo:** Líder del área funcional de Tecnologías y Sistemas de Información. Jefe de Oficina de Control Interno. Jefe de la Oficina Asesora de Planeación
Fecha: 2022-09-19	**Fecha: 2022-10-28**	**Fecha: 2022-11-21**