



ESE UNIVERSITARIA DEL ATLANTICO
MANUAL DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO
OPERATIVO (SARO)

CODIGO: ML-GR-009

VIGENCIA: Octubre 2024

VERSION: 02

Página 1 de 26

MANUAL DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERATIVO (SARO)

ESE UNIVERSITARIA DEL ATLANTICO

TABLA DE CONTENIDO

| | | |
|----------|---|----|
| 1. | INTRODUCCION | 4 |
| 2. | ALCANCE | 4 |
| 3. | OBJETIVO..... | 4 |
| 4. | MARCO NORMATIVO | 4 |
| 5. | DEFINICIONES..... | 5 |
| 6. | POLITICA DE RIESGO OPERACIONAL (SARO)..... | 6 |
| 7. | ETAPAS DE GESTION DE RIESGOS OPERACIONALES | 9 |
| 7.1. | IDENTIFICACIÓN DEL RIESGO | 9 |
| 7.1.1. | Registro de riesgos identificados en matriz de Riesgo institucional | 11 |
| 7.1.1.1. | Descripción de riesgo operacional identificado | 11 |
| 7.1.1.2. | Definir causas y consecuencias | 11 |
| 7.1.1.3. | Definir tipo de impacto del riesgo operacional..... | 12 |
| 7.2. | EVALUACIÓN Y MEDICIÓN DEL RIESGO | 12 |
| 7.2.1. | Semaforización de riesgos Operacionales..... | 12 |
| 7.2.2. | Determinación de nivel de probabilidad del riesgo..... | 13 |
| 7.2.3. | Determinación de nivel de impacto del riesgo..... | 14 |
| 7.3. | CONTROL DEL RIESGO (estrategias para tratamiento y control)..... | 17 |
| 7.3.1. | Tipos de control..... | 17 |
| 7.3.2. | Naturaleza del control | 18 |
| 7.3.3. | Opciones de manejo de tratamiento del riesgo..... | 18 |
| 7.3.4. | Aceptación de riesgos..... | 18 |
| 7.3.5. | Control de riesgo operacional, Plan de continuidad del negocio | 19 |
| 7.3.6. | Control de riesgo operacional, Acreditación de soportes de operaciones, negocios y contratos.. | 19 |
| 7.4. | SEGUIMIENTO Y MONITOREO | 19 |
| 7.4.1. | Las prioridades de monitoreo y revisión pueden comprender:..... | 20 |
| 7.4.2. | Las prácticas de monitoreo y revisión pueden ser de los siguientes tipos:..... | 20 |
| 7.4.3. | Seguimiento a los planes de acción..... | 21 |
| 7.4.4. | Herramientas para seguimiento a controles riesgos operacionales..... | 21 |
| 7.5. | EVALUACIÓN DE CONTROLES | 21 |
| 7.6. | PERFIL DE RIESGO RESIDUAL | 23 |
| 8. | RESPONSABILIDADES DE LIDERES DE PROCESOS INVOLUCRADOS EN LA GESTIÓN DEL RIESGO OPERACIONAL..... | 24 |



ESE UNIVERSITARIA DEL ATLÁNTICO
MANUAL DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO
OPERATIVO (SARO)

| |
|------------------------|
| CODIGO: ML-GR-009 |
| VIGENCIA: Octubre 2024 |
| VERSION: 02 |
| Página 3 de 26 |

| | |
|-------------------------------------|----|
| 9. FICHA DE CONTROL DE CAMBIOS..... | 25 |
| 10. APROBACIÓN DEL DOCUMENTO | 26 |

1. INTRODUCCION

El Riesgo Operacional corresponde a la probabilidad que una entidad presente desviaciones en los objetivos misionales, como consecuencia de deficiencias, inadecuaciones o fallas en los procesos, en el recurso humano, en los sistemas tecnológicos, legal y biomédicos, en la infraestructura, por fraude, corrupción y opacidad, ya sea por causa interna o por la ocurrencia de acontecimientos externos, entre otros.

Es así como los Riesgos Operacionales en la entidad pueden generar pérdidas de tres tipos:

- i) Pérdidas en los resultados en salud de los pacientes, los cuales, por su relevancia son tratados como riesgos en salud.
- ii) Pérdidas en los resultados operativos esperados, incluyendo la satisfacción de la población en su área de influencia, que deben ser tratados en el resultado de la gestión de los riesgos operacionales.
- iii) Pérdidas financieras en la entidad, que corresponden a la contabilización de los eventos de riesgo y los riesgos que se materializaron, tratados en la evaluación de los riesgos financieros.

Es por ello, que la ESE UNIVERSITARIA DEL ATLANTICO adopta diferentes políticas y procedimientos encaminados a la implementación de acciones que promuevan el fortalecimiento continuo de una cultura ética, transparente y que se encuentra en constante lucha contra la corrupción, opacidad y fraudes.

La implementación y seguimiento a estos riesgos van estrechamente ligados a las políticas, principios y valores institucionales establecidos en Código de Conducta y de Buen Gobierno, de ahí la importancia de su implementación y mejoramiento continuo. Una adecuada gestión de riesgos y prácticas son indispensables para mitigar el nivel de riesgo inherente al que está expuesta la ESE UNIVERSITARIA DEL ATLANTICO.

2. ALCANCE

El siguiente manual va dirigido a los líderes de los procesos directamente relacionados con la gestión de los riesgos operacionales potenciales, los líderes de dichos procesos y los funcionarios bajo su cargo encargados de proporcionar la información necesaria para cumplir con todas las etapas de gestión de riesgo operacional.

3. OBJETIVO

Impartir al personal ESE Universitaria del Atlántico las instrucciones generales relativas al Subsistema de administración de riesgos operacionales. Esto con el fin de facilitar la identificación, evaluación, medición, control y monitoreo eficaz de los riesgos operacionales a los que está expuesta la institución.

4. MARCO NORMATIVO

- El artículo 4° de la Ley 1751 de 2015: por medio de la cual se reguló el derecho fundamental a la salud y se dictaron otras disposiciones, definió al Sistema de Salud como "...el conjunto articulado y armónico de principios y normas; políticas públicas; instituciones; competencias y procedimientos;

facultades, obligaciones, derechos y deberes; financiamiento, controles; información y evaluación, que el estado disponga para la garantía y materialización del derecho fundamental de la salud.”

- **Decreto 1011 de 2006 y 780 de 2016:** implementación del Sistema de Gestión de los Riesgos en Salud de las Instituciones Prestadoras de Servicios de Salud que deben acogerse a lo definido por el marco normativo de los componentes del Sistema Obligatorio de la Garantía de la Calidad en Salud (SOGCS)
- **Resolución 2626 de 2019:** adopción de la Política de Atención Integral en Salud (PAIS) con énfasis en resultados en salud y disminución de la carga de enfermedad.
- **Ley 1122 de 2007:** Sistema de Inspección, Vigilancia y Control (IVC) del sector salud.
- **Artículo 12 de la Ley 1474 de 2011 o Estatuto Anticorrupción:** crea el Sistema Preventivo de Prácticas Riesgosas Financieras y de Atención en Salud del SGSSS y ordena a la SNS, el cual define que, para sus sujetos vigilados, un conjunto de medidas preventivas para control, así como la implementación de indicadores de alerta temprana y ejercer sus funciones de IVC sobre la materia.
- **Resolución 518 de 2015:** se dictaron disposiciones en relación con la Gestión de la Salud Pública (...) y en cumplimiento del parágrafo del artículo 5 de dicha Resolución, el Ministerio de Salud y Protección Social (MSPS) generó las Directrices para la caracterización y ejecución de los procesos para la Gestión de la Salud Pública en el contexto de la Política de Atención Integral en Salud (PAIS).
- **NTC-ISO 31000:** principios y directrices genéricos para la gestión del riesgo en una organización sin importar su naturaleza, industria y sector.
- **Resolución 4559 de 2018:** “Por la cual se adopta el modelo de Inspección, Vigilancia y Control para la Superintendencia Nacional de Salud para el ejercicio de la supervisión de los riesgos inherentes al Sistema General de Seguridad Social en Salud”
- **CIRCULAR EXTERNA 20211700000004-5 DE 2021:** por la cual se imparten instrucciones generales relativas al código de conducta y de buen gobierno organizacional, el sistema integrado de gestión de riesgos y a sus subsistemas de administración de riesgos
- **Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6, 2022**

5. DEFINICIONES

- **Adquisición:** Acuerdo en el que una empresa compra otra para ampliar sus operaciones o diversificar su negocio. Puede implicar la compra de todos o parte de los activos y pasivos de la empresa objetivo.
- **Cadena de valor:** Modelo de negocios que describe las actividades que realiza una empresa para crear y entregar un producto o servicio. Este modelo permite identificar los costes, la ventaja competitiva y las fuentes de una empresa. El objetivo de la cadena de valor es mejorar la eficiencia de la producción y entregar el máximo valor al cliente.
- **Cesión de activos / pasivos:** La cesión de activos es un proceso legal en el que una empresa vende una parte o la totalidad de sus activos a otra empresa. La cesión de pasivos es una operación que consiste en transferir las deudas de una empresa a otra. Este proceso puede ser una fusión impropia o una reestructuración societaria
- **Ciclo de gestión de riesgo:** Son las etapas que incorpora un Subsistema de Administración de Riesgos para cada uno de los tipos o categorías de riesgo identificadas.
- **Controles:** Medidas prudenciales, preventivas y correctivas que ayudan a contrarrestar la exposición a los diferentes riesgos. Entre estas se encuentra la implementación de políticas, procesos, prácticas u otras estrategias de gestión.

- **Evento de pérdida:** Son las situaciones que generan pérdidas a las entidades al exponerse a cualquier riesgo.
- **Fallas de proceso:** Evento no previsible, inherente a los sistemas productivos que impide que estos cumplan su función bajo las condiciones establecidas o que no la cumplan.
- **Fusión:** Proceso en el que dos o más empresas se unen para formar una nueva entidad.
- **Gestión de Riesgo:** Es un enfoque estructurado y estratégico liderado por la Alta Gerencia que busca implementar un conjunto de acciones y actividades coordinadas para disminuir la probabilidad de ocurrencia o mitigar el impacto de un evento de riesgo potencial (incertidumbre) que pueda afectar los resultados y, por ende, el logro de los objetivos de cada entidad, así como el cumplimiento de sus objetivos y obligaciones. Dentro de este conjunto de acciones se incluye, entre otros, el *ciclo general de gestión de riesgo*.
- **Nivel/Perfil de riesgo:** Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.
- **Objetivos misionales:** Son los que se establecen para alcanzar el propósito de una entidad, que puede ser una empresa o una institución. Estos objetivos se basan en la misión, que es el compromiso de la entidad y su razón de ser.
- **Procesos de control:** Son aquellos que se encargan de garantizar que los productos o servicios cumplan con los requisitos establecidos. También permiten identificar fallas y oportunidades de mejora.
- **Riesgo:** Posibilidad que ocurra un evento que pueda afectar negativamente el cumplimiento de la operación de una Entidad y que atenten contra los objetivos del SGSSS.
 - **Riesgo inherente:** Nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.
 - **Riesgo neto o residual:** Nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes.
- **Semaforización:** proporciona señales inmediatas sobre cómo van los distintos aspectos de un proyecto (control de riesgo, nivel inherente de riesgo, nivel de riesgo residual)

6. POLITICA DE RIESGO OPERACIONAL (SARO)

La Junta Directiva y Gerencia de ESE UNIVERSITARIA DEL ATLANTICO manifiesta clara y expresamente su compromiso y respaldo con la implementación de sistemas que mitiguen o reduzcan la posibilidad de desviaciones en los objetivos misionales, como consecuencia de deficiencias, inadecuaciones o fallas en los procesos.

La ESE UNIVERSITARIA DEL ATLÁNTICO como empresa social del estado debidamente establecida bajo la normatividad legal colombiana declara que:

- La Junta Directiva y Gerencia de ESE UNIVERSITARIA DEL ATLANTICO manifiesta clara y expresamente su compromiso y respaldo con la implementación de sistemas que mitiguen o reduzcan la posibilidad de desviaciones en los objetivos misionales, como consecuencia de deficiencias, inadecuaciones o fallas en los procesos.
- El proceso de gestión del riesgo y colaboradores a los que se delegaron funciones relacionadas con la mitigación de riesgos operacionales, cuentan con el respaldo de la Junta Directiva para hacer uso de los recursos técnicos, humanos y financieros necesarios para el cumplimiento de la Circular Externa

2021170000004-5 DE 2021 y demás normas y/o recomendaciones internacionales frente al subsistema de riesgos operacionales.

- La ESE UNIVERSITARIA DEL ATLANTICO en su sistema integrado de gestión de riesgos, proporciona los medios para poner en marcha el ciclo de riesgo como se describe en la circular Externa 2021170000004-5 de 2021, identificando, evaluando, midiendo, controlando y monitoreando los riesgos operacionales que se hayan presentado o puedan presentarse en un futuro.
- ESE UNIVERSITARIA DEL ATLANTICO ha instrumentado las diferentes etapas y elementos del Riesgo Operacional, a través de la parametrización de las herramientas establecidas por la entidad para la medición del perfil de riesgo operacional de la institución en cada una de sus sedes.
- La ESE UNIVERSITARIA DEL ATLANTICO ha establecido los procedimientos y manuales para la adecuada implementación y funcionamiento del subsistema de riesgo operacional y la mitigación de eventos que puedan afectar: la salud del paciente, resultados operativos esperados, satisfacción del cliente y/o pérdidas financieras. La ESE UNIVERSITARIA DEL ATLANTICO proporciona los medios para que los dichos procedimientos sean debidamente socializados a los funcionarios a los que les concierne es deber de estos su permanente consulta y aplicación.
- La ESE UNIVERSITARIA DEL ATLANTICO define, implementa y mantiene un plan con el fin de asegurar la continuidad del negocio en situaciones de emergencia o materialización de riesgos que puedan tener un impacto significativo sobre la correcta operación de la institución.
- Los órganos de administración, de control, el oficial de cumplimiento y todas las personas que conforman la institución, asegurarán el cumplimiento del reglamento interno, y conocerán políticas, principios y valores institucionales establecidos en el código de conducta y buen gobierno.
- Todas las personas que conforman la institución tienen el deber de conocer y dar cumplimiento a las políticas, manuales, procedimientos y demás disposiciones relacionadas con los riesgos operacionales y de anteponerlas frente a cualquier negociación contractual o comercial en curso.
- En ESE UNIVERSTIRARIA DEL ATLANTICO, los riesgos son aceptados conforme lo establecido en el nivel admisible del apetito de riesgo, cuando su severidad se encuentra dentro de la categoría de MODERADO y BAJO. A los riesgos Moderados se les recomienda la asignación de un plan de acción para su mitigación, pero la intensidad del seguimiento a sus controles puede ser definida por la institución.
- Los riesgos ubicados en categorías POR ENCIMA DEL PROMEDIO y ALTOS no pueden ser asumidos por la institución y la asignación de controles y seguimientos de carácter mensual es obligatoria.
- Los medios para reporte de riesgos operativos se deben socializar desde la dirección del proceso a todos los colaboradores (funcionarios y contratistas), y debe socializarse como tema de inducción obligatoria y reinducción.
- Cualquier funcionario o contratista que detecte la materialización de un riesgo operacional ha de reportarlo a su jefe directo o hacer llegar el reporte al correo de gestión de riesgo, especificando: área o dependencia, proceso donde se produjo el riesgo, fecha de descubrimiento, inicio y finalización del

riesgo, descripción detallada de los hechos, productos o servicios afectados, tipo de evento que se produjo, tipo de pérdida y cuantía de la pérdida, entre otros detalles. Para ellos se debe hacer uso de los canales de reporte y las herramientas facilitadas desde el proceso de gestión del riesgo para hacer estos reportes.

- Se dejará registro de posibles pérdidas financieras o impacto operacional resultante de los de la materialización de todo riesgo operacional detectado y reportado. Se deben identificar los factores y actores (usuarios, clientes y/o contrapartes, socios, trabajadores, empleados, proveedores, entre otros) tanto externos como internos, que puedan afectar los objetivos de una institución, y de esta manera poderlos trabajar de directamente a través de planes de acción para mitigación de riesgos.
- La información acerca del riesgo se reportará de manera adecuada, con la finalidad de generar alternativas de acción y ser utilizada como base en la toma de decisiones.
- Se diseñarán e implementarán controles para cada proceso de manera que se pueda mitigar los riesgos inherentes detectados y registrados en la matriz institucional de riesgo, ya sea reduciendo su probabilidad, impacto o ambos
- Al poner en práctica el ciclo de gestión integral de riesgos, se debe considerar en cada una de sus etapas las recomendaciones publicadas por la Dirección de Gestión y Desempeño Institucional en su “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6” publicada en 2022. Se tendrán en cuenta las practicas aquí descritas para temas como la redacción y descripción de un riesgo y sus causas, los criterios de valoración de un riesgo según su impacto económico y reputacional, y las zonas de peligro en las matrices de semaforización. Las metodologías propuestas en esta guía se integrarán y alinearan con las definidas por la institución, con el fin de crear un Sistema Integrado de Gestión del Riesgo que este armonizado con las recomendaciones de la Función Pública.
- Después de definido un nivel de riesgo inherente, se proyecta un nivel de riesgo residual para cada riesgo. Este funcionará como un estimado del nivel de riesgo final una vez se implementen controles y se validará después de medida la calidad de los controles que se asignaron a los riesgos
- Se asignarán indicadores que medirán la eficiencia de los controles, así como la frecuencia de materialización de los riesgos a los que están asignados. La frecuencia de entrega de indicadores se definirá dependiendo de la severidad del riesgo y la disponibilidad de información para alimentar el indicador.
- La efectividad de los controles se medirá una vez pase el periodo de implementación anual, en base al grado de calidad del control y su capacidad de reducir el nivel de impacto y probabilidad del riesgo al que se le asigno.
- Incumplir los lineamientos y procedimientos previstos en los manuales SARO podrá dar lugar a sanciones y/o responsabilidades ante los organismos de vigilancia y control.

7. ETAPAS DE GESTION DE RIESGOS OPERACIONALES

Los riesgos operacionales de una institución pueden ser resultado de una deficiencia o ruptura en los controles internos o procesos de control, informalidad en desarrollo de procedimientos, fallas tecnológicas, errores humanos, deshonestidad o corrupción, prácticas inseguras y catástrofes naturales, entre otras causas, que afectan diferentes procesos.

Una adecuada gestión de riesgos es indispensable para mitigar el nivel de riesgo operacional inherente al que está expuesta la ESE UNIVERSITARIA DEL ATLANTICO. Como resultado de la mitigación de los riesgos a través de la adecuada definición y puesta en marcha de un ciclo de gestión de riesgo operacional, se obtiene el riesgo neto de la entidad.

La adopción del Subsistema de Administración de Riesgo Operacional debe cumplir como mínimo con cada una de las etapas del ciclo de gestión de riesgo, las cuales son las siguientes:

7.1. IDENTIFICACIÓN DEL RIESGO

El Subsistema debe permitir definir e identificar la exposición al riesgo operacional, por lo cual, en esta etapa se elabora un perfil de los procesos de las actividades de la institución con las siguientes acciones:

a) Para el óptimo desarrollo del **SARO** los siguientes procesos apoyan para el cumplimiento de las funciones de la institución y recopilación de información veraz en cuanto al comportamiento de los riesgos operacionales:

- Planeación estratégica institucional
- Subgerencias corporativas y científicas
- Planeación estratégica de la calidad y gestión del riesgo:
- Gestión del talento humano
- Gestión de recursos físicos
- Planeación Financiera
- Gestión jurídica
- Gestión de TICS
- Gestión de riesgo en salud / Seguridad del paciente
- Control interno

b) Identificación de los eventos de riesgo operacional, potenciales y ocurridos, en cada uno de los procesos y *estimación de las posibles pérdidas financieras relacionadas con la materialización de los mismos*. Para ellos se considerará anualmente con líderes o profesionales pertenecientes a cada uno de los procesos anteriormente mencionados, cuáles son los riesgos potenciales y ocurridos que han de incluirse en las matrices de riesgo para su control y seguimiento durante el periodo.

c) Identificación de procesos jurídicos en los que se encuentra la institución, dejar registro de posibles pérdidas financieras o impacto operacional resultante de los mismos. Los riesgos jurídicos serán registrados en la matriz de riesgo institucional.

d) Identificar pérdidas en los resultados de salud de los pacientes, los cuales por su relevancia son tratados como riesgos de salud.

Los riesgos identificados por el equipo de subgerencia científica serán registrados en una matriz aparte, puesto que desde esta área se implementa el Subsistema de Gestión de Riesgo de Salud (SARS). Sin embargo la

materialización de dichos riesgos y su impacto sobre las operaciones institucionales deben ser registrados siguiendo los procedimientos adoptados desde el subsistema de gestión del riesgo operacional.

La etapa de identificación debe realizarse previamente a la implementación de nuevos procesos o a la modificación de cualquier proceso, así como en los casos de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

Para el reporte de un riesgo operacional, se implementa un **formato para registro de eventos de riesgo operacional**, con la información relacionada con los eventos de riesgo operacional presentados. A continuación, se presenta la información relevante mínima que debe tener un registro de eventos de riesgo operativo:

| | | | | | |
|---|--|--|---|---|---------------------|
| 1. Referencia (Matriz de riesgo) | | 2. Proceso | | | |
| | | | | | |
| 3. Fecha de descubrimiento | | 4. Fecha de inicio del evento | | 5. Fecha de finalización del evento | |
| Fecha: | | Fecha: | | Fecha: | |
| Hora militar: | | Hora militar: | | Hora militar: | |
| 6. Descripción del evento | | | | | |
| | | | | | |
| 7. Causas | | | 8. Consecuencias | | |
| | | | | | |
| 9. Producto o Servicio Afectado: | | | | | |
| 10. Clase de Evento Operativo Para Señalar (Marque con una X) | | | | | |
| <input type="checkbox"/> Fraude | | <input type="checkbox"/> Relaciones laborales | | <input type="checkbox"/> Clientes o usuarios | |
| <input type="checkbox"/> Fallas tecnológicas | | <input type="checkbox"/> Ejecución de procedimientos | | <input type="checkbox"/> Daños Activos fijo | |
| <input type="checkbox"/> Otro, ¿Cuál? _____ | | | | | |
| 11. Tipo de pérdida (Marque con X) | | | | | |
| <input type="checkbox"/> Genera pérdidas y afecta el estado de resultados de la entidad | | <input type="checkbox"/> Genera pérdidas y no afecta el estado de resultados de la entidad | | <input type="checkbox"/> No Genera pérdidas y no afecta el estado de resultados de la entidad | |
| 12. Registro | | | | | |
| Cuantía (COP) | Cuantía total recuperada por acción directa (COP) | Cuantía total recuperada por otros conceptos o seguros (COP) | | Cuentas del plan de cuentas afectadas por el evento | |
| | | | | | |
| 13. Fecha de Contabilización: | | Día | Mes | Año | Hora militar |
| | | | | | |
| 14. Diligenciamiento de formato y reporte a la unidad de riesgos operativos | | | | | |
| Diligenciado por: | | | | | |
| Dependencia/Área/Proceso: | | | Fecha de Reporte del riesgo operativo: | | |
| Fecha de Diligenciamiento: | | | Hora militar del diligenciamiento: | | |
| Reportado por: (Colocar Nombre, Cargo y Fima): | | | | | |

Anexo 1: Formato FT-GR-028 de reporte de riesgos operacionales.

Asimismo, cabe mencionar que, dentro de todos los procesos de la institución, se debe identificar que dentro del riesgo operacional se puede encontrar inmerso el riesgo de corrupción y opacidad, el cual puede impedir el funcionamiento efectivo de las instituciones, afectando directamente la misión y la visión y el flujo normal y efectivo de los recursos, a través de acciones y actitudes contrarias a los valores y principios éticos promovidos.

7.1.1. Registro de riesgos identificados en matriz de Riesgo institucional

Los posibles escenarios que puedan provocar una pérdida económica por la materialización de un riesgo de operacional se registran anualmente en una matriz de riesgo en su **sección de identificación de riesgo**.

Para identificar dichos escenarios de riesgos operativos se utilizará la metodología de Delphi. Esta consiste en la definición de un panel de expertos, que en el caso de E.S.E UNIVERSITARIA DEL ATLANTICO, serán los coordinadores o delegados de los procesos mencionados en el *numeral 7.1 a)*.

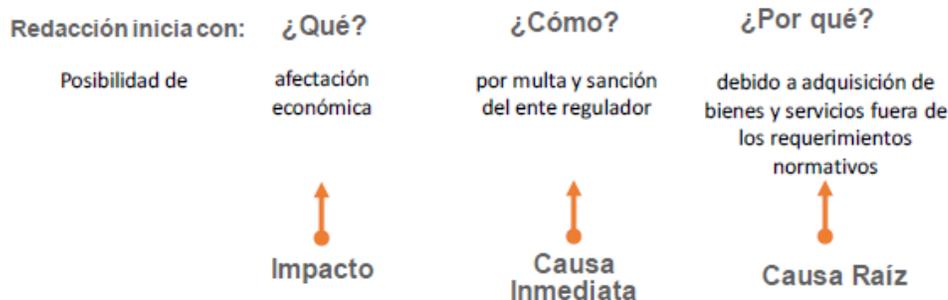
El método Delphi es un sistema que se basa en el uso estratégico de las opiniones de un panel de expertos sobre algún tema en particular, con el fin de llegar a soluciones específicas y una mejor toma de decisiones. En el caso de riesgo operacional se registrarán los riesgos que afectan o pueden afectar la consecución de los objetivos misionales de la institución, a criterio de cada uno de los integrantes de la reunión de expertos.

A cada riesgo identificado se relaciona el proceso donde se origina el riesgo o el que es directamente impactado en caso de materialización, así como las posibles causas internas o externas que puedan producir su materialización, y las posibles consecuencias o impacto que pueda tener sobre la institución en el escenario en el que ocurriese la situación riesgosa descrita.

Nota: el registro de los riesgos operacionales se realizará por primera vez durante el ejercicio de definición de nivel de riesgo residual, la incorporación de nuevos riesgos a la matriz o la supresión de riesgos de la matriz se realizarán anualmente durante el primer comité de riesgo institucional. Los riesgos aquí registrados son los que han de ser reportados a través del formato de reporte de materialización de riesgo operacional, mencionado en el *numeral 7.1 d)*.

7.1.1.1. Descripción de riesgo operacional identificado

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso.



Anexo 1. Ejemplo de redacción de riesgo, adaptado de “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, Versión 6, 2022”

7.1.1.2. Definir causas y consecuencias

Se registrará en la matriz cuales son las posibles causas o han sido las causas de materialización de riesgo. Diferenciar si las causas que provocan la materialización del riesgo son internas o externas, algunas causas

internas es la falta de capacitación del personal, la mala planificación y la falta de mantenimiento de la maquinaria, por otro lado las causas externas pueden ser cambios en el mercado, desastres naturales y cambios políticos.

Las consecuencias de un riesgo son los efectos que se producen cuando un riesgo se materializa. Pueden ser negativas o positivas, dependiendo del tipo de riesgo y su impacto. En este caso se listarán en la matriz las posibles consecuencias en caso de materialización del riesgo descrito, estas irán relacionadas al tipo de impacto del riesgo, por lo menos una consecuencia principal por tipo de impacto.

7.1.1.3. Definir tipo de impacto del riesgo operacional

El impacto de un riesgo está directamente relacionado con las posibles consecuencias del mismo, el grupo de expertos define cuales son los tipos de impacto relacionados a la posible materialización del riesgo descrito. Estos son:

- **Impacto Operativo / Operacional o sistémico:** Valoración del nivel en el cual la interrupción del proceso genera incumplimientos y/o retrasos en la cadena de valor de E.S.E UNIVERSITARIA DEL ATLÁNTICO
- **Impacto Legal:** Contempla repercusiones a nivel de incumplimiento con compromisos contractuales o exigencias de entes supervisores producidas por la interrupción del proceso.
- **Impacto Económico:** Criterio que incorpora variables asociadas a la afectación económica que pueda presentarse por la materialización del riesgo. La descripción asociada a este impacto se define teniendo en cuenta la Utilidad Neta del año inmediatamente anterior al que se está realizando el análisis.
- **Impacto Reputacional:** Acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad.
- **Impacto a la Salud:** Variables asociadas a la afectación de la salud de un paciente o colaborador por la materialización del riesgo.

7.2. EVALUACIÓN Y MEDICIÓN DEL RIESGO

Es la valoración de los efectos asociados a los riesgos que han sido identificados, considerando la frecuencia y la severidad de su ocurrencia. Se entenderá por valoración del riesgo, la medida cualitativa o cuantitativa de su probabilidad de ocurrencia y su posible impacto.

Para la evaluación y medición de cada uno de los riesgos identificados, la institución debe contar con información suficiente, completa y de calidad para generar los mejores pronósticos. La valoración de los riesgos ha de realizarse con cada uno de los riesgos identificados, y tendrá como resultado un nivel inherente de riesgo después de realizada la primera valoración. Esta se realizará durante las sesiones de experto con todos los integrantes cada uno de los procesos de la institución.

7.2.1. Semaforización de riesgos Operacionales

Esta se llevará a cabo en la **sección de evaluación de riesgo de la matriz de riesgo**. El ejercicio implica determinar el riesgo operacional inherente para cada uno de los procesos y para la institución en general,

ubicando cada riesgo en un mapa calor. Se realiza la evaluación preliminar del riesgo (multiplicando la calificación preliminar de probabilidad con la del impacto), estableciendo así la clasificación en la cual se encuentra el riesgo.

Cada miembro del grupo de expertos valorara el riesgo a su consideración y bajo los criterios que se describirán a continuación en el numeral 7.2.2. Se tabula la información y se integra el consolidado en la matriz de riesgo. De no haber opiniones distintas respecto al valor de probabilidad e impacto que se le asignará a cada riesgo, se pondrá el puntaje al que se llegó en consenso de todos los participantes de la reunión de expertos.

RIESGO INHERENTE (RI) = VECTOR (PROBABILIDAD INHERENTE (PI)* IMPACTO INHERENTE (II))

7.2.2. Determinación de nivel de probabilidad del riesgo

Para determinar la **Probabilidad/Frecuencia** inherente se tomará el factor más alto de uno los siguientes criterios (el criterio de Futuro se toma en el caso de que no exista registro previo de materialización del riesgo en la institución):

- **Historia:** número de veces que se ha materializado en un periodo de tiempo determinado.

| Calificación | Descripción | Factor |
|--------------|---|--------|
| Raro | Nunca ha ocurrido y, de hecho, se considera casi imposible que ocurra | 1 |
| Improbable | No se sabe si ha ocurrido o no, pero cabe alguna posibilidad de ocurrencia, aunque se considera muy remota. | 2 |
| Posible | Ha ocurrido, hace más de dos años, pero se considera que las posibilidades de volver a suceder no son remotas. | 3 |
| Probable | No ha ocurrido durante el año en curso, pero sí el año anterior y se considera probable que vuelva a presentarse. | 4 |
| Casi seguro | Ha ocurrido, durante el año en curso, y se considera que las posibilidades de repetirse son muy altas. | 5 |

- **Futuro:** Probabilidad estimada de su ocurrencia en un futuro

| Calificación | Descripción | Factor |
|--------------|---|--------|
| Raro | Prácticamente imposible que ocurra el próximo año | 1 |
| Improbable | Poco probable que ocurra en el próximo año | 2 |
| Posible | Es probable que ocurra el próximo año | 3 |
| Probable | Bastante probable que ocurra el próximo año | 4 |
| Casi seguro | Ocurrirá con alto nivel de certeza el próximo año | 5 |

7.2.3. Determinación de nivel de impacto del riesgo

Para determinar el **Impacto** inherente se tomará el factor más alto de los siguientes criterios (solo aquellos relacionados con el riesgo identificado durante la primera etapa, ver *título 7.1.1.3 Definir impacto de riesgo*):

- **Impacto Sistémico/Operativo:** Valoración del nivel en el cual la interrupción del proceso genera incumplimientos y/o retrasos en la cadena de valor.

| Calificación | Descripción | Factor |
|----------------|---|--------|
| Insignificante | No existe una afectación. | 1 |
| Menor | Podría generar impactos cuantitativos y/o cualitativos a nivel de pocos clientes. El impacto es concentrado no generalizado | 2 |
| Moderado | Podría generar impactos cuantitativos y/o cualitativos en un grupo clientes de alto impacto para el negocio. | 3 |
| Mayor | Podría generar impactos en la eficiencia operacional de todos los clientes o participantes de la cadena de valor. | 4 |
| Catastrófico | Podría generar impactos cuantitativos y en la reputación de todos los clientes y participantes de la cadena de valor. | 5 |

- **Impacto Legal:** Contempla repercusiones a nivel de incumplimiento con compromisos contractuales o exigencias de entes supervisores producidas por la interrupción del proceso.

| Calificación | Descripción | Factor |
|----------------|--|--------|
| Insignificante | Evento de riesgo registrado que podría llamar la atención de la SNS o las autoridades | 1 |
| Menor | Sanciones económicas menores por incumplimiento de normatividad / EJ: Glosas de la SNS | 2 |
| Moderado | Eventos derivados de las categorías de riesgo legal que pueden implicar procesos de investigación por parte de la SNS y sanciones económicas significativas. Determinación de responsabilidades a los administradores o Suspensión de administradores. Se puede generar un impacto en la continuidad en la prestación de servicios no principales del negocio. | 3 |
| Mayor | Eventos derivados de las categorías de riesgo legal que generen un impacto en la capacidad de operar parcialmente afectando una línea de negocio (CORE) u objeto principal, generando un incumplimiento normativo de disposiciones legales y normativas o emisión o cambio de normas que afecten el normal desarrollo de las actividades de la organización o emisión de sanciones judiciales a cargo produciendo: - Declaración de práctica insegura y no autorizada - Determinación de responsabilidades a los administradores - Sanciones a la entidad integrada | 4 |

| | | |
|--------------|---|---|
| Catastrófico | <p>Situaciones o eventos derivados de las categorías de riesgo legal que generen un impacto en la capacidad de operar afectando de manera sistémica la capacidad de operar las líneas de negocio CORE u objeto principal derivadas de elementos tales como el incumplimiento normativo, la misión de nuevas normas o de nuevas disposiciones legales que afecten el normal desarrollo de las actividades de la INSTITUCIÓN.</p> <p>Igualmente se predica de la emisión de sanciones judiciales a cargo produciendo entre otras la declaración de práctica insegura y no autorizada, y procesos legales en contra de la entidad integrada y sus administradores.</p> | 5 |
|--------------|---|---|

- Impacto Económico:** Criterio que incorpora variables asociadas a la afectación económica que pueda presentarse por la materialización del riesgo. La descripción asociada a este impacto se define teniendo en cuenta la Utilidad Neta del año inmediatamente anterior al que se está realizando el análisis.

| Calificación | Descripción | Factor |
|----------------|-----------------------------|--------|
| Insignificante | Afectación menor a 10 SMLMV | 1 |
| Menor | Entre 10 y 50 SMLMV | 2 |
| Moderado | Entre 50 y 100 SMLMV | 3 |
| Mayor | Entre 100 y 500 SMLMV | 4 |
| Catastrófico | Mayor a 500 SMLMV | 5 |

- Impacto Reputacional:** Acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de una entidad, tales como el impacto de la publicidad negativa sobre las prácticas comerciales, conducta o situación financiera de la entidad.

| Calificación | Descripción | Factor |
|----------------|--|--------|
| Insignificante | El riesgo afecta la imagen de algún área de la institución | 1 |
| Menor | El riesgo afecta la imagen de la institución internamente, de conocimiento general nivel interno, de junta directiva y accionistas o proveedores | 2 |
| Moderado | El riesgo afecta la imagen de la institución con algunos usuarios de relevancia frente al logro de los objetivos | 3 |
| Mayor | El riesgo afecta la imagen de la institución con efecto publicitario sostenido a nivel sector administrativo, nivel departamental o municipal | 4 |
| Catastrófico | El riesgo afecta la imagen de la institución a nivel nacional con efecto publicitario sostenido a nivel país, potencialmente impidiendo la relación con contrapartes | 5 |

- **Impacto a la Salud:** Variables asociadas a la afectación de la salud de un paciente o colaborador por la materialización del riesgo.

| Calificación | Descripción | Factor |
|----------------|--|--------|
| Insignificante | No genera una lesión o complicación en el paciente. Puede afectar transitoriamente la ejecución de una tarea pero sin interrupción a la prestación del servicio. | 1 |
| Leve | Puede ocasionar una lesión transitoria en el paciente sin secuelas, no requiere tratamiento médico, afecta transitoriamente la ejecución de una tarea pero no la prestación del servicio | 2 |
| Moderado | Genera lesión o complicación a la salud del paciente, requiere tratamiento médico en un periodo limitado. Afecta la ejecución de una tarea temporalmente y la prestación del servicio en un periodo corto de tiempo. | 3 |
| Grave | Genera lesión o complicación grave en el paciente con discapacidad irreversible. Requiere tratamiento médico por tiempo indefinido, causa interrupción prolongada en la prestación de un servicio. | 4 |
| Catastrófico | Muerte(s) de paciente, suspensión definitiva de la prestación del servicio. | 5 |

Basado en el total obtenido en la evaluación preliminar de del riesgo, se les asigna la siguiente clasificación de nivel de riesgo, junto con una serie de opciones de tratamiento a partir de la clasificación obtenida.

| PROBABILIDAD \ IMPACTO | IMPACTO | | | | |
|------------------------|----------------|-------|----------|-------|--------------|
| | Insignificante | Menor | Moderado | Mayor | Catastrófico |
| | 1 | 2 | 3 | 4 | 5 |
| Casi seguro | 5 | 10 | 15 | 20 | 25 |
| Probable | 4 | 8 | 12 | 16 | 20 |
| Posible | 3 | 6 | 9 | 12 | 15 |
| Improbable | 2 | 4 | 6 | 8 | 10 |
| Raro | 1 | 2 | 3 | 4 | 5 |

Anexo 2. Semaforización - Calificación de riesgo probabilidad x impacto

| Nivel de Riesgo | Calificación | Definición | Tratamiento de Riesgo |
|-----------------|-----------------|--|--|
| 0 a 5 | Bajo | Cuando hay una probabilidad menor que el promedio de una perdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo | Se ACEPTARA el riesgo y se administrará por medio de las actividades propias del proceso asociado, y su control y registro de avance, se realizará en el reporte mensual de su desempeño. Los planes de acción para la implementación de controles no se priorizarán. |
| 6 a 10 | Moderado | Cuando hay una probabilidad promedio de una perdida debido a la exposición y a la | Se establecerán acciones de Control Preventivas, que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se administrarán mediante seguimiento preferiblemente BIMESTRAL y se |

| | | | |
|---------|-------------------------|--|---|
| | | incertidumbre derivada de la materialización de un riesgo | registrarán sus avances en el Sistema de Planificación Institucional- SGI. |
| 11 a 16 | Por encima del promedio | Cuando hay una probabilidad mayor el promedio de una pérdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo | Se establecerán acciones de Control Preventivas, que permitan EVITAR la materialización del riesgo. La Administración de estos riesgos será con periodicidad sugerida al menos MENSUAL y su adecuado control se registrará en el Sistema de Planificación Institucional- SGI. |
| 17 a 25 | Alto | Cuando hay una probabilidad mucho mayor que la del promedio de una pérdida debido a la exposición y a la incertidumbre derivada de la materialización de un riesgo | Se establecerán acciones de Control Preventivas y correctivas, que permitan EVITAR la materialización del riesgo. La Administración de estos riesgos será con periodicidad MÍNIMA MENSUAL y su adecuado control se registrará en el Sistema de Planificación Institucional- SGI. Adicionalmente se deberán documentar al interior del proceso, planes de contingencia para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación del servicio; estos planes estarán documentados. |

Anexo 3. Tabla de calificación de riesgo probabilidad x impacto y tratamiento por nivel de riesgo

Nota: al calificar el por nivel de probabilidad o impacto tener en cuenta dentro de la evaluación, los *planes de contingencia* y el *Plan de Continuidad del Negocio*, todos los recursos (físicos, humanos, técnicos y financieros) necesarios para enfrentar la exposición al riesgo operacional bajo cualquier eventualidad.

7.3. CONTROL DEL RIESGO (estrategias para tratamiento y control)

Una vez identificados y evaluados los riesgos, deben compararse con los *límites* (tolerancia) de riesgos aprobados por la instancia definida en la institución y su política de riesgos, siempre dentro del marco normativo establecido. Todo riesgo que exceda los límites o desviaciones aceptadas, debe ser objeto de actividades de mitigación y control a fin de regresar al nivel de riesgo tolerado, conforme la estrategia adoptada. Se deben determinar las acciones tendientes a gestionar los riesgos a los que se ve expuesta la entidad, de acuerdo con los niveles de riesgo determinados y las tolerancias al riesgo definidas.

Se asocian **controles** a cada riesgo identificado, al igual que el tipo/objetivo del control (preventivo, correctivo, detectivo), el/los responsables de la implementación del control, frecuencia de seguimiento, fecha de inicio de la implementación y fecha final de la implementación y seguimiento. Se asociará a cada control un indicador que ayudará a medir la efectividad de este durante el periodo de seguimiento definido. Se priorizará la asignación de indicadores a riesgos que sobrepasen el límite de tolerancia de la institución (Riesgos con valoración de nivel de riesgo ALTO o POR ENCIMA DEL PROMEDIO)

La información referente a los controles y su seguimiento se registrarán en la **sección de Control y tratamiento de riesgo en el formato de Matriz de riesgo institucional**.

7.3.1. Tipos de control

- **Preventivo:** Antes de que se presente un evento
- **Correctivo:** Posterior a la materialización de un riesgo

- **Detectivo:** Se realiza al identificar la exposición del riesgo

7.3.2. Naturaleza del control

- **Manual:** Las realiza una persona
- **Automático:** lo realiza una herramienta tecnológica
- **TI:** Se apoya en tecnología pero depende de que lo realice una persona

7.3.3. Opciones de manejo de tratamiento del riesgo

- **Evitar el riesgo:** Implica dejar de ejecutar las actividades o desistir de una decisión que posiblemente generaría que el evento se materialice, o tomar planes de contingencia para reducir el impacto del riesgo materializado.
- **Reducir el Riesgo:** Desarrollar actividades que propendan por reducir la probabilidad o la severidad en caso de materializarse el evento.
- **Aceptar el riesgo:** Tiene lugar cuando la organización decide no impartir ningún tipo de acción que evite su materialización y/o severidad en el impacto. Está dispuesta a asumir los costos derivados de la materialización del evento. También se puede tomar esta opción de manejo cuando las actividades propias del proceso relacionado son suficientes para impedir la materialización del mismo.
- **Transferir el riesgo:** Tiene lugar cuando se traslada el riesgo a otra compañía, ya sea por medio de la tercerización, contratación de una póliza de seguros u otros.
- **Tercerización – Outsourcing:** Se podrá contratar bajo la modalidad de tercerización a personas naturales y/o jurídicas para el desarrollo de sus procesos, siempre que no implique la delegación de la profesionalidad.

Tratándose de los procesos y/o actividades identificadas como críticos o que sobrepasan límites de aceptación para la ESE UNIVERSTIRARIA DEL ATLÁNTICO, se debe cumplir como mínimo con los siguientes requerimientos:

- Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros.
- Incluir en los contratos que se celebren con los terceros, o en aquellos que se prorroguen, al menos, aspectos tales como obligaciones de las partes, niveles de servicio, operación en situaciones contingentes, gestión de los riesgos operacionales que puedan afectar el cumplimiento de las obligaciones del tercero, acuerdos de confidencialidad sobre la información manejada y las actividades desarrolladas.
- Gestionar los riesgos que se derivan de la prestación del servicio por parte del tercero, en particular, cuando atiende a varias entidades.
- Contar con los procedimientos necesarios para verificar el cumplimiento de las obligaciones por parte del tercero.
- Incluir dentro del alcance de las evaluaciones que haga la función de gestión de riesgos y la auditoría interna, las actividades tercerizadas.

7.3.4. Aceptación de riesgos.

En ESE UNIVERSTIRARIA DEL ATLÁNTICO, los riesgos son aceptados conforme lo establecido en el nivel admisible del apetito de riesgo, cuando su severidad se encuentra dentro de la categoría de **Moderado** y **Bajo** presentadas en el anexo 3 del presente manual. A los riesgos Moderados se les recomienda la asignación de un plan de acción para su mitigación, pero la intensidad del seguimiento a sus controles puede ser definida por la institución.

Los riesgos ubicados en categorías **Por encima del Promedio** y **Altos** no pueden ser asumidos por la institución y la asignación de controles y seguimientos de carácter mensual es **obligatoria**.

7.3.5. Control de riesgo operacional, Plan de continuidad del negocio

La institución debe tomar las medidas adecuadas para controlar el riesgo operacional inherente al que se ve expuesta en el desarrollo de sus operaciones con el fin de disminuir la probabilidad de ocurrencia y/o impacto en caso de que se materialicen. Para ello un control muy común es la formulación de acciones preventivas para evitar ocurrencia del evento, controles sobre dichas acciones, así como acciones de contingencia ante la posible materialización del mismo. Se debe implementar un Plan de Continuidad del Negocio aprobado por Gerencia.

ESE Universitaria del Atlántico define, implementa, prueba y mantiene un proceso para administrar y asegurar la continuidad del negocio en situaciones de emergencia o desastre, incluyendo elementos como la prevención y la atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal en su plan de continuidad del negocio.

Este contiene:

- a. Eventos que pueden afectar la operación.
- b. Actividades por realizar cuando se presentan las fallas.
- c. Alternativas de operación.
- d. Proceso de retorno a la actividad normal.

7.3.6. Control de riesgo operacional, Acreditación de soportes de operaciones, negocios y contratos.

Todo documento que acredite transacciones, negocios o contratos de ESE UNIVERSITARIA DEL ATLANTICO, además de constituir el soporte de la negociación y del registro contable, constituye el respaldo probatorio para cualquier investigación que puedan adelantar las autoridades competentes. Para ello se manejan informes de gestión por parte de los miembros de la dirección que se encargan de velar por el cumplimiento de objetivos de los contratos o negocios realizados en la institución.

7.4. SEGUIMIENTO Y MONITOREO

Una vez establecidos los mecanismos o un conjunto de estos, para la mitigación y control de los riesgos que se han identificado como relevantes para la entidad y después de realizar un análisis de causa y efecto para determinar los puntos más críticos a intervenir con mayor prelación, la institución deberán poner en práctica tales mecanismos y reflejarlos en un plan de implementación de las acciones planteadas en la fase anterior.

Con el fin de realizar el respectivo seguimiento y monitoreo permanente y continuo de la evolución de los perfiles de riesgo y la exposición frente a posibles pérdidas a causa de la materialización de cada uno de los riesgos identificados, la entidad debe desarrollar un sistema de alertas tempranas que facilite la rápida detección, corrección y ajustes de las deficiencias en cada uno de sus Subsistemas de Administración de Riesgo para evitar su materialización. Lo anterior, con una periodicidad acorde con los eventos y factores de riesgo identificados.

7.4.3. Seguimiento a los planes de acción

Mensualmente los líderes de cada proceso (ver responsables de gestión de riesgo por subsistema en Anexo 6) deberán reportar al Proceso de Gestión del Riesgo el porcentaje de avance en la implementación de los planes de acción relacionados con los riesgos que no dan cumplimiento a los criterios de aceptación del riesgo.

Los resultados generados a través de los análisis y evaluaciones desarrolladas por la Coordinación de Riesgos y Procesos deben ser soportados e informados a la Gerencia, como también el reporte de cualquier hallazgo, anomalías, oportunidades y/o debilidades; así como, las consideraciones individuales detectadas en los análisis y evaluaciones de riesgo desarrollados de forma particular a cada proceso.

Para la ejecución de este paso del ciclo se empleará las secciones de **Seguimiento materialización del riesgo en la Matriz de Riesgos**.

7.4.4. Herramientas para seguimiento a controles riesgos operacionales

Formulación de indicadores

De acuerdo con el perfil del riesgo que tiene la organización, existen diferentes indicadores que sirven para generar alertas tempranas, para ello existen dos tipos de indicadores que se ajustan a las necesidades que requiere ESE UNIVERSITARIA DEL ATLANTICO para gestionar sus riesgos Operacionales:

- **Los indicadores clave de Riesgo - (KRI):** cuantifican el perfil de riesgo de la compañía. Se constituyen de acuerdo con el nivel de relevancia en los indicadores de riesgo y de control. Por ejemplo, el volumen de operaciones, rotación de personal, número de veces que cae el sistema, etc. Cada KRI deberá ser capaz de ser medido con precisión y reflejar de manera precisa el impacto negativo que tendría sobre los indicadores de desempeño clave de la organización. Estas métricas permiten llevar un registro de incidencias, monitorear su comportamiento, informar sobre su evolución, reportarlos y establecer planes de acción cuando salen de la tendencia esperada.
- **Los indicadores clave de control – (KCI):** Se encargan de medir la efectividad, tanto del diseño como de desempeño de un control específico. Un deterioro en un KCI puede significar un aumento en la probabilidad e impacto de un riesgo.

La asignación de indicadores se priorizará sobre riesgos que presenten niveles de riesgos Operacionales por encima del promedio y altos en la matriz de riesgos. La información dada por indicadores permitirá generar planes de acción en aquellos indicadores que estén por debajo de los límites permitidos de aceptación y brindaran información cuantitativa confiable al momento de valorar la efectividad de los controles al final de un periodo de gestión de los riesgos.

7.5. EVALUACIÓN DE CONTROLES

En base al grado de tolerancia (clasificación del nivel de riesgo), se aclaran cuáles son los **controles** que se llevan actualmente para la mitigación y como evidencia o sustento del tratamiento. Se evaluará a través de un sistema de valoración de controles la calidad de los mismos para tratar con los riesgos analizados.

La calidad de los controles se medirá a través de un cálculo de valoración donde el puntaje de calidad de los controles se dividirá en cuatro posibles opciones dependiendo de su desempeño para la mitigación de los riesgos asociados. Se tendrán en cuenta también otros aspectos relacionados con la efectividad de las

herramientas y del seguimiento hecho a dichos controles. La ponderación de los resultados arrojará un porcentaje que ubicará al control en **cuatro categorías** (Fuerte, Aceptable, Requiere Mejora, Débil).

Ver Anexo 4. A continuación para explicación detallada del cálculo para valoración de la calidad de los controles por riesgo.

| Calidad de las funciones de control | |
|--|-----------|
| Las funciones de control muestran de forma consistente un desempeño efectivo y superior a las prácticas de la industria de los seguros comúnmente observadas y/o Clasificación del control con énfasis en lo preventivo. | 20 |
| Las funciones de control muestran desempeño efectivo y similar a las prácticas de la industria comúnmente observadas. | 15 |
| Las funciones de control muestran potencial para un desempeño efectivo, pero pueden ser mejoradas y no arriesgan la situación financiera de la compañía. | 10 |
| Las funciones de control muestran un desempeño inferior a las prácticas observadas de la industria y su efectividad debe ser mejorada para no comprometer la situación financiera y operativa de la compañía. | 5 |



| Valoración de los controles | | |
|--------------------------------------|---|---|
| Parámetros | Criterios | Puntaje |
| Herramientas para ejercer el control | Posee una herramienta para ejercer el control. | 0 - 1 |
| | Existen manuales instructivos o procedimientos para el manejo de la herramienta | 0 - 1 |
| | En el tiempo que lleva la herramienta ha demostrado ser efectiva. | 0 - 1 |
| Seguimiento al control | Están definidos los responsables de la ejecución del control y del seguimiento. | 0 - 1 |
| | La frecuencia de la ejecución del control y seguimiento es adecuada. | 0 - 1 |
| | TOTAL | Sumatoria de cada uno de los criterios (0-5) |



| Rangos de calificación de los controles | | |
|---|---|----------|
| Calidad del control | Definición | Rangos |
| Fuerte | Existen controles fuertes: acciones preventivas, planes de mejora y contingencia. | 80 - 100 |
| Aceptable | Existen controles aceptables: acciones preventivas, planes de mejora. | 60 - 79 |
| Necesita mejora | Existen controles mínimos que requieren mejoras. | 40 - 59 |
| Débil | No existen controles o son mínimos. | 0 - 39 |

Anexo 5: Calificación de controles de Gestión del riesgo.

Para el **tratamiento** de cada riesgo individual se deberán identificar las acciones preventivas a tomar, responsables de la acción, periodos de seguimiento, plazos de inicio y terminación de la acción y acciones de contingencia ante la posible materialización del riesgo.

Para la ejecución de este paso del ciclo se utilizarán las secciones de **Evaluación de calidad de controles y Tratamiento de riesgos** en la **Matriz de Riesgos**

7.6. PERFIL DE RIESGO RESIDUAL

La efectividad de los controles asociados a los riesgos operacionales lleva como resultado el nivel del riesgo residual. Esto quiere decir que al determinar los atributos de eficiencia e informativos del control será posible identificar la zona del riesgo en estado residual.

El riesgo residual de **ESE UNIVERSTIRARIA DEL ATLÁNTICO** será determinado por los riesgos inherentes que hayan obtenido una valoración **Por encima del promedio y Alta**.

Finalmente, si en el riesgo residual de **ESE UNIVERSTIRARIA DEL ATLÁNTICO** se ha obtenido como resultado riesgos operacionales que mantienen una valoración muy alta, se deberán analizar las opciones de planes de mejora que permitan bajar el nivel de los riesgos a una zona aceptable. Para lo anterior se hace pertinente evaluar el costo beneficio de las acciones a tomar, si la institución está dispuesta a administrar el riesgo, si se está en capacidad de reducir la probabilidad o si se pudiera optar por transferir el riesgo (pólizas de seguros, tercerización).

Para definir el nivel de **riesgo residual** de la institución se utilizará la siguiente metodología, que se apoyará en la evaluación de efectividad de los controles para reducción del nivel de riesgo inherente:

- Definir el periodo de seguimiento a los riesgos identificados. Durante este periodo los colaboradores encargados del seguimiento de cada riesgo deberán hacer entrega de los indicadores relacionados.
- Definir el **nivel de riesgo esperado** de cada riesgo identificado.
- Una vez se termine el periodo de seguimiento de los riesgos y de implementación de controles y planes se valoran los controles como se describió en el 7.5 de evaluación de controles.
- Se empleará la **matriz de escala de clasificación para riesgo residual**, cruzando el resultado de riesgo inherente del riesgo evaluado y el resultado de valoración de calidad de control.
- De cumplirse con el mínimo aceptable para que el control pueda considerarse como efectivo, el nivel de riesgo propuesto cambiará.
- El nuevo nivel de riesgo será sobre el que se trabajará para el próximo periodo.

Se incluirá este resultado de riesgo residual en la **matriz de riesgo** y se construirá un nuevo mapa de calor, donde se visualizará la evolución del nivel de riesgo de la institución después de implementados los controles.

| Riesgo Residual | | | | |
|--------------------------|----------------------------|-------------------------|-------------------------|-------------------------|
| Calidad de los controles | Nivel del Riesgo Inherente | | | |
| | Bajo | Moderado | Por encima del promedio | Alto |
| Fuerte | Bajo | Bajo | Moderado | Por encima del promedio |
| Aceptable | Bajo | Moderado | Por encima del promedio | Alto |
| Necesita mejorar | Moderado | Por encima del promedio | Alto | Alto |
| Débil | Por encima del promedio | Alto | Alto | Alto |

Anexo 6. Matriz - escala de clasificación para riesgo residual

8. RESPONSABILIDADES DE LIDERES DE PROCESOS INVOLUCRADOS EN LA GESTIÓN DEL RIESGO OPERACIONAL

| PROCESO | LIDER | FUNCION |
|---|--|---|
| Planeación estratégica de la calidad y gestión del riesgo | Líder de proceso de gestión del Riesgo Líder de gestión de la calidad | - Recopilación de la información suministrada por los procesos para identificación y registró en la matriz de los riesgos operacionales a tener en cuenta en la institución y del cumplimiento de los planes de acción asignados a riesgos operacionales categorizados como altos o |

| | | |
|-----------------------------|--|---|
| | | <p>resultantes de la materialización de los riesgos operacionales.</p> <p>- Registro de riesgos identificados en la matriz y supervisión de cumplimiento del ciclo de gestión del riesgo.</p> |
| Gestión del talento humano | Director de talento Humano | Utilización de información histórica de la institución para identificación de riesgos operacionales potenciales en el área de talento humano, dejar registro de materialización en los formatos designados |
| Planeación financiera | Director financiero | Utilización de información histórica financiera de la institución para identificación de riesgos operacionales potenciales en el área de financiera, dejar registro de materialización en los formatos designados |
| Gestión jurídica | Jefe Oficina Jurídica | Utilización de información histórica jurídica y conocimiento en procesos jurídicos activos de la institución para identificación de riesgos operacionales potenciales en el área jurídica, dejar registro de materialización en los formatos designados |
| Gestión de TICS | Director TICS | Utilización de información histórica y conocimiento en TICS de la institución para identificación de riesgos operacionales potenciales que puedan ocurrir en áreas vigiladas por este proceso, dejar registro de materialización en los formatos designados |
| Gestión de recursos físicos | Jefe de proceso | Utilización de información histórica y conocimiento en todos los procesos que componen la gestión de recursos físicos (ambiente, almacén, etc.) en la institución para identificación de riesgos operacionales potenciales que puedan ocurrir en áreas vigiladas por este proceso, dejar registro de materialización en los formatos designados |
| Gestión del riesgo en salud | Subgerencia científica Dirección de Seguridad del Paciente Directores técnicos de sedes Soledad, Sabanalarga, pediátrico, mental | Notificar al líder de gestión del riesgo sobre la materialización de riesgos de salud que tengan efectos sobre las operaciones de la institución y dejar registro en los formatos designados. |

9. FICHA DE CONTROL DE CAMBIOS

| FICHA DE CONTROL DE CAMBIOS | | |
|-----------------------------|------------|---|
| VERSIÓN | FECHA | DESCRIPCIÓN DE LA MODIFICACIÓN |
| 01 | 13/09/2024 | Creación del documento |
| 02 | 30/12/2024 | Actualización del documento. Inclusión de explicación detallada al desarrollo de cada una de las etapas del ciclo de riesgo. Se incluyó metodología para evaluación de controles una vez finalice el periodo de seguimiento. Se incluyó metodología para cálculo de riesgo residual. Se añadieron definiciones. Se actualizó política relacionada |

10. APROBACIÓN DEL DOCUMENTO

| APROBACIÓN DEL DOCUMENTO | | |
|---------------------------------------|---|---|
| ELABORO | REVISO | APROBÓ |
| Nombre: Armando Zabarrain Lara | Nombre: Aura Cortizo Cabana | Nombre: Rafael Fernández De Castro Riascos |
| Cargo: Gestión de Riesgos | Cargo: Coordinador(a) de Calidad | Cargo: Subgerencia Corporativa |
| Fecha: 13/09/2024 | Fecha: 25/10/2024 | Fecha: 28/10/2024 |
| Firma: | Firma: | Firma: |