POLITICA DE ADMINISTRACION DEL RIESGO

RED SALUD ARMENIA ESE

Octubre de 2019

Contenido

1. Introducción

Red Salud Armenia ESE, define su política de administración del riesgo, tomando como base los parámetros establecidos en el Modelo Integrado de Planeación y Gestión (MIPG) y en la metodología AMFE en las diferentes áreas o servicios, en lo referente a las líneas de defensa y los lineamientos de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" de la Función Pública, versión 4 de 2018.

Todas las áreas o servicios de la organización, deben establecer los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales, en el marco de los programas, proyectos, planes, procesos de la ESE, mediante:

a) La identificación y documentación de riesgos de gestión (financieros, contractuales, jurídicos, entre otros), corrupción, asistenciales y de seguridad digital.

b) El establecimiento de acciones de control detectivas y preventivas para los riesgos identificados.

c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

Para administrar adecuadamente los riesgos, Red Salud Armenia ESE, determina las acciones para asumir, reducir y mitigar el riesgo al igual que establece planes de contingencia ante la materialización del riesgo.

Intención de la Dirección con esta política

Mediante una adecuada administración de los riesgos, la Alta Dirección pretende alcanzar los mejores niveles de conocimiento respecto a la gestión de estos en la entidad, elevar la productividad y garantizar la eficiencia y la eficacia de los procesos organizacionales.

2. Justificación

Con la entrada en vigencia del Modelo Integrado de Planeación y Gestión, (MIPG), que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el sistema de control interno, por lo cual, se hace evidente la importancia de aplicar controles que permitan, a través de las herramientas disponibles por la Función Pública y el Ministerio de Salud y Protección Social, tanto para el manejo de los riesgos, como para su control en todos los niveles de la organización, brindar una seguridad razonable frente al logro de los objetivos, utilizando para ello un enfoque preventivo que permita la identificación y tratamiento de cada uno de los riesgos.

3. Objetivos

3.1 Objetivo General

Definir e implementar una metodología que permita la identificación y tratamiento de todo tipo de riesgos institucionales (administrativos y asistenciales), con el propósito de evitar la materialización de ellos y el logro de los objetivos institucionales.

3.2 Objetivos específicos

- Adoptar una herramienta institucional que permita determinar los roles y responsabilidades de cada uno de los servidores de la entidad (esquema de las líneas de defensa) en los riesgos de gestión.
- Realizar una adecuada gestión del riesgo y control a los mismos, que permitan a la Alta Dirección tener una seguridad razonable en el logro de sus objetivos.
- Identificar los posibles fallos que se puedan presentar durante la atención en salud a través de la adopción de acciones correctivas o preventivas que permitan asegurar que todas las posibilidades de fallo hayan sido consideradas.

4. Glosario

Aceptación del riesgo: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Administración de riesgos: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar con sus

diferentes elementos le permite a la entidad pública, auto controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

AMFE / AMEF: Análisis Modal de Fallos y Efectos.

Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Apetito al riesgo: Magnitud y tipo de riesgo que la entidad está dispuesta a buscar o retener.

Atención en salud: Servicios recibidos por los individuos o las poblaciones para promover, mantener, monitorizar o restaurar la salud.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

CICCI: Comité Institucional de Coordinación de Control Interno.

Compartir el riesgo: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es

posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

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

Consecuencia: Son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Control detectivo: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Control preventivo: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Evento adverso: Es el resultado de una atención en salud que de manera no intencional produjo daño. Los eventos adversos pueden ser prevenibles y no prevenibles.

Factores de riesgo: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgos o tienden a aumentar la exposición, pueden ser internos o externos de la entidad.

Falla de la atención en salud: Una deficiencia para realizar una acción prevista según lo programado o la utilización de un plan incorrecto, lo cual se puede manifestar mediante la ejecución de procesos incorrectos (falla de acción) o mediante la no ejecución de los procesos correctos (falla de omisión) en las fases de planeación o de ejecución. Las fallas son por, definición, no intencionales.

Fallas activas o acciones inseguras: Son acciones u omisiones que tiene el potencial de generar daño o evento adverso. Es una conducta que ocurre durante el proceso de atención en salud por miembros del equipo misional de salud (enfermeras, médicos, regente de farmacia, fisioterapeuta, bacteriólogos, auxiliares de laboratorio, auxiliar de enfermería, odontólogos etc).

Fallas latentes: Son acciones u omisiones que se dan durante el proceso de atención en salud por miembros de los procesos de apoyo (Personal administrativo).

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Identificación del riesgo: Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender

como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Indicio de atención insegura: Un acontecimiento o una circunstancia que pueden alertar acerca del incremento del riesgo de ocurrencia de un incidente o evento adverso.

Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

Nivel de aceptación del riesgo: Son los criterios de aceptación de riesgos establecidos que se emplean durante la etapa de evaluación de riesgos.

NPR: Numero de prioridad de riesgo.

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

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.

Riesgos de cumplimiento: Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.

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.

Riesgo de imagen o reputacional: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

Riesgo de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgos estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.

Riesgos gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.

Riesgos operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad

Riesgos financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.

Riesgos tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgos de seguridad digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Seguridad del paciente: Es el conjunto de elementos estructurales, procesos, instrumentos y metodologías basadas en evidencias científicamente probadas que propenden por minimizar el riesgo de sufrir

un evento adverso en el proceso de atención de salud o de mitigar sus consecuencias.

Tolerancia al riesgo: Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Tratamiento del riesgo: Consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

Valoración del riesgo: Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.

Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. Alcance

La Política de Administración de Riesgos es aplicable a todas las áreas y servicios, en todas las sedes de la Entidad (Unidad Intermedia Del Sur y Centros de Salud) y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

6. Riesgos definidos para Red Salud Armenia ESE

Red Salud Armenia ESE por ser una entidad de Salud, requiere de la identificación de riesgos tanto para el área administrativa como asistencial, es por ello, que se adoptaron los lineamientos de la Función Pública "Guía para la administración del riesgo y el diseño de controles en entidades públicas" así como la metodología establecida por el Ministerio de Salud y Protección Social, "Guía técnica Buenas prácticas para la seguridad del paciente en la atención en salud", las cuales se describirán en capítulos separados.

7. Administración del Riesgo y Control Administrativo

7.1 Identificación del Riesgo

7.1.1 Contexto

Para la identificación de los riesgos que pueden afectar los diferentes procesos de la entidad, se contemplan los siguientes factores para cada categoría:

7.1.1.1 Contexto externo

Económicos: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.

Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.

Sociales: Demografía, responsabilidad social, orden público.

Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

Medioambientales: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.

Comunicación Externa: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

7.1.1.2 Contexto Interno

Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

Personal: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.

Procesos: Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

7.1.1.3 Contexto del Proceso

Diseño del Proceso: Claridad en la descripción del alcance y objetivo del proceso.

Interacciones con otros procesos: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

Transversalidad: Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.

Procedimientos Asociados: Pertinencia en los procedimientos que desarrollan los procesos.

Responsables del Proceso: Grado de autoridad y responsabilidad de los funcionarios frente al proceso.

Comunicación entre los procesos: Efectividad en los flujos de información determinados en la interacción de los procesos.

7.2 Valoración de Riesgos

7.2.1 Análisis de Probabilidad

La probabilidad es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos de la entidad, pudiendo entorpecer el desarrollo de sus funciones. La forma de medir su probabilidad y ocurrencia para los distintos tipos de riesgos (gestión, corrupción y seguridad digital), es la siguiente:

Probabilidad:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

7.2.2 Análisis del Impacto

Por impacto se entienden las consecuencias que puede ocasionar a la entidad la materialización del riesgo. De acuerdo con el tipo de riesgo, el impacto se calcula de manera diferente, así:

Criterios para calificar el impacto para riesgos de gestión:

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
1	Insignificante	Impacto que afecte la ejecución presupuestal en un valor ≥0,5% Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5% Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad	No hay interrupción de las operaciones de la entidad. No se generan sanciones económicas o administrativas. No se afecta la imagen institucional de forma significativa
2	Menor	Impacto que afecte la ejecución presupuestal en un valor ≥1% Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1% Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las	Interrupción de las operaciones de la Entidad por algunas horas. Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

		cuales afectan en un valor ≥1% del presupuesto general de la entidad.	
3	Moderado	Impacto que afecte la ejecución presupuestal en un valor ≥5% Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad	Interrupción de las operaciones de la Entidad por un día. Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. Investigaciones penales, fiscales o disciplinarias
4	Mayor	Impacto que afecte la ejecución presupuestal en un valor ≥20% Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la Comisión	Interrupción de las operaciones de la Entidad por más de dos (2) días. Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. Sanción por parte del ente de control u otro ente regulador. Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos
5	Catastrófico	Impacto que afecte la ejecución presupuestal en un valor ≥50% Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la Entidad	Interrupción de las operaciones de la Entidad por más de cinco (5) días. Intervención por parte de un ente de control u otro ente regulador. Pérdida de Información crítica para la entidad que no se puede recuperar. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

Criterios para calificar el impacto para riesgos de seguridad digital

NIVEL	IMPACTO	CONSECUENCIAS CUANTITATIVAS	CONSECUENCIAS CUALITATIVAS
1	Insignificante	Afectación ≥1% de la población. Afectación ≥0,5% del presupuesto anual de la entidad.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
2	Menor	Afectación ≥5% de la población. Afectación ≥1% del presupuesto anual de la entidad.	Afectación leve de la integridad. Afectación leve de la disponibilidad.

			Afectación leve de la confidencialidad.
3	Moderado	Afectación ≥10% de la población. Afectación ≥5% del presupuesto anual de la entidad.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
4	Mayor	Afectación ≥20% de la población. Afectación ≥20% del presupuesto anual de la entidad.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros
5	Catastrófico	Afectación ≥50% de la población. Afectación ≥50% del presupuesto anual de la entidad.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Criterios para calificar el impacto para riesgos de corrupción

Para calificar el impacto de los riesgos de corrupción, se debe dar respuesta a las siguientes preguntas:

Pregunta. Si el riesgo de corrupción se materializa, podría…	SI	NO
1 ¿Afectar al grupo de funcionarios del proceso?		
2 ¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3 ¿Afectar el cumplimiento de misión de la entidad?		
4 ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5 ¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6 ¿Generar pérdida de recursos económicos?		
7 ¿Afectar la generación de los productos o la prestación de servicios?		
8 ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9 ¿Generar pérdida de información de la entidad?		
10 ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11 ¿Dar lugar a procesos sancionatorios?		
12 ¿Dar lugar a procesos disciplinarios?		

13 ¿Dar lugar a procesos fiscales?		
14 ¿Dar lugar a procesos penales?		
15 ¿Generar pérdida de credibilidad del sector?		
16 ¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17 ¿Afectar la imagen regional?		
18 ¿Afectar la imagen nacional?		
19 ¿Generar daño ambiental?		

La calificación de impacto de riesgos de corrupción no tiene los niveles de insignificante y menor, y se califica de la siguiente manera:

Nivel	Calificación	Consecuencia
MODERADO	Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado	Genera medianas consecuencias sobre la entidad
MAYOR	Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.	Genera altas consecuencias sobre la entidad.
CATASTRÓFICO	Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.	Genera consecuencias desastrosas para la entidad

7.2.2.1 Niveles de tratamiento de los riesgos y mapa de calor

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión (Proceso, Producto y Proyecto) y de Corrupción	Baja	Se **ASUMIRÁ** el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza seguimiento cuatrimestral.
	Medio o Moderada	Se deberá incluir este riesgo en el Mapa de riesgos Institucional, se establecerán acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento cuatrimestral.
	Alta	Se deberá incluir el riesgo en el Mapa de riesgos Institucional y se establecerán acciones de control preventivas que permitan **EVITAR** o **COMPARTIR** la materialización del riesgo. Se hace seguimiento cuatrimestral.
	Extremo o Catastrófico	Si bien el primer llamado es a abandonar la actividad que genera el riesgo, no se considera prudente, por ahora eliminar actividades dado que las mismas pueden generar el no cumplimiento de su misión, por lo que se incluirá el riesgo en el Mapa de riesgos Institucional, se establecerán acciones de control preventivas y correctivas que permitan **EVITAR** o **COMPARTIR** la

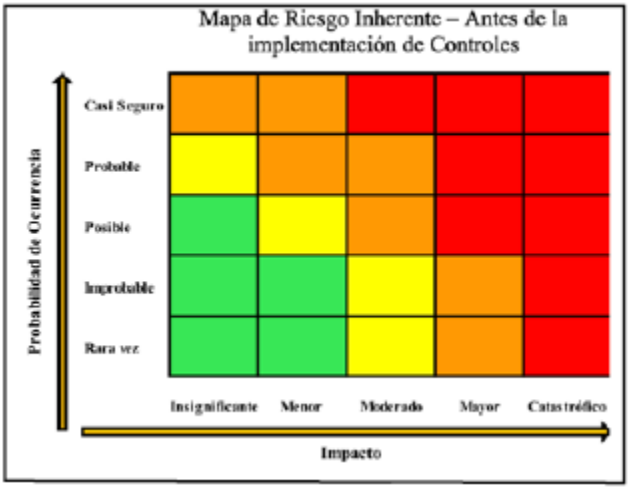
		materialización del riesgo. Se hace seguimiento cuatrimestral.

Se debe tener en cuenta que, en los casos de riesgos de corrupción, estos no pueden ser aceptados.

Adicionalmente, se deberán documentar al interior de los procesos planes preventivos (antes de que ocurra el evento) y contingencia (después de que ocurra el evento) para tratar el riesgo materializado, con criterios de oportunidad, evitando el menor daño en la prestación de los servicios; estos planes estarán documentados.

La valoración de los riesgos se realiza multiplicando la calificación de la **Probabilidad** por la calificación del **Impacto** dando como resultado los niveles de severidad del riesgo:

Mapa de Calor



Nivel de severidad del riesgo:

BAJO	Aceptar riesgo
MEDIO	Aceptar o reducir riesgo
ALTO	Reducir, evitar, compartir riesgo
EXTREMO	Evitar, reducir, compartir riesgo

7.2.2.2 Clasificación del Riesgo

Existen dos tipos de riesgo para su tratamiento, los cuales se detallan a continuación:

Riesgo Inherente (antes de controles): Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. El tratamiento se realiza mediante la definición de una serie de acciones o controles, los cuales tienen un responsable y una fecha para el seguimiento, buscando de esta forma asegurar la correcta administración de los riesgos. Esta información se puede evidenciar en el mapa de riesgos de la entidad. Para esto, la Política de Riesgos de Red Salud Armenia ESE establece los principios para dar correcto tratamiento de los riesgos, mediante el establecimiento de planes de acción estratégicos y asegurando la continuidad del proceso.

Riesgo Residual (después de controles): El riesgo residual es el riesgo resultante después de aplicar los controles necesarios para su mitigación y prevenir su ocurrencia. El tratamiento de estos riesgos se clasifica de acuerdo con el nivel de severidad.

De acuerdo con la probabilidad e impacto de los riesgos y a los controles aplicados se evalúa el riesgo residual y dependiendo de este resultado se analiza si los riesgos (i) se asumen (ii) se reducen (iii) se comparten o transfieren, o (iv) se evitan. Teniendo en cuenta lo anterior, Red Salud Armenia ESE, ha establecido seguimientos con cierta periodicidad en cada uno de sus procesos de control, donde se evidencia también el responsable.

7.3 Periodicidad para el seguimiento

Se deberá incluir la administración de riesgos dentro de los sistemas de gestión organizacional para facilitar la apropiación de este tema, y se seguirá realizando el seguimiento el cual estará a cargo de cada líderes de área o servicio y su equipo de trabajo, quien de forma cuatrimestral deberá diligenciar el Formato Mapa de Riesgos Institucionales o de Corrupción código ES-PL-FO-005, y remitirlo a la oficina de Planeación quien se encargará de consolidar y enviar a la oficina de Control Interno para que se realice el respectivo seguimiento al cumplimiento.

Anualmente se deberá revisar el mapa de riesgos completo de la Entidad, en los plazos establecidos dentro del Plan Anticorrupción y de Atención al Ciudadano de cada vigencia, para lo cual se tomará como insumo, las auditorías realizadas por la Oficina de Control Interno y Organismos de Control. Esta revisión será realizada por los líderes de área o servicio y con el acompañamiento de su equipo de trabajo, de esta manera se ajustará el mapa de riesgos, de acuerdo con los cambios normativos sectoriales y nacionales.

Se deberá presentar cuatrimestralmente los resultados del análisis de riesgos a la Alta Dirección, con el fin de evidenciar si se materializó algún riesgo, si es necesario crear alguno nuevo, o si se requiere eliminar alguno que con el tiempo no aplique a la entidad.

Además, se deberá fortalecer el cumplimiento de la presente política a través de capacitaciones establecidas dentro del Plan Anual de Capacitaciones de la entidad.

7.4 Niveles de responsabilidad sobre el seguimiento y evaluación

A partir de las líneas de defensa establecidas dentro del Modelo Integrado de Planeación y Gestión, las responsabilidades respecto la gestión, seguimiento y evaluación de los riesgos son las siguientes:

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta dirección y Comité Institucional de Coordinación de Control Interno.	*Establecer y aprobar la Política de Administración del Riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico. *Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. *Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. *Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. *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 en el cumplimiento de los objetivos. *Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. *Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. *Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
Primera Línea	Líderes de Procesos, Áreas o Servicio	*Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso. *Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. *Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. *Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

		*Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos. *Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. *Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
Segunda Línea	Líderes de Procesos, Áreas o Servicio	*Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos. *Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. *Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos. *Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad. *Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos. *Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.
Tercera Línea	Oficina de Control Interno	*Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. *Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. *Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. *Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. *Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. *Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se

		establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

8. Administración del Riesgo y Control Asistencial

La gestión del riesgo identifica y aprovecha oportunidades para mejorar el desempeño y emprender acciones para evitar o reducir las oportunidades de que algo salga mal. La alta dirección de una institución expresa su compromiso permanente de trabajo con la seguridad de sus prácticas clínicas a través de unas actividades de gestión de riesgos; tendientes a analizar los riesgos inherentes a la eficiencia de las operaciones en las actividades de sus procesos y de sus puestos de trabajo para prevenir eventos adversos.

Una potencial falla de un proceso se define como la manera en que el proceso pudiera fallar en cubrir sus requerimientos. Se describe en términos de lo que los clientes internos y externos pueden notar o experimentar. El AMEF es una metodología que se utiliza para gestionar el riesgo de una potencial falla. Describe un grupo sistematizado de actividades que pretende reconocer y evaluar la falla potencial del proceso y sus efectos, e identificar las acciones que puedan eliminar o reducir la posibilidad de su ocurrencia. Por lo tanto, el AMEF completo y bien hecho, debe ser una acción antes del evento y no un ejercicio posterior a los hechos.

8.1 Fases para elaborar AMFE

8.1.1 Definir el Área Objeto de análisis y el equipo de trabajo

Se deberá seleccionar el proceso y procedimiento al cual se va a realizar la intervención, teniendo en cuenta los servicios de mayor vulnerabilidad.

En lo referente al equipo de trabajo se deberá elegir expertos y personas no expertas en el tema, así como considerar incluir a personas representativas en áreas críticas del proceso.

8.1.2 Descripción del Proceso y/o Procedimiento

Se deberá contar con la caracterización del proceso y el procedimiento a analizar, si el procedimiento es muy complejo, se deberá identificar las actividades las cuales serán numeradas, y posterior a ello se definirán las tareas asociadas, las cuales se relacionarán con el número de la tarea adicionando literales por cada actividad. Como se muestra en el siguiente ejemplo: Procedimiento: Llegar a tiempo al trabajo

8.1.3 Análisis de Riesgo

Se hace una lista de todas las posibles causas de falla asignables a cada modo de falla potencial y se tiene en cuenta:

Probabilidad de ocurrencia: Qué tan frecuentemente se proyecta que ocurra la causa o el mecanismo de falla específico. Se estima la posibilidad de ocurrencia en una escala de 1 a 10. Teniendo en cuenta la siguiente tabla:

Efecto	Valoración	Criterio
Casi Nunca	1	Fallo Improbable, la historia dice que no hay fallos.
Remota	2	La probabilidad de fallos es muy poco probable.
Muy Leve	3	Solo muy pocos fallos son probables
Leve	4	Solo alguno pocos fallos son probables.
Baja	5	Solo ocasionalmente es probable.
Media	6	Los fallos son medianamente probable.
Moderadamente Alta	7	Los fallos son moderadamente probable.
Alta	8	Los fallos son altamente probable.

Muy Alta	9	Los fallos son muy altamente probable.
Casi Segura	10	Los fallos son casi seguros. Procedentes de fallos de servicios, diseños, procesos o sistemas similares.

Gravedad: Es una evaluación de la seriedad del efecto del modo de falla potencial en el cliente. Se estima la posibilidad de gravedad en una escala de 1 a 10. Teniendo en cuenta la siguiente tabla:

Efecto	Valoración	Criterio
No	1	No hay efecto.
Muy Leve	2	No hay efecto en el cliente, efecto muy leve en el rendimiento del sistema o servicio.
Leve	3	Hay un mínimo efecto en el cliente. Mínimo efecto muy leve en el rendimiento del sistema o servicio.
Mínimo	4	El cliente detecta un leve ruido. Se ve un leve efecto en el servicio y el rendimiento del sistema o servicio.
Moderado	5	El cliente experimente alguna insatisfacción. Se ve un efecto moderado en el servicio y el rendimiento del sistema o servicio.
Significativo	6	El cliente experimente alguna inquietud. El rendimiento del servicio se ve degradado, pero operativo y fuera de peligro falla parcialmente, pero es operativo.
Mayor	7	Cliente insatisfecho. El rendimiento del servicio se ve gravemente afectado, pero funcional y fuera de peligro. El sistema Diseño, Proceso o Servicio se ve perjudicado.
Extremo	8	Cliente muy insatisfecho. Servicio no operativo, Pero a salvo (Fuera de Peligro). El Sistema o Servicio no está operativo.
Serio	9	Existe un peligro potencial. Capaz de parar el servicio. El fallo depende del tiempo. La conformidad con regulaciones gubernamentales se encuentra en peligro.
Peligroso	10	Efecto peligroso. La seguridad se ve afectada. El fallo sobreviene de repente, sin previo aviso.

Controles actuales del proceso: Se describen los controles que previenen que en cierto grado ocurra el modo de falla o que detectan el modo de falla que se presentará.

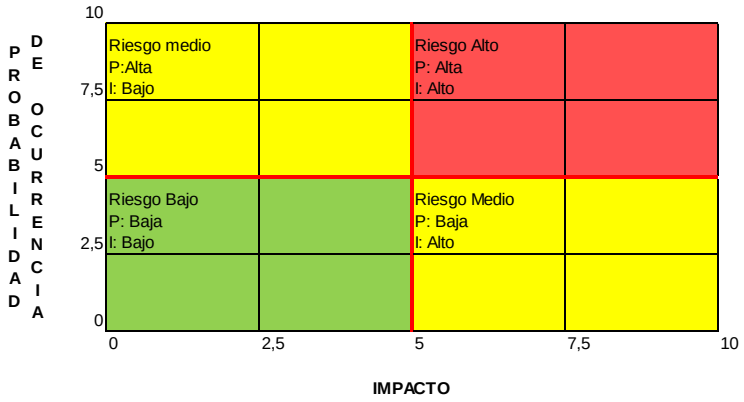
Detección: Evalúan la probabilidad de que los controles de proceso que se proponen detecten una causa potencial o el modo de falla subsecuente. Se usa una escala de 1 a 4.

Efecto	Valoración	Criterio
Alta	1	El error será frecuentemente detectado antes de que llegue al paciente (75-100%)
Moderado	2	El error no será detectado frecuentemente antes de llegar al paciente (40-74%)
Baja o Remota	3	El error raramente será detectado antes de llegar al paciente (6-39%)
Remota	4	La detección no será posible en ningún punto del sistema. (0-5%)

NPR: Este es el valor que se utiliza para ordenar los problemas de diseño o de proceso por orden de importancia, según la Probabilidad X Severidad X Detección, indicando la ocurrencia de que una falla pueda causar un evento adverso y se deben abordar las fallas.

8.1.4 Acciones y Mediciones

Una vez se cuenta con la calificación de Probabilidad y Severidad, se clasificará el riesgo de acuerdo al siguiente mapa de calor:



Para el riesgo bajo, no se requieren acción alguna de intervención, para el riesgo medio, se requiere implementar acciones de control y para el riesgo alto se deberán implementar acciones de mejoría y control.

Con la definición de las acciones a intervenir, están deberán ser analizadas a través de la valoración de Probabilidad X Severidad X Detección, se calculará un nuevo NPR.

Con esto, podremos comparar su "NPR inicial" (antes de aplicar AMFE) con su "NPR final" (el NPR que hayamos fijado como meta después de actuar para reducir la gravedad del modo de fallo).

El objetivo final del análisis AMFE es que se tengan todos los posibles fallos controlados, habiendo actuado para disminuir el NPR de los más graves.

Para obtener el riesgo residual, se evaluará un nuevo mecanismo de detección y control, se calculará un nuevo NPR, así mismo, se obtendrá el porcentaje de reducción del NPR.

Acciones asociadas al control:

Con base en el resultado obtenido se deberá describir las acciones de mejoramiento asociadas al control, la fecha de cumplimiento, responsable, registro, así como el indicador asociado al cumplimiento del mismo.

Se deberá realizar actualización del análisis de riesgos, si se cumple con los siguientes indicativos:

- Al comenzar un ciclo (nueva prestación del servicio).

- Al cambiar las condiciones de funcionamiento, teniendo en cuenta el resultado de los eventos adversos presentados en la institución.
- Cuando se realizan cambios en el diseño del procedimiento o actividades.
- Con la aprobación de nuevas leyes y normativas.
- Según realimentación de los usuarios, que indiquen que hay un problema en la prestación del servicio.