|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Elaboró** | | **Revisó** | | **Aprobó** | |
| **Nombre:** | Edward Izquierdo | **Nombre:** | Jaime Cárdenas | **Nombre:** | Yina Cubillos |
| **Cargo:** | Asesor de Procesos | **Cargo:** | Administrador De Riesgos | **Cargo:** | Gerente |
| **Fecha:** | 1/06/2022 | **Fecha:** | 01/06/2022 | **Fecha:** | 01/06/2022 |

1. **OBJETIVO**

Documentar las actividades requeridas para la ejecución de la gestión de riesgo operativo que involucra las etapas de identificación, medición, control y monitoreo de riesgos hasta la definición de los elementos que hacen parte del Sistema de Administración de Riesgo Operativo de acuerdo con los lineamientos normativos establecidos por la Superintendencia de Economía Solidaria- SES.

1. **ALCANCE**

El procedimiento inicia con la identificación de un riesgo operativo y finaliza con las actividades de monitoreo semestral.

1. **NORMATIVIDAD.**
   1. **INTERNA.**
      1. Estatuto – Reglamentos
      2. Manuales del Sistema Integral de Administración de Riesgos
      3. Procedimientos vinculados a los procesos de la Cooperativa
   2. **EXTERNA.**
      1. Circular Básica Contable y Financiera
      2. Circular Básica Jurídica
2. **DEFINICIONES.**
   1. **Amenaza**: Causa potencial de un incidente no deseado, que puede causar daños a un sistema u organización.
   2. **Apetito de riesgo**: Es el nivel de exposición al riesgo que una organización solidaria está dispuesta a asumir en el desarrollo de sus actividades, con el propósito de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios.
   3. **Área de impacto**: Es todo recurso, bien u oportunidad, al cual la organización le ha (o debe) asignar un valor y su afectación o generación (en mayor o menor valor) podría comprometerse el cumplimiento de sus objetivos y metas.
   4. **Cadena de valor de una organización solidaria**: La cadena de valor es un concepto que hace referencia al conjunto de procesos encadenados que estratégicamente son fundamentales para entender y gestionar las ventajas competitivas de una organización solidaria. Se dividen en tres conjuntos de procesos: estratégicos, misionales, y de apoyo y control.
   5. **Procesos estratégicos**: Son los que permiten definir y desplegar las estrategias y objetivos de la organización. Es decir, aquellos procesos que definen el direccionamiento del “negocio” de la organización; como, por ejemplo: marketing estratégico y estudios de mercado, planificación y seguimiento de objetivos, revisión del sistema, evaluación de la satisfacción de los asociados, etc.
   6. **Procesos misionales:** Son aquellos procesos que añaden valor al asociado o inciden directamente en su satisfacción o insatisfacción. Son procesos claves que intervienen en la misión de la organización y en el cumplimiento del objeto social.
   7. **Procesos de apoyo y control:** Los procesos de apoyo son los que suministran los recursos necesarios para el buen desempeño de las operaciones del negocio, como son: financieros, humanos, tecnológicos, jurídicos, físicos e intangibles, entre otros y en los procesos de control se tiene la gestión de riesgos, control interno, etc**.**
   8. **Clasificación de los riesgos operativos**: Para los efectos del presente capítulo los riesgos operativos se clasifican de la siguiente manera:
   9. **Fraude Interno**: Hace referencia a actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la organización, o incumplir normas o leyes, en los que está implicado, al menos, un empleado, tercero contratado o administrador de la organización.
   10. **Fraude Externo**: Corresponde a actos realizados por un externo a la organización, que busca defraudar, apropiarse indebidamente de activos de la misma o incumplir normas o leyes.
   11. **Relaciones laborales incompatibles**: Hace referencia a actos que son incompatibles con la legislación laboral y con los acuerdos internos de trabajo.
   12. **Asociados o clientes**: Se relaciona con fallas negligentes o involuntarias de las obligaciones de la organización frente a los asociados o clientes, que impiden cumplir una obligación contraída con estos, o fallas de la naturaleza o diseño de un producto o servicio.
   13. **Daños a activos físicos**: Hace referencia a pérdidas derivadas de daños o perjuicios a activos físicos de la organización.
   14. **Fallas tecnológicas:** Se relaciona con pérdidas derivadas de incidentes por fallas tecnológicas.
   15. **Ejecución y administración de procesos**: Tiene que ver con las pérdidas derivadas de errores en la ejecución y administración de los procesos.
   16. **Confidencialidad**: La propiedad de que la información sólo sea conocida por aquellas personas que tienen derecho legítimo a conocerla.
   17. **Consecuencia**: resultado de un evento que afecta a los objetivos.
   18. **Control**: Son los dispositivos, mecanismos, practicas u 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. Medida o acción que modifica un riesgo para prevenir su materialización.
   19. **Disponibilidad**: La propiedad de que la información se encuentre disponible en los puntos de uso cuando ésta sea requerida por una persona autorizada, al igual que los recursos necesarios para su uso.
   20. **Dueño del proceso:** Responsable de la administración de un proceso; es decir, de su planeación, organización, dirección y control.
   21. **Entidad Externa o Tercero**: Cualquier persona o empresa ajena a la entidad (cliente, proveedor, usuario, contratista, etc.) que por razón de sus actividades deba acceder a información contenida o bajo custodia de la entidad.
   22. **Evento del riesgo operativo**: Los eventos de riesgo operativo son situaciones que generan impactos no deseados en las organizaciones solidarias asociados al riesgo operativo. Ocurrencia o cambio de un conjunto particular de circunstancias. Un evento puede tener una o más ocurrencias y puede tener varias causas y varias consecuencias. Un evento también puede ser algo previsto que no llega a ocurrir, o algo no previsto que ocurre. Un evento puede ser una fuente de riesgo.
   23. **Eventos de pérdida**: Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades.
   24. **Factores de riesgo operativo**: Se entiende por factores de riesgo las principales situaciones generadoras de riesgos operativos que pueden o no generar pérdidas. Son factores de riesgo: el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Dichos factores se deben clasificar en internos o externos, según se indica a continuación:
   25. **Factores internos**: Se entiende por factores de riesgos internos, aquellas situaciones generadoras de eventos de riesgo operativo al interior de la organización solidaria relacionados con: el recurso humano, los procesos, la tecnología y la infraestructura física.
   26. **Recurso humano**: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la organización. a. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente. b. La vinculación indirecta hace referencia a aquellas personas que tienen con la organización una relación jurídica de prestación de servicios, diferente a aquella que se origina en un contrato de trabajo.
   27. **Procesos**: Es el conjunto de acciones o actividades sistemáticas y repetitivas por las que unas entradas (inputs) se convierten en un producto o servicio final (outputs).
   28. **Tecnología**: Es el conjunto de herramientas empleadas para soportar los procesos de la organización solidaria, que incluye: hardware, software y telecomunicaciones.
   29. **Infraestructura física**: Es el conjunto de elementos de apoyo para el funcionamiento de una organización que incluye entre otros los siguientes: edificios, espacios de trabajo, almacenamiento y transporte.
   30. **Factores externos**: Son situaciones asociadas a la fuerza de la naturaleza, u ocasionadas por proveedores o terceros, que escapan en cuanto a su causa y origen al control de la organización.
   31. **Fuente de riesgos**: elemento que, por sí solo o en combinación con otros, tiene el potencial de generar riesgo. Es todo individuo, grupo humano, entidad, elemento físico, o fenómeno del entorno, de los cuales se pueden derivar eventos que podrían afectar las unidades de impacto (objetos en riesgo).
   32. **Impacto**: Esta variable hace referencia a los efectos adversos sobre la organización, es decir, lo que ésta podría perder y/o lo que podría salir mal.
   33. **Incidente**: Cualquier situación que tenga características observables y que afecte negativamente la confidencialidad, integridad o disponibilidad de un activo de información.
   34. **Información Privada**: Aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, solo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.
   35. **Infraestructura**: Es el conjunto de elementos de apoyo para el funcionamiento de una organización que incluye entre otros los siguientes: edificios, espacios de trabajo, almacenamiento y transporte.
   36. **Integridad**: La propiedad de que la información sea integra, confiable y no haya sido alterada en ninguna circunstancia, siempre se debe prevenir modificaciones no autorizadas de la información.
   37. **Medio**: Cualquier elemento o dispositivo que contenga información.
   38. **Nivel de riesgo**: Evaluación del riesgo identificando su posible materialización frente al impacto y probabilidad de ocurrencia.
   39. **Parte interesada**: persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
   40. **Pérdidas**: Es la cuantificación económica de la ocurrencia de un evento de riesgo operativo, así como los gastos derivados de su atención.
   41. **Perfil de Riesgo**: Resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la entidad.
   42. **Plan de continuidad del negocio**: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.
   43. **Plan de contingencia**: Es el conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.
   44. **Probabilidad**: Posibilidad del riesgo que se pueda materializar frente a un incidente de seguridad de la información.
   45. **Recurso Humano**: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente. La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.
   46. **Relaciones laborales**: Actos que son incompatibles con la legislación laboral y con los acuerdos internos de trabajo.
   47. **Riesgo legal**: Es la posibilidad de pérdida en que incurre una organización solidaria al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones, obligaciones contractuales, fallas en los contratos y transacciones. El riesgo legal surge también como consecuencia de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.
   48. **Riesgo inherente**: es aquel que puede existir de manera intrínseca en toda actividad. Puede generarse por factores internos o externos y afectar la rentabilidad y el capital de las empresas.
   49. **Riesgo operativo**: En el contexto del SARO, se entenderá por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas, ausencias o inadecuaciones en: a. los procesos, b. el recurso humano, c. la tecnología, d. la infraestructura física; o e. por la ocurrencia de acontecimientos externos. El Riesgo Operativo está asociado al riesgo legal y al riesgo reputacional.
   50. **Riesgo reputacional**: Es la posibilidad de pérdida en que incurre una organización por desprestigio, mala imagen, publicidad negativa, cierta o no relacionadas con sus prácticas de negocios, que puede causar el retiro de sus asociados, disminución de ingresos o el inicio de procesos judiciales.
   51. **Riesgo residual**: Nivel resultante del riesgo después de aplicar los controles al riesgo inherente.
   52. **Sistema de Administración del Riesgo Operativo – SARO**: Corresponde al conjunto de etapas y elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales las organizaciones solidarias vigiladas identifican, miden, controlan y monitorean el riesgo operativo.
   53. **Seguridad de la Información**: Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.
   54. **Tecnología**: Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.
   55. **Tratamiento**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como a recolección, almacenamiento, uso, circulación o supresión.
   56. **Vulnerabilidad:** Situación anómala que crea una debilidad, generalmente causada por el hombre y que puede ser explotada por una amenaza para poner en riesgo un activo de información. Debilidad de un activo o control que puede ser explotado por una o más amenazas.
3. **RESPONSABLES**
   1. Líderes de Procesos
   2. Administrador de Riesgos
   3. Subgerente Administrativo
   4. Subgerente Financiero
   5. Gerente
   6. En general todos los funcionarios
4. **POLÍTICA DE OPERACIÓN**
   1. **REQUISITOS GENERALES**
      1. Dar cumplimiento a la normatividad vigente en la Cooperativa a través del estatuto, reglamentos, entre otros.
      2. Todos los funcionarios de COOPEAIPE deben garantizar y participar activamente en la gestión de riesgo operativo como parte de sus funciones independiente del área en el cual se desarrollan.
      3. Consultar los documentos de apoyo teniendo en cuenta que el Sistema de Administración de Riesgo Operativo incorpora políticas, procedimientos, metodologías y demás herramientas que garantizan la ejecución de actividades de gestión del riesgo operativo, y hace parte del Sistema Integral de Administración de Riesgos de COOPEAIPE.
      4. El Consejo de Administración de COOPEAIPE con el apoyo del Comité de SIAR, la Gerencia, el Administrador de Riesgos, entre otros deben establecer y realizar la evaluación periódica de la gestión del riesgo operativo de la Cooperativa.
      5. El Consejo de Administración debe aprobar la estrategia de gestión del riesgo operativo, las políticas, procedimientos y demás requisitos para la identificación, medición, control y monitoreo del riesgo operativo, asignando las responsabilidades a cada uno de los funcionarios vinculados.
      6. Todos los funcionarios que ingresen a COOPEAIPE deben recibir una inducción sobre el Sistema de Administración de Riesgo Operativo, al igual que terceros vinculados tales como proveedores, a la vez se debe reforzar el conocimiento con una capacitación anual para todos los funcionarios con el apoyo de Talento Humano.
      7. Los líderes de los procesos de COOPEAIPE y el Administrador de Riesgos deben ser y son los responsables de coordinar las actividades de gestión de riesgos con sus equipos de trabajo.
      8. El manejo del riesgo operativo es responsabilidad de todo el personal de la Cooperativa, independientemente de su nivel y funciones asignadas.
      9. Las políticas, procedimientos y demás documentación relacionada con riesgo operativo se deben revisar y actualizar, cada vez que se identifique la necesidad y se debe aprobar por parte El Consejo de Administración.
      10. La aplicación de la metodología de identificación, medición, control y monitoreo del riesgo operativo es un proceso continuo en el cual el Administrador de Riesgos debe liderar su permanente revisión y como mínimo semestralmente realizar el monitoreo y actualización según corresponda.
      11. Por lo menos, una vez al año y como parte de las actividades de auditoría interna se debe realizar una revisión del Sistema de Administración de Riesgo Operativo – SARO, haciendo las correspondientes recomendaciones para el mejoramiento continuo del sistema.
      12. El Administrador de Riesgos es el encargado de apoyar a los líderes de procesos y sus equipos de trabajo en la realización y aplicación de la calificación del riesgo inherente y residual, de acuerdo con las variables incorporadas en la metodología y se realizarán los ajustes a través de un consenso de las partes, de acuerdo con la herramienta o formato que COOPEAIPE está aplicando en la actualidad.
      13. Para los riesgos identificados se debe medir la probabilidad de ocurrencia y la magnitud del impacto, de acuerdo con las escalas y definiciones estipuladas en la metodología de identificación, medición, control y monitoreo de riesgo operativo que la Cooperativa ha desarrollado con base en los lineamientos de la SES.
      14. El Administrador de Riesgos debe verificar permanentemente los cálculos aplicados en la matriz de riesgo operativo consolidada y efectuar los ajustes que corresponda de acuerdo con la actualización que pueda darse durante el ciclo de aplicación de la metodología de identificación, medición, control y monitoreo de riesgo operativo aprobada en COOPEAIPE, se debe dejar registro de los cambios o actualizaciones aplicados.
      15. El Administrador de Riesgos con el apoyo de la Gerencia deberá gestionar con los líderes de procesos los planes de acción o tratamiento para mitigar la materialización de los riesgos o su impacto, teniendo en cuenta los niveles de riesgo aceptados y aprobados por parte de El Consejo de Administración.
      16. Los planes de acción o tratamiento deben ser documentados incluyendo las actividades a desarrollar, los responsables, recursos requeridos y el tiempo de ejecución establecido.
      17. Como complemento de la metodología aplicada para la gestión de riesgo operativo, el Administrador de Riesgos cuenta con una serie de indicadores que permiten evaluar la eficiencia y eficacia de la gestión de riesgo operativo, entre otros indicadores se tiene:

* # de riesgos identificados durante un período de tiempo (últimos 6 meses) comparados con el período anterior,
* # de planes de acción finalizados / # de planes de acción establecidos o propuestos
* # de no conformidades corregidas sobre SARO / # de no conformidades reportadas en auditoría
* Riesgos más frecuentes
* # de riesgos por procesos
* # de controles implementados
* % de disminución de impacto y/o probabilidad de riesgos durante un período de tiempo
* $ afectación estado de resultados por riesgos materializados
  + 1. Estos indicadores se deben evaluar mensualmente y semestralmente incluir en el informe de resultados del SARO que incluye:
* Matriz de Riesgo Operativo que incluye mapa de riesgos inherente y residual
* Planes de Acción ejecutados y resultados alcanzados
* Registro de eventos de riesgo operativo
* Solicitudes de cambio o actualización manual de políticas de riesgo operativo
* Nuevos riesgos identificados y control implementados
* Entre otros
  + 1. El Consejo de Administración y la Gerencia deben revisar los resultados de la gestión de riesgos presentados por parte del Comité de SIAR y el Administrador de Riesgos de COOPEAIPE como mínimo cada 6 meses y se pronunciará respecto del perfil global de riesgo operativo de la Cooperativa, las observaciones frente a la gestión y las medidas a tomar para dar continuidad a las actividades vinculadas con la gestión de riesgo operativo.
    2. Permanentemente la Cooperativa debe verificar los requerimientos normativos establecidos por la Superintendencia de Economía Solidaria en relación con el SARO, incorporando los ajustes que haya lugar y socializando con todos los funcionarios los cambios que se incluya, adicionalmente se debe tener en cuenta que la metodología aplicada para la gestión de riesgo operativo es continua, por lo tanto, es una actividad de frecuencia permanente y el Administrador de Riesgos se encargará de mantener vigentes las actividades que correspondan.
    3. El Administrador de Riesgosy los líderes de procesos deberán documentar el plan de tratamiento estableciendo responsables, tiempos de ejecución, recursos que se necesitan y actividades a desarrollar para corregir o mejorar los resultados de la evaluacióndel perfil de riesgo operativo de la Cooperativa, acordando con la auditoría interna el tiempo de presentación de resultados y correcciones en caso de existir.
    4. El Administrador de Riesgospresentará el informe con los resultados alcanzados posteriores a la evaluación del perfil de riesgo, incorporando las mejoras, actualizaciones requeridas en la documentación, lecciones aprendidas del ejercicio realizado, entre otros elementos que permiten una gestión proactiva de riesgos, el compromiso de parte de los líderes de procesos para el mejoramiento continuo, identificando nuevos riesgos, nuevos controles y en general, aportando en la mitigación de riesgos.
    5. Semestralmente el Administrador de Riesgospresentará al Comité de SIAR y la Gerencia el resultado de los planes de tratamiento de acuerdo con el informe de auditoría interna.
    6. El perfil global de riesgo operativo también puede verse impactado directa o indirectamente como resultado del análisis de los siguientes insumos:
* Actualización de procesos y procedimientos de la Cooperativa.
* Incorporación de nuevos productos y servicios.
* Registro de eventos de riesgo operativo (Ver procedimiento).
* Informes de entes de control: Revisoría Fiscal, Superintendencia de Economía Solidaria, Fogacoop, entre otros.
* Conocimiento de eventos de riesgo operativos presentados en otras entidades solidarias o con actividad similar a la desarrollada por la Cooperativa.
* Registro de incidentes de seguridad de información.
* Registro de peticiones, quejas, reclamos, sugerencias y felicitaciones por parte de los asociados.
* Otra información generada por los diferentes procesos, por ejemplo, informes de comités de SIAR, Consejo de Administración, entre otros.
  + 1. Con estos insumos también se debe aplicar las correspondientes acciones correctivas que aporten en la evaluación y evolución del perfil de riesgo operativo de COOPEAIPE, actividad que estará liderada por el Líder en Gestión de Riesgos y el apoyo de los líderes de procesos.
    2. La evolución del perfil de riesgo operativo siempre estará vinculada con la aplicación de la metodología de identificación, medición, control y monitoreo del riesgo operativo desarrollado por la Cooperativa, por lo tanto, cada una de las actividades aquí mencionadas se incorporará en el momento que corresponda a la metodología.
    3. Como mínimo cada 6 meses se debe actualizar los resultados de la evaluación del perfil de riesgo revisando los hallazgos encontrados, situaciones de riesgo, causas, riesgos asociados, factores de riesgo, medición del riesgo inherentes de la probabilidad de ocurrencia y la magnitud del impacto, los controles actuales, la clasificación de los controles actuales, medición del riesgo residual y los indicadores del SARO, generando así un proceso de mejora continua.
  1. **MEDIDAS POR INCUMPLIMIENTO EN LA GESTIÓN DEL RIESGO OPERATIVO**
     1. Los líderes de proceso, Subgerente Financiero y el Subgerente Administrativo deben informar al Administrador de Riesgos y la Gerencia el incumplimiento por parte de los funcionarios en el desarrollo de las actividades definidas en políticas, procedimientos, metodología de identificación, medición, control y monitoreo de riesgo operativo.
     2. De acuerdo con el reglamento interno de trabajo, el código de ética y conducta, código de buen gobierno se adelantarán las acciones que corresponda ante el incumplimiento en la aplicación de la gestión de riesgo operativo que COOPEAIPE ha definido.

1. **DESCRIPCIÓN DE ACTIVIDADES**
   1. **GESTIÓN DEL RIESGO OPERATIVO**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **ACTIVIDAD** | **RESPONSABLE** | **REGISTRO** |
| 1 | El Administrador de Riesgos con los líderes de procesos y la Gerencia realizan actividades de socialización e identificación de riesgos operativos de acuerdo con cada uno de los procesos como mínimo una vez cada 6 meses y en la medida que sea requerido el acompañamiento por parte del Subgerente Administrativo, esta actividad se encuentra alineada con la actualización y documentación de procedimientos, apoyándose con el área de gestión de calidad. | Administrador De Riesgos  Líderes De Procesos  Gerencia | N/A |
| 2 | El grupo de trabajo conformado identifica las causas que originan los riesgos a partir de la experiencia y criterio de los funcionarios, como también de los eventos materializados a través del tiempo | Administrador De Riesgos  Líderes De Procesos  Gerencia | N/A |
| 3 | El grupo de trabajo identifica los factores de riesgo asociados de acuerdo con los lineamientos de la metodología de identificación, medición, control y monitoreo de riesgo operativo. | Administrador De Riesgos  Líderes De Procesos  Gerencia | N/A |
| 4 | El grupo de trabajo analiza las consecuencias o el impacto de los riesgos identificados considerando los impactos derivados a nivel financiero, legal, reputacional, del proceso, entre otros aspectos que podrían afectar a la Cooperativa | Administrador De Riesgos  Líderes De Procesos  Gerencia | N/A |
| 5 | El grupo de trabajo identifica controles para cada una de las causas y que puedan prevenir o mitigar la materialización de un riesgo, teniendo en cuenta la metodología de identificación, medición, control y monitoreo de riesgo operativo que la Cooperativa ha desarrollado | Administrador De Riesgos  Líderes De Procesos  Gerencia | N/A |
| 6 | Registrar los resultados en la matriz de riesgo operativo consolidada y por procesos que la Cooperativa ha definido, asimismo, dejar registro de las reuniones realizadas por parte del Administrador de Riesgos con los Líderes de Procesos e informando permanentemente a la Gerencia en caso de presentarse cambios o requerir de igual forma el apoyo frente a la identificación de los riesgos. | Administrador De Riesgos  Líderes De Procesos  Gerencia | Registro en la matriz de riesgo |
| 7 | El Administrador de Riesgos presenta **mensualmente** al Comité de SIAR los resultados relacionados con la gestión de riesgo operativo incluyendo la consolidación de la información respecto a los eventos de riesgo operativo para su validación, observaciones y ajustes que corresponda antes de presentar a El Consejo de Administración | Administrador De Riesgos | Informe de resultados |

* 1. **EVALUACIÓN DEL PERFIL DE RIESGO OPERATIVO**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **ACTIVIDAD** | **RESPONSABLE** | **REGISTRO** |
| 1 | El Administrador de Riesgos, realizará cada 6 meses la verificación del cumplimiento en la aplicación de las etapas e incorporación de elementos del Sistema de Administración de Riesgo Operativo, evaluando el resultado de acuerdo con las metodologías vinculadas al SARO, el programa de capacitación para funcionarios y terceros, los informes mensuales del Comité de SIAR con el resultado de indicadores, el registro de eventos de riesgo, entre otros insumos que permiten conocer el grado de apropiación del SARO en COOPEAIPE. | Administrador de Riesgos | Informe de Auditoria |
| 2 | El Administrador de Riesgos, emitirá un informe con el detalle de los aspectos evaluados y el resultado obtenido, dando a conocer las fortalezas y debilidades del Sistema de Administración de Riesgo Operativo y el perfil de riesgo de la Cooperativa, a partir de la evaluación en el cumplimiento de la aplicación de etapas y elementos, y su ejecución a través del tiempo en COOPEAIPE. | Administrador de Riesgos | Informe de Auditoria |
| 3 | Como resultado del informe de auditoría debe establecer planes de tratamiento generales y particulares de acuerdo con cada uno de los procesos y el análisis de la matriz de riesgos consolidada con los hallazgos encontrados | Administrador de Riesgos  Consejo de Administración | planes de tratamiento generales y particulares |

1. **REGISTROS REFERENCIADOS.**
   1. Matriz de Riesgo Operativo COOPEAIPE
2. **ACTUALIZACIÓN**

|  |  |  |
| --- | --- | --- |
| **FECHA** | **DESCRIPCIÓN** | **VERSIÓN** |
| 01/06/2022 | Elaboración inicial del documento | 1 |