

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Aprobada en Comité Institucional de Coordinación de
Control Interno mediante acta No. 100.1.44.03- 2022
Deroga la Resolución No. 100.16.1-218 de noviembre 27 de 2019

Versión 02
Julio 05 de 2022

INTRODUCCIÓN

La política de Administración del Riesgo en la Red de Salud del Sur Oriente E.S.E. es un documento de nivel estratégico y se establece para asegurar el cumplimiento de la misión, visión, objetivos estratégicos y de proceso permitiendo apoyar la toma de decisiones fortaleciendo el enfoque preventivo y la cultura del control.

La política, está basada en la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 emitida por la Dirección de Gestión y Desempeño Institucional, y está compuesta por el objetivo, alcance, nivel de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

OBJETIVO

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la E.S.E.

GLOSARIO

- Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- Apetito del Riesgo: es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- CICI: Comité Institucional de Coordinación de Control Interno.
- Contingencia: posible evento futuro, condición o eventualidad.
- Continuidad del negocio: capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- Crisis: ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- CGDI: Comité de Gestión y Desempeño Institucional.
- Mapa de Riesgos: documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- MIPG: Modelo Integrado de Planeación y Gestión.
- TIC: Tecnologías de la Información y las Comunicaciones.
- Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos de la Red de Salud del Sur Oriente E.S.E, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

La Red de Salud del Sur Oriente E.S.E. cuenta con una herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, para lo cual el encargado de planeación revisa periódicamente su adecuado funcionamiento, el cargue de información por parte de los diferentes procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar anualmente, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

OBJETIVO DE LA POLÍTICA DE RIESGOS

Alcanzar en los siguientes cuatro (4) años un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, la visión, los objetivos estratégicos y de procesos vigentes.

ALCANCE

Aplica a todos los procesos de la E.S.E, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

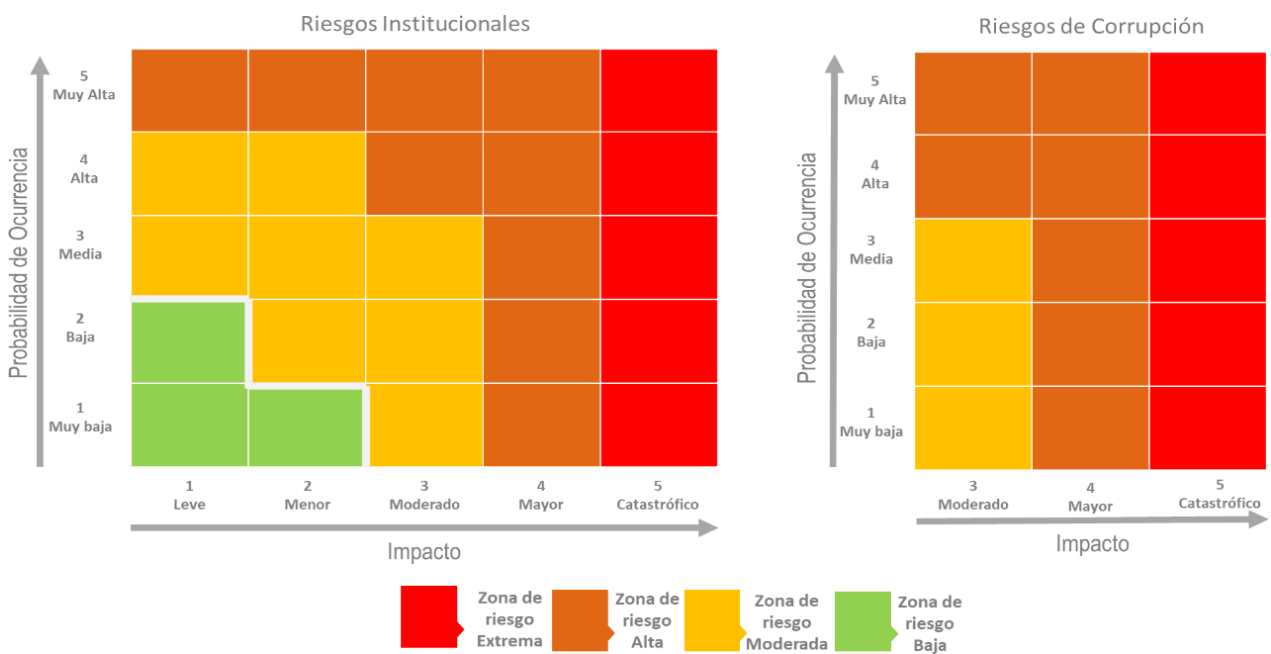
NIVELES DE ACEPTACIÓN DEL RIESGO

Para los riesgos de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto aceptar el riesgo y no se requiere la documentación de planes de acción, salvo que el líder de proceso lo considere pertinente. Estos riesgos se deben monitorear anualmente con el fin de identificar si la zona de riesgo final ha tenido alguna variación.

La Red de Salud del Sur Oriente E.S.E determina que para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

A continuación se presenta la matriz de calificación del nivel de severidad de los riesgos institucionales (gestión y seguridad digital) y los riesgos de corrupción.

Matriz de calificación de nivel de severidad del riesgo



RESPONSABILIDADES

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Responsabilidades de las Líneas de Defensa

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité De Gerencia Comité de Gestión y Desempeño Institucional	- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. - Definir el marco general para la gestión del riesgo. - Recomendaciones de mejoras a la política de operación para la administración del riesgo.
	Comité institucional de coordinación de control interno	- Someter a aprobación del Gerente y Comité Institucional de Coordinación de Control Interno la política de administración del riesgo previamente estructurada por el encargado de Planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. - Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. - Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. - Garantizar el cumplimiento de los planes de la entidad.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Primera Línea	Líderes de Procesos	Los líderes de procesos y proyectos deben: • Asegurar que al interior de su grupo de trabajo se reconozcan los riesgos del proceso. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo y a sus controles. • Asignar responsabilidades al equipo de trabajo para que se implementen los controles y planes de acción del mapa de riesgos del proceso. • Informar al encargado de planeación los cambios de responsables cuando se presenten. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Reportar a planeación los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Informar a planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. • En caso de la materialización de un riesgo no identificado, este debe ser gestionado e incluido en el mapa de riesgo institucional.
	Responsable del proyecto	
	Servidores en general	Los servidores en general deben: • Participar en el diseño de los controles que tienen a cargo. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda Línea	Coordinadores de Gestión Contractual, Administrativa, Financiera, Servicio al Ciudadano, Gestión Documental, Talento Humano y Defensa Jurídica	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • El Abogado de Defensa Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
	Encargado de Planeación	• Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y planes de acción. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Tercera Línea	Oficina de Control Interno	- Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. - Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de acuerdo con la priorización establecida en el Plan Anual de Auditoría y reportar los resultados al CICCI. - Recomendar mejoras a la política de operación para la administración del riesgo. - Recomendar la adopción de riesgos identificados dentro del ejercicio auditor y seguimientos.

Nivel de calificación de probabilidad para riesgos de proceso y seguridad digital

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Nivel de calificación de probabilidad para riesgos de corrupción

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

Niveles de calificación de impacto

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad de Función Pública.

Calificación de impacto para riesgos de proceso y seguridad digital

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la Republica. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

No.	Pregunta:		Respuesta	
	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?			
Nivel	Descriptor	Descripción	Respuestas afirmativas	
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5	
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11	
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19	

Acciones ante los riesgos materializados

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Acciones de respuesta a riesgos

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	• Informar al encargado de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y registrar en la matriz de riesgos su materialización. • Una vez surtido el conducto regular establecido por la E.S.E. y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	• Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión y Seguridad digital	Oficina de Control Interno	• Informar al líder del proceso sobre el hecho encontrado • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.

Seguimiento al mapa de riesgos y controles

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento - Controles
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el mapa de riesgos por proceso.
	Moderada	Se realiza seguimiento a los controles con periodicidad CUATRIMESTRAL y se registran sus avances en el mapa de riesgos por proceso.
	Alta	Se realiza seguimiento a los controles con periodicidad CUATRIMESTRAL y se registran sus avances en el mapa de riesgos por proceso.
	Extrema	Se realiza seguimiento a los controles con periodicidad CUATRIMESTRAL y se registran sus avances en el mapa de riesgos por proceso.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento CUATRIMESTRAL y se registran sus avances en el mapa de riesgos por proceso.	

Finalizada la vigencia el líder del proceso debe evaluar la efectividad de los controles teniendo en cuenta si se materializó el riesgo o no.

Estrategia de seguimiento al plan de acción

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Riesgos de Gestión, y Seguridad digital	Baja	No es necesario realizar plan de acción por que está dentro del nivel de aceptación del riesgo por la Red de Salud del Sur Oriente E.S.E
	Moderada Alta Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y realiza seguimiento a la ejecución de las acciones de manera cuatrimestral, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles.

Política de Administración de Riesgos

VERSIÓN 02

Julio 05 de 2022



CARLOS EDUARDO ARIZABALETA CORRAL
Gerente