1. INTRODUCCION

La ESE BelloSalud asume la gestión del riesgo como un pilar fundamental para garantizar la sostenibilidad, la seguridad del paciente y la generación de valor público.

En cumplimiento de los lineamientos del Departamento Administrativo de la Función Pública (DAFP) y el Sistema Obligatorio de Garantía de Calidad (SOGCS), este manual define la metodología para abordar la incertidumbre en todos los niveles de la organización.

Dentro del modelo de supervisión basada en riesgos efectuado por la Superintendencia Nacional de Salud, se establecen instrucciones generales sobre el Sistema Integrado de Gestión de Riesgos y sus Subsistemas de Administración de Riesgos. Estos subsistemas facultan a las entidades para identificar, evaluar, medir, controlar y monitorear eficazmente los riesgos prioritarios a los que se enfrentan en sus operaciones. El propósito de este enfoque es mejorar los resultados en salud de la población, incrementar la satisfacción de los usuarios, asegurar la estabilidad financiera del sistema, fortalecer la confianza de la comunidad en los componentes del SGSSS y prevenir posibles impactos negativos.

Este documento trasciende el cumplimiento normativo; busca instaurar una cultura de prevención donde cada colaborador comprende que gestionar el riesgo es proteger la vida y los recursos. El manual integra bajo una visión sistémica los riesgos de gestión, corrupción, seguridad de la información y seguridad clínica, la metodología presentada se fundamenta en las directrices de la norma ISO 31000:2018 para la gestión del riesgo y se orienta con algunos lineamientos del Departamento Administrativo de la Función Pública, específicamente en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas, versión 7.

2. OBJETIVOS

2.1. Objetivo General

Establecer la metodología institucional para identificar, analizar, valorar y tratar los riesgos que puedan afectar el cumplimiento de la misión y los objetivos estratégicos de la E.S.E. BelloSalud, abarcando la totalidad de los procesos Estratégicos, Misionales, de Gestión de Recursos y de Evaluación de mejora.

2.2. Objetivos Específicos

De acuerdo con el contexto organizacional y la visión estratégica de la ESE, se definen los siguientes objetivos específicos.

1. **Visión Sistémica:** Desarrollar una visión integral y sistémica para la administración y evaluación de riesgos en la E.S.E. BelloSalud, asegurando que todos los subsistemas (Salud, Operativo, Fiscal, Corrupción) y procesos se alineen con la metodología establecida.
2. Aprendizaje Organizacional: Mejorar el aprendizaje organizacional en la administración de riesgos, promoviendo prácticas eficientes y efectivas a través de la capacitación continua y el intercambio de conocimientos entre las áreas operativas (asistenciales y administrativas).
3. Monitoreo Efectivo: Establecer mecanismos de monitoreo y retroalimentación que aseguren la aplicación efectiva de la metodología de gestión de riesgos y su ajuste continuo en función de los resultados y cambios en el entorno normativo o epidemiológico.
4. Cultura de Gestión: Fomentar una cultura de gestión de riesgos dentro de la organización mediante la integración de este componente en la toma de decisiones gerenciales y la planificación estratégica.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

Este manual cubre todos los procesos definidos en el Mapa de Procesos de la ESE BelloSalud, aplicándose a servidores públicos, contratistas y partes interesadas. Cubre desde la identificación de riesgos hasta su monitoreo y seguimiento, con el objetivo de estandarizar las actividades de gestión de riesgos y asegurar la implementación y cumplimiento efectivo de las acciones de mejora.

Estructura de Procesos (Ámbito de Gestión)

La gestión del riesgo se desplegará en los siguientes macroprocesos:

A. Procesos Estratégicos

- **Gerencia:** Riesgos de direccionamiento y toma de decisiones.
- **Planeación Estratégica (MIPG):** Riesgos de cumplimiento de metas y proyectos.
- **Contratación:** Riesgos de corrupción y gestión contractual.

B. Procesos Misionales (Prestación de Servicios de Salud)

Donde se materializa la atención y la seguridad del paciente:

- **Consulta Externa:** Medicina General, Enfermería, Odontología, Optometría, Psicología, Nutrición.

- **Atención de Urgencias:** Atención médica y Transporte Asistencial Básico.
- **Atención de Hospitalización y Partos:** Atención del parto, hospitalización adultos y pediátrica.
- **Promoción y Mantenimiento:** Promoción y Mantenimiento y Vacunación.
- **Apoyo Diagnóstico y Terapéutico:** Laboratorio Clínico, Servicio Farmacéutico, Imágenes Diagnósticas (Ionizantes y Odontológicas).
- **Participación Social:** Sistema de Información y Atención al Usuario-SIAU

C. Gestión de Recursos (Apoyo)

- **Gestión de la Información:** Sistemas y comunicaciones.
- **Talento Humano:** Selección, bienestar y SG-SST.
- **Jurídica:** Defensa judicial.
- **Bienes y Servicios:** Suministros y activos fijos.
- **Gestión Financiera:** Facturación, cartera, contabilidad, tesorería, costos.
- **Gestión Documental:** Archivo clínico y administrativo.

D. Evaluación de Mejora

Control Interno, Control de Gestión y Gestión de Calidad.

4. MARCO CONCEPTUAL (TÉRMINOS CLAVE)

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Amenazas: Todo aquello que tiene el potencial de causar un evento que modifique el cumplimiento de los objetivos.

Fuente de riesgos: Elemento del contexto que, en combinación, tiene el potencial intrínseco de originar un riesgo u oportunidad.

Risk Driver o Desencadenante: Momento en el cual todas las fuentes de riesgo o peligro entran en contacto y desencadenan la ocurrencia de un evento.

Evento y/o suceso: Ocurrencia o cambio en un conjunto particular de circunstancias.

Riesgo: Posibilidad de que ocurra un evento que pueda afectar el cumplimiento de las operaciones de una entidad y que pueda atentar contra los objetivos del Sistema General de Seguridad Social en Salud (SGSSS).

Riesgo inherente: Nivel de riesgo propio de una actividad, evaluado sin considerar el efecto de los mecanismos de mitigación y control.

Nivel de riesgo que permanece después de identificar y evaluar la efectividad de los controles para mitigarlo.

Riesgo residual global: Resultado de combinar todos los riesgos residuales de la entidad, considerando la importancia relativa asignada a cada categoría de riesgo por la institución.

Riesgo significativo: Riesgo identificado y valorado como una posible corrección material que, según el auditor, requiere una consideración especial en la auditoría.

Incertidumbre: Situación en la cual no hay certeza sobre los resultados esperados.

Contexto: Entorno externo e interno en el cual la organización busca definir y alcanzar sus objetivos.

Identificación del riesgo: Proceso de encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos.

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

Causa Inmediata: Circunstancia o situación más evidente que presenta el riesgo, pero que no constituye la causa principal o base para su ocurrencia.

Causa Raíz y/o Sub-causa: Causa principal o básica que corresponde a las razones por las cuales puede presentarse el riesgo.

Descripción del riesgo: Narración, explicación o redacción de cómo puede presentarse un riesgo.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y sus características.

Probabilidad: Posibilidad de ocurrencia del riesgo asociada a la exposición al riesgo del proceso o actividad analizada. También es la forma de medir cualitativa o cuantitativamente la incertidumbre o certidumbre sobre el resultado de un experimento aleatorio.

Frecuencia: Número de sucesos o eventos que ocurren en un periodo de tiempo determinado y en una ubicación específica.

Impacto: Efecto o consecuencia que la materialización del riesgo puede ocasionar a la organización, expresado cualitativa o cuantitativamente.

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

Nivel de riesgo: Valor determinado al combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que tendría sobre la capacidad institucional de alcanzar sus objetivos.

Controles: Medidas prudenciales, preventivas y correctivas que ayudan a contrarrestar la exposición a diferentes riesgos.

Valoración del riesgo: Comparación de los resultados del análisis del riesgo con los criterios establecidos para determinar cuándo se requiere una acción adicional o decisión.

Tratamiento del riesgo: Acciones definidas por la institución para establecer o fortalecer controles que permitan evitar, reducir o transferir un riesgo.

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

Integridad: Propiedad de exactitud y completitud.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera un usuario o proceso autorizado.

Reputación: Percepción general que tienen los agentes relacionados con una organización, como clientes, accionistas, grupos de interés, partes vinculadas o público en general. Esta percepción puede afectar la confianza en la entidad, influenciando su volumen de negocios y su situación general. Puede variar debido a factores como el desempeño, escándalos, menciones en la prensa, entre otros.

Pérdidas: Cuantificación económica que representa la materialización de un evento de Riesgo Operacional, incluyendo los gastos derivados de su atención.

Mapa de calor: Representación gráfica (usualmente en cuadrantes) de los datos de probabilidad e impacto de un riesgo, utilizando colores y números para indicar el nivel de criticidad de dicho riesgo.

Matriz de riesgo: Herramienta metodológica que permite visualizar un inventario de los riesgos de manera ordenada y sistemática, definiéndolos, evaluándolos, priorizándolos y estableciendo los controles y acciones de manejo específicas.

Perfil de riesgo: Resultado consolidado de la medición de los riesgos a los que se ve expuesta una entidad.

Monitoreo: Verificación, supervisión, observación crítica o determinación continua de los riesgos con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Lineamientos generales del SIGR: Declaración de la alta dirección, intenciones generales y compromisos de la organización respecto a la gestión de riesgos.

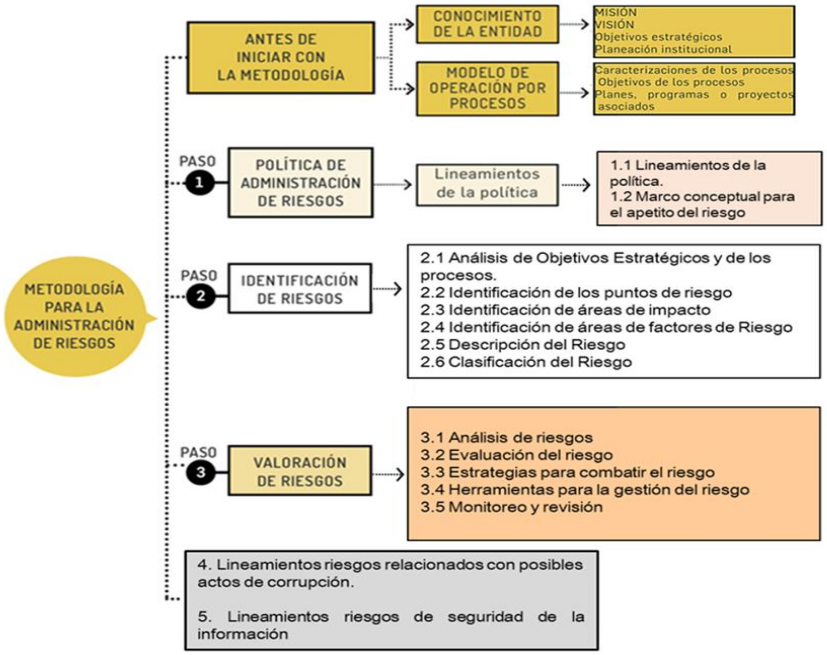
Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Amenazas: Todo aquello que tiene el potencial de causar un evento que modifique el cumplimiento de los objetivos.

Fuente de riesgos: Elemento del contexto que, en combinación, tiene el potencial intrínseco de originar un riesgo u oportunidad.

5. METODOLOGÍA DE ADMINISTRACIÓN DEL RIESGO

La ESE BelloSalud adopta la metodología basada en la norma ISO 31000 y la Guía DAFP, con cumplimiento del ciclo PHVA:



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6. LINEAMIENTOS GENERALES DEL SIGR

La Alta Dirección de la **ESE Bellosalud**, plenamente consciente de su responsabilidad frente a la protección de los recursos públicos y la seguridad del paciente, ha definido los lineamientos generales, compromisos y herramientas necesarios para garantizar una gestión integral de riesgos eficiente, efectiva y oportuna.

El propósito fundamental de estos lineamientos es minimizar cualquier desviación o efecto nocivo que pueda impactar el logro de los objetivos estratégicos, la prestación del servicio y el cumplimiento de las obligaciones contractuales y normativas de la institución. Estos Lineamientos Generales, articulados con el presente Manual, constituyen la **Política de Administración y Gestión de Riesgos** de la entidad, la cual es de obligatorio conocimiento y aplicación para todos los colaboradores y partes interesadas.

7. PROCESO PARA LA GESTIÓN DEL RIESGO

En la ESE Bellosalud, el proceso de gestión del riesgo se entiende como la aplicación sistemática y estructurada de políticas, procedimientos y prácticas en cada una de las etapas del ciclo de gestión: comunicación y consulta, establecimiento del contexto, evaluación (identificación, análisis y valoración), tratamiento, seguimiento, revisión y registro del riesgo.

Reconocemos que este proceso no es estático; por el contrario, considera la naturaleza dinámica y variable del comportamiento humano y de la cultura organizacional propia de una institución prestadora de salud. A continuación, se detallan sus componentes esenciales:

7.1. Comunicación y Consulta

La gestión de riesgos en la ESE Bellosalud es un proceso eminentemente participativo. Promovemos el intercambio claro de información entre todos los actores involucrados (colaboradores, usuarios, entes de control), quienes aportan juicios de valor sobre los riesgos basados en su conocimiento técnico, experiencia diaria y percepción del entorno.

El propósito de este componente es asegurar que las partes interesadas comprendan la naturaleza del riesgo, los fundamentos sobre los cuales la Alta Dirección toma decisiones y la justificación de las acciones específicas implementadas.

- La Comunicación busca elevar la toma de conciencia y la comprensión transversal del riesgo en la ESE

- La Consulta tiene como fin obtener retroalimentación e información valiosa del personal operativo y los usuarios para apoyar una toma de decisiones informada y asertiva.

7.2. Establecimiento del Contexto

En la ESE Bellosalud, entendemos que la gestión del riesgo no ocurre en el vacío. Por ello, definimos con claridad el entorno en el cual buscamos alcanzar nuestros objetivos estratégicos y misionales:

Contexto Externo: Analizamos las variables fuera de la institución que pueden afectar nuestra operación y sostenibilidad:

- **Entorno Normativo y Legal:** Cumplimiento de los lineamientos del Ministerio de Salud, Supersalud, DAFP y la Alcaldía de Bello.
- **Entorno Social y Cultural:** Perfil epidemiológico de la ESE y sus sedes, necesidades de los usuarios y expectativas de la comunidad.
- **Entorno Financiero y Económico:** Flujo de recursos del SGSSS, contratación con EAPB y situación económica del sector salud.
- **Entorno Tecnológico y Natural:** Avances en tecnología biomédica, sistemas de información y riesgos ambientales o de desastres naturales que puedan afectar la infraestructura hospitalaria.
- **Partes Interesadas:** Relación con usuarios, entes de control, proveedores y la comunidad en general.

Contexto Interno: Evaluamos los factores propios de la ESE que influyen en nuestra capacidad para gestionar el riesgo:

Gobierno y Estructura: Directrices de la Junta Directiva, la Gerencia y la estructura organizacional definida en el Mapa de Procesos.

- **Políticas y Objetivos:** Alineación con la Plataforma Estratégica, la Política de Humanización y el Modelo de Atención.
- **Recursos y Capacidades:** Disponibilidad y competencia del Talento Humano (asistencial y administrativo), infraestructura física, equipos biomédicos, insumos y solvencia financiera.
- **Cultura y Procesos:** Clima organizacional, sistemas de información (Historia Clínica, ERP) y la fluidez en la toma de decisiones.

7.3. Identificación del Riesgo

Esta etapa es crucial para la ESE Bellosalud, pues su objetivo es detectar, reconocer y describir los riesgos que pueden facilitar o impedir el logro de nuestros objetivos institucionales, independientemente de si su origen está bajo nuestro control directo o no.

Para una identificación efectiva, partimos del contexto estratégico y de la caracterización de cada proceso (Misionales, Estratégicos, Gestión de recursos y Evaluación de mejora). Analizamos factores internos y externos, así como las amenazas y vulnerabilidades que podrían materializarse en eventos adversos (clínicos o administrativos).

Aplicamos las siguientes fases metodológicas para asegurar un análisis integral:

Análisis de Objetivos: Revisamos qué busca lograr cada proceso (ej. "Prestar atención oportuna en Urgencias") para identificar qué podría impedirlo.

Identificación de Puntos de Riesgo: Determinamos en qué actividades específicas del flujo del proceso (ej. "Triage", "Dispensación de medicamentos") existe mayor probabilidad de falla.

Identificación de Áreas de Impacto: Definimos si la consecuencia sería clínica (seguridad del paciente), financiera, jurídica o reputacional.

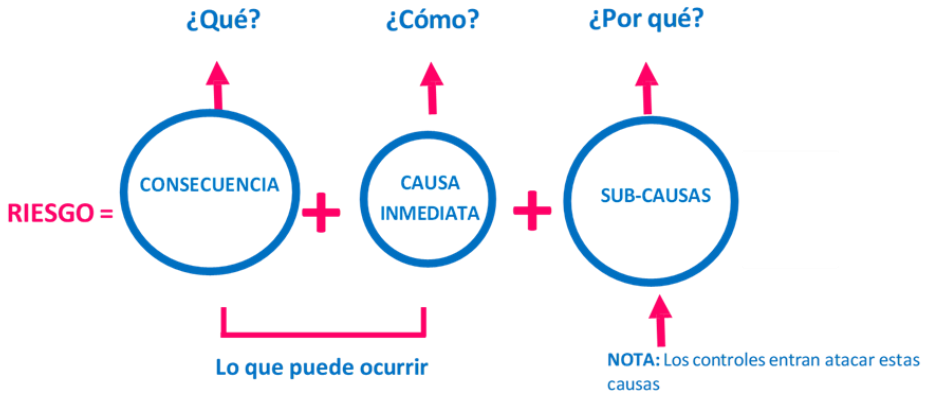
Identificación de factores de riesgo: Son las fuentes generadoras de riesgos.

CONTEXTO EXTERNO: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad	**CAMBIOS ECONÓMICOS/POLÍTICO/MERCADO:** Afecta la estabilidad financiera y la demanda de servicios.
	MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	TERCEROS: Aborda los riesgos asociados con la interacción y dependencia de entidades externas.
	PROVEEDORES: Impacta la calidad y continuidad de los insumos y servicios necesarios para operar.
	CAMBIOS REGULATORIOS: Factor que puede introducir nuevas obligaciones y requerir ajustes operativos.
	COMUNICACIÓN EXTERNA: Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la institución
	EVENTO EXTERNO: Atentados, vandalismo, asalto, suplantación, orden público.
CONTEXTO INTERNO: Se determinan las características o aspectos esenciales del ambiente en cual la organización busca alcanzar sus objetivos.	**FINANCIEROS:** Presupuesto de funcionamiento, recursos de inversión, capacidad instalada.
	TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional, capacitación, rotación y bienestar.
	PROCESOS: Esencial para la eficiencia y seguridad en la prestación de servicios tanto asistenciales como administrativos, capacidad, diseño, ejecución, entradas, salidas, gestión del conocimiento.

	TECNOLOGÍA/SISTEMAS DE INFORMACIÓN: Integridad, disponibilidad, confidencialidad de datos, soporte técnico, aplicaciones, hardware, software que se deben proteger para garantizar el funcionamiento interno de cada proceso.
	GOBERNANZA: Direccionamiento estratégico, planeación institucional, liderazgo, implica una dirección efectiva y el cumplimiento de objetivos estratégicos y operativos.
	COMUNICACIÓN INTERNA: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.
	CULTURA ORGANIZACIONAL: Impacta la ética, clima laboral, y la adherencia a la misión y visión de la institución.
	INFRAESTRUCTURA: Critico para garantizar un entorno seguro y adecuado para la prestación de servicios.

Figura 3. Estructura propuesta para la redacción del riesgo.

Descripción del riesgo: La descripción del riesgo debe contener todos los detalles necesarios y ser fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilite su redacción y claridad, comenzando con la frase "POSIBILIDAD DE", y analizando los siguientes aspectos:



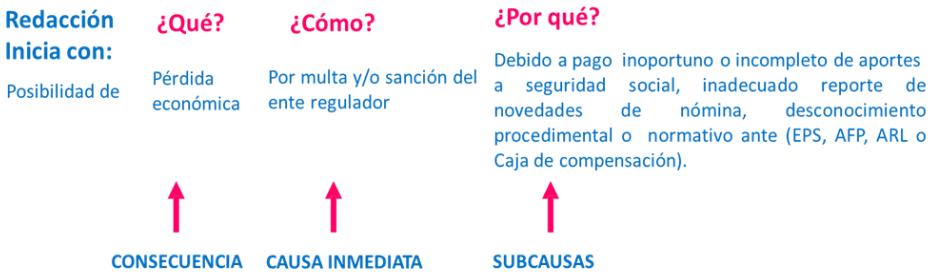


Figura 4. Ejemplo de riesgo redactado bajo la estructura propuesta.

La anterior estructura evita la subjetividad en la redacción y permite entender cómo puede manifestarse el riesgo, así como sus causas y consecuencias. Esta información es esencial para la definición de controles en la etapa de valoración del riesgo.

7.4. Análisis y Valoración

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características, incluyendo, cuando sea apropiado, el nivel del riesgo. En este punto, se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto. Realizar el análisis de los riesgos de forma inherente como residual permitirá determinar la madurez de los controles al interior de la organización. El análisis del riesgo se puede realizar con diferentes grados de detalle, dependiendo del riesgo, de la finalidad del análisis y de la información, datos y recursos disponibles.

7.4.1. Determinar la probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, que también puede ser entendida como la frecuencia estimada.

Probabilidad Inherente

PESO %	CRITERIO (ESCALA ORDINAL)		FRECUENCIA
25%	IMPROBABLE	**Baja probabilidad de ocurrencia.** Es casi imposible que ocurra, pero puede ocurrir en circunstancias excepcionales. Ha ocurrido una vez en más de un año, o solo en una oportunidad en la historia de la Empresa.	1 vez cada 2 años
50%	OCASIONAL	**Media probabilidad de ocurrencia.** No es habitual, pero ocurre algunas veces. Se ha presentado una ocasión en el año, o por semestre o trimestre en el año.	1 a 5 veces al año
75%	POSIBLE	**Alta probabilidad de ocurrencia.** Es posible que se dé y suceda varias veces. Se ha presentado una ocasión por bimestre en el año.	6 a 11 veces al año
100%	PROBABLE	**Muy Alta probabilidad de ocurrencia.** Es probable que ocurra muchas veces. Se posee certeza de su ocurrencia, una vez o más por mes en el año.	Mas de 11 veces al año

7.4.2. Determinar el impacto

El impacto se mide según el grado en que las consecuencias o efectos pueden perjudicar a la institución si se materializa el riesgo.

Impacto Inherente

	ESCALA DE IMPACTO	ECONÓMICO	EN PERSONAS	OPERACIONAL	LEGAL / CUMPLIMIENTO	SEGURIDAD INFORMATICA	REPUTACIONAL
25%	LEVE	Pérdidas entre 1 SMLMV y 5 SMLMV	Afectación mínima o temporal a la salud del paciente. No requiere intervención médica significativa. No se producen consecuencias permanentes ni prolongadas. Molestias menores para el paciente. Posibles quejas o insatisfacción con el servicio, pero sin mayores repercusiones.	Interrupciones menores en las operaciones que no afectan significativamente el servicio al paciente. Los problemas pueden ser resueltos rápidamente con recursos internos. Mínimo impacto en la eficiencia operativa. No hay afectación notable en la calidad del servicio al paciente.	Incumplimiento menor, genera solicitud de aclaraciones por parte de órganos de control u otras entidades o autoridades competentes. NO implica afectación en la continuidad de la prestación del servicio. No resulta en sanciones graves ni en un impacto significativo en la operación de la institución.	Incidentes menores que afectan la seguridad de la información, sin repercusiones significativas en la operación de la institución. Los datos comprometidos son limitados y el impacto es fácilmente manejable. Requiere corrección y revisión de las políticas de seguridad, o en las herramientas de protección, pero sin afectaciones graves a la calidad del servicio	El suceso genera comentarios adversos de algunos grupos de interés, solicitudes de información, no logra convertirse en hecho noticioso o tiene niveles bajos o poco perceptibles de cobertura en medios de comunicación, las publicaciones duran algunas horas, pero son de poco interés. Su explicación o solución no toma más de un día.
50%	MODERADO	Pérdidas entre 5 SMLMV y 10 SMLMV	Afectación intermedia a la salud del paciente que puede requerir intervención médica. No causa daño permanente, pero puede requerir seguimiento y tratamiento. Necesidad de atención médica adicional o ajustes en el tratamiento. Posible extensión de la estancia hospitalaria o visitas adicionales a la clínica.	Interrupciones que afectan una parte de las operaciones, requiriendo esfuerzos de resolución moderados. Puede implicar ajustes en los horarios de atención o reprogramación de ciertos servicios. Afectación limitada de la eficiencia y la calidad del servicio. Pueden generarse retrasos en algunos servicios, pero	Incumplimiento genera investigaciones con posibles sanciones económicas impuesta por órganos administrativos o judiciales. Puede implicar o no afectación en la continuidad de la prestación del servicio y necesidad de ajustar prácticas.	Incidentes que afectan de manera amplia la seguridad informática, con posible exposición de datos no críticos o interrupciones parciales en los servicios. Posibles sanciones o requisitos regulatorios para cumplir con normativas de protección de datos, necesidad de reforzar las medidas de	El suceso genera críticas por parte de grupos de interés, peticiones formales, puede o no convertirse en hecho noticioso para medios locales de comunicación, tiene niveles importantes de cobertura, las publicaciones duran un (1) día y son de interés, Su explicación o solución no toma más de una semana.

	ESCALA DE IMPACTO	ECONÓMICO	EN PERSONAS	OPERACIONAL	LEGAL / CUMPLIMIENTO	SEGURIDAD INFORMATICA	REPUTACIONAL
				sin comprometer la atención en servicios prioritarios.		seguridad y realizar correcciones. Posible necesidad de notificar a las autoridades y a los afectados.	
75%	**MAYOR**	Pérdidas entre 10 SMLMV y 20 SMLMV	Afectación significativa a la salud del paciente con consecuencias notables. Puede causar daño físico o psicológico, con necesidad de tratamiento intensivo o especializado. Posibles secuelas a largo plazo, pero sin llegar a ser incapacitantes o mortales. Tratamiento adicional y seguimiento prolongado. Impacto en la calidad de vida del paciente y posibles repercusiones económicas y emocionales.	Interrupciones significativas que afectan una parte importante de las operaciones de la institución. Requiere una gestión de crisis y recursos adicionales para la resolución. Reducción significativa en la capacidad de la institución para prestar servicios. Aumento de tiempos de espera y potencial disminución en la calidad del servicio. Compromete la atención en servicios prioritarios.	Incumplimiento significativo genera investigaciones y/o demandas que concluyen en reconocimiento de sanciones graves, impuesta por órganos administrativos o judiciales. Implica cierre parcial o temporal de sedes o servicios. Necesidad de cambios importantes en las políticas y procedimientos, posible reestructuración administrativa.	Incidentes graves que tienen un impacto significativo en la seguridad informática, con exposición de datos sensibles y/o interrupciones importantes en los servicios. Requiere una respuesta urgente y extensa para mitigar el daño y restaurar la seguridad. Daño considerable a la operación y reputación, con sanciones regulatorias y una necesidad urgente de medidas correctivas extensas. Requiere una reestructuración de las políticas de seguridad informática y una recuperación exhaustiva para restaurar la confianza y la funcionalidad.	El suceso genera señalamientos por parte de grupos de interés quienes reconsideran la relación con la institución, reclamaciones con pretensiones formales, es un hecho noticioso para medios locales y nacionales de comunicación, tiene niveles sostenidos de cobertura, las publicaciones duran más de (1) día y son centro de atención, Su explicación o solución no toma más de un mes.
100%	**CATASTROFICO**	Pérdidas superiores a 20 SMLMV	Afectación extrema a la salud del paciente, con riesgo de muerte o discapacidad permanente. Resulta en eventos	Interrupciones severas que paralizan total o casi totalmente las operaciones de la institución. Requiere una	Incumplimiento genera investigaciones, litigios prolongados, y/o denuncias que concluyen en de	Incidentes críticos que provocan una crisis total en la seguridad informática, con pérdida	El suceso genera señalamientos y juicios por parte de grupos de interés quienes cancelan la relación con la

	ESCALA DE IMPACTO	ECONÓMICO	EN PERSONAS	OPERACIONAL	LEGAL / CUMPLIMIENTO	SEGURIDAD INFORMATICA	REPUTACIONAL
			adversos graves como fallecimiento, parálisis, o pérdida de función vital. Muerte o daño irreversible para el paciente. Consecuencias legales y éticas significativas para la institución. Potencial daño a la reputación de la institución y pérdida de confianza por parte de la comunidad.	respuesta de emergencia a gran escala y puede involucrar a múltiples agencias o entidades externas. Cierre parcial o total de la institución. Incapacidad para prestar servicios, con un impacto negativo significativo en la comunidad. Potencial daño a la reputación y pérdidas financieras sustanciales.	sanciones graves, cuantiosas, perdida de derechos impuesta por órganos judiciales, pérdida de licencias impuesta por órganos administrativos. Implica cierre total o definitivo de sedes o servicios, y una recuperación a largo plazo para restaurar la confianza pública y cumplir con los requisitos legales.	masiva de datos, daño irreparable a la infraestructura y paralización de las operaciones. Implica un colapso total de la capacidad de gestionar la seguridad de la información, con consecuencias devastadoras para la institución. Daño catastrófico a la operación y reputación, con posible cierre permanente o reestructuración completa de la institución. Necesidad de una recuperación a largo plazo, incluyendo la reconstrucción de sistemas, procesos y la restauración de la confianza pública.	institución, y advierten demandas, es un hecho noticioso que produce un concepto masivo desfavorable en medios de alta difusión a nivel local, nacional e inclusive internacional, tiene niveles prolongados de cobertura, las publicaciones duran más de (7) días y persisten en la agenda informativa, no es posible para la institución dar una explicación o solución.

***La valoración del impacto causado por la materialización del riesgo estará asociado con la mayor afectación.**

Ejemplo aplicado:

Riesgo identificado: Posibilidad de pérdida económica por sanción y/o multa del ente regulador debido a pago inoportuno o incompleto de aportes a seguridad social, inadecuado reporte de novedades de nómina, desconocimiento procedimental o normativo ante (EPS, AFP, ARL o Caja de compensación).

Para el ejemplo, el líder del proceso ha indicado que este riesgo en su área no es habitual, pero se tiene conocimiento y registro de su ocurrencia 1 vez en el último año, por lo tanto, resulta OCASIONAL según la tabla:

PROBABILIDAD INHERENTE			
PESO %	**CRITERIO (ESCALA ORDINAL)**		**FRECUENCIA**
25%	**IMPROBABLE**	**Baja probabilidad de ocurrencia.** Es casi imposible que ocurra, pero puede ocurrir en circunstancias excepcionales. Ha ocurrido una vez en más de un año, o solo en una oportunidad en la historia de la Empresa.	**1 vez cada 2 años**
50%	**OCASIONAL**	**Media probabilidad de ocurrencia.** No es habitual, pero ocurre algunas veces. Se ha presentado una ocasión en el año, o por semestre o trimestre en el año.	**1 a 5 veces al año**
75%	**POSIBLE**	**Alta probabilidad de ocurrencia.** Es posible que se dé y suceda varias veces. Se ha presentado una ocasión por bimestre en el año.	**6 a 11 veces al año**
100%	**PROBABLE**	**Muy Alta probabilidad de ocurrencia.** Es probable que ocurra muchas veces. Se posee certeza de su ocurrencia, una vez o más por mes en el año.	**Mas de 11 veces al año**

La opción seleccionada indica que la probabilidad de ocurrencia del riesgo es Media

Según el líder la afectación económica de la última vez que se materializó este riesgo tuvo una cuantía mayor a 20 SMLMV, por tanto, resulta un impacto económico CATASTRÓFICO.

	IMPACTO			
CATEGORIA DE AFECTACION	LEVE 25%	MODERADO 50%	MAYOR 75%	CATASTROFICO 100%
Económico	Perdidas entre 1 SMLV y 5 SMLV	Perdidas entre 5 SMLV y 10 SMLV	Perdidas entre 10 SMLV y 20 SMLV	Perdidas superiores a 20 SMLV
Reputacional	El suceso genera comentarios adversos de algunos grupos de interés, solicitudes de información, no logra convertirse en hecho noticioso o tiene niveles bajos o poco perceptibles de cobertura en medios de comunicación, las publicaciones duran algunas horas, pero son de poco interés. Su explicación o solución no toma más de un día.	El suceso genera críticas por parte de grupos de interés, peticiones formales puede o no convertirse en hecho noticioso para medios locales de comunicación, tiene niveles importantes de cobertura, las publicaciones duran (1) día y son de interés, su explicación o solución no toma más de una semana.	El suceso genera señalamientos por parte de los grupos de interés quienes reconsideran la relación con la institución, reclamaciones con pretensiones formales es un hecho noticioso para medios locales y nacionales de comunicación, tiene niveles sostenidos de cobertura, las publicaciones duran más de un mes.	El suceso genera señalamientos y juicios por parte de grupos de interés quienes cancelan la relación con la institución, y advierten demandas, es un hecho noticioso que produce un concepto masivo desfavorable en medios de alta difusión a nivel local, nacional e inclusive internacional, tiene niveles prolongados de cobertura, las publicaciones duran más de (7) días y persisten en la agenda informativa, no es posible para la institución dar una explicación o solución
Legal/Cumplimiento	Incumplimiento contractual o extracontractual e incumplimiento legal, genera solicitud de aclaraciones por parte del órgano de control u otras entidades o autoridades competentes, NO implica afectación en la continuidad de la prestación del servicio.	Incumplimiento contractual o extracontractual e incumplimiento legal, genera investigaciones que concluyen en sanción económica impuesta por órganos administrativos o judiciales. Puede implicar o no afectación en la continuidad de la prestación del servicio	Incumplimiento contractual o extracontractual e incumplimiento legal, genera investigaciones y/o demandas que concluyen en sanciones o reconocimiento de indemnizaciones de cuantía importante, impuesta por órganos administrativos o judiciales. Implica cierre parcial o temporal de sedes o servicios	Incumplimiento contractual o extracontractual e incumplimiento legal, genera investigaciones, demandas, y/o denuncias que concluyen en sanciones, reconocimiento de indemnizaciones en cuantías superiores, y/o perdida de derechos impuesta por órganos administrativos o judiciales. Implica cierre total o definitivo de sedes de servicio.
Contagio	Mención de la Empresa por acción ilícita de un tercero relacionado	Investigación abierta a la Empresa por acción ilícita de un tercero relacionado	Sanciones administrativas a la Empresa por acción de un tercero relacionado	Sanción administrativa y penal, cierre de la Empresa por acción ilícita de un tercero relacionado
En personas	Consecuencias con incapacidad menos a 15 días en uno hasta 3 usuarios por evento. Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias	Consecuencias con incapacidad mayor a 15 días en uno hasta 3 usuarios por evento. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor >=5%	Consecuencias con incapacidad mayor a 15 días en más de 5 usuarios por evento. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad de un valor >=20%	Consecuencias mortales o de invalidez total de usuarios. Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor >=50%
Operacional	Perdida de información de la Empresa o de terceros que sea recuperable y que no ocasiona retrasos en las labores de las áreas. Interrupción de las operaciones de la Empresa menor a 2 horas. Riesgo cuya materialización podría tener un efecto PEQUEÑO O NULO a procesos o colaboradores, no acarrea costos.	Perdida de información de la Empresa o de terceros que sea recuperable y que ocasione retrasos significativos en las labores de las áreas. Interrupción de las operaciones de la Empresa entre 2 y 6 horas. Riesgo cuya materialización CAUSARIA UN DAÑO MENOR. Impacto mínimo hacia las PI, los costos de reproceso son moderados.	Pérdida de la información de la Empresa o de terceros de fácil recuperación. Generan reproceso o retrasos que impactan a nivel Empresa. Interrupción de las operaciones de la Empresa entre 1 y 2 días. Riesgo cuya materialización CAUSARÍA UN DETERIORO en el desarrollo DIFICULTANDO O RETRASANDO el cumplimiento de los objetivos, genera un daño temporal a las PI y los reprocesos afectan los costos.	Pérdida de información de la Empresa de terceros que no se puede recuperar. Interrupción de las operaciones de la Empresa más de 2 días. Riesgo cuya materialización DAÑARIA GRAVEMENTE y genera un daño permanente a las PI, sobrepasan los costos por indemnizaciones. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.

La opción seleccionada indica que el impacto es de tipo económico

Probabilidad inherente: OCASIONAL = 50% Impacto inherente: CATASTRÓFICO = 100%

Análisis preliminar (Riesgo inherente): A partir del análisis de la probabilidad de ocurrencia del riesgo y su impacto, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). La combinación o multiplicación de probabilidad e impacto, a su vez, determina los niveles de severidad. Para representar gráficamente este

resultado, utilizamos el MAPA DE CALOR. A continuación, conoceremos dicho mapa y veremos la zona en la que se ubica el riesgo, según el ejemplo:

MAPA DE CALOR 4 X 4

PROBABILIDAD					
	100%	25%	50%	75%	100%
	75%	19%	38%	56%	75%
	50%	13%	25%	38%	50%
	25%	6%	13%	19%	25%
		25%	50%	75%	100%
		IMPACTO			

ZONA DEL MAPA

EXTREMA	ALTA	MODERADA	BAJA

PROBABILIDAD					
	Probable	25%	50%	75%	100%
	Posible	19%	38%	56%	75%
	Ocasional	13%	25%	38%	50%
	Improbable	6%	13%	19%	25%
		Leve	Moderado	Mayor	Catastrófico
		IMPACTO			

EXTREMA	ALTA	MODERADA	BAJA

Cruzando los datos de probabilidad e impacto definidos se tiene: Zona de riesgo alta.

Probabilidad inherente 50% *Impacto inherente 100%
Riesgo Inherente = 50%

El mapa de calor permite visualizar los riesgos en las zonas definidas (extrema, alta, moderada y baja), permitiendo identificar y priorizar los riesgos asociados a la gestión que requieren mayor atención, así como aquellos que la institución está dispuesta a aceptar (apetito del riesgo) en función del impacto que puedan tener.

7.4.3. Valoración de Controles

Se evaluará la Solidez del Control considerando su diseño (documentado, responsable asignado) y ejecución (evidencia, frecuencia):

- **Fuerte:** Control bien diseñado que mitiga la causa raíz.

- **Regular:** Cumple parcialmente, requiere ajustes.
- **Débil:** No es efectivo o no se aplica.

Valoración de controles: en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Se busca confrontar los resultados del análisis del riesgo inicial (INHERENTE).

frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RESIDUAL).

Riesgo inicial (Inherente) – Efecto de los controles = Riesgo Final (Residual)

Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración.

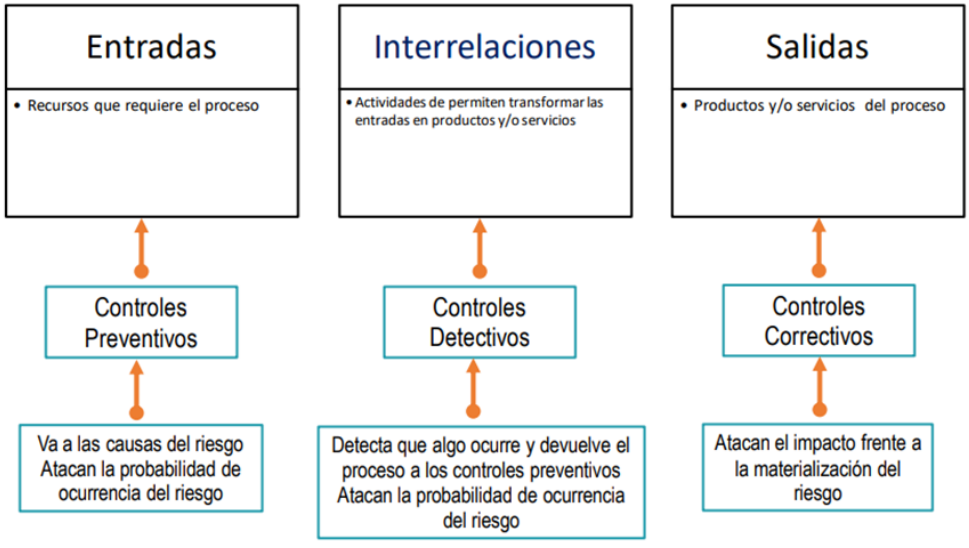
- **Responsable de ejecutar el control:** Se identifica el cargo del colaborador que ejecuta el control. En el caso de controles automáticos, se especifica el sistema que realiza la actividad.
- **Acción:** Se determina mediante verbos que indican la acción que debe realizarse como parte del control.
- **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo aplicado bajo la estructura propuesta para la redacción del control

El coordinador de nómina	Verifica consistencia en datos, salarios, novedades y aportes antes de realizar el pago	a través del cruce de las bases de datos de empleados activos e inactivos, con reportes del aplicativo de nómina y los pre-registros de la plataforma del operador de pago
Responsable	**Acción**	**Complemento**

Naturaleza de controles y procesos: A través del ciclo de los procesos, es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología o naturaleza con mayor precisión, para comprender esta estructura conceptual, en la figura 8 se consideran 3 fases globales del ciclo de un proceso así:

Ciclo del proceso y naturaleza de controles



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

TIPO DE CONTROL	Descripción
Preventivo	Son las acciones y mecanismos que se implementan para evitar un error o las desviaciones de un objetivo (Implementar políticas y procedimientos claros, capacitaciones al personal, póliza de seguro).
Detectivo	Son las acciones implementadas para identificar, descubrir un error, omisión o un acto desviado una vez se ejecuta el procedimiento. (Monitoreo continuo de sistemas, auditorías internas, revisiones periódicas de informes, o alarmas que detectan actividades inusuales).
Correctivo	Son las acciones implementadas con el fin de corregir las desviaciones presentadas, una vez concluido el procedimiento (Planificación de contingencia, Procedimientos de respaldo, Procedimientos para el reproceso de la operación, actualización de procedimientos).

No se trata solo de seleccionar la tipología o naturaleza asociada; la calificación de controles debe considerar diversos aspectos para evaluar su efectividad. A continuación, se presentan los criterios adicionales requeridos, que se dividen en dos grandes atributos: el diseño y la ejecución del control. También se detallan las opciones de respuesta correspondientes.

CLASE DE CONTROL	Descripción
Automático	Se ejerce a través de un sistema o mecanismo donde no interviene el hombre.
Semiautomático	Se ejerce a través de un sistema o mecanismo y con la intervención del hombre.
Manual	Interviene exclusivamente el hombre para su ejecución.
DOCUMENTACIÓN DEL CONTROL	**Descripción**
Total	El Control se encuentra actualizado, aprobado y divulgado en el sistema de gestión de la institución.
Parcial	El documento donde se formaliza el Control no se encuentra aprobado y divulgado en el sistema de gestión de la institución.
No documentado	El Control no se encuentra documentado.

EVIDENCIA DEL CONTROL	Descripción
Formal	El registro del control se encuentra formalizado (Aprobado y divulgado en el sistema de gestión de la institución.
Informal	La evidencia del control no se encuentra en un registro formal (Aprobado y divulgado en el sistema de gestión de la institución.
No existe	No se deja registro o evidencia del control.
APLICACIÓN DEL CONTROL	**Descripción**
Siempre	El control se realiza en todos los casos en que se realiza la actividad. (Del 90% al 100% de las veces)
Frecuente	El control se realiza casi todas las veces en que se realiza la actividad. (Del 60% al 90% de las veces)
Ocasional	El control no se realiza con frecuencia y este se realiza de manera aleatoria. (Menor al 60% de las veces)
AMBIENTE DEL CONTROL	**Descripción**
Muy estable	El control no tiene margen de error y siempre es efectivo
Estable	El control tiene un margen de falla muy mínimo. (10% de margen de falla)
Inestable	El control puede fallar en cualquier momento.
IDONEIDAD DEL CONTROL	**Descripción**
Total	El control mitiga directamente la causa raíz que origina el riesgo.
Parcialmente	El control mitiga las causas secundarias que originan el riesgo más no la causa raíz.
No cumple	El control aplicado no está encaminado a mitigar las causas identificadas que generan el riesgo.
COMPETENCIA Y AUTORIDAD DEL RESPONSABLE DEL CONTROL	**Descripción**
Cumple	La persona que aplica el control tiene la formación, experiencia y autoridad para desempeñar el control.
Parcialmente	La persona que aplica el control tiene la experiencia o formación, pero no la autoridad.
No cumple	La persona que aplica el control no cumple con formación, experiencia y autoridad para desempeñar el control.

Estos criterios permiten evaluar el control durante su ejecución para determinar si se está llevando a cabo como se esperaba. En otras palabras, sirven para verificar si el control diseñado e implementado es efectivo, es decir, si cumple o no con su objetivo de mitigación.

Para expresar numéricamente la calificación de los controles, la Coordinación de Riesgos, con el apoyo de la Mesa de Riesgos, debe preestablecer y asignar las unidades de medida para cada atributo y para cada respuesta según el criterio. Estas unidades de medida estarán parametrizadas dentro del método evaluativo del sistema de gestión definido por la institución, lo que permitirá visualizar el inventario de riesgos de manera ordenada y sistemática.

Control	Riesgo	Tipo	Clase	Documentado	Evidencia	Aplicación	Ambiente de control	Idoneidad	Competencia y autoridad del responsable del control	Resultado
El coordinador de nómina verifica consistencia en datos, y aportes antes de realizar el pago, a través de una lista de chequeo física donde están los de datos de empleados activos e inactivos, sus salarios, y novedades.	Posibilidad de pérdida económica por sanción y/o multa del ente regulador debido a pago inoportuno o incompleto de aportes a seguridad social, inadecuado reporte de novedades de nómina, desconocimiento procedimental o normativo ante (EPS, AFP, ARL o Caja de compensación).	Preventivo	Manual	Total	Formal	Frecuente	Inestable	Parcialmente	Cumple	Regular 3,60

En la parametrización del método evaluativo del sistema de gestión definido por la institución, se establecerán los rangos que indicarán la solidez final de un control. La solidez de un control se refiere a su capacidad para cumplir eficazmente con su propósito de mitigar riesgos, lo que incluye un diseño robusto, una implementación efectiva y un impacto positivo en la gestión de riesgos. Estos rangos permitirán categorizar la efectividad de cada control según su capacidad para alcanzar su objetivo de mitigación.

Solidez del control

Débil	Control presenta deficiencias significativas que limitan su efectividad y requiere mejoras sustanciales.
Regular	Control cumple parcialmente con su objetivo, mostrando algunas deficiencias menores que necesitan vigilancia continua.
Fuerte	Control bien diseñado y ejecutado, cumpliendo efectivamente con su objetivo y mostrando alta capacidad para mitigar riesgos.

¿Cómo se calcula el riesgo residual?

El sistema de gestión de la institución, que presenta el inventario de riesgos de manera sistemática, utiliza fórmulas internas basadas en las unidades de medida preestablecidas para evaluar los atributos y criterios del riesgo. A continuación, se ofrece una explicación simplificada de estos cálculos.

El riesgo residual es el riesgo que queda después de aplicar todas las medidas de control y mitigación. Para calcularlo de manera efectiva, se siguen estos pasos:

1) **Determina el Riesgo Inherente:**
   - **Impacto:** Evalúa cuánto daño podría causar el riesgo si se materializa. Puedes usar una escala cualitativa (alto, medio, bajo) o cuantitativa (por ejemplo, en una escala del 1 al 5).
   - **Probabilidad:** Evalúa la probabilidad de que el riesgo ocurra. También puedes usar una escala cualitativa o cuantitativa similar.

Cálculo del Riesgo Inherente: Multiplica el impacto por la probabilidad

Fórmula: Riesgo Inherente = Impacto x Probabilidad

2) **Evalúa la Efectividad de los Controles:**
   - Identificación de Controles: Enumera los controles que has implementado para mitigar el riesgo.
   - Efectividad de los Controles: Asigna un porcentaje a la efectividad de cada control. Este porcentaje representa la reducción del riesgo lograda gracias a los controles. Por ejemplo, si crees que los controles reducen el riesgo a la mitad, su efectividad es del 50%.

3) **Calcula la Reducción del Riesgo:**
   - **Reducción del Riesgo:** Multiplica el riesgo inherente por la efectividad de los controles.

Fórmula: Reducción del Riesgo = Riesgo Inherente x Efectividad de los Controles

4) **Calcula el Riesgo Residual**
   - Cálculo del Riesgo Residual: Resta la reducción del riesgo del riesgo inherente.

Fórmula: Riesgo Residual = Riesgo Inherente - Reducción del Riesgo

Ejemplo Práctico:

Imagina que has identificado un riesgo con un impacto alto valorado en 4 y una probabilidad media valorada en 3:

Riesgo Inherente:

- Impacto (4) x Probabilidad (3) = 12

Has implementado controles que consideras tienen una efectividad del 50% (0.5):

Reducción del Riesgo:

- Riesgo Inherente (12) x Efectividad de los Controles (0.5) = 6

Riesgo Residual:

- Riesgo Inherente (12) - Reducción del Riesgo (6) = 6

  Por lo tanto, el riesgo residual es 6.

Resumen: Para calcular el riesgo residual.

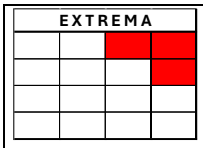
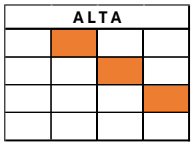
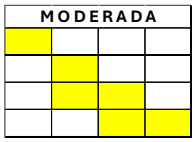
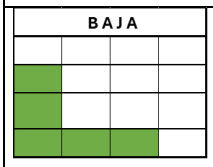
1. Evalúa el impacto y la probabilidad del riesgo para obtener el riesgo inherente.
2. Determina la efectividad de los controles aplicados
3. Calcula cuánto se reduce el riesgo gracias a los controles.
4. Resta esta reducción del riesgo inherente para obtener el riesgo residual.
5.

8. VALORACIÓN DEL RIESGO

El propósito de la valoración del riesgo es apoyar la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos, como el apetito y la tolerancia al riesgo, para determinar las acciones a seguir.

Es esencial partir de las Estrategias de Gestión de Riesgos por Niveles de Severidad, que clasifican y priorizan los riesgos según su impacto y probabilidad. A partir de esta clasificación, se procede a analizar el apetito de riesgo declarado por la alta dirección en los lineamientos generales, asegurando que las decisiones de gestión se alineen con la tolerancia organizacional hacia el riesgo.

Estrategias de Gestión de Riesgos por Niveles de Severidad.

	**Acción inmediata:** Situaciones o tendencias que cambian rápidamente con alta incertidumbre, exigiendo acciones inmediatas y prioritarias. Tienen alta probabilidad de ocurrir y evolucionan ágilmente, impactando significativamente. Se deben comunicar a la Gerencia General, Consejo de Administración y Mesa de Riesgos para tratamiento inmediato.
	**Acción estratégica:** Situaciones inminentes o con alta probabilidad de ocurrencia que requieren la implementación de planes contingentes proactivos y ajustes dinámicos en la estrategia. Aunque su evolución es más lenta que la del riesgo extremo, exigen un tratamiento y monitoreo riguroso, así como atención del Gerente General y de los líderes de procesos. Deben ser informadas al Consejo de Administración y a la Mesa de Riesgos.
	**Prepararse para posibles cambios:** Situaciones que evolucionan lentamente con alta incertidumbre, pero con posibilidad de intensificarse rápidamente al ocurrir. Tienen una probabilidad media de ocurrencia, requiriendo planes contingentes planificados. Deben ser gestionadas por los líderes de procesos, con monitoreo cercano e informado a la Gerencia General y la Mesa de Riesgos.
	**Monitoreo continuo:** Se aplica a tendencias o situaciones que evolucionan gradualmente con impacto predecible. Requiere monitoreo constante y gestión bajo los controles actuales por parte de los líderes de procesos, con reportes periódicos a la Gerencia General y la Mesa de Riesgos.

9. TRATAMIENTO

El propósito del tratamiento del riesgo es seleccionar e implementar opciones efectivas para abordarlo. Este proceso es iterativo e incluye la formulación y selección de alternativas, planificación e implementación del tratamiento, evaluación de su eficacia y determinación de si el riesgo residual es aceptable. En caso de que el riesgo no sea aceptable, se debe llevar a cabo un tratamiento adicional. La selección de la opción más adecuada para el tratamiento implica realizar un análisis de costos y beneficios. Cada líder de proceso será responsable del tratamiento de los riesgos, que deberá ser revisado por la Gerencia y la mesa de riesgos para cumplir con los siguientes objetivos:

- Mejorar el conocimiento sobre los controles establecidos y su capacidad para mitigar los riesgos del proceso.
- Validar que el costo de implementación de los controles sea menor que los beneficios obtenidos.
- Adicionar, eliminar o modificar controles y tratamientos según sea necesario.

Las opciones de tratamiento del riesgo pueden incluir, entre otras, las siguientes alternativas:

TRATAMIENTO	DESCRIPCIÓN
EVITAR	Eliminar la exposición al riesgo al no realizar la actividad que lo genera o modificar procesos para que no se materialice. ***Ejemplo*:** *Una empresa decide no entrar en un mercado internacional debido a la alta volatilidad política y económica que podría afectar su inversión.*
REDUCIR	Se enfoca en disminuir la probabilidad de que ocurra el riesgo o su impacto antes de que suceda. Implica implementar controles o medidas preventivas para evitar que el riesgo se materialice o minimizar sus efectos desde un principio. ***Ejemplo*:** *Mejorar la infraestructura de seguridad de una planta química para reducir la probabilidad de accidentes.*
TRANSFERIR	Se trata de pasar completamente el riesgo a un tercero, que asume la responsabilidad y las posibles consecuencias. Comúnmente incluye seguros o contratos donde una parte cubre el impacto del riesgo. La empresa que transfiere el riesgo ya no se encarga de gestionarlo directamente. ***Ejemplo:** Una fábrica adquiere un seguro contra incendios para transferir el riesgo de pérdidas financieras en caso de siniestro.*
ACEPTAR	Decidir no tomar medidas adicionales y asumir el riesgo, reconociendo que el nivel residual es tolerable. Esta opción se utiliza generalmente cuando el riesgo es de bajo impacto o cuando el costo de mitigación supera el beneficio. ***Ejemplo:** Una empresa tecnológica reconoce que el riesgo de ciberataques existe, pero decide no invertir en medidas adicionales de seguridad porque considera que el riesgo residual es aceptable.*
COMPARTIR	Distribuir el riesgo entre varias partes, como mediante alianzas o convenios, donde cada parte asume una porción del riesgo. ***Ejemplo:** Dos empresas de construcción acuerdan compartir los riesgos financieros de un proyecto a través de una sociedad temporal.*
MITIGAR	Implica tomar acciones una vez que el riesgo se ha materializado o está cerca de hacerlo, para disminuir el impacto o la severidad de sus consecuencias. Es una medida correctiva o de contención cuando el evento ya ha ocurrido o es inminente. ***Ejemplo:** Activar protocolos de emergencia y evacuación durante un derrame químico para mitigar el daño causado.*
RETENER	Mantener el riesgo dentro de la organización, aceptando sus posibles consecuencias sin realizar acciones específicas para mitigarlo.

	***Ejemplo*:** *Una pequeña empresa decide mantener el riesgo de fluctuaciones en el precio de materias primas, asumiendo los costos sin hacer cobertura financiera*.
MONITOREAR	Supervisar continuamente el riesgo y sus factores para detectar cambios o emergencias y tomar decisiones oportunas. ***Ejemplo*:** *Una institución financiera monitorea constantemente las tasas de interés para ajustar sus estrategias de inversión cuando detecta cambios importantes*.
EXPLORAR	Adoptar una postura proactiva hacia el riesgo, buscando oportunidades que puedan surgir del mismo. **Ejemplo:** *Una compañía farmacéutica identifica el riesgo de nuevas regulaciones para ciertos medicamentos, pero ve en ello una oportunidad para desarrollar nuevas fórmulas que cumplan con las normas futuras*.

Los planes de tratamiento deben integrarse en los procesos y planes de gestión de la organización, en consulta con las partes interesadas pertinentes. Dichos planes de tratamiento deben incluir al menos los siguientes aspectos:

- Justificación de la selección del tratamiento, incluyendo los beneficios esperados.
- Identificación de las personas responsables de la aprobación y la implementación del plan.
- Descripción de las acciones propuestas.
- Requisitos de recursos, incluyendo posibles contingencias.
- Indicadores de desempeño y limitaciones
- Requisitos de información y seguimiento.
- Calendario y programación del plan.

La aceptación del riesgo estará a cargo del Profesional de MIPG, Gerente y Junta Directiva según su nivel de criticidad y exposición para la ESE.

10. SEGUIMIENTO Y REVISIÓN

El seguimiento y la revisión son fundamentales para asegurar la calidad y eficacia del proceso de gestión de riesgos. Esta revisión se llevará a cabo anualmente por la Profesional de MIPG, los líderes de procesos y el área de calidad. Incluirá la evaluación de todos los aspectos del proceso, la efectividad de los controles y la recopilación de información para mejorar la valoración del riesgo. Se analizarán eventos, cambios, tendencias, éxitos y fallos, así como el impacto del contexto interno y externo, identificando riesgos emergentes y ajustando las estrategias según sea necesario.

Adicionalmente, se realizará una valoración trimestral de los controles en los diferentes procesos para detectar debilidades o ineficiencias de manera oportuna, permitiendo ajustes inmediatos que mantengan la mitigación del riesgo en niveles

aceptables. Esta revisión trimestral también evaluará el cumplimiento de los planes de acción, asegurando la ejecución efectiva de las medidas correctivas y preventivas, lo que propicia una gestión proactiva y adaptativa ante cambios.

11. REGISTRO E INFORME

El registro y la comunicación tienen como objetivos:

- Comunicar las actividades de gestión del riesgo y sus resultados en toda la organización.
- Proporcionar información relevante para la toma de decisiones.
- Mejorar las actividades de gestión del riesgo de manera continua.
- Facilitar la interacción con las partes interesadas, incluidas aquellas personas responsables de rendir cuentas sobre las actividades de gestión del riesgo

Para el registro de la Gestión de Riesgos se cuenta inicialmente con la Matriz de Riesgo, es una herramienta metodológica que permite visualizar un inventario de los riesgos de manera ordenada y sistemática, definiéndolos, evaluándolos, priorizándolos y estableciendo los controles y acciones de manejo específicas.

Periódicamente se presentará un informe de gestión de riesgos a la alta dirección, detallando los riesgos y amenazas a los que está expuesta la institución. Este documento facilitará la toma de decisiones oportunas y bien fundamentadas, destacando los principales riesgos estratégicos y operativos, así como las acciones y controles implementados. Incluirá conclusiones y recomendaciones para los directivos, con una estructura clara que facilite su lectura y comprensión.

12. ROLES Y RESPONSABILIDADES

- Junta Directiva: Aprueba la política y el manual.
- Gerente: Lidera la gestión estratégica y rinde cuentas.
- Comité Institucional de Coordinación de Control Interno: Supervisa el mapa de riesgos institucional. (O Cambiar con el nombre de la ESE)
- Líderes de Procesos:(Evaluar si de esta manera se denominan los perfiles directivos en la ESE) Identifican, analizan y tratan los riesgos de su área (Ej. Coordinador Médico, Líder de Talento Humano).
- MIPG: Evalúa la efectividad de los controles.

DESCRIPCIÓN	FECHA
Elabora: Asesor Riesgos	Diciembre 2025
Revisa: Profesional MIPG	Enero 2026
Aprueba: Comité de Gestión y Desempeño	Febrero 2026

CONTROL DE ACTUALIZACIONES			
Versión	Fecha	Item Modificado	Descripción del cambio
1	diciembre 2025	Se modifica con la normatividad vigente	Se realiza cambio en el documento de acuerdo con la normatividad vigente, la guía de DAFP y la norma ISO 31000 de 2018