**INSTITUTO SUPERIOR DE EDUCACIÓN RURAL - ISER**

# POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

**PAMPLONA**
**NORTE DE SANTANDER**
**2026**

# POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO


**Mg. JOSÉ JAVIER BUSTOS CORTÉS**
**Rector**

**MÓNICA ENITH SALANUEVA ABRIL**
**Profesional Especializado adscrito al proceso de Direccionamiento Estratégico y Planeación**



**PAMPLONA**
**NORTE DE SANTANDER**
**2026**

**CONTENIDO**

## INTRODUCCIÓN

De acuerdo con las políticas de mejora definidas en el Modelo Integrado de Planeación y Gestión - MIPG y alineado con las directrices definidas en Sistema de Gestión de la Calidad y lo establecido en el Decreto 1122 de 2024, el Instituto Superior de Educación Rural - ISER presenta la Política para la Gestión Integral del Riesgo, la cual, busca garantizar un adecuado modelo de gobierno, así como las directrices necesarias para una efectiva e integral administración del riesgo.

Es por ello por lo que el Instituto Superior de Educación Rural - ISER se compromete a implementar un modelo de administración integral de riesgos con el propósito de prevenir la afectación al despliegue de los objetivos estratégicos, la seguridad de su información y el cumplimiento de las metas y resultados definidos en el marco del Programa de Transparencia y Ética Pública - PTEP; lo anterior conlleva al fomento de una cultura de gestión del riesgo para que el Instituto pueda responder de manera efectiva a las expectativas de nuestros grupos de valor, en el marco de nuestro compromiso con la gestión transparente y el despliegue de sus valores institucionales.

Esto obliga a la institución a la definición de políticas y lineamientos para la gestión integral del riesgo y la adopción de mejoras requeridas a partir de su ciclo de maduración, de tal forma que se propicie en los diferentes procesos la adopción del Sistema de Gestión de Riesgos para la Integridad Pública - SIGRIP, así como metodologías, el despliegue de mecanismos de gestión del conocimiento para su uso y apropiación y el acompañamiento decidido en su implementación. La Política para la Gestión Integral del Riesgo, busca que todos los funcionarios, contratistas y servidores públicos de la organización apliquen los controles en la ejecución de sus actividades y con ello se aporte al cumplimento de los objetivos institucionales.

En esta línea, las Dimensiones de Direccionamiento Estratégico, Gestión con Valores para Resultados, Talento Humano, Evaluación de Resultados y Control Interno del MIPG, aportan las directrices para establecer una política alineada con los objetivos estratégicos y la metodología para manejar los riesgos basados en su valoración, siendo insumos para que la alta dirección pueda tomar decisiones oportunas y pertinentes y fijar los lineamientos para gestionar de manera integral los riesgos al interior de la organización.

Con este documento se define la intencionalidad y relevancia de este tema para la gestión y el cumplimiento de las metas institucionales y da cumplimiento a lo establecido en la versión 7 de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública - DAFP, que contempla la metodología de administración del riesgo general de gestión, corrupción, fiscal y seguridad de la información, entre otros.

## 1. DEFINICIONES

**1.1. ACCIÓN CORRECTIVA:** Acción tomada para eliminar y/o mitigar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

**1.2. ACCIÓN PREVENTIVA:** Acción tomada para eliminar la(s) causa(s) de una no conformidad u otra situación potencial no deseable.

**1.3. ACEPTAR EL RIESGO:** Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

**1.4. 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.

**1.5. ACTIVO DE INFORMACIÓN DIGITAL:** En el contexto de seguridad de la información son elementos tales como aplicaciones de la entidad, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la institución para funcionar en el entorno digital.

**1.6. ACTIVO CIBERNÉTICO:** En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**1.7. ADMINISTRACIÓN DEL RIESGO:** Es la capacidad que tiene la organización para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

**1.8. ALA / CFT:** Antilavado de Lavado de activos y Contra la Financiación del Terrorismo.

**1.9. AMENAZAS:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

**1.10. AMENAZA CIBERNÉTICA:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. Documento CONPES 3854.

**1.11. ANÁLISIS DEL RIESGO:** Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. NTC ISO 31000:2018.

**1.12. 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.

**1.13. ATAQUE CIBERNÉTICO:** Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. Ministerio de Defensa de Colombia.

**1.14. CCOC:** Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

**1.15. 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.

**1.16. CAUSA:** todos aquellos Factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

**1.17. CAUSA INMEDIATA:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

**1.18. CAUSA RAÍZ:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

**1.19. COMISIÓN DE COORDINACIÓN INTERINSTITUCIONAL PARA EL CONTROL DEL LAVADO DE ACTIVOS (CCICLA):** La Comisión de Coordinación Interinstitucional para el Control del Lavado de Activos, CCICLA, fue creada mediante el Decreto 950 de 1995, modificado por los Decretos 754 de 1996, 2000 de 2003 y 3420 de 2004, de carácter permanente y adscrita el Ministerio de Justicia y del Derecho, y es el organismo consultivo del Gobierno Nacional y ente coordinador de las acciones que desarrolla el Estado Colombiano para combatir el lavado de activos y la financiación del terrorismo.

**1.20. COMPONENTES DE RED:** Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.

**1.21. 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.

**1.22. CONFIDENCIALIDAD:** Propiedad de la información que la hace no disponible, es decir divulgada a individuos, entidades o procesos no autorizados.

**1.23. CONTROL:** Medida que permite reducir o mitigar un riesgo.

**1.24. CONTROL CORRECTIVO:** Aquel que permite el restablecimiento de la actividad, después de detectarse un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

**1.25. CONTROL DETECTIVO:** Accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

**1.26. CONTROL PREVENTIVO:** Aquel que actúa para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.

**1.27. CORRUPCIÓN:** Es el abuso de poder o de confianza para el beneficio particular en detrimento del interés colectivo, en el que se incurre al ofrecer o solicitar, entregar o recibir bienes o dinero en especie, en servicios o beneficios a cambio de acciones, decisiones u omisiones (Transparencia Internacional, 2017).

**1.28. DELITO:** Es un comportamiento culpable y contrario a la Ley que conlleva una pena o sanción.

**1.29. DELITO FUENTE:** Comportamientos graves o peligrosos para la sociedad, listados de manera expresa por el legislador que generan el lavado de activos.

**1.30. DETECCIÓN:** Cuando se determina la ocurrencia de posibles operaciones de lavado de activos o financiación del terrorismo.

**1.31. DISPONIBILIDAD:** Propiedad de ser accesible y utilizable a demanda por la entidad.

**1.32. EFECTOS:** Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y vulneración de los derechos de las personas privadas de la libertad, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

**1.33. EVALUACIÓN DEL RIESGO:** Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

**1.34. FACTORES DE RIESGO:** Son las fuentes generadoras de riesgos.

**1.35. FINANCIACIÓN DEL TERRORISMO (FT):** Corresponde al conjunto de acciones que permiten la circulación de recursos que tienen como finalidad la realización de actividades terroristas o que pretenden el ocultamiento de activos provenientes de dichas actividades.

**1.36. GAFI:** Grupo de Acción Financiera Internacional para la Prevención del Lavado de Activos.

**1.37. GAFISUD / GAFILAT:** Organización Intergubernamental de base regional que agrupa 16 países de América del sur y Centroamérica para combatir el LA/FT.

**1.38. GESTIÓN DEL RIESGO:** Un 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.

**1.39. HARDWARE:** Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información

**1.40. ICC:** Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

**1.41. IMPACTO:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

**1.42. INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**1.43. INFORMACIÓN:** Datos almacenados en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema de gestión de la calidad, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.

**1.44. INTANGIBLE:** Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.

**1.45. INTEGRIDAD:** Propiedad de exactitud y completitud.

**1.46. LAVADO DE ACTIVOS (LA):** Es el proceso mediante el cual organizaciones criminales buscan dar apariencia de legalidad a los recursos generados de sus actividades ilícitas. En términos prácticos, es el proceso de hacer que dinero sucio parezca limpio, haciendo que las organizaciones criminales o delincuentes puedan hacer uso de dichos recursos y en algunos casos obtener ganancias sobre los mismos.

**1.47.** Línea estratégica: Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección, el equipo directivo, incluyendo el Comité Institucional de Gestión y Desempeño y el Comité de Coordinación de Control Interno.

**1.48. LISTAS VINCULANTES O RESTRICTIVAS:** Es la relación de personas naturales y jurídicas que pueden estar vinculadas con actividades de lavado de activos o financiación del terrorismo.

**1.49. MAPA DE RIESGOS:** Documento con la información resultante de la gestión del riesgo.

**1.50. MITIGACIÓN:** Planificación y ejecución de medidas dirigidas a reducir o disminuir el riesgo identificado.

**1.51. MSPI:** Modelo de Seguridad y Privacidad de la Información.

**1.52. MONITOREO:** Comprobar, supervisar, observar críticamente, o registrar el proceso de una actividad, acción o sistema en forma sistemática, para identificar cambios.

**1.53. 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.

**1.54. OFICIAL DE CUMPLIMIENTO:** Es la persona responsable del cumplimiento del sistema SARLAFT.

**1.55. OPERACIÓN INUSUAL:** Es aquella operación que se sale de los parámetros normales o que por su cuantía y características no guarda relación con la actividad económica o comercial de cada uno de los grupos de interés.

**1.56. PERSONAS PÚBLICAMENTE EXPUESTAS (PEP):** Personas nacionales o extranjeras que por su perfil o por las funciones que desempeñan pueden exponer en mayor grado a la entidad al riesgo de LA/FT, tales como personas que por razón de su cargo manejan recursos públicos, detentan algún grado de poder público o gozan de reconocimiento público.

**1.57. POLÍTICA DE GESTIÓN INTEGRAL DEL RIESGO:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO 31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimientos a los riesgos.

**1.58. PRIMERA LÍNEA DE DEFENSA:** A cargo de gestionar los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través de la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos, está a cargo de los gerentes públicos y los líderes de procesos.

**1.59. PROBABILIDAD:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

**1.60. REPORTE DE OPERACIONES SOSPECHOSA (ROS):** Corresponde a un hecho relacionado con la posible comisión de actividades relacionadas con los delitos de Lavado de Activos o Financiación del Terrorismo.

**1.61. RIESGO:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

**1.62. 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.

**1.63. 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.

**1.64. RIESGO DE LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO – LA/FT:** Se define como la posibilidad de pérdida o daño que puede sufrir una Entidad por su propensión a ser utilizada directamente o a través de sus operaciones, como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.

**1.65. RIESGOS DE SEGURIDAD DE LA INFORMACIÓN:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía, la integridad, el orden y los intereses de la entidad. Incluye aspectos relacionados con ambiente físico, digital y personas.

**1.66. 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/IEC 27000).

**1.67. RIESGO INHERENTE:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

**1.68. RIESGO RESIDUAL:** El resultado de aplicar la efectividad de los controles al riesgo inherente.

**1.69. SARLAFT:** Sistema de Administración del Riesgo de Lavado de Activos y de la Financiación del Terrorismo.

**1.70. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI:** Es el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son

administrados colectivamente por una Entidad, en la búsqueda de proteger sus activos de información esenciales de acuerdo con lo definido en la ISO/IEC 27000.

**1.71. SEGUNDA LÍNEA DE DEFENSA:** Asiste y guía a la línea estratégica y a la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.).

**1.72. SERVICIOS:** Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).

**1.73. SERVICIOS ESENCIALES:** Son los necesarios para el mantenimiento de las funciones sociales básicas la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del estado y las administraciones públicas.

**1.74. SOFTWARE:** Informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.

**1.75. TABLA DE RETENCIÓN DOCUMENTAL - TRD:** Es el listado de series, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, es decir se considera como el Instrumento que permite establecer cuáles son los documentos de una entidad, su necesidad e importancia en términos de tiempo de conservación y preservación y que debe hacerse con ellos una vez finalice su vigencia o utilidad.

**1.76. TERCERA LÍNEA DE DEFENSA:** Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera línea y la segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.

**1.77. 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.

**1.78. TRATAMIENTO AL RIESGO:** Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

**1.79. UIAF:** Unidad de Información y Análisis Financiero es un organismo de inteligencia económica y financiera que centraliza, sistematiza y analiza la información suministrada por las entidades reportantes y fuentes abiertas, para prevenir y detectar posibles operaciones de lavado de activos, sus delitos fuente, y la financiación del terrorismo.

**1.80. VULNERABILIDAD:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## 2. JUSTIFICACIÓN

La definición de una política para la gestión integral del riesgo constituye un elemento esencial dentro del Sistema de Control Interno y del Modelo Integrado de Planeación y Gestión - MIPG, dado que establece el marco normativo y metodológico que orienta la gestión institucional frente a amenazas y oportunidades.

Adicionalmente, la Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 07 exige que las entidades adopten un enfoque sistemático para la identificación, análisis, valoración, tratamiento, monitoreo y comunicación de riesgos; además, la NTC ISO 3100:2018, en su numeral 4.3.2 establece que toda organización debe contar con una política que i) defina el propósito y compromiso institucional con la gestión del riesgo, ii) establezca la integración del riesgo en todos los procesos, iii) reconozca la responsabilidad compartida de directivos y servidores públicos y, iv) promueva la mejora continua del sistema de gestión.

Igualmente, la política asegura que la gestión del riesgo se articule con la planeación estratégica y operativa, garantizando que los objetivos institucionales se definan considerando riesgos y oportunidades, los procesos financieros y presupuestales, evitando desviaciones en el uso de recursos públicos y los planes de desarrollo y proyectos institucionales, fortaleciendo la sostenibilidad y resiliencia de las acciones gubernamentales.

En este contexto, la política para la gestión integral del riesgo no es únicamente un requisito normativo, sino un instrumento estratégico de gobernanza que garantiza la sostenibilidad institucional, la eficiencia en el uso de recursos, la transparencia en la gestión y la confianza ciudadana. Su definición asegura que la entidad cumpla con los estándares nacionales e internacionales, y que disponga de un marco sólido para enfrentar los desafíos del entorno con responsabilidad y resiliencia.

## 3. POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

El Instituto Superior de Educación Rural - ISER se compromete a administrar y mantener un sistema de administración de riesgos que permita asegurar el cumplimiento de la misión, los objetivos institucionales y la satisfacción de los grupos de valor, garantizando la asignación de los recursos necesarios para analizar, valorar, tratar, monitorear, revisar y realizar seguimiento periódico, de acuerdo con los procesos y lineamientos establecidos en el Sistema de Control Interno y el Sistema de Gestión de la Calidad.

Para la administración y control de riesgos se establecen los niveles de responsabilidad para el manejo de riesgos, niveles de tolerancia, capacidad y apetito de riesgo, tratamiento de los riesgos, lineamientos para su información, comunicación y consulta, seguimiento, monitoreo y acciones frente a la materialización de estos.

## 4. OBJETIVOS

### 4.1. OBJETIVO GENERAL

Establecer los lineamientos estratégicos y operativos que orienten la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos en el Instituto Superior de Educación Rural - ISER, que puedan afectar el logro de los objetivos institucionales, en concordancia con el Modelo

Integrado de Planeación y Gestión – MIPG y las mejores prácticas internacionales basadas en el marco COSO ERM.

Así mismo, esta política tiene como propósito fortalecer la gobernanza, la toma de decisiones informadas y la generación de valor público asegurando la integridad, transparencia y eficiencia en la administración de recursos. Igualmente, busca promover una cultura organizacional orientada a la anticipación y gestión proactiva de riesgos, contribuyendo al cumplimiento de la misión institucional, la mejora continua y la confianza ciudadana en el Instituto Superior de Educación Rural.

### 4.2. OBJETIVOS ESPECÍFICOS

- Asegurar el cumplimiento de la misión institucional y los objetivos estratégicos.
- Garantizar la integridad, confidencialidad y disponibilidad de la información.
- Mitigar los posibles efectos de los riesgos sobre los objetivos institucionales y la operación normal del Instituto Superior de Educación Rural - ISER.
- Fortalecer la cultura y el pensamiento basado en riesgos en todos los niveles de la institución.
- Promover una gestión pública más armónica, transparente y eficiente.

## 5. MARCO LEGAL

**5.1.** Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.

**5.2.** Ley 489 de 1998, por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.

**5.3.** Ley 1474 de 2011, 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 la gestión pública.

**5.4.** Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

**5.5.** Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

**5.6.** Decreto 1081 de 2015, por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República.

**5.7.** Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.

**5.8.** 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 y se establece el MIPG.

**5.9.** Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

**5.10.** 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 del 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Telecomunicaciones.

**5.11.** Decreto 1122 de 2024, Por el cual se reglamenta el artículo 73 de la Ley 1474 de 2011, modificado por el artículo 31 de la Ley 2195 de 2022, en lo relacionado con los Programas de Transparencia y Ética Pública.

**5.12.** Decreto 1600 de 2024, Por el cual se modifica el Capítulo 1 y 3 del Título 4 de la Parte 1 del Libro 2 del Decreto 1081 de 2015, Decreto Reglamentario Único del Sector Presidencia de la República, en lo relacionado con las Subcomisiones Técnicas de la Comisión Nacional de Moralización y la Estrategia Nacional de Lucha Contra la Corrupción.

**5.13.** CONPES 3995 de 2020. La Política Nacional de Confianza y Seguridad Digital, señala el objetivo de establecer medidas para desarrollar la confianza digital a través de la mejora en la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

**5.14.** Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la Estrategia de Seguridad Digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital.

**5.15.** Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 07. Metodología para la gestión integral del riesgo.

## 6. ALCANCE

La Política para la Gestión Integral del Riesgo, inicia con la definición de los roles y responsabilidades, el análisis del contexto interno y externo, continua con la metodología establecida al interior del Instituto para la administración del riesgo y finaliza con el seguimiento, monitoreo y mejoramiento de los riesgos identificados.

La administración de riesgos es un proceso continuo que permite abordar y mitigar los riesgos organizacionales conforme las políticas establecidas, la cual aplica a todos los funcionarios, contratistas y servidores públicos del Instituto Superior de Educación Rural - ISER, así como a todos los procesos definidos en el Sistema de Gestión de la Calidad.

Así mismo, la presente política aplica a todas las dependencias, procesos, servidores públicos de la institución, contratistas, en todos los niveles jerárquicos y áreas misionales, estratégicas, de apoyo y evaluación. Incluye la gestión de riesgos en la planeación, ejecución presupuestal, prestación de servicios, adopción de tecnologías, fortalecimiento organizacional, así como en la implementación de proyectos y programas institucionales.

## 7. RESPONSABILIDADES

En el marco del Esquema de Líneas, el Instituto Superior de Educación Rural establece las periodicidades con sus responsables para el seguimiento a los riesgos estratégicos y claves de la entidad, considerando con especial relevancia las responsabilidades de la Línea estratégica y Alta Dirección en términos de la definición del apetito de riesgo, la aprobación de la política y la asignación de recursos y responsabilidades para su implementación. Las de la primera línea o líderes de proceso, responsables de identificar, evaluar y controlar riesgos en sus diferentes procesos, proyectos o iniciativas estratégicas, dentro de estas las propias de todos los Servidores, responsables de reportar oportunamente los riesgos materializados, aplicar los controles establecidos y proponer proactivamente mejoras en los mismos cuando sean necesarias.

Las del proceso de Control Interno de Gestión, en cuanto a la evaluación de la efectividad de los controles y la proposición de mejoras para hacer más efectiva la gestión de los diferentes tipos de riesgos.

**LÍNEA ESTRATÉGICA.** Define el marco general para la gestión del riesgo y el control, supervisa su cumplimiento.

| RESPONSABLE | RESPONSABILIDAD |
|---|---|
| Alta Dirección – Comité Institucional de Coordinación de Control Interno | Evaluar el estado del Sistema de Control Interno, acorde con la información generada por parte de las instancias de segunda línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema del cual son responsables a fin de generar acciones y una toma de decisiones con enfoque preventivo.<br><br>A continuación, las responsabilidades específicas:<br><br>▪ Definir e impartir lineamientos relacionados con el marco general para la gestión integral de los riesgos.<br>▪ Aprobar la Política para la Gestión Integral del Riesgo.<br>▪ Realizar recomendaciones orientadas a la mejora y actualización de la política.<br>▪ Supervisar el cumplimiento de la política.<br>▪ Revisar los resultados del monitoreo y seguimiento de los riesgos, generar alertas y recomendaciones cuando sea necesario.<br>▪ Conocer y resolver los conflictos de interés que afecten la independencia de las auditorías basadas en riesgos. |

**PRIMERA LÍNEA DE DEFENSA.** En esta línea entran los servidores de todos los niveles y tienen como responsabilidad definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineados con las metas y objetivos de la institución y proponer mejoras a la gestión del riesgo en su proceso y reportar en el sistema o esquema definido por la institución los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos.

| RESPONSABLE | RESPONSABILIDAD |
|---|---|
| Líderes de Proceso | ▪ Asegurar la implementación de la Política de Gestión Integral del Riesgo y los instrumentos asociados para su mitigación, reportando a la segunda línea sus avances y dificultades.<br>▪ Identificar, valorar y definir la opción de tratamiento a los riesgos que tiene alcance la presente política y que pueden afectar el logro de los objetivos de los procesos, programas o proyectos en los cuales participe, acorde con la política.<br>▪ Realizar monitoreo permanente a la gestión de riesgos y controles con el fin de detectar las deficiencias de los controles.<br>▪ Ejecutar los controles como están diseñados.<br>▪ Informar la materialización de riesgos, siguiendo el conducto asociado para su tratamiento.<br>▪ Aplicar las medidas de control para evitar la materialización de riesgos asociadas a la ejecución de sus actividades.<br>▪ Reportar y realizar el cargue de evidencias en los repositorios de información destinados para ello, en los tiempos estipulados por el proceso de Direccionamiento Estratégico y Planeación.<br>▪ En cada vigencia identificar, valorar y actualizar cuando se requiera los riesgos que pueden afectar los objetivos del proceso y/o institucionales.<br>▪ Gestionar ante el proceso de Direccionamiento Estratégico y Planeación la materialización de un riego no identificado, para su inclusión en la matriz de riesgos del proceso e institucional. |
| Servidores Públicos | ▪ Participar en cada una de las etapas de la implementación del modelo de gestión integral del riesgo, desde la naturaleza de sus funciones y procesos relacionados, apoyando la construcción y actualización de mapas de riesgos, la caracterización de controles y seguimiento correspondiente.<br>▪ Informar la materialización de riesgos, siguiendo el conducto asociado para su tratamiento.<br>▪ Aplicar las medidas de control para evitar la materialización de riesgos asociadas a la ejecución de sus actividades.<br>▪ Los supervisores de contrato realizar seguimiento a los riesgos relacionados con su ejercicio e informar las alertas respectivas. |
| Contratistas | ▪ Participar en cada una de las etapas de la implementación del modelo de gestión integral del riesgo, desde la naturaleza de sus funciones y procesos relacionados, apoyando la construcción y actualización de mapas de riesgos, la caracterización de controles y seguimiento correspondiente.<br>▪ Informar la materialización de riesgos, siguiendo el conducto asociado para su tratamiento.<br>▪ Aplicar las medidas de control para evitar la materialización de riesgos asociadas a la ejecución de sus actividades. |

**SEGUNDA LÍNEA DE DEFENSA.** Tiene como objetivo definir los lineamientos en materia de seguridad de la información, compras y contratación pública, gestión financiera así como consolidar el mapa de riesgos institucional, con un enfoque para el análisis de los riesgos de mayor criticidad frente al logro de los objetivos y presentarlo cuatrimestralmente ante la Línea Estratégica para su análisis y toma de decisiones correspondiente.

| RESPONSABLE | RESPONSABILIDAD |
|---|---|
| Direccionamiento Estratégico y Planeación | ▪ Asesorar a la Línea Estratégica en el análisis del contexto interno y externo, para la definición de la Política de Gestión Integral del Riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.<br>▪ Brindar acompañamiento metodológico a los responsables de procesos y a sus equipos de trabajo en la formulación o actualización de los mapas de riesgos.<br>▪ Acompañar al proceso en el establecimiento de los controles de los riesgos identificados y a su diseño.<br>▪ Consolidar la matriz de riesgos por proceso y el mapa institucional de riesgos.<br>▪ Acompañar, orientar y entrenar a los Líderes de Procesos en la identificación, análisis y valoración del riesgo.<br>▪ Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los Líderes de Procesos.<br>▪ Diseñar, implementar y socializar la metodología para la valoración, seguimiento y control de los riesgos institucionales.<br>▪ Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.<br>▪ Generar recomendaciones y posibles ajustes a los mapas de riesgos, de manera tal que las instancias de 1ª Línea puedan establecer mejoras a los riesgos y controles, así mismo garantizar su aplicación efectiva.<br>▪ Solicitar la publicación del Mapa de riesgos institucional en la sección de Transparencia de la página web institucional, previo al cumplimiento de los requisitos establecidos por la normatividad vigente.<br>▪ Informar sobre la incidencia de los riesgos en el logro de los objetivos institucionales.<br>▪ Revisar el diseño de los riesgos y controles a través de la metodología adoptada por el ISER, para la mitigación de los riesgos y realizar las recomendaciones y monitoreos para el fortalecimiento de estos. |
| Gestión de Recursos Financieros | ▪ Establecer objetivos presupuestales y financieros que apoyen el logro de los objetivos estratégicos previstos<br>▪ Proveer los recursos financieros necesarios para la implementación de la política. |
| Gestión de Tecnologías de la Información y la Comunicación | ▪ Definir los lineamientos para el Inventario y Clasificación de Activos de Información en articulación con el proceso de Gestión Documental. |
| Gestión Jurídica y Gestión de Contratación | ▪ Establecer los lineamientos para la implementación de la Política de Compras y Contratación Pública. |

**TERCERA LÍNEA DE DEFENSA.** Garantiza la efectividad del Sistema de Control Interno. A diferencia de las primeras dos líneas, que están enfocadas en la gestión operativa y el cumplimiento,

la tercera línea proporciona una evaluación independiente y objetiva, identifica áreas de mejora y propone acciones correctivas. Se encarga de realizar la medición de los avances de las acciones de respuesta y evaluación de la política.

| RESPONSABLE | RESPONSABILIDAD |
|---|---|
| Control Interno de Gestión | 1. Evaluar de manera independiente y objetiva la efectividad del diseño e implementación del Sistema de Administración del Riesgo del Instituto.<br>2. Verificar que la política de riesgos esté alineada con el MIPG, el direccionamiento estratégico y el contexto institucional.<br>3. Evaluar la coherencia entre riesgos, controles, tratamiento e indicadores<br>4. Revisar la efectividad y aplicación de controles, planes de contingencia y actividades de monitoreo vinculados a riesgos clave del Instituto.<br>5. Realizar el seguimiento y evaluación de acuerdo con la periodicidad definida en la política de gestión integral del riesgo a la matriz de riesgos.<br>6. Evaluar si los controles definidos están adecuadamente diseñados, funcionan de manera efectiva y mitigan el riesgo identificado.<br>7. Identificar debilidades en la identificación de riesgos y controles y formular las recomendaciones de mejora.<br>8. Asesorar a la primera línea de defensa de forma coordinada con el proceso de Direccionamiento Estratégico y Planeación en la identificación de riesgos y diseño de controles<br>9. Informar a la alta Dirección y al Comité Institucional de Coordinación de Control Interno los resultados de las evaluaciones<br>10. Formular recomendaciones de mejora orientadas al fortalecimiento de la Política para la Gestión Integral del Riesgo y realizar seguimiento a la implementación de las acciones correctivas derivadas de auditorías, evaluaciones y ejercicios de seguimiento.<br>11. Alertar sobre la probabilidad de riesgo de fraude o corrupción significativo en los procesos auditados.<br>12. Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos o unidades auditables que tienen mayor nivel de exposición al riesgo.<br>13. Informar sobre las auditorías basadas en riesgos que se ejecuten, con énfasis en riesgos fiscales.<br>14. Comunicar regularmente al Comité Institucional de Coordinación de Control Interno, y como resultado de la evaluación independiente, cambios e impactos en la evaluación del riesgo.<br>15. Brindar asesoría y acompañamiento a la primera y segunda línea de defensa.<br>16. Realizar seguimiento a la efectividad de la gestión de riesgos realizada por la primera y segunda línea de defensa. Las evidencias correspondientes a los controles y al plan de acción deben ser consultadas en los medios dispuestos que para tal fin sean definidos.<br>17. Realizar seguimiento a la implementación de las acciones de mejora propuestos en la matriz de riesgos. |

## 8. ETAPAS DE LA POLÍTICA PARA LA GESTIÓN INTEGRAL DEL RIESGO

El Instituto Superior de Educación Rural – ISER adopta para la gestión integral del riesgo la metodología establecida por el Departamento Administrativo de la Función Pública - DAFP en el documento denominado Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7. Este documento, proporciona los lineamientos necesarios para una gestión estructurada, coherente de los riesgos, alineada con los objetivos institucionales.

En concordancia con lo anterior, el enfoque aplicado es cíclico y participativo, y permite identificar, analizar, valorar y gestionar los riesgos de forma continua. A través de este proceso, el Instituto fortalece la toma de decisiones, anticipa situaciones críticas y promueve una cultura de prevención y mejora permanente.

A continuación, se presentan las etapas que componen este ciclo, junto con una breve descripción de cada una:


### 8.1. PLANEACIÓN Y PREPARACIÓN

La fase de planeación y preparación constituye el momento estratégico inicial en el que se definen las bases para implementar de manera efectiva la política de gestión integral del riesgo. Su propósito

es garantizar que la gestión de riesgos se integre de forma coherente con los objetivos institucionales y se convierta en un proceso sistemático y sostenible.

Los elementos clave a considerar durante esta fase son:

- La definición de objetivos y alcance, en la cual se debe establecer qué se busca lograr con la Política de Gestión Integral del Riesgo.
- Determinar el alcance de la administración y gestión de riesgos (procesos, áreas y niveles de la organización que abarca la Política de Gestión Integral del Riesgo).
- Asignar los roles y responsabilidades, lo cual permita identificar los responsables de liderar la gestión de riesgos (comités, líderes de proceso, equipos técnicos, etc.), así como la necesidad de definir los mecanismos de coordinación y comunicación entre los diferentes procesos.
- Finalmente, se debe terminar el diseño metodológico y selección de herramientas para la administración de riesgos, lo cual permita adoptar metodologías para identificar, analizar, evaluar y tratar riesgos.

Esta fase es el pilar fundamental de la Política de Gestión Integral del Riesgo, pues permite estructurar objetivos, metodologías, responsables y recursos de manera organizada, lo cual asegura que la gestión de riesgos no sea un ejercicio aislado, sino un componente transversal de la estrategia institucional, orientado a la prevención y mitigación frente a amenazas internas y externas.

### 8.1.1. Determinación de la Capacidad del Riesgo

La capacidad del riesgo para el Instituto Superior de Educación Rural - ISER, siguiendo los lineamientos de la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se entiende como el nivel máximo de riesgo que la institución puede manejar de manera efectiva, considerando sus recursos, estructuras de control, talento humano y sistemas de gestión. A diferencia del apetito del riesgo, que refleja la disposición a asumir ciertos riesgos, la capacidad del riesgo está determinada por las condiciones reales de la entidad para responder y mitigar los impactos que estos puedan generar.

En el caso de los riesgos generales de gestión, la capacidad del ISER depende de su infraestructura administrativa, la solidez de sus procesos internos y la competencia del personal. La institución puede gestionar riesgos moderados en este ámbito, siempre que cuente con planes de contingencia, sistemas de monitoreo y mecanismos de mejora continua que le permitan mantener la prestación del servicio educativo sin interrupciones significativas.

Respecto a la seguridad de la información, la capacidad del riesgo es limitada, pues requiere inversiones constantes en tecnología, capacitación y protocolos de protección de datos. Aunque el ISER puede implementar medidas de control como políticas de acceso, respaldos y auditorías, su capacidad para enfrentar ataques cibernéticos sofisticados o vulneraciones masivas es reducida, lo que obliga a mantener un margen de riesgo muy bajo y fortalecer alianzas con entidades especializadas.

En el ámbito de los riesgos fiscales, la capacidad del ISER está condicionada por la disponibilidad de recursos financieros, la disciplina presupuestal y la eficiencia en la ejecución del gasto. La institución tiene una capacidad restringida para asumir riesgos de carácter fiscal, ya que cualquier desviación significativa podría comprometer su sostenibilidad económica y limitar su capacidad de inversión en programas académicos y de infraestructura.

Finalmente, frente a los riesgos para la integridad pública, la capacidad del ISER es prácticamente nula. La institución no puede gestionar ni tolerar situaciones que afecten la ética, la transparencia o la lucha contra la corrupción, dado que estos riesgos trascienden los controles internos y comprometen directamente la legitimidad institucional. Por ello, la capacidad de riesgo en este ámbito se traduce en la implementación de políticas de cero tolerancias, mecanismos de denuncia y fortalecimiento de la cultura organizacional basada en valores.

### 8.1.2. Determinación del Apetito del Riesgo

El apetito del riesgo para el Instituto Superior de Educación Rural - ISER, de acuerdo con la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se entiende como el nivel de riesgo que la institución está dispuesta a aceptar en el cumplimiento de sus objetivos estratégicos y misionales. Este concepto no implica la eliminación total de los riesgos, sino la definición clara de hasta qué punto la entidad puede asumirlos sin comprometer su sostenibilidad, transparencia y confianza pública.

En cuanto a los riesgos generales de gestión, el ISER puede aceptar un nivel moderado de riesgo, especialmente en procesos de innovación académica, gestión administrativa y proyectos de mejora institucional. Estos riesgos son necesarios para avanzar en la modernización y fortalecimiento institucional, siempre que existan controles adecuados que garanticen la continuidad del servicio educativo para la satisfacción de los grupos de valor e interés.

Respecto a los riesgos de seguridad de la información, el apetito del riesgo es bajo. La protección de datos personales, académicos y administrativos constituye un eje fundamental para la confianza institucional y el cumplimiento de la normativa vigente en materia de protección de datos. Por ello, cualquier vulnerabilidad debe ser gestionada de manera inmediata y con medidas preventivas sólidas.

En el ámbito de los riesgos fiscales, el apetito es muy reducido. La administración de los recursos públicos exige disciplina presupuestal y cumplimiento estricto de las normas financieras, evitando situaciones que puedan generar sanciones o comprometer la sostenibilidad económica de la institución. El ISER debe priorizar la eficiencia y la transparencia en el uso de los recursos.

Finalmente, frente a los riesgos para la integridad pública, el ISER adopta una postura de cero tolerancias. No se admite ningún nivel de riesgo que pueda afectar la ética institucional, la transparencia en la gestión o la lucha contra la corrupción. La integridad es un valor esencial que sostiene la legitimidad de la institución y su relación con la comunidad educativa y la sociedad en general.

### 8.1.3. Tolerancia del Riesgo

La tolerancia del riesgo para el Instituto Superior de Educación Rural - ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se entiende como el nivel específico de variación aceptable respecto al apetito del riesgo. Mientras el apetito define la disposición general de la entidad a asumir riesgos, la tolerancia establece los límites cuantitativos o cualitativos dentro de los cuales dichos riesgos pueden materializarse sin comprometer los objetivos estratégicos ni la confianza institucional.

En relación con los riesgos generales de gestión, la tolerancia del ISER puede ubicarse en un rango moderado. Esto significa que la institución admite ciertas desviaciones en la ejecución de procesos administrativos o académicos, siempre que no afecten de manera significativa la calidad del servicio educativo ni la satisfacción de los grupos de valor. La tolerancia aquí se traduce en aceptar retrasos menores, ajustes en cronogramas o variaciones presupuestales controladas, siempre bajo mecanismos de seguimiento y mejora continua.

Para la seguridad de la información, la tolerancia es mínima. El ISER no puede permitir fallas recurrentes en la protección de datos personales, académicos o administrativos. La tolerancia se limita a incidentes menores que no comprometan la confidencialidad, integridad o disponibilidad de la información, y que puedan ser corregidos de manera inmediata mediante protocolos de respuesta y medidas preventivas.

En cuanto a los riesgos fiscales, la tolerancia es igualmente reducida. La institución puede aceptar variaciones menores en la ejecución presupuestal, como ajustes en la distribución de recursos o retrasos en la ejecución de proyectos, siempre que no generen déficit financiero ni incumplimiento de la normatividad fiscal. La tolerancia se establece en márgenes estrechos que aseguren disciplina y sostenibilidad económica.
Finalmente, frente a los riesgos para la integridad pública, la tolerancia es nula. El ISER no admite ningún nivel de desviación que pueda afectar la ética, la transparencia o la lucha contra la corrupción. Cualquier indicio de irregularidad debe ser gestionado de manera inmediata, con políticas de cero tolerancia y mecanismos de control que refuercen la confianza de la comunidad educativa y de la sociedad en general.

### 8.2. IDENTIFICACIÓN DE RIESGOS

De acuerdo con los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, resulta fundamental que el ISER avance en la identificación sistemática de los riesgos que pueden afectar el cumplimiento de sus objetivos institucionales. Este proceso permite reconocer de manera anticipada las amenazas y vulnerabilidades que se presentan en ámbitos como la gestión administrativa y académica, la seguridad de la información, la sostenibilidad fiscal y la integridad pública.

La identificación de riesgos no solo constituye el primer paso para su adecuada valoración y tratamiento, sino que también fortalece la transparencia, la rendición de cuentas y la confianza de la comunidad educativa y la sociedad en general. En este sentido, el ISER debe consolidar una cultura organizacional orientada a la prevención y al control, asegurando que cada riesgo detectado se traduzca en acciones concretas de mitigación y mejora continua.

#### 8.2.1. Análisis de Objetivos Estratégicos y de los Procesos

Los riesgos identificados deben tener impacto en el cumplimiento de objetivos estratégicos, estar alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos.

Para su adecuada formulación, deben contener unos atributos mínimos, para lo cual se puede hacer uso de las características SMART:

| | | |
|---|---|---|
| **S** | **ESPECÍFICO** | Resuelve cuestiones como qué, cuándo, cómo, dónde, con qué, quién considerando el orden y los necesarios para el cumplimiento de la misión. |
| **M** | **MEDIBLE** | Involucra algunos números en su definición. Ejemplo: porcentajes o cantidades cuando aplique. |
| **A** | **ALCANZABLE** | Realizar un análisis de los que se ha hecho y logrado hasta el momento para determinar si lo que se propone es posible o cómo resultaría mejor. |
| **R** | **RELEVANTE** | Considera recursos, factores externos e información de actividades previas. |
| **T** | **TEMPORAL** | Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y las mediciones finales. |

De acuerdo con lo anterior, se debe tener en cuenta que los indicadores del Sistema de Gestión de la Calidad permiten medir el cumplimiento del objetivo de cada proceso, alineados con los objetivos, política, misión y visión y, de la misma manera, los riesgos se identifican a partir de los factores de riesgo que puedan afectar el cumplimiento del objetivo de cada proceso.

Con relación a los Riesgos de Seguridad de la Información, primero debe identificarse la Matriz del Inventario de Activos de Información, la cual es el insumo principal para la gestión de este tipo de riesgos.

### 8.2.2. Identificación de Puntos de Riesgo

La definición de puntos de riesgo para el Instituto Superior de Educación Rural – ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, constituye un paso esencial para focalizar la gestión institucional en aquellos aspectos que pueden comprometer el logro de los objetivos estratégicos. Los puntos de riesgo son áreas críticas donde la probabilidad de ocurrencia y el impacto potencial requieren atención prioritaria, pues de su adecuada identificación depende la efectividad de las medidas de control y mitigación.

En el ámbito de los riesgos generales de gestión, los puntos de riesgo se relacionan con la planificación académica, la eficiencia administrativa y la coordinación interinstitucional. Una deficiente gestión de procesos puede generar retrasos en la prestación del servicio educativo, baja satisfacción de los estudiantes y pérdida de credibilidad institucional. Por ello, se deben identificar como puntos de riesgo la falta de infraestructura adecuada, la limitada capacidad de respuesta frente a cambios normativos y las debilidades en la cultura organizacional.

Respecto a los riesgos de seguridad de la información, los puntos de riesgo se concentran en el manejo de datos personales, académicos y administrativos, así como en la protección frente a accesos no autorizados o ataques cibernéticos. La pérdida, alteración o divulgación indebida de información constituye un riesgo crítico que afecta la confianza de la comunidad y puede derivar en sanciones legales. En este sentido, los sistemas de almacenamiento, las políticas de acceso y los protocolos de respaldo deben ser considerados puntos de riesgo prioritarios.

En el caso de los riesgos fiscales, los puntos de riesgo se vinculan con la planeación presupuestal, la ejecución de recursos y el cumplimiento de la normatividad financiera. Una administración inadecuada puede comprometer la sostenibilidad económica del ISER, limitar la inversión en programas estratégicos y generar sanciones por incumplimiento. Por ello, la disciplina presupuestal, la transparencia en el gasto y la eficiencia en la gestión financiera deben ser reconocidos como puntos de riesgo clave.

Finalmente, los riesgos para la integridad pública representan puntos de riesgo de máxima sensibilidad. Se refieren a cualquier situación que pueda afectar la ética institucional, la transparencia en la gestión o la lucha contra la corrupción. La existencia de prácticas indebidas, conflictos de interés o debilidades en los sistemas de control interno son puntos de riesgo que deben ser identificados y gestionados con políticas de cero tolerancias, fortaleciendo la cultura organizacional basada en valores.

### 8.2.3. Identificación de Áreas de Impacto

La identificación de áreas de impacto en el Instituto Superior de Educación Rural - ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, permite reconocer los efectos que la materialización de los riesgos puede generar sobre los objetivos institucionales, la confianza pública y la sostenibilidad de la entidad. Este análisis es clave para priorizar acciones de mitigación y orientar la toma de decisiones estratégicas, ya que define las consecuencias que cada tipo de riesgo tendría en el cumplimiento de la misión educativa y en la relación con la comunidad.

En el caso de los riesgos generales de gestión, el impacto se refleja en la eficiencia administrativa, la calidad de los procesos académicos y la capacidad de respuesta institucional. Una gestión deficiente puede afectar directamente la prestación del servicio educativo, disminuir la satisfacción de los estudiantes y debilitar la credibilidad institucional frente a sus grupos de interés.

Respecto a los riesgos de seguridad de la información, el impacto es crítico, pues cualquier vulneración compromete la confidencialidad, integridad y disponibilidad de los datos personales, académicos y administrativos. La pérdida o filtración de información puede generar sanciones legales, pérdida de confianza de la comunidad y afectaciones a la reputación institucional.

En el ámbito de los riesgos fiscales, el impacto se traduce en la sostenibilidad financiera y en la capacidad del ISER para ejecutar proyectos estratégicos. Una administración inadecuada de los recursos públicos puede derivar en déficit presupuestales, limitaciones en la inversión y sanciones por incumplimiento normativo, lo que afectaría directamente la continuidad de los programas académicos.

Finalmente, los riesgos para la integridad pública tienen un impacto devastador, ya que comprometen la ética institucional, la transparencia y la legitimidad frente a la sociedad. Cualquier situación de corrupción, conflicto de interés o falta de probidad afecta de manera irreversible la confianza ciudadana y debilita la misión institucional como institución pública orientada al servicio de la comunidad.

### 8.2.4. Identificación de Áreas de Factores de Riesgo

La identificación de áreas de riesgo en el Instituto Superior de Educación Rural - ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, constituye un proceso

esencial para anticipar amenazas que puedan afectar el cumplimiento de los objetivos institucionales y la confianza de la comunidad educativa. Este ejercicio permite reconocer de manera estructurada los ámbitos críticos en los que la institución debe concentrar sus esfuerzos de prevención, control y mejora continua.

En primer lugar, los riesgos generales de gestión abarcan aspectos relacionados con la planificación, la ejecución de procesos administrativos y académicos, la calidad del servicio educativo y la eficiencia institucional. La identificación en esta área busca reconocer debilidades en la infraestructura, la cultura organizacional, la coordinación interinstitucional y la capacidad de respuesta frente a cambios normativos o sociales que puedan impactar la misión del ISER.

En segundo lugar, la seguridad de la información constituye un área prioritaria de riesgo. Aquí se incluyen las amenazas vinculadas con el manejo de datos personales, académicos y administrativos, así como la protección frente a accesos no autorizados, pérdida de información o ataques cibernéticos. La identificación de riesgos en este ámbito permite establecer controles tecnológicos y normativos que garanticen la confidencialidad, integridad y disponibilidad de la información institucional.

Por otra parte, los riesgos fiscales se relacionan con la administración de los recursos públicos, la disciplina presupuestal y el cumplimiento de las normas financieras. La identificación en esta área busca prevenir desviaciones en la ejecución presupuestal, deficiencias en la planeación financiera o situaciones que puedan comprometer la sostenibilidad económica del ISER. Reconocer estos riesgos es clave para asegurar la transparencia y la eficiencia en el uso de los recursos.

Finalmente, los riesgos para la integridad pública constituyen un área de riesgo de máxima sensibilidad. Se refieren a cualquier situación que pueda afectar la ética institucional, la transparencia en la gestión o la lucha contra la corrupción. La identificación en este ámbito implica reconocer prácticas indebidas, conflictos de interés o vulnerabilidades en los sistemas de control que puedan comprometer la legitimidad del ISER frente a la sociedad.

### 8.2.5. Descripción del Riesgo

La identificación y descripción de los riesgos generales de la gestión, fiscales, de seguridad de la información y aquellos que afectan la integridad pública se llevará a cabo siguiendo los lineamientos establecidos en la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7. Este enfoque garantiza que el análisis se realice bajo criterios técnicos uniformes, promoviendo la coherencia institucional y la alineación con las mejores prácticas de control interno. La guía establece parámetros claros para reconocer amenazas, vulnerabilidades y posibles impactos, lo que permite estructurar un diagnóstico integral que facilite la toma de decisiones estratégicas y la implementación de medidas preventivas y correctivas.

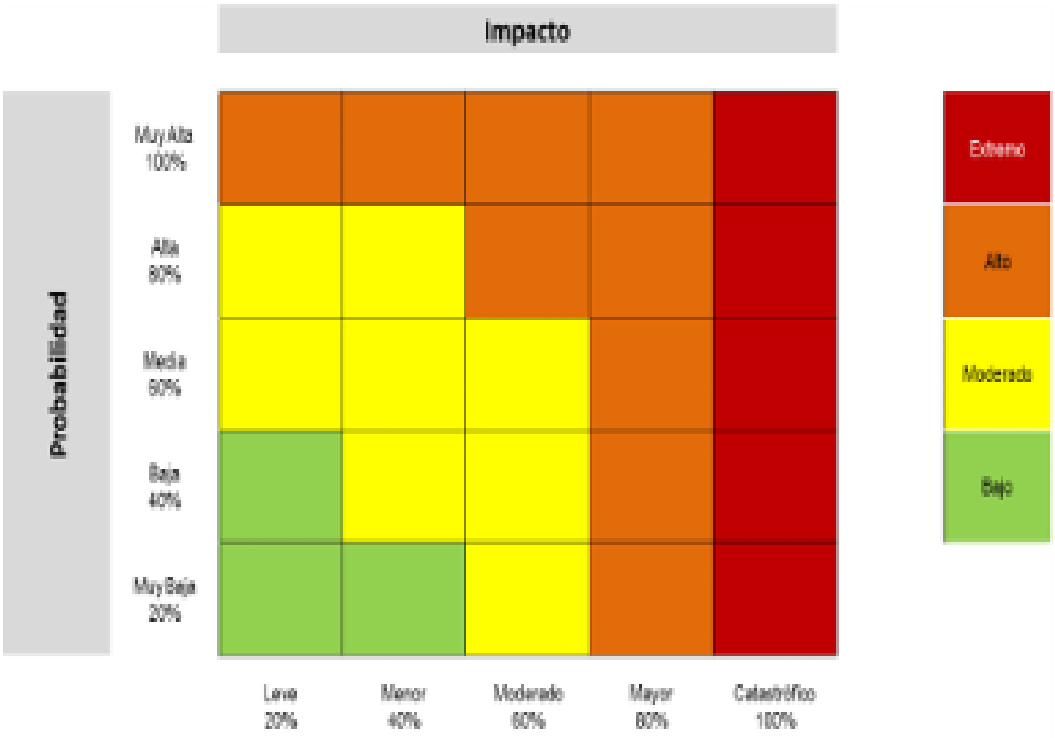
Asimismo, la aplicación de estos lineamientos asegura que la gestión de riesgos se articule con los objetivos institucionales y con los principios de transparencia y responsabilidad pública. La descripción de los riesgos se fundamentará en metodologías que priorizan la identificación de factores críticos, la valoración de su probabilidad e impacto, y la definición de acciones de mitigación. De esta manera, se fortalece la capacidad de las entidades para anticipar escenarios adversos, proteger la información y los recursos fiscales, y salvaguardar la confianza ciudadana en la administración pública.

### 8.3. ANÁLISIS DE RIESGOS

Esta fase permite determinar la frecuencia con la que puede ocurrir un riesgo y la magnitud de sus efectos, lo cual permite categorizar los riesgos como altos, medios o bajos, esto basado en las escalas cualitativas y cuantitativas definidas.

#### 8.3.1. Análisis de Riesgo Inherente

El método de valoración de riesgos para el Instituto Superior de Educación Rural ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se fundamenta en la necesidad de evaluar de manera sistemática la probabilidad de ocurrencia y el impacto que cada riesgo puede generar sobre los objetivos institucionales. Este proceso permite priorizar los riesgos más críticos y orientar la implementación de medidas de control y mitigación, asegurando que la gestión se realice con criterios objetivos y alineados con la misión y la transparencia institucional.




En el caso de los riesgos generales de gestión, la valoración debe considerar factores como la frecuencia con la que pueden presentarse fallas en los procesos institucionales, así como el nivel de afectación que estas tendrían. La combinación de probabilidad e impacto permite determinar si el riesgo es bajo, moderado, alto o extremo y, establecer planes de acción proporcionales.

Respecto a los riesgos de seguridad de la información, la valoración se centra en identificar la vulnerabilidad de los sistemas de información y la sensibilidad de los datos que maneja el ISER. Aquí, la probabilidad de incidentes como accesos no autorizados o pérdida de información se cruza con el impacto que tendría sobre la confidencialidad, integridad y disponibilidad de los datos. Dado

el carácter crítico de esta área, incluso riesgos de baja probabilidad pueden ser valorados como altos si su impacto compromete la confianza institucional.

En el ámbito de los riesgos fiscales, la valoración debe considerar la probabilidad de desviaciones en la ejecución presupuestal y el impacto que estas tendrían en la sostenibilidad financiera de la institución. La metodología implica analizar escenarios de déficit, retrasos en la asignación de recursos o incumplimientos normativos, clasificando los riesgos según su capacidad de afectar la estabilidad económica y la transparencia en el manejo de fondos públicos. La combinación de probabilidad e impacto permite determinar si el riesgo es bajo, moderado, alto o extremo y, establecer planes de acción proporcionales.

Finalmente, frente a los riesgos para la integridad pública, la valoración se realiza bajo un enfoque de cero tolerancias. Aunque la probabilidad de ocurrencia pueda ser baja, el impacto de cualquier situación que afecte la ética, la transparencia o la lucha contra la corrupción es considerado crítico. Por ello, estos riesgos deben ser valorados siempre en niveles altos, priorizando su gestión inmediata y el fortalecimiento de los mecanismos de control interno.

### 8.3.2. Diseño de Controles

El método para la definición de controles en el Instituto Superior de Educación Rural - ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, consiste en establecer medidas preventivas, detectivas y correctivas que respondan proporcionalmente a los riesgos identificados en las áreas críticas de gestión institucional, seguridad de la información, fiscales e integridad pública; los controles preventivos buscan anticipar y reducir la probabilidad de ocurrencia mediante la planificación adecuada, la capacitación, la adopción de políticas claras y el fortalecimiento de la cultura organizacional; los controles detectivos permiten identificar oportunamente desviaciones o incidentes a través de auditorías, sistemas de monitoreo, indicadores de desempeño y canales de denuncia; y los controles correctivos se orientan a la implementación de acciones inmediatas para mitigar el impacto, tales como planes de mejora, ajustes presupuestales, recuperación de información y sanciones disciplinarias, asegurando que la institución mantenga la transparencia, la sostenibilidad y la confianza pública en el cumplimiento de su misión institucional.

### 8.3.3. Análisis de Riesgo Residual

El método de valoración del riesgo residual para el Instituto Superior de Educación Rural - ISER, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se centra en determinar el nivel de riesgo que permanece después de aplicar los controles preventivos, detectivos y correctivos definidos por la institución. Este proceso permite evaluar la efectividad de los mecanismos de control y establecer si el riesgo residual se encuentra dentro de los límites aceptables de apetito y tolerancia previamente definidos.

Este método de valoración del riesgo residual consiste en evaluar la efectividad de los controles aplicados y determinar si el nivel de riesgo que permanece es aceptable dentro de los parámetros institucionales. Este enfoque asegura que la gestión del riesgo sea dinámica, que se ajusten los controles cuando sea necesario y que la institución mantenga su compromiso con la transparencia, la sostenibilidad y la confianza pública.

## 8.4. VALORACIÓN Y PRIORIZACIÓN

El método de valoración y priorización de los riesgos, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se fundamenta en analizar el nivel de riesgo que permanece después de aplicar los controles definidos y establecer un orden de atención según su criticidad. Este proceso permite determinar si los riesgos residuales se encuentran dentro de los límites aceptables de apetito y tolerancia, y facilita la asignación de recursos hacia aquellos que representan mayor amenaza para la misión institucional.

Este método de valoración y priorización de los riesgos combina la evaluación de la efectividad de los controles con la clasificación de los riesgos según su impacto y probabilidad, lo cual asegura que los riesgos más críticos reciban atención inmediata, fomentando que los riesgos se gestionen en función de su relevancia, fortaleciendo la cultura de prevención, transparencia y la sostenibilidad institucional.

### 8.5. TRATAMIENTO DE RIESGOS

El tratamiento es indispensable porque permite garantizar la continuidad de la misión y la sostenibilidad institucional y la confianza de los grupos de valor e interés. Los riesgos no pueden ser ignorados, ya que su materialización puede afectar de manera directa la calidad del servicio, la transparencia en la gestión y la legitimidad del Instituto. Por ello, se deben aplicar estrategias diferenciadas como reducir, compartir, aceptar o evitar, de acuerdo con la naturaleza y el impacto de cada riesgo.

### 8.6. IDENTIFICACIÓN Y PRIORIZACIÓN DE OPORTUNIDADES

La norma ISO 9001 define el Riesgo como el efecto de la incertidumbre sobre un resultado esperado. La Oportunidad, en cambio, es la posibilidad de obtener un resultado favorable. Ambos pueden afectar a la calidad de los productos y servicios y al desempeño del Sistema de Gestión de la Calidad.

Las Oportunidades pueden conducir a la adopción de nuevas prácticas, lanzamiento de nuevos productos, apertura de nuevos mercados, acercamiento a nuevos clientes, establecimiento de asociaciones, utilización de nuevas tecnologías y otras posibilidades deseables y viables para abordar las necesidades de la organización o las de sus clientes.

La gestión de Oportunidades es la evaluación que se realiza de la gestión interna y externa, la cual tiene como objetivo mejorar la eficacia del sistema de gestión de calidad obteniendo unos mejores resultados, adelantándose o previniendo efectos negativos.

En tal sentido, el Instituto Superior de Educación Rural – ISER, dando cumplimiento al numeral 6.1 de la NTC ISO 9001:2015, pretende identificar las Oportunidades que fomenten la mejora integral institucional y abordar las acciones necesarias que conlleven a su materialización.

### 8.7. SEGUIMIENTO Y MONITOREO

El seguimiento, monitoreo y revisión se conciben como procesos estratégicos que garantizan la gestión integral del riesgo en las entidades públicas. Estos componentes permiten verificar la implementación de las acciones, evaluar su impacto y ajustar las estrategias para asegurar la mejora continua.

Las acciones de seguimiento, monitoreo y revisión de los riesgos se desarrollarán en estricto cumplimiento de los lineamientos establecidos en el numeral 10 del presente documento. Dichos

lineamientos proporcionan el marco metodológico necesario para garantizar que la gestión del riesgo se ejecute de manera ordenada, coherente y con criterios de transparencia, asegurando que cada actividad responda a los objetivos institucionales.

Este proceso se encuentra plenamente articulado con las responsabilidades definidas en el esquema de Líneas de Defensa del Modelo Integrado de Planeación y Gestión – MIPG, lo que permite una distribución clara de roles y funciones. De esta manera, se fortalece la capacidad institucional para anticipar amenazas, evaluar la efectividad de los controles y promover la mejora continua en la gestión pública.

### 8.7.1. Seguimiento

El seguimiento consiste en la verificación periódica de las acciones definidas en los planes de tratamiento del riesgo. Este proceso busca constatar que las medidas implementadas se ejecuten conforme a lo planeado y que los responsables cumplan con los tiempos e indicadores establecidos. El seguimiento no se limita a revisar el cumplimiento formal, sino que se orienta a identificar desviaciones, evaluar la pertinencia de los controles y generar información útil para la toma de decisiones estratégicas.

### 8.7.2. Monitoreo

El monitoreo se entiende como la observación sistemática y continua de los riesgos y sus controles, con el fin de detectar oportunamente cambios en el contexto interno o externo que puedan alterar su nivel de impacto o probabilidad. La Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, enfatiza el uso de Indicadores Clave de Riesgo - KRI y de Desempeño Institucional, lo que permite activar alertas tempranas y ajustar las estrategias de mitigación. Este proceso se articula con el Modelo Integrado de Planeación y Gestión - MIPG, asegurando que la información generada sea confiable y relevante para la dirección.

### 8.7.3. Revisión de los Riesgos

La revisión corresponde al análisis integral de los resultados obtenidos en el seguimiento y monitoreo. En la Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7, se plantea como un ejercicio de evaluación crítica y participativa, donde se valoran la efectividad de los controles, la pertinencia de las políticas y la suficiencia de los planes de acción. La revisión permite introducir ajustes, fortalecer la cultura de control y garantizar la transparencia en la gestión institucional. Además, se convierte en un insumo clave para la rendición de cuentas y la mejora continua.

## 8.8. COMUNICACIÓN Y RETROALIMENTACIÓN

El método de comunicación de la gestión integral del riesgo se fundamenta en la transmisión oportuna, clara y veraz de la información hacia todos los niveles del Instituto. Este proceso busca garantizar que los responsables de cada línea de defensa cuenten con datos relevantes sobre la identificación, valoración y tratamiento de los riesgos, promoviendo la transparencia y la articulación con el Modelo Integrado de Planeación y Gestión - MIPG. La comunicación se realiza mediante informes periódicos, reuniones estratégicas y el uso de herramientas tecnológicas que faciliten la trazabilidad y el acceso a la información.

La retroalimentación, por su parte, se concibe como un mecanismo participativo que permite evaluar la efectividad de las acciones implementadas y ajustar las estrategias de manera continua. Este proceso debe ser bidireccional, desde los procesos institucionales hacia la alta dirección y viceversa, generando un ciclo de mejora permanente. A través de la retroalimentación, se fortalecen las alertas tempranas, se consolidan aprendizajes institucionales y se fomenta una cultura organizacional orientada a la prevención, la rendición de cuentas y la sostenibilidad de la gestión del riesgo.

## 9. INDICADORES

Los Indicadores Clave de Riesgo – KRI, por su enfoque preventivo, constituyen una herramienta esencial para anticipar posibles amenazas que puedan afectar el cumplimiento de los objetivos institucionales. Su valor radica en la capacidad de identificar señales tempranas que permitan actuar de manera oportuna, evitando que los riesgos se materialicen y generen impactos negativos en la gestión pública.

Estos indicadores se deben articular con los Indicadores Clave de Proceso - KPI, lo que asegura una visión integral del desempeño institucional. La relación entre ambos permite no solo medir la eficiencia y eficacia de los procesos, sino también vincular dichos resultados con la gestión del riesgo, fortaleciendo la coherencia entre el control interno y la planeación estratégica.

Para lograr este propósito, se requiere que cada uno de los roles identificados en el esquema institucional asuma un trabajo conjunto y coordinado. La acción colectiva orientada a la generación de alertas tempranas fortalece la capacidad de respuesta del Instituto, promueve la cultura de prevención y consolida un sistema de gestión del riesgo más robusto y confiable.

A continuación, se define el esquema de roles y responsabilidades frente a los Indicadores Clave de Proceso – KPI:

| LÍNEA DE ASEGURAMIENTO | RESPONSABLE | RESPONSABILIDAD FRENTE A LOS INDICADORES CLAVE DE PROCESO – KPI |
|---|---|---|
| Línea Estratégica | Alta Dirección<br>Comité Institucional de Coordinación de Control Interno | ▪ Incorporar en la Política para la Gestión Integral de Riesgos lineamientos sobre los Indicadores Clave de Riesgo – KRI.<br>▪ Realizar seguimiento y análisis periódico a los indicadores claves de riesgos institucionales y proponer mejoras a su estructura.<br>▪ Analizar los umbrales definidos para los Indicadores Clave de Riesgo (KRI) y sugerir ajustes de ser necesario, de tal forma que estos se alineen con los niveles aceptables para el Instituto.<br>▪ Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a los indicadores claves de riesgo, así como a los indicadores clave de proceso asociados. |

| | | |
|---|---|---|
| | Comité Institucional de Gestión y Desempeño | ▪ Realizar seguimiento y análisis periódico a los indicadores claves de desempeño de manera articulada con los indicadores clave de riesgo.<br>▪ Generar las alertas que correspondan, de acuerdo con los umbrales definidos para los Indicadores Clave de Riesgo – KRI. |
| 1ª Línea | Líderes de Proceso | ▪ Identificar y formular los indicadores clave de riesgos que puedan alertar sobre la exposición al riesgo para los procesos, programas o proyectos bajo su responsabilidad.<br>▪ Aplicar, medir y hacer seguimiento a los indicadores clave de riesgos, alineados con los indicadores clave de proceso.<br>▪ Reportar en el sistema o esquema definido por el Instituto los avances y evidencias de la gestión de los riesgos de acuerdo con los indicadores claves de riesgo dentro de los plazos establecidos.<br>▪ Informar al proceso de Direccionamiento Estratégico y Planeación sobre las alertas críticas resultado de la medición de los indicadores claves de riesgo bajo su responsabilidad.<br>▪ Si se identifica que un indicador claves de riesgo está fuera del umbral esperado, la primera línea de defensa debe actuar para corregir las desviaciones identificadas.<br>▪ Establecer y aplicar las acciones de mejora requeridas para optimizar la operación de los procesos, planes, programas o proyectos de acuerdo con los resultados de las métricas aplicadas. |

| | | |
|---|---|---|
| 2ª Línea | Direccionamiento Estratégico y Planeación | ▪ Asegurar que los indicadores claves de riesgo estén alineados con los objetivos estratégicos y de gestión del Instituto.<br>▪ Proponer la inclusión de los lineamientos en materia de indicadores claves de riesgo en la estructura de la Política para la Gestión Integral de Riesgos, para aprobación por parte de la Alta Dirección.<br>▪ Establecer las metodologías que guíen la medición, seguimiento y monitoreo de los indicadores claves de riesgo, asegurando que se utilicen las mejores prácticas y se implementen de manera efectiva.<br>▪ Consolidar los indicadores 2claves de riesgo con mayor criticidad frente al logro de los objetivos y presentarlos cuatrimestralmente ante la Línea Estratégica para su análisis y toma de decisiones.<br>▪ Asesorar y supervisar a la 1ª línea para la correcta identificación, formulación e implementación de los indicadores claves de riesgo. |
| 3ª Línea | Control Interno de Gestión | ▪ Verificar si los indicadores claves de riesgo están definidos y se aplican por parte de los responsables.<br>▪ Evaluar si los indicadores claves de riesgo son pertinentes y eficaces para la oportuna generación de alertas y/o implementación de correctivos.<br>▪ Informar a la Alta Dirección en coordinación con la 2ª línea, cuando se detecten deficiencias o brechas en los indicadores claves de riesgo para que tomen decisiones sobre las medidas preventivas y correctivas que deben implementarse.<br>▪ Asesorar y acompañar a la Alta Dirección en el análisis de los resultados de los indicadores claves de riesgo, así como en la incorporación de estrategias para la identificación y monitoreo estratégico de los indicadores claves de riesgo. |

Para formular los Indicadores Clave de Riesgo - KRI, de acuerdo con los lineamientos definidos por parte del proceso de Direccionamiento Estratégico y Planeación, se debe precisar como mínimo lo siguiente:

a. Nombre del Indicador
b. Descripción de lo que se va a medir
c. Fórmula de cálculo
d. Fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas y/o externas u otras fuentes.
e. Frecuencia de medición y seguimiento

f. Umbrales de alerta.

Adicionalmente, durante el diseño de los Indicadores Clave de Riesgo – KRI se deben tener en cuenta los siguientes lineamientos para su construcción:

- **IDENTIFICACIÓN DEL RIESGO CRÍTICO:** Seleccionar los riesgos que, por su probabilidad e impacto, requieren monitoreo constante.
- **DEFINICIÓN DE VARIABLES MEDIBLES:** Establecer factores cuantitativos o cualitativos que reflejen el comportamiento del riesgo (ejemplo: número de incidentes reportados, variaciones presupuestales, rotación de personal).
- **ESTABLECIMIENTO DE UMBRALES Y TOLERANCIAS:** Determinar valores límite que activen alertas tempranas y permitan la toma de decisiones oportunas.
- **ARTICULACIÓN CON LOS KPI:** Asegurar que los KRI se relacionen con los indicadores de desempeño, de modo que exista coherencia entre gestión del riesgo y gestión institucional.
- **ASIGNACIÓN DE RESPONSABLES:** Definir claramente qué línea de defensa (primera, segunda o tercera) monitorea y reporta cada indicador.
- **PERIODICIDAD DE REVISIÓN:** Establecer la frecuencia con la que se mide y analiza el indicador, garantizando información actualizada y confiable.

## 10. SEGUIMIENTO Y EVALUACIÓN

El monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la entidad, el nivel de ejecución de los planes de manejo o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

Es necesario para la gestión del riesgo realizar un continuo monitoreo, seguimiento y control de cada uno de los planes de tratamiento del riesgo donde se determinen cuáles son los controles que permitirán mitigar los riesgos y solucionarlos, por medio de mantenerlos, reducir su nivel, eliminarlos o transferirlos. Así mismo, que variables externas e internas pueden modificar el riesgo, su valoración o controles para su mitigación. A continuación, se establecen las directrices para el monitoreo asociado a primera y segunda línea de defensa, el seguimiento asociado a tercera línea y las acciones a emprender cuando se identifica materialización de riesgos.

### 10.1. MONITOREO

El monitoreo se llevará a cabo desde primera y segunda línea de defensa como se define a continuación:

#### 10.1.1. Primera Línea de Defensa

Una vez identificado, valorado y establecido el tratamiento de los riesgos de gestión, corrupción, fiscales, seguridad de la información y LA / FT, el Líder de Proceso junto con su equipo de trabajo, deben realizar el monitoreo de manera permanente y, registrar de manera cuatrimestral, el avance

de las acciones del plan de implementación frente a la zona residual resultante, la referencia a la continuidad y efectividad de los controles y los resultados de materialización o no de los riesgos.

El Líder de Proceso debe considerar modificaciones sobre el riesgo identificado, cuando en el monitoreo se presentan variables que así lo ameriten, tales como aplicación de nuevos controles, materialización del riesgo, mayor exposición del riesgo u otras situaciones que impacten la probabilidad o impacto. Las modificaciones deben ser comunicadas al proceso de Direccionamiento Estratégico y Planeación para que sean incorporadas en la matriz de riesgos.

### 10.1.2. Segunda Línea de Defensa

El proceso de Direccionamiento Estratégico y de Planeación debe realizar el informe consolidado del monitoreo cuatrimestral de los riesgos de gestión, corrupción, fiscales y LA / FT previo reporte de los Líderes de Proceso.

El proceso de Direccionamiento Estratégico y de Planeación debe revisar el avance de acciones del plan de implementación o tratamiento de riesgos, materializaciones y debe analizar las deficiencias del modelo para realizar recomendaciones sobre la mejora y ajuste correspondiente.

El informe debe ser socializado a los Líderes de Proceso, representante legal y, debe publicarse en la página web institucional www.iser.edu.co.

## 10.2. SEGUIMIENTO

El seguimiento se adelanta desde la Tercera Línea de Defensa, es decir, el proceso de Control Interno de Gestión debe adelantar el seguimiento de los riesgos que administra el Instituto Superior de Educación Rural - ISER en los siguientes términos:

- El seguimiento del mapa de riesgos institucional se debe realizar semestralmente, del cual se deben generar los informes de resultados correspondientes. Adicionalmente, proceso de Control Interno de Gestión puede incluir en sus auditorías internas la revisión de riesgos institucionales dado su enfoque basado en el riesgo.

- Como resultado del seguimiento semestral adelantado, el proceso de Control Interno de Gestión que debe publicar el informe correspondiente en la página web institucional, en su enlace de *Transparencia*, en los diez (10) primeros días hábiles siguientes al corte del semestre.

## 10.3. EVALUACIÓN

El Comité Institucional de Coordinación de Control Interno, semestralmente debe:

- Revisar los informes presentados, en el cual se analicen los eventos de riesgos que se han materializado, así como las causas que dieron origen a esos eventos.

- Adoptar las decisiones pertinentes frente a los resultados de la gestión del riesgo, monitoreo y seguimiento del mapa de riesgos institucional.

- Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando.

Los resultados de la evaluación adelantados por el Comité Institucional de Coordinación de Control Interno deben quedar consignados en un informe semestral emitido por parte la Secretaría Técnica.

## 11. PRESUPUESTO

De acuerdo con lo dispuesto en el Estatuto Presupuestal, el Instituto Superior de Educación Rural – ISER asignará los recursos financieros necesarios para la ejecución de esta política y los planes y programas que de ella se deriven, los cuales estarán incluidos en el presupuesto anual, conforme a la disponibilidad de recursos y a las prioridades establecidas por la institución. Estos recursos se destinarán al diseño, implementación, mantenimiento y mejora continua de la Política de Gestión Integral del Riesgo, así como a la ejecución de los planes y programas derivados de estos, con el fin de identificar, analizar y controlar los riesgos institucionales que podrían afectar el logro de los objetivos estratégicos.

## 12. RESPONSABLE

Mónica Enith Salanueva Abril

**MÓNICA ENITH SALANUEVA ABRIL**

Profesional Especializado adscrito al proceso de
Direccionamiento Estratégico y Planeación