NORMA:
SISTEMA DE GESTIÓN DE CALIDAD. NTC ISO 9001: 2015

Elaborado por	Revisado por	Aprobado por
Director de Aseo y Calidad	Representante de Dirección	Gerente

Tabla de Contenido

1 Objetivo

Establecer los lineamientos para la adecuada gestión de riesgos de la Empresa de Obras Sanitarias de Santa Rosa de Cabal **EMPOCABAL E.S.P. – E.I.C.E.** a través de una metodología que permita de manera integral, eficaz, eficiente y efectiva, la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos que pueden afectar el cumplimiento los objetivos estratégicos y de proceso, orientando a la Empresa hacia un nivel de aseguramiento razonable y una estructura de prevención y gestión de riesgos.

2 Alcance

Esta Manual debe ser aplicado por todas las Direcciones de la Empresa.

3 Documentos de Referencia

- Constitución Política de 1991
- Ley 142 de 1994
- NTC ISO 9001 2015
- NTC ISO 27000
- c
- Decreto 1072 de 2015
- NTC 5224 de 2004
- NTC – ISO 31000 de 2011
- Norma Internacional ISO 45001 de 2018

4 Definiciones

Administración 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. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Activo de información: en el contexto de seguridad de la información 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.

Amenaza: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.

Autocontrol: capacidad que tiene cada servidor público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades.

Autoevaluación: comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o

programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.

Bien Público: son todos aquellos muebles e inmuebles de propiedad pública.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

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

Confidencialidad: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

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

Contexto externo: ambiente externo en el cual la organización busca alcanzar sus objetivos.

Control: medida que permite reducir o mitigar un riesgo.

Control preventivo: está diseñado para evitar un evento no deseado en el momento en que se produce.

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

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

Evento: ocurrencia o cambio de un particular conjunto de circunstancias. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un “incidente” o “accidente”.

Establecimiento del contexto: definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo. ∴

Factores de riesgo: son las fuentes generadoras de riesgos.

Fuentes de riesgo externas: son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del riesgo: etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

Impacto: consecuencia o efecto que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Líder o responsable del proceso: persona con la responsabilidad y autoridad para gestionar un riesgo.

Matriz de riesgos: representación final de la probabilidad e impacto de uno o más riesgos de un proceso, plan, proyecto o programa.

Nivel de riesgo/severidad: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo o severidad es la combinación entre Probabilidad y la Consecuencia.

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

Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

Riesgo ambiental: son los riesgos que están relacionados con la responsabilidad y compromiso de la entidad hacia el cuidado del ambiente.

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.

Riesgo estratégico: se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos financieros: se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Riesgo fiscal: es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

Riesgo de fraude: consisten en la posible pérdida financiera, material o reputacional que derivan de acciones, fraudulentas por actores internos o externos de la entidad.

Riesgos de imagen: están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución, considerando el cumplimiento de requisitos legales.

Riesgo inherente: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. Este nivel se determina antes de controles.

Riesgo legal: se refiere al incumplimiento de leyes, normativas y regulaciones de diferente tipo, que son emitidas por el Gobierno Nacional y por otras entidades. ∴ Riesgo operativo: derivados de la definición y ejecución de los procesos, la operación de los sistemas de información y herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.

Riesgo operativo: derivados de la definición y ejecución de los procesos, la operación de los sistemas de información y herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.

Riesgo reputacional: Es aquel que está asociado a los cambios de percepción u opinión sobre la entidad, que tienen sus grupos de valor.

Riesgos de tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgo de seguridad y salud en el trabajo: son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios, contratistas y pasantes.

Riesgos de seguridad de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

5 RESPONSABILIDAD EN LA GESTIÓN DEL RIESGO

Para realizar un análisis y valoración del riesgo que permita mitigar efectivamente los riesgos identificados, la Empresa de Obras Sanitarias de Santa Rosa de Cabal EMPOCABAL E.S.P. – E.I.C.E. tiene en cuenta las siguientes responsabilidades:

Línea de Defensa	Responsable	Responsabilidad frente al Riesgo
	Gerencia 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. • Definir y hacer seguimiento semestral a los niveles de aceptación de riesgos. • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un

Estratégica	Comité Institucional de Gestión y Desempeño	impacto significativo en la operación de la Empresa y que puedan generar cambios en la estructura de riesgos y controles • Analizar los eventos y los riesgos críticos • Realizar seguimiento y análisis semestral a la gestión de riesgos y aplicar mejoras. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.
Primera Línea de defensa	Directores Líderes de procesos	• Identificar, valorar y hacer seguimiento a los riesgos que pueden afectar los procesos, programas, proyectos, planes entre otros, a su cargo y actualizarlos cuando se requiera. • Diseñar, ejecutar y hacer seguimiento a los controles definidos para mitigar los riesgos identificados. • Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • 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 materializan. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles, esto a través de los Subcomités de Control Interno • Reportar a la segunda línea de defensa los riesgos materializados en los procesos, programas, proyectos, y/o planes a su cargo. • Revisar los tratamientos establecidos para cada uno de los riesgos, con el fin de que se implementen y sean eficaces frente a la exposición de riesgo identificado. • Los líderes de Procesos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información.

Segunda Línea de defensa	**Asesor Planeación**	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional y presentarlo para análisis y seguimiento en las instancias correspondientes • Presentar al Comité Institucional de Coordinación de Control Interno el Sistema de Administración de Riesgos que adelanta la Empresa • Acompañar, orientar, entrenar y establecer con los líderes de procesos la identificación, análisis y valoración de los riesgos. • 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 realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. • Monitorear los riesgos y controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Desarrollar procesos de capacitación en temas relacionados con la gestión de riesgos de la Empresa • 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 • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
Tercera Línea de defensa	**Control Interno**	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo de la Empresa, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento

		de los objetivos de los procesos, incluyendo los riesgos de corrupción • Evaluar la eficacia 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, así como el perfil 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 no sea coherente con los resultados de las auditorías realizadas. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados.

6 METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

Las fases para la gestión integral del riesgo de la Empresa de Obras Sanitarias de Santa Rosa de Cabal son: Establecer el contexto, identificación, análisis, evaluación y tratamiento del riesgo y de manera transversal: comunicación, consulta, monitoreo y seguimiento de los riesgos. Estas fases se aplican en la a través de la herramienta establecida para tal fin.

6.1 ESTABLECIMIENTO DEL CONTEXTO:

Se establecen los parámetros internos y externos que se van a considerar para la administración del riesgo en la Empresa de Obras Sanitarias de Santa Rosa de Cabal, se establece el objetivo, el alcance, los roles y responsabilidades con base en la normativa vigente.

La definición o actualización de la política se debe realizar cada vigencia y debe incluir los siguientes criterios:

• El objetivo que se espera alcanzar a partir de la administración de los riesgos.
• El alcance de aplicación, teniendo en cuenta la plataforma estratégica, el modelo de operación por procesos, los recursos, las actividades que se desarrollan en la Empresa para el cumplimiento de sus funciones.

• La tipología de los riesgos que se van a abordar, teniendo en cuenta la normativa aplicable y los modelos internacionales implementados.
• La definición de las responsabilidades y lineamientos para tener en cuenta en cada una de las fases del riesgo establecidas por la Empresa

6.2 IDENTIFICACION DE RIESGOS

Permite conocer los riesgos que pueden afectar el logro de los objetivos o la gestión de Empresa según con la aplicación correspondiente.
La identificación de riesgos consiste en generar una lista de los posibles eventos indeseados que pueden tener impacto en los objetivos estratégicos, proceso, servicios, actividad operativa al cual se le está documentando el riesgo. De igual manera, la identificación de riesgos se realiza de manera conjunta con el Director de cada dependencia, teniendo en cuenta su experiencia, los registros, diagramas de flujo, lluvia de ideas, análisis de sistemas o análisis de escenarios. Para adelantar una adecuada identificación de riesgos es necesario tener en cuenta el análisis de indicadores, los mapas de riesgos anteriores, los resultados de las auditorías internas y externas, los informes de seguimiento y evaluación a la gestión de los procesos y las dependencias, los informes de PQRS y la retroalimentación de los grupos de valor, entre otros. Estas fuentes de información permiten evidenciar la materialización de riesgos, por tanto, es indispensable su análisis al momento de identificar posibles riesgos en los procesos. Lo anterior con el propósito de observar algún riesgo que se haya presentado con anterioridad, cuya evidencia se hubiese identificado en alguna de las fuentes mencionadas. La identificación de riesgos es desarrollada mediante el análisis y diligenciamiento de la siguiente información:

6.3 CLASIFICACIÓN DEL RIESGO:

Los riesgos se clasifican de la siguiente manera:

• **Estratégicos:** Hace relación a los riesgos de los objetivos e iniciativas estratégicas, se identifican los riesgos asociados a la toma de decisiones en el momento de estructurar la planificación de la entidad y que pueden afectar el cumplimiento de los objetivos estratégicos.

• **Tácticos:** Hace relación a los riesgos de los objetivos de los procesos y productos (bienes o servicios) generados por la Empresa para la gestión por parte de la primera línea.

• **Operativos:** hace relación a los riesgos asociados a activos de información (en función de tipo y criticidad de activo, según inventario de activos), infraestructura física y actividades.

6.4 DESCRIPCIÓN DEL RIESGO:

En este campo se describe el riesgo considerando las siguientes indicaciones:

- Redactar de forma clara y concisa para expresar específicamente el evento indeseado que podría presentarse.
- Considerar los eventos que pueden impedir, afectar, degradar o retrasar el logro de los objetivos o la gestión a nivel estratégico, táctico u operativo según el nivel de aplicación.

NOTA: Tener en cuenta la descripción de los tipos de riesgos considerados en en la Empresa de Obras Sanitarias de Santa Rosa de Cabal. MEPOCABAL E.S.P. – E.IC.E. No incluir la causa ni el efecto en la redacción del riesgo, sólo la situación o evento indeseado.

6.5 TIPO DE RIESGO

En esta columna selecciona con X la opción que se adhiera a la siguiente tipología de riesgos.

• **Riesgo estratégico:** están relacionados con la planificación, diseño y conceptualización de la Entidad por parte de la Gerencia, en relación con su marco estratégico: misión, visión, cumplimiento de los objetivos estratégicos y la definición de políticas.

• **Riesgo operativo**: derivados del funcionamiento de los sistemas de gestión institucional, la definición y ejecución de los procesos, herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre las direcciones.

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

• **Riesgo legal:** se refiere al incumplimiento de leyes, normativas y regulaciones de diferente tipo, que son emitidas por el Gobierno Nacional y por otras entidades.

• **Riesgo reputacional:** se refiere a los cambios en la percepción u opinión sobre la entidad, que tienen sus grupos de valor.

• Riesgo de fraude: actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un participante interno de la entidad, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

• Riesgo fiscal: se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

• Riesgo de tecnología: están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

• **Riesgo ambiental Natural:** es un daño o catástrofe potencial en el medio ambiente, debido tanto a un fenómeno natural.

• **Riesgo ambiental Antrópico:** son afectaciones directamente atribuibles a la acción humana sobre los elementos de la naturaleza (agua, aire y tierra) y sobre la población que ponen en peligro la integridad física y la calidad de vida de las comunidades.

• **Riesgo de seguridad y salud en el trabajo:** son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios, contratistas y pasantes.

6.6 Causas:

se enumeran los medios, circunstancias y/o agentes que generan el riesgo identificado o que propician su materialización. Estas causas pueden ser intrínsecas (internas) al ser atribuidas a personas, métodos, equipos, materiales e instalaciones, directamente involucradas en el proceso, es decir debilidades de la entidad, o extrínsecas (externas) cuando provienen del entorno en el que se desarrolla el proceso, es decir amenazas.

7. ANALISIS DEL RIESGO

Posterior a la identificación, se realiza el análisis del riesgo puro o inherente donde se evalúan los riesgos sin considerar los controles que pudieran existir, analizando la naturaleza, las condiciones y la forma como se desarrolla la gestión en la entidad. Para ello, se determina la probabilidad de ocurrencia y el impacto de la materialización de cada riesgo identificado, en un escenario hipotético en donde los controles para prevenir o mitigar el riesgo no existen o no se aplican

7.1 ANALISIS DE LA PROBABILIDAD

Se establece la probabilidad de ocurrencia con la que se ha presentado o puede presentarse el riesgo antes de controles, seleccionando un nivel de probabilidad en una escala de 1 (muy baja), 2 (baja), 3 (moderada),4 (alta) y 5 (muy alta).
Para seleccionar la calificación más adecuada se cuenta con varios criterios de análisis:

Descripción: basada en una escala cualitativa para establecer el nivel de probabilidad de materialización del riesgo.
Frecuencia: escala cuantitativa que se basa en él % de materialización del riesgo y por tanto aplica cuando se cuenta con medición de la ocurrencia de eventos de materialización, es decir datos históricos.
Frecuencia para actividades continuas: escala cualitativa que presenta criterios de calificación de la probabilidad de materialización de eventos cuando las actividades que originan el riesgo son continuas.
Frecuencia para actividades o eventos ocasionales: escala cuantitativa que presenta criterios para calificar la probabilidad de materialización de eventos cuando las actividades que originan el riesgo no son continuas ni frecuentes.
Frecuencia en función de la exposición: esta escala ofrece criterios cualitativos para calificar la probabilidad de ocurrencia de un riesgo, asociándola con el nivel de exposición al peligro que lo genera; apoya especialmente, aunque no de forma exclusiva, el análisis de riesgos para la seguridad y salud en el trabajo.
Frecuencia en función de especialización requerida para que el riesgo ocurra: escala cualitativa que aplica básicamente a riesgos de seguridad de la información, mediante criterios que indican el nivel de especialización necesario para explotar la vulnerabilidad que origina el riesgo.

7.2 ANALISIS DEL IMPACTO

Establece la magnitud de los efectos ocasionados con la materialización del riesgo antes de controles, seleccionando un nivel de impacto en una escala de 1 (leve), 2 (menor), 3 (moderado), 4 (mayor), y 5 (catastrófico). Para realizar la calificación más adecuada se cuenta con los siguientes criterios establecidos:

Criterios transversales

• **Afectación en cumplimiento y resultados:** escala para calificación de impactos en el negocio, considerando la operación y los resultados de la gestión Empresarial.

• **Afectación a grupos de valor:** escala para calificación de impactos que afectan de manera directa a los grupos de valor generando quejas, insatisfacción.

• **Afectación reputacional o de imagen:** escala para calificación del impacto en la reputación, imagen y/o credibilidad de la dependencia y procesos.

• **Afectación económica/fiscal:** escala para calificación del impacto económico o fiscal, en función de la afectación como sobrecostos, pérdidas financieras, variaciones de presupuesto, intereses, multas o sanciones pecuniarias.

• **Afectación disciplinaria/legal:** escala para calificar el impacto disciplinario hasta las posibles implicaciones legales (penales o fiscales), sancionatorias, intervención de órganos de control.

Criterios específicos

• **Afectación SST:** escala para calificar el impacto en la salud y seguridad de los colaboradores en términos de lesiones, enfermedad e incapacidad.

• **Impacto ambiental:** escala para calificar el impacto en función de la intensidad, extensión y reversibilidad de los aspectos ambientales.

• **Intensidad:** Grado de transformación que el impacto ambiental puede causar sobre el ambiente. Extensión: refleja la fracción del medio afectado respecto al entorno total Reversibilidad: capacidad del medio para recuperarse mediante mecanismos de autorregulación en el corto, mediano o largo plazo. El impacto es irreversible cuando el tiempo de permanencia a partir del cese de la actividad es superior a 15 años.

• **Afectación en la seguridad de la información:** escala para calificar el impacto de los riesgos de seguridad de la información en función de la criticidad de los servicios, procesos, elementos o funciones afectadas por la disrupción, la cual se califica de manera consolidada a partir de la valoración de la propiedad del activo que haya sido afectado: confidencialidad, integridad y disponibilidad.

7.3 VALORACION DEL RIEGOS

El nivel o zona de riesgo se determina por la combinación de probabilidad y efecto/impacto, resultado que se ubica en alguna zona del mapa de calor. A continuación, se observa el Mapa de Riesgo que utilizará la Empresa de Obras Sanitarias de Santa Rosa de Cabal.

		IMPACTO				
		LEVE	MENOR	MODERADA	MAYOR	CATASTROFICO
PROBABILIDAD		1	2	3	4	5
MUY ALTA	5	5	10	15	20	25
ALTA	4	4	8	12	16	20
MEDIA	3	3	6	9	12	15
BAJA	2	2	4	6	8	10
MUY BAJA	1	1	2	3	4	5

Ilustración 2 Mapa de calor valoración del Riesgo

7.4 CLASIFICACIÓN DEL RIESGO

Una vez obtenidos los valores de riesgo, clasifique cada evento según su nivel de riesgo. Use una tabla donde los resultados de la multiplicación sean interpretados en cuatro categorías y asigne un color cada uno:

Zona de riesgo baja, representa un inconveniente menor.
Zona de Riesgo Moderada debe ser considerado, pero con menor urgencia.
Zona de Riesgo Alta urgencia necesita atención significativa.
Zona de Riesgo Extrema, requiere atención inmediata y protocolos estrictos.

		IMPACTO				
		LEVE	MENOR	MODERADA	MAYOR	CATASTROFICO
PROBABILIDAD		1	2	3	4	5
MUY ALTA	5	Moderada	Moderada	Alta	Extrema	Extrema
ALTA	4	Baja	Moderada	Alta	Extrema	Extrema
MEDIA	3	Baja	Moderada	Moderada	Alta	Extrema
BAJA	2	Baja	Baja	Moderada	Moderada	Alta
MUY BAJA	1	Baja	Baja	Baja	Baja	Baja

Ilustración 3 Fase de análisis

7.5 EVALUACION DEL RIESGO

Para esta fase se identifican los controles existentes, se evalúan y califican según criterios que permiten determinar su robustez y a partir de ello se valora el riesgo.
Los criterios definidos para evaluación de los controles existentes en la Empresa de Obras Sanitarias de Santa Rosa de Cabal EMPOCABAL E.S.P. – E.I.C.E. son:

Descripción del control	Control se define como una medida de reduce o mitiga la causa generadora del riesgo.
Tipos de Control	Hace referencia a la naturaleza y función del control. Los tipos de control son los siguientes: • **Preventivos:** son aquellas acciones encaminadas a eliminar las causas generadoras de un riesgo, de tal manera que eviten o disminuyan su ocurrencia o materialización. • **Correctivos:** son aquellas acciones que permiten el restablecimiento de la actividad, después de ser detectada la materialización del riesgo. • **Detectivos:** son aquellas acciones que permiten verificar o alertar sobre la posible materialización del riesgo. Para la eliminación de los peligros y la reducción o control de los riesgos para la Seguridad y Salud en el Trabajo, se utiliza la siguiente Jerarquización de los Controles: • **EPP:** uso de elementos de protección personal: Orientados a disminuir el impacto del peligro en la persona. •**Administrativo:** establecer políticas, procedimientos, prácticas del trabajo y programas de entrenamiento para reducir la exposición del riesgo. Pueden prevenir o detectar la presencia del riesgo. • **Ingeniería:** controles técnicos o de infraestructura que se aplican para aislar a las personas del peligro. Pueden ser preventivos o detectivos. • **Sustitución:** controles orientados a remplazar lo peligroso por una condición de menor grado de peligro. • **Eliminación:** controles orientados a eliminar el peligro.
Clase de Control	Hace referencia a la manera en que se ejecuta el control: • **Control automático:** es aquel que funciona por sí solo, sin ayuda humana, generalmente está asociado a un sistema o tecnología informática. • **Control semiautomático**: ejerce su función a través de aplicativos o tecnología, pero requiere de la interacción humana para su funcionamiento. • **Control manual**: es aquel que se activa y funciona con acción humana.
Nivel de documentación del control	Esta información permite identificar si el control está documentado y si se conservan los soportes de su aplicación. Las opciones disponibles para seleccionar son: • Documentado y con soportes o evidencia de su aplicación. • Documentado, sin soportes de aplicación. • No documentado, con soportes de aplicación. • No documentado.
Definición de la responsabilidad del control	Se indica si la responsabilidad por la aplicación del control está asignada.

Frecuencia de aplicación del control	se selecciona de la lista desplegable la frecuencia con la cual es aplicado el control, las opciones son: • **Permanente:** cuando el control se aplica continuamente aun cuando la actividad que genera el riesgo no se esté ejecutando. • **Periódica:** cuando el control se aplica habitualmente bajo una frecuencia establecida (semanal, mensual, trimestral, semestral, anual, etc.). •**Cada vez que se realiza la actividad:** se selecciona cuando el control se activa con la ejecución de la actividad generadora del riesgo. • **Aleatoria o no definida:** cuando no se ha establecido una frecuencia para el control o no se ha aplicado regularmente o el control se aplica sobre una muestra seleccionada.
Eficacia del control en términos de su utilidad según el tipo de control	se valora si el control es útil siempre o algunas veces, para prevenir, corregir o detectar la materialización de un riesgo según el tipo de control seleccionado previamente.

7.6 VALORACION DEL RIESGO

Esta valoración utiliza la evaluación de los controles realizada en la fase de evaluación del riesgo, para determinar si con ellos se reduce la probabilidad de materialización del riesgo o el impacto que se calificó en la valoración del riesgo antes de controles (riesgo inherente), determinando así el riesgo no cubierto por los controles establecidos (riesgo residual)

7.7 TRATAMIENTO DEL RIESGO

Una vez realizado el análisis de riesgos y la evaluación de controles se establece el riesgo residual, para este se debe identificar la opción para su tratamiento teniendo en cuenta la siguiente tabla*:*

Zona de Riesgo	Color	Evitar o prevenir el riesgo	Reducir o mitigar	Reducir el riesgo controles ingeniería	Reducir el riesgo EPP	Compartir o transferir	Asumir	Compensar	Corregir:
Extremo		X	X	X	X	X		X	X
Alto		X	X	X	X	X		X	X
Moderado		X	X	X	X	X	X	X	X
Bajo						X	X		

La opción seleccionada debe estar acorde con las necesidades y posibilidades de manejo.
El tratamiento para el respectivo riesgo se registra en la matriz, según se explica a continuación:

• **Evitar o prevenir el riesgo:** tomar las medidas encaminadas para impedir la ejecución de la actividad que genera el riesgo / acciones encaminadas a evitar los impactos y efectos negativos que pueda generar la entidad sobre el ambiente.

• **Reducir o mitigar:** tomar las medidas que permitan mitigar o atenuar la probabilidad de materialización del riesgo, puede ser mediante acciones de naturaleza preventiva, correctiva o de mejora, fortalecimiento de controles existentes o la sustitución de un peligro por otro que no genere riesgo o que genere un riesgo de menor significancia / acciones dirigidas a minimizar los impactos negativos generados por la entidad sobre el medio ambiente.

Reducir el riesgo mediante controles administrativos: tomar medidas encaminadas a disminuir la probabilidad de materialización del riesgo a través de decisiones administrativas que fortalezcan el proceso. En la gestión de riesgos de seguridad y salud en el trabajo, incluyen medidas que tienen como fin reducir el tiempo de exposición al peligro y acciones de señalización, advertencia, demarcación de zonas de riesgo, implementación de sistemas de alarma, diseño e implementación de procedimientos y trabajos seguros, controles de acceso a áreas de riesgo, permisos de trabajo, entre otros.

• **Reducir el riesgo mediante controles de ingeniería**: decisiones encaminadas a disminuir la probabilidad a través del rediseño de los procesos, así como las medidas técnicas para controlar peligros de seguridad y salud en el trabajo en su origen (fuente) o en el medio.

• **Reducir el riesgo mediante el uso de Elementos de Protección Personal (EPP):** tomar medidas basadas en el uso de dispositivos, accesorios y vestimentas con el fin de proteger las personas contra posibles daños a su salud o su integridad física derivados de la exposición a los peligros en el lugar de trabajo; estas medidas deben ser complementarias a los controles administrativos o de ingeniería.

• **Compartir o transferir el riesgo:** tomar medidas que reduzcan el efecto de la materialización del riesgo a través del traspaso de las pérdidas a otras organizaciones (externas e internas), como en el caso de los contratos de seguros, u otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

• **Asumir un riesgo:** cuando el riesgo es aceptable o tolerable puede quedar un riesgo residual que se decide mantener y en ese caso el Líder del Proceso acepta la pérdida residual. Si la materialización del riesgo que se decide asumir tiene un impacto moderado o de mayor significancia, el Líder del proceso debe definir las acciones o plan de contingencia que aplicará en caso de que el evento ocurra.

• **Compensar:** acciones dirigidas a resarcir y retribuir a la comunidad, región, localidad y al entorno natural por los impactos negativos generados por la entidad, que no puedan ser evitados, corregidos o mitigados.

• **Corregir:** acciones dirigidas a recuperar, restaurar o reparar las condiciones del ambiente afectado por la entidad.

7.8 TRATAMIENTO DEL RIESGO

Una vez valorado el riesgo se deben establecer los planes de tratamiento que contengan las acciones requeridas para cumplir con la opción de tratamiento seleccionada. Para los riesgos que queden en zona alta y extrema, en caso de que se considere necesario se pueden establecer planes de tratamiento para los riesgos que queden valorados en zona moderada y baja. concluidas las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de gestión de la Entidad, se deben clasificar aquellos riesgos cuya calificación residual se encuentren en zonas Altas o Extremas. En estos casos, los procesos en los cuales se obtenga dicha calificación deberán formular un plan de tratamiento de riesgos que contenga las acciones requeridas para mitigar su ocurrencia e impacto dentro de la Empresa.

7.9 . REGISTRO MATERIALIZACION DEL RIESGO

En la ejecución de los procesos se pueden materializar riesgos para la Empresa que deben ser reportados y manejados formalmente según lo descrito a continuación.
La identificación de eventos de materialización se puede dar en el desarrollo de los procesos, en la aplicación de los controles definidos o en la ejecución del monitoreo de riesgos. Cuando un riesgo aplica a varias dependencias de la entidad, quien identifique un evento de materialización debe comunicar al responsable del monitoreo de dicho riesgo o al enlace de su Dirección, para que éste aplique el reporte y manejo según lo indicado a continuación.
Los eventos de materialización de riesgos deben ser registrados la matriz por el responsable del monitoreo del riesgo, de modo que en el Grupo de Planeación consolide la información para el Monitoreo de Riesgos.
El reporte incluye indicar:
• **Fecha del evento de materialización:** día en el que ocurrencia del evento de materialización.
• **Descripción del riesgo**: se debe relacionar el riesgo materializado.
• **Situación de materialización:** se debe incluir la descripción de la situación en la que se presentó el evento de materialización.
• **Responsable que reporta el evento:** se debe relacionar el nombre, rol y la dirección a la que pertenece la persona que realiza el reporte.
• **Acción de manejo del evento:** se debe relacionar las actividades que se ejecutaron para atender la materialización del riesgo.
• **Duración hasta la contención de la situación:** Tiempo de ejecución de las acciones tomadas.
• **Análisis de la materialización del riesgo**: a partir del análisis de la situación, se debe identificar la causa que generó el evento, los controles asociados a esta y las posibles modificaciones del riesgo en términos de probabilidad e impacto.
• **Recomendaciones de ajuste:** a partir del registro realizado por la dependencia, el grupo de planeación puede realizar recomendaciones sobre la identificación, análisis, evaluación o tratamiento del riesgo materializado

Cuando la materialización de un riesgo modifica la calificación de probabilidad o impacto de manera que el nivel de riesgo residual no se mantiene (aumento en la probabilidad de ocurrencia o en el impacto del riesgo), es necesario formular un plan de mejoramiento.

La materialización de los riesgos de Seguridad y Salud en el Trabajo se manejan teniendo en cuenta lo establecido por el Grupo de Recursos Humanos frente a el reporte, registro, investigación y análisis de accidentes e incidentes de trabajo y presuntas enfermedades laborales. La gestión de incidentes de seguridad y privacidad de la información se realiza teniendo en cuenta lo establecido por el Grupo de Tecnología de la Información.

7.10 MONITOREO DEL RIESGO

El monitoreo se realiza de manera semestral por parte de la segunda línea de defensa por medio del siguiente cuestionario que debe ser diligenciado por los enlaces de planeación designados en las dependencias:

1. Fecha de monitoreo
2. ¿Riesgo se materializo durante el periodo?
3. En caso afirmativo describa brevemente como se materializó, sus efectos y que acciones se tomaron para su mitigación y prevención
4. ¿El contexto sobre el cual existe la exposición del riesgo ha tenido algún cambio?
5. ¿Los controles se han aplicado sin novedad?
6. Validación de controles
7. Si el control no fue efectivo haga una breve explicación de porque fallo el control
8. Tiene alguna observación sobre el riesgo
9. Comentario de monitoreo
10. Fecha de próximo monitoreo

Nota: Las preguntas del cuestionario pueden variar teniendo en cuenta las necesidades del monitoreo de la gestión del riesgo de la empresa. Una vez consolidada y validada la información la segunda línea de defensa, se elabora el informe del monitoreo y mide el indicador.

7 Herramientas.

Computador, sumadora.

8 Indicadores

9 Factores de riesgo, normas de seguridad y elementos protección.

10 Control de Producto no conforme, acciones Preventivas y Correctivas

Producto No Conforme:

11 Anexos

11.1 Anexo 1: MASR- 01-R01 Matriz Identificación De Riesgos

Versión No.	Fecha de vigencia	Descripción del cambio	Numeral de la norma
01	Enero 13 de 2025	Creación del procedimiento	