


| | | |
|---|-------------------------|---------------------|
|  | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 1 de 15 Página |

**ACUERDO No. 018 DE 2019
(Noviembre 27)**

Por medio del cual se aprueba la Política para la Gestión Integral del Riesgo en el Instituto Superior de Educación Rural ISER de Pamplona

EL CONSEJO DIRECTIVO DEL INSITUTO SUPERIOR DE EDUCACIÓN RURAL ISER DE PAMPLONA

En uso de sus facultades legales, en especial las que le confiere los literales a y p del artículo 14 del Acuerdo número 10 del 02 de 1993, y

CONSIDERANDO


Que el literal f) del artículo 2º de la Ley 87 de 1993, establece como uno de los objetivos del Sistema de Control Interno, la definición y aplicación de las medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puede afectar el logro de sus objetivos.

Que, según la Ley 87 de 1993, conforme con el artículo 1º, párrafo único, los manuales de procedimientos son instrumentos a través de los cuales se cumple el control interno.

Que mediante el Decreto 1537 de 2001 se reglamentó parcialmente la Ley 87 de 1993, y en el artículo 4 señala la administración de riesgos *"Como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis de riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quienes haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para consecución de los objetivos organizaciones, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente los procedimientos"*.

Que el Decreto 261 de 2012, en el artículo 1º, señala como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano", en cuyo primer componente incorpora la "Metodología para la identificación de riesgos de corrupción y acciones para su manejo"

Que el Decreto 124 de 2016, en su artículo 2.1.4.1 y 2.1.4.2, establece la Estrategia de lucha contra la corrupción y de Atención al Ciudadano. Señalando como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano – Mapas de Riesgo de Corrupción de que trata el artículo 73 de la Ley 1474 de 2011, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano-Versión 2".

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 2 de 15 Página |

Que el Departamento Administrativo de la Función Pública, publicó la "Guía para la administración de Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, en octubre de 2018, con el fin de unificar la metodología existente para la administración de los riesgos de gestión, corrupción y de seguridad digital y facilitarles a las entidades públicas el ejercicio de la administración de riesgo.

Que, en consecuencia el Instituto Superior de Educación Rural ISER de Pamplona, define su política para la gestión del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión (MIPG) en los procesos, así como los del Modelo Estándar de Control Interno (MECI), en lo concerniente a las líneas de defensa y las directrices de la Guía para la administración del riesgo de la Función Pública 2018, la cual articula los riesgos de gestión, corrupción y de seguridad digital y la estructura del Sistema Integrado de Gestión – SGI en el módulo de riesgos.


Que, para la correcta administración de los riesgos, el Instituto Superior de Educación Rural ISER de Pamplona mediante la guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital, establecerá la metodología y determinará las acciones para asumir, reducir y mitigar los riesgos y los planes de contingencia, así como el monitoreo y seguimiento ante la materialización del riesgo.

Que, por lo anteriormente considerando,

ACUERDA:

ARTÍCULO PRIMERO: Definir y aprobar la Política para la Gestión Integral del Riesgo en del Instituto Superior de Educación Rural ISER de Pamplona, conforme a los siguientes directrices:


1. **OBJETIVO.** Orientar a los líderes de procesos del Instituto Superior de Educación Rural sobre las acciones que se deben adelantar, encaminadas a disminuir la probabilidad de ocurrencia y posible impacto de todas aquellas situaciones que puedan entorpecer el propósito de alcanzar de manera eficaz y efectiva el logro de los objetivos y la misión institucional, mediante el monitoreo, seguimiento y evaluación en los periodos de tiempos establecidos en esta política.
2. **ÁMBITO DE APLICACIÓN.** La política para la gestión integral del riesgo aplica para los planes, procesos y acciones ejecutadas por los líderes de procesos y servidores durante el ejercicio de sus funciones, desde el establecimiento del contexto, la identificación de los riesgos, la implementación de las acciones que minimicen el impacto o la probabilidad de ocurrencia de estos, hasta el monitoreo, seguimiento, evaluación y la comunicación del riesgo.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 3 de 15 Página |

3. TERMINOS Y DEFINICIONES

Definiciones tomadas de la Norma NTC-ISO 31000 (ICONTEC 2011) y de la nueva guía de administraciones del riesgo de Gestión, Corrupción y Seguridad Digital y, Diseño de Controles en Entidades Públicas (publicada por el DAFP en el 2018).


- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información digital física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Administración del riesgo:** Es la capacidad que tiene la entidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales, protegerla de los efectos ocasionados por su ocurrencia.
- **Amenazas:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis del riesgo:** El uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.
- **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.
- **Autoevaluación del Control:** Elemento de Control que basado en un conjunto de mecanismo de verificación y evaluación determinada la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.
- **Cadena de valor:** Es la interrelación de los procesos dirigidos a satisfacer las necesidades y requisitos de los usuarios.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.
- **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.
- **Control:** Son las políticas, procesos, dispositivos, prácticas y otras acciones que actúan para eliminar o minimizar los riesgos, adversos o mejorar oportunidades positivas. Proveen una seguridad razonable relativa al logro de los objetivos.
- **Evaluación del riesgo:** El proceso utilizado para determinar prioridades en la administración del riesgo por la comparación de niveles de riesgo frente a estándares determinados, límites de niveles del riesgo u otros criterios.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 4 de 15 Página |


- **Gestión de Riesgo:** Proceso efectuando 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.
- **Identificación del riesgo:** Proceso que determina que puede suceder, por qué y el cómo.
- **Integridad:** propiedad de exactitud y completitud.
- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Mapa de Riesgos:** documento con la información resultante de la gestión del riesgo.
- **Reducción del Riesgo:** Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.
- **Riesgo:** Es toda posibilidad de ocurrencia de una situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidad 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 medidas de tratamiento de riesgo.
- **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.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Valoración del Riesgo:** Es el conjunto de procesos que permiten analizar y evaluar el riesgo.
- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. MARCO DE REFERENCIA

- CONGRESO DE LA REPÚBLICA DE COLOMBIA, Ley 87 de 1993 Por la cual se establecen normas para el ejercicio del control interno de las entidades y

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 5 de 15 Página |

- organismos del Estado y se dictan otras disposiciones, artículo 2 literal a). Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2 literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
- CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009 “Ley De Delitos Informáticos: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos” – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
 - CONGRESO DE LA REPÚBLICA. Ley 1474 de 2011 – ESTATUTO ANTICORRUPCIÓN: por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de gestión pública.
 - CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012 – Ley Protección De Información de Datos: Por la cual se dictan disposiciones generales para la protección de datos personales.
 - MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, Manual de Estrategias de Gobierno en Línea. Bogotá 2015.
 - DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la Gestión de Riesgo de Corrupción. Bogotá, 2015.
 - DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano, Bogotá. 2015.
 - PRESIDENTE DE LA REPÚBLICA DE COLOMBIA, Decreto 1499 de 2017, “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
 - CONSEJO PARA LA GESTIÓN Y EL DESEMPEÑO INSTITUCIONAL, Presidencia de la República de Colombia. Manual Operativo del Modelo Integrado de Planeación y Gestión Versión 2 – MIPG. Bogotá, agosto de 2018.
 - DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
 - MINTIC Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto único Reglamentario del sector de Tecnologías de la información y las comunidades.
 - INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC Internacional). Norma Técnica Colombiana NTC-ISO 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
 - INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC Internacional). Norma Técnica Colombiana NTC-ISO 27005.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 6 de 15 Página |

Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.

- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC Internacional). Norma Técnica Colombiana NTC-ISO 31000:2011. Gestión del Riesgo Sistemas de Gestión de la Calidad.
- DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Riesgos de gestión, corrupción y seguridad digital. Versión 4, octubre 2018.


5. POLÍTICA

El Instituto Superior de Educación Rural ISER de Pamplona, se compromete a gestionar los riesgos, monitorearlos y hacer seguimiento en forma cuatrimestral, identificando y administrando los eventos potenciales que pueden afectar los objetivos y los procesos del Instituto.

5.1 LINEAMIENTOS

Para la adecuada gestión integral del riesgo en el Instituto Superior de Educación Rural ISER de Pamplona, se presentan los siguientes lineamientos:

- Se establecerá la metodología que permita identificar, analizar, valorar y administrar los riesgos de gestión, de corrupción y de seguridad digital que se puedan presentar en el normal desarrollo de las actividades que dan cumplimiento a la Misión Institucional y su posterior tratamiento, manejo, monitoreo y seguimiento que afecten el logro de los objetivos institucionales.
- Asegurar los recursos necesarios para gestionar y tratar el riesgo institucional.
- Los riesgos identificados en el Instituto Superior de Educación Rural ISER de Pamplona serán monitoreados cuatrimestralmente, asegurando controles eficientes y eficaces, obteniendo información para mejorar continuamente la evaluación y gestión de los riesgos e identificar su posible materialización.
- La tolerancia al riesgo que el Instituto Superior de Educación Rural ISER de Pamplona puede o está dispuesto a soportar, corresponden a los riesgos que se encuentren en zona residual Baja. Los que se encuentran en otra zona se tratarán de acuerdo con los lineamientos establecidos en el procedimiento para la administración del riesgo Institucional.
- Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo al procedimiento para la administración del riesgo Institucional descrito en el formato respectivo.
- Comunicar internamente, los resultados de la gestión del riesgo desarrollada institucionalmente, reportando en el Mapa Institucional de Riesgos, los riesgos priorizados de acuerdo con los lineamientos establecidos en procedimiento para la administración del riesgo institucional.
- Los mecanismos de comunicación utilizados para dar a conocer la política de riesgo en todos los niveles del instituto, será a través de la inducción, reinducción, socialización del Sistema de Gestión Integrado y por medio de diferentes

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | ACUERDO | 00 Versión |
| | | 26/11/2015 Fecha |
| | | 7 de 15 Página |


mecanismos de comunicación internos del Instituto Superior de Educación Rural ISER de Pamplona.

5.2 METODOLOGÍA


El Instituto Superior de Educación Rural ISER de Pamplona definió la metodología que permite identificar, analizar, valorar y administrar los riesgos descrita a continuación, este proceso se realiza con el acompañamiento del líder de planeación.

5.2.1 Identificación, valoración, definiciones de acciones

- a. Asegurar que en cada proceso se reconozca el concepto de "administración del riesgo", la política y metodología definida, los actores y entorno del proceso.
- b. Definir el grupo de trabajo y los profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociado a sus procesos.
- c. Participar de las mesas de trabajo para la identificación/validación de los riesgos del proceso, teniendo en cuenta los siguientes tipos de riesgos:
 - **Riesgos Estratégicos:** Se asocia con posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos y la forma en que se administra el Instituto relacionados con la misión, la clara definición de políticas, y la conceptualización de la entidad por parte de la alta dirección.
 - **Riesgos Operativos:** Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad. Implica comprender los riesgos provenientes del funcionamiento, de los sistemas de información institucional, de los procesos y su articulación, así como de la estructura de la entidad.
 - **Riesgos Financieros:** Se relacionan con la posibilidad de ocurrencia de eventos que afecten el manejo de recursos económicos del instituto, incluyendo la ejecución presupuestal, la elaboración de estados financieros, los pagos, el manejo de excedentes, la incorporación de recursos y el manejo sobre los bienes.
 - **Riesgos De Cumplimiento:** Se asocian a la posibilidad de ocurrencia de eventos que afecten la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
 - **Riesgos De Imagen:** Están relacionados con la posibilidad de ocurrencia de un evento que afecte la imagen, la confianza y la buena percepción por parte de la comunidad hacia el Instituto.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | ACUERDO | 00 Versión |
| | | 26/11/2015 Fecha |
| | | 8 de 15 Página |

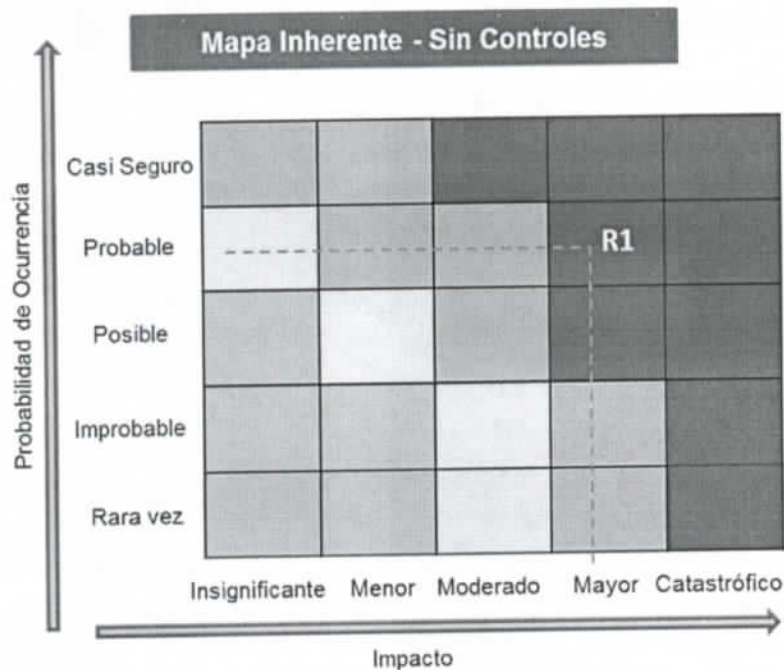
- **Riesgos Tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) que interrumpa el óptimo funcionamiento actual y futuras, así como el cumplimiento de los objetivos y misión institucional.
 - **Riesgos De Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
 - **Riesgos De Seguridad Digital:** Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, 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 Ambiental:** Posibilidad de que se produzca un daño o catástrofe en el medio ambiente debido a un fenómeno natural o a una acción humana.
- d. Registrar en la herramienta los pasos requeridos en el instructivo para la identificación, calificación, valoración de los riesgos.
- e. Redactar conjuntamente con los responsables de los procesos, las acciones de mitigación para los riesgos y registrarlas en el formato **respectivo**, previo visto bueno del líder de Direccionamiento estratégico, las cuales tendrán las siguientes opciones de tratamiento de riesgos:
- Evitar el riesgo:** tomar las medidas encaminadas a eliminar la actividad que genera el riesgo previniendo su materialización.
- Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Se consigue mediante la optimización de los procedimientos y la implementación de controles.
- Compartir el riesgo:** medida encaminada a reducir la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este.
- Aceptar el riesgo:** Medida en la que el riesgo ha sido reducido o transferido quedando un riesgo mínimo o residual que se mantiene, en este caso el responsable del proceso debe contar con planes de contingencia para su manejo.
- f. Determinar los responsables de las acciones y las fechas de realización de las acciones de mitigación.
- g. Elaborar el mapa de riesgos de proceso con toda la información en el formato **respectivo**
- h. El mapa de riesgos construye en conjunto con el líder del proceso, para posterior aprobación por parte de la Oficina de Planeación.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 9 de 15 Página |

- i. Una vez aprobado, el líder del proceso debe socializar el mapa de riesgos al interior del proceso para asegurar el compromiso de todos los responsables.
- j. Acorde con lo aprobado la información será cargada en base documental del proceso.


5.2.2 Seguimiento

- a. Según la periodicidad definida para cada riesgo, se debe verificar las acciones de mitigación y registrar el avance junto con la evidencia en el formato **respectivo**
- b. Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación, teniendo en cuenta el nivel de aceptación del riesgo conforme a las siguiente tablas de evaluación




Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4

| Tipo de Riesgo | Zona de Riesgo | Nivel de Aceptación |
|---|----------------|---|
| Riesgos de Gestión (estratégicos, de imagen, operativos, financieros, de cumplimiento, de tecnología y ambientales) | Baja | Se asumirá el riesgo y se administrará por medio de las actividades propias del proceso asociado y se realiza en el reporte CUATRIMESTRAL de su desempeño a la oficina de control interno. |
| | Moderada | Se establecen acciones de control preventivas que permitan reducir la |

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 10 de 15 Página |

| | | |
|------------------------------|----------------|---|
| | | probabilidad de ocurrencia del riesgo, se hace seguimiento CUATRIMESTRAL y sus avances se registran en el formato Seguimiento a Mapa de Riesgos . |
| | Alta y extrema | Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan mitigar la materialización del riesgo. Se monitorea de acuerdo con la fecha programada por el líder del proceso y su cumplimiento se registra en el formato Seguimiento a Mapa de Riesgos . |
| | Baja | Ningún riesgo de corrupción podrá ser aceptado. Periodicidad CUATRIMESTRAL de monitoreo y seguimiento para evitar a toda costa su materialización por parte de los procesos. |
| Riesgos de Corrupción | Moderada | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia de riesgo. Periodicidad CUATRIMESTRAL de monitoreo y seguimiento para evitar a toda costa su materialización por parte de los procesos y se registra en los formatos respectivo |
| | Alta y extrema | Se adoptarán las siguientes medidas: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. EVITAR las actividades que dan lugar al riesgo, decidiendo no iniciar y/o continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad CUATRIMESTRAL de monitoreo y seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en los formatos respectivos. |

- c. Comunicar al líder del proceso y la alta dirección las desviaciones del riesgo según el nivel de aceptación del riesgo.

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 11 de 15 Página |


- d. Documentar las acciones de correctivas o preventivas en el **formato respectivo**
- e. Revisar y actualizar el mapa de riesgo cuando se modifique las acciones de mitigación o ubicación del riesgo.

5.2.3 Responsabilidades por línea de defensa para la Información, comunicación y reporte:


- **Línea Estratégica:** Corresponde al Comité de control interno establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
- **Primera Línea de Defensa:** Corresponde a los líderes de proceso del instituto (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades.
- **Segunda Línea de Defensa:** Corresponde la **oficina de Planeación** (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.
- **Tercera Línea de Defensa:** Le corresponde a la **oficina de Control Interno**, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

5.2.4. Accionar ante los riesgos materializados

| TIPO DE RIESGO | RESPONSABLE | ACCIÓN |
|-----------------------------|------------------|---|
| Riesgo de Corrupción | Líder de Proceso | <ol style="list-style-type: none"> 1. Informar a la Línea Estratégica sobre el hecho encontrado. 2. Una vez surtido el conducto regular establecido en el Procedimiento Interno para el Ejercicio del Proceso Disciplinario dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente. 3. Identificar las acciones correctivas necesarias y documentarlas en el Plan de Mejoramiento formato respectivo 4. Efectuar el análisis de causas y determinar |

| | | |
|--|-------------------------|--|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | ACUERDO | 00 Versión 26/11/2015 Fecha 12 de 15 Página |

| | | |
|--|----------------------------|--|
| | | <p>acciones preventivas y de mejora formato respectivo.</p> <p>5. Actualizar el mapa de riesgos.</p> |
| | Oficina de Control Interno | <p>1. Informar al líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.</p> <p>2. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgo</p> |
| Riesgo de Gestión (zona extrema, alta y moderada) | Líder de Proceso | <p>1. Proceder de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), documental en el Plan de mejoramiento formato respectivo</p> <p>2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora, documentar en el Plan de mejoramiento Institucional formato respectivo y replantear los riesgos del proceso.</p> <p>3. Analizar y actualizar el mapa de riesgos.</p> <p>4. Informar al Proceso de Direccionamiento Estratégico sobre el hallazgo y las acciones tomadas.</p> |
| Riesgo de Gestión (zona baja) | | <p>1. Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgo.</p> |
| Riesgo de Gestión (zona extrema, alta y moderada) | Oficina de Control Interno | <p>1. Informar al líder del proceso sobre el hecho encontrado.</p> <p>2. Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.</p> <p>3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.</p> <p>4. Verificar que se tomaron las acciones correctivas y registrarlas en el formato respectivo y actualizar el mapa de riesgos correspondientes.</p> |
| Riesgo de Gestión (zona baja) | | <p>1. Informar al líder del proceso sobre el hecho encontrado.</p> <p>2. Informar a la segunda línea de defensa con el fin de facilitar en inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.</p> <p>3. Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.</p> |


| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | | 00 Versión |
| | ACUERDO | 26/11/2015 Fecha |
| | | 13 de 15 Página |

| | | |
|--|--|--|
| | | 4. Verificar que se tomaron las acciones correctivas y registrarlas en el formato respectivo y actualizar el mapa de riesgos correspondientes. 5. |
|--|--|--|


6. RESPONSABILIDAD Y COMPROMISO DE LA POLÍTICA

Las siguientes son las responsabilidades y compromisos para la adecuada gestión del riesgo:

| Líneas de Defensa | Responsable | Responsabilidad frente al Riesgo |
|----------------------|-----------------------|--|
| Estratégica | Alta dirección | <ol style="list-style-type: none"> Definir y hacer seguimiento a los niveles de aceptación. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación del instituto y que puedan generar cambios en la estructura de riesgos y controles. Realizar seguimiento y análisis a los riesgos institucionales. (cuatrimestralmente). |
| Primera línea | Líderes de proceso | <ol style="list-style-type: none"> Identificar y valorar los riesgos que pueden afectar los planes y procesos a su cargo y actualizarlo cuando se requiera con énfasis en la prevención de daño antijurídico. Definir, aplicar y hacer seguimiento continuo a los controles para mitigar los riesgos identificados alineados con las metas y objetivos del instituto y proponer mejoras a la gestión del riesgo supervisado. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora que haya lugar. Informar a la oficina de Planeación (segunda línea de defensa) sobre los riesgos materializados en los planes y procesos a su cargo. Reportar a la oficina de Planeación los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. |
| Segunda línea | Oficina de Planeación | <ol style="list-style-type: none"> Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y |

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | ACUERDO | 00 Versión |
| | | 26/11/2015 Fecha |
| | | 14 de 15 Página |

| | | |
|----------------------|----------------------------|--|
| | | <p>el nivel de aceptación del riesgo.</p> <ol style="list-style-type: none"> 2. Consolidar el Mapa de riesgos institucionales (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el comité Institucional de Coordinación de Control Interno – CICC. 3. Presentar al comité Institucional de Coordinación de Control Interno – CICC el monitoreo a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación del Instituto. 4. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo. 5. Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones. 6. Identificar cambios en los niveles de aceptación del riesgo en el instituto, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno. 7. Monitorear en forma cuatrimestral los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. 8. Evaluar que los riesgos sean consistentes con la presente política, conjuntamente con la primera línea de defensa. 9. Aprobar a través de soporte SIGUTS, las acciones de mejora a que haya lugar propuestas por los líderes de los procesos. 10. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico. 11. Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia. |
| Tercera línea | Oficina de Control Interno | <ol style="list-style-type: none"> 12. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. |

| | | |
|--|-------------------------|---------------------|
|  ISER | GESTIÓN JURÍDICA | F-GJ-23 Código |
| | ACUERDO | 00 Versión |
| | | 26/11/2015 Fecha |
| | | 15 de 15 Página |

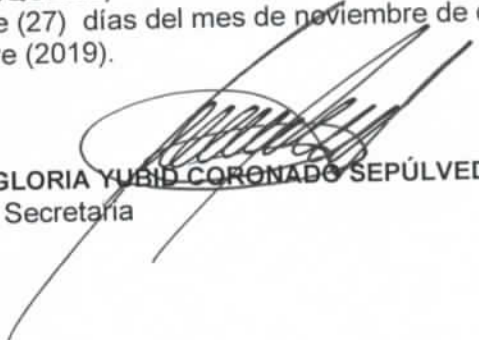
| | | |
|--|--|--|
| | | <p>13. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.</p> <p>14. Asesorar de forma coordinada con la oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño y controles.</p> <p>15. Llevar a cabo el seguimiento en forma cuatrimestral a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al comité Institucional de Coordinación de Control Interno – CICC.</p> <p>16. Recomendar mejoras a la política de administración del riesgo.</p> |
|--|--|--|

ARTÍCULO SEGUNDO: El presente Acuerdo rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias.

PUBLIQUESE, COMUNÍQUESE, Y CÚMPLASE

Dado en la ciudad de Cúcuta a los veintisiete (27) días del mes de noviembre de dos mil diecinueve (2019).


NELSON ENRIQUE PARADA SANTAMARIA
 Presidente Delegado


GLORIA YUBID CORONADO SEPÚLVEDA
 Secretaria

Proyectó: **GABRIEL FERNANDO GÓMEZ CARRILLO**
 P. E. PLANEACIÓN

Revisó: **JANETH LEON TARZONA**
 P. E. JURÍDICA