Manual Integral para la Gestión del Riesgo

POL-GES-008

Clínica Imbanaco

Grupo quirónsalud

Clínica Imbanaco

Grupo quirónsalud

Contenido

Clínica Imbanaco

Grupo quirónsalud

Contenido

I. LINEAMIENTOS CORPORATIVOS

Clínica Imbanaco

Grupo quirónsalud

1. Objeto y Alcance

- La gestión eficaz de los riesgos ayuda a proteger la viabilidad futura de Quirónsalud y a mantenerse como un agente de salud activo y responsable en las poblaciones donde actuamos, asegurando en última instancia que podamos cumplir con nuestro propósito.

- El objetivo de la presente Política es establecer los principios y procedimientos para diseñar, mantener e implantar una gestión del riesgo operacional eficaz.

- Quirónsalud está comprometida con la excelencia en la Gestión de Riesgos, lo que nos ayudará a alcanzar nuestros objetivos y a garantizar la protección de nuestros clientes, pacientes y personas.

  Esta Política establece las expectativas de la Junta Directiva en relación con la Gestión de Riesgos en todo Quirónsalud y establece los principios que sustentan un Marco de Gestión de Riesgos robusto, que asegurará:

  - Que identificamos y entendemos los riesgos actuales y emergentes de nuestra actividad y las posibles consecuencias de los mismos;
  - Que adoptamos medidas adecuadas y eficaces para mitigar y gestionar los riesgos identificados;
  - Que utilizamos la información sobre la Gestión de Riesgos para tomar decisiones basadas en el riesgo en todo el Grupo;
  - Que existe una clara propiedad y responsabilidad sobre el riesgo; y
  - Que existe una cultura en la que:
    - Se fomenta la “elusión” del riesgo;
    - Se cuestionan y sancionan los comportamientos de riesgo inadecuados; y
    - Se conocen los riesgos por parte de las partes implicadas en la gestión del negocio.

- Esta Política es aplicable a todas las Entidades legales que formen el Grupo Quirónsalud.

¿Qué ocurre si no cumplimos?

Es menos probable que Quirónsalud logre sus objetivos y más probable que se vea afectada negativamente por eventos adversos si los riesgos no se identifican, entienden o mitigan adecuadamente. Al contar con una Gestión de Riesgos eficaz, Quirónsalud se protege frente a impactos de reputación, financieros y éticos.

2.Terminología

Funciones Claves

Riesgos: La función debe supervisar y ayudar al funcionamiento eficaz del sistema de Gestión de Riesgos, mantener una visión de toda la entidad del perfil de riesgo, asesorar sobre asuntos de Gestión de Riesgos, incluidos los asuntos estratégicos, y proporcionar informes detallados información detallada sobre las exposiciones al riesgo.

Compliance: La función debe identificar, evaluar, supervisar e informar sobre la exposición al riesgo de cumplimiento para garantizar que Quirónsalud gestiona sus responsabilidades en materia de riesgo normativo, cumplimiento y conducta de acuerdo con los objetivos acordados. La función también supervisa los posibles cambios en el entorno legal y su posible efecto y el control del cumplimiento de las leyes y reglamentos aplicables.

Auditoría Interna: La función ayuda al Comité de Dirección de Quirónsalud y a los distintos Consejos de Administración a proteger los activos, la reputación y la sostenibilidad de la organización. Esto lo logrará evaluando si todos los riesgos significativos se identifican y se informan adecuadamente, evaluando si están adecuadamente controlados y ayudando a la Dirección Ejecutiva a mejorar la eficacia de la gobernanza, la Gestión de Riesgos y los controles internos.

3 Líneas de defensa

Quirónsalud aplica, como parte de su diseño organizativo básico, un modelo de *"3 líneas de defensa"* (LoD) para estructurar funciones y responsabilidades (accountability) dentro de la empresa. Así, las *"3 líneas de defensa"* se traducen en:

1ª Línea de defensa: Engloba al Negocio y a las funciones de la compañía. Su misión es:

- **Identificar, Gestionar y Reportar:** Identificar, evaluar, controlar y mitigar los riesgos para los objetivos de QS; Cumplir con las Políticas Empresariales y las Regulaciones Externas; Identificar, escalar y aprender de los incidentes; Reportar las posiciones de riesgo, las debilidades y los incidentes.
- **Asesoramiento y apoyo:** Asesorar sobre la aplicación de las Políticas de la empresa y las regulaciones externas; Establecer normas y proporcionar asesoramiento sobre el diseño y las pruebas de los controles para apoyar su cumplimiento.
- **Supervisión:** Supervisar y comprobar la eficacia de los controles y el cumplimiento de las Políticas empresariales, así como la normativa externa.

2ª Línea de defensa: Engloba a las funciones de Riesgos y Cumplimiento. Su misión es:

- **Supervisión y reto:** Supervisión y reto independientes (incluyendo pruebas y seguimiento) de las prácticas de gobernanza y gestión de riesgos llevadas a cabo por la 1 Línea de defensa (LOD); Formar una opinión independiente sobre la calidad y suficiencia de las actividades de gestión de riesgos del negTocio y el entorno de control interno.
- **Asesorar y apoyar:** Establecer el Marco de Gestión de Riesgos de QS (RMF) a través del cual el negocio gestiona el riesgo; Proporcionar orientación y apoyo a la 1LOD sobre cómo integrar el RMF; Agregar información sobre el riesgo para el análisis y la presentación de informes al Comité de Riesgos y Compliance de QS.

3 Líneas de defensa

3ª Línea de defensa: Engloba la función de Auditoría Interna. Su misión es:
Aseguramiento independiente: Examinar y evaluar la adecuación y eficacia de los procesos de gobernanza, gestión de riesgos y control interno de QS en relación con las metas y objetivos definidos por la misma. Evaluar todos los procesos QS ("universo de auditoría"), incluidos los procesos de gobernanza y de gestión de riesgos.

- El modelo permite una cultura de transparencia y responsabilidad y tiene como objetivo garantizar que todo el personal tenga claras sus funciones y responsabilidades en relación con las actividades de Gestión de Riesgos, así como para reducir posibles áreas de conflicto y promover formas de trabajo eficientes y eficaces. El modelo se describe en el Marco de Gestión de Riesgos de QS.

Gobernanza Interna

La *gobernanza interna* se define como los marcos y prácticas clave en relación con la gobernanza, la cultura y la responsabilidad. Estos incluyen: el papel del Consejo, la eficacia del Consejo, el papel de los comités ejecutivos y la supervisión de la alta dirección, las autoridades delegadas, el papel de las Funciones Clave, la remuneración y la cultura.

Risk Owner

El *Risk owner (o propietario del riesgo)* son los propietarios y gestores en el día a día de los riesgos operacionales y controles que los mitigan, contando con el apoyo y la supervisión de la Función de Control de Riesgos Corporativa. Sus principales responsabilidades son:

- **La puesta en práctica de las políticas, directrices y metodologías** relativas a riesgo operacional.
  Identifican, documentan y evalúan los riesgos asociados a los procesos y procedimientos operativos y de negocio que gestionan, implantando, ejecutando y evaluando los controles que eviten, transfieran o mitiguen dichos riesgos con el objeto de mantenerlos dentro de los límites establecidos, aplicando para ello el principio de auto-evaluación y las metodologías y herramientas establecidas.

- **Mantener continuamente identificados y documentados los procesos,** procedimientos, los riesgos a los que están expuestos y controles aplicados sobre los mismos informando, a la mayor brevedad posible, a las unidades de control y supervisión (auditoría interna, verificación del cumplimiento normativo, gestión de riesgos) y de organización de las modificaciones, deficiencias significativas o incumplimientos que hayan podido sufrir o detectar.

- **Definir e implantar los controles y las medidas correctoras** que sean necesarias para la subsanación de las deficiencias y debilidades de control que se hayan detectado.

- **Custodiar las evidencias** que garanticen la ejecución de los controles y los resultados de éstos y ponerlas a disposición de los revisores que las soliciten: áreas de control, auditores internos o externos, supervisores, etc.

Modelo de categorización de Riesgos QS

El modelo de categorización de riesgos de Quirónsalud proporciona un enfoque estándar para clasificar el universo de diferentes tipos de riesgos a los que se enfrenta QS en la consecución de su objetivo. Su objetivo es:

- **Apoyar** una identificación exhaustiva de los riesgos
- **Permitir** una agregación más significativa de la información sobre riesgos
- **Permitir** la presentación de informes claros a la alta dirección y a los comités de compliance y riesgos

Se ha definido un desglose detallado de cada categoría de riesgo dentro del Marco de Gestión de Riesgos

Incidente

Un fallo en los procesos internos, controles, personas, sistemas, equipos o un evento externo que ha tenido o puede tener un impacto adverso en los objetivos de QS, clientes, personas y/o otros individuos (como visitantes o terceros proveedores) y/o en el negocio.

3. Reglas Generales

El Departamento/Función de Riesgos tendrá que asegurar una serie de requisitos funcionales:
Comunicar al Consejo de Administración, a través del titular de la Función de Gestión de Riesgos y del foro de Comité de Riesgos y Compliance, cualquier hecho o circunstancia relevante que se presente relativo a esta política y al Sistema de Gestión de Riesgo Operacional.

- **Facilitar el diseño y las herramientas** necesarias de un sistema eficaz de Gestión del Riesgo bajo los criterios y parámetros establecidos por el Consejo de Administración, que forme parte y sea coherente con el Sistema de Control Interno de la entidad.
- **Supervisar, y asesorar** cuando sea necesario, a los responsables de los diferentes procesos operativos de Quirónsalud, en la identificación y evaluación de los riesgos y controles asociados bajo el alcance del Sistema de Gestión de Riesgo Operacional.
- **Supervisar que el Sistema de Gestión de Riesgo Operacional** funciona de forma eficaz y que el funcionamiento de los controles que forman parte de éste mantiene el riesgo dentro de los parámetros del riesgo establecido por el Consejo de Administración.

Como **2ª Línea de defensa (LoD), dar apoyo a la 1ª LoD** (mandos intermedios y personal técnico) en la ejecución de sus responsabilidades relativas al Sistema de Gestión de Riesgo Operacional.
Anualmente, presentar al Comité de Compliance y Riesgos el plan de supervisión y control que contenga el detalle y alcance de las iniciativas de monitorización y control a desarrollar a lo largo del ejercicio.

- **Informar al Comité de Dirección,** Comité de Compliance y Riesgos, y al Consejo de Administración de los resultados obtenidos tras las labores de supervisión y control antes detalladas proponiendo, en su caso, la aprobación de las medidas correctoras que se hayan establecido.

A continuación, se detallan los riesgos más relevantes relacionados con esta Política, así como las medidas correctivas asociadas:

3.1 Inadecuada gestión del cambio en la adaptación e implementación de Qualios

Desde la función de Riesgos se ha diseñado una nueva metodología de evaluación de riesgos para QS, la cual tiene que estar respaldada por una herramienta corporativa (en este caso, Qualios). En la misma se tendrán que adaptar los parámetros y campos, haciendo de esta una herramienta que sirva tanto para valorar nuevos riesgos, como para poder asignar controles, planes de acción, procesos, políticas, etc., por lo que será necesario gestionar una adaptación y un cambio en la implementación de esta metodología.

Para tratar de mitigar que se materialice este riesgo, tendrán que diseñarse e implementarse ciertos controles:

- Actualizaciones de manuales de usuario de la herramienta
- Formación a grupos de interés sobre la misma y sobre cambios.
- Plan de despliegue gradual
- Fomento de la cultura de Riesgos por medio de talleres de formación, comunicación masiva, etc.
- Reuniones periódicas de seguimiento del plan de implementación de la herramienta.

3.2 Riesgo de falta de verificación y actualización del perfil de riesgo de la entidad conforme a la tolerancia al riesgo

- La gestión de la tolerancia al riesgo de Quirónsalud debe estar alineada con la exposición de la compañía respecto a sus riesgos. Será necesaria una revisión y actualización del perfil de riesgo, teniendo en cuenta qué límites se han establecido.

Para tratar de mitigar que se materialice este riesgo, tendrán que diseñarse e implementarse ciertos controles:

- Aprobación de los statements de tolerancia al riesgo por el Consejo (Risk Tolerance Framework) y revisión periódica de los mismos.
- La evaluación de la tolerancia al riesgo se revisa semestralmente y se presenta al Comité de Compliance y Riesgos.
- Las políticas definidas y aprobadas en 2022 incluyen un apartado específico de tolerancia donde se recogen los riesgos a considerar para la medición de la tolerancia al riesgo. En muchos casos los límites están ahí recogidos.

3.3 Riesgo de no identificación, definición o asignación incorrecta, falta de control o seguimiento de los riesgos, controles y propietarios; que lleven a la toma de decisiones erróneas para la compañía

- Desde la función de Riesgos de Quirónsalud se debe asegurar una óptima gestión de riesgos, fomentando actividades que lo promuevan e identificando aquellas que empeoren o dificulten la gestión.

Para tratar de mitigar que se materialice este riesgo, tendrán que diseñarse e implementarse ciertos controles:

- Elaboración de un Top Risk Report con carácter semestral que se presenta en el Comité de Compliance y Riesgos y se reporta de manera periódica a Fresenius.

Existencia y cumplimiento de un Framework de Riesgos aprobado por el Comité de Dirección.

- Formación a risk owners para mejorar la cultura de riesgos de Quirónsalud

- Los riesgos son validados regularmente en los registros de riesgos, incluyendo el perfil de riesgo local y la posición de tolerancia al riesgo
- Revisión, actualización y validación trimestral/semestral de los mapas de riesgo por los propietarios de los riesgos.
- Testeo de efectividad de los controles

4. Procedimiento de denuncia

Quirónsalud debe asegurar que se establecen los canales de comunicación e información adecuados con las áreas de referencia para que puedan cumplir con sus obligaciones a nivel Grupo. Esto se consigue incluyendo canales de comunicación y procedimientos para informar de forma rápida y al nivel apropiado, de cualquier deficiencia significativa junto con las medidas necesarias para corregirla.
Cualquier posible incumplimiento de lo establecido en esta Política deberá ser comunicado por medio de:

- Canal de denuncias corporativo
- Función de Riesgos del Grupo

Esta denuncia será de forma anónima y totalmente confidencial.

5. Tolerancia al riesgo y límites

- Esta Política apoya la Declaración de Tolerancia al Riesgo Operacional del Grupo que establece: "Quirónsalud no tiene tolerancia por los fallos de riesgo operacional que resulten en un impacto material para los clientes, las personas o la actividad de Quirónsalud"
- Los umbrales que convierten la declaración de tolerancia al riesgo en métricas medibles que pueden utilizarse para gestionar el negocio día a día están incluidos en las políticas empresariales. Cualquier fallo en la gestión efectiva del riesgo de acuerdo con esta política se identificará a través de la supervisión de los umbrales en otras políticas empresariales y la escalada de cualquier incumplimiento.

6. Régimen Disciplinario

- Esta Política será aplicable a todos los empleados que forman parte del Grupo Quirónsalud. El cumplimiento de ésta estará alineado con el desempeño del puesto de trabajo de cada uno de los empleados.

- La comunicación de prácticas que supongan un incumplimiento de la Política se podrá hacer a través de los responsables directos o, de forma anónima, mediante el canal de denuncias corporativo.

7. Acciones formativas

Desde la Función de Control de Riesgos se ha desarrollado un Plan de Concienciación de Cultura de Riesgos en el que se encuentra actualmente trabajando. El objetivo final es familiarizar al trabajador con el concepto de riesgo, alejando de su percepción el prejuicio negativo, y tratar de conseguir un acercamiento con el control de los riesgos de Quirónsalud, de tal manera que sea parte de la rutina inherente a actividad diaria. En concreto, el objetivo se puede resumir en tres pilares:

- Cultura
- Concienciación
- Conocimiento

- Hay que determinar las expectativas de formación en los diferentes tipos de funciones y definir un plan/calendario de formación (que determine la formación obligatoria/obligatoria y la de los nuevos empleados).

- Como primera fase de formación, se focalizará la misma en los responsables de riesgos (Risk owners) identificados por área y por categoría, con el objetivo de crear cultura de riesgo en todas las áreas y que sean los propios responsables los que transmitan dicha cultura a los equipos correspondientes.

- El departamento de Formación, junto con la Función de Riesgos, incorporarán en el Onboarding del portal del empleado una formación sobre Gestión de Riesgos, la cual tendrá carácter opcional.

- Además, se añadirá, tanto en la intranet corporativa (Universidad Corporativa) como en la herramienta Qualios, un apartado específico para la Gestión de Riesgos, con documentación de interés y accesible a toda la compañía.

II. LINEAMIENTOS GENERALES

Clínica Imbanaco

Grupo quirónsalud

1. Introducción

El Centro Médico Imbanaco de Cali S.A. (en adelante La Clínica Imbanaco) se enfrenta a factores e influencias internas y externas que hacen incierto saber si y cuando conseguirá sus objetivos. La incidencia que esta incertidumbre tiene sobre la consecución de los objetivos constituye el "riesgo".

La Clínica, a través de todos sus colaboradores, deben gestionar el riesgo mediante la identificación, análisis y evaluación del riesgo. Lo anterior permitirá a la Administración establecer un tratamiento que satisfaga los criterios de riesgo.

2.Objetivo

Establecer de forma integral los lineamientos generales para la gestión de riesgos en el Centro Médico Imbanaco de Cali S.A. Los lineamientos toman como referencia la norma ISO 31000- Gestión de Riesgos.

3.Alcance

El alcance de estos lineamientos está enmarcado en las etapas de la gestión de riesgo (Identificar, Medir, Monitorear, Controlar o Mitigar y reportar las exposiciones a todos los riesgos de la entidad) y se aplican de manera transversal a la organización.

4.Definiciones

Alta Gerencia: Personas del más alto nivel jerárquico en el área administrativa (denominados administradores) u organizacional de la entidad. La Junta Directiva la hace responsable del giro ordinario del negocio de la sociedad y la encarga de idear, ejecutar y controlar los objetivos y estrategias de la misma. También se incluye en la Alta Gerencia al Gerente de Auditoría.

Apetito de riesgo:

Es el nivel de riesgo que la empresa quiere aceptar y lo define la Junta Directiva.

Causa de riesgo:

Causa del riesgo: Elemento que, por sí solo o en combinación con otros, presenta el potencial intrínseco de ocasionar un riesgo.

Cómite de Auditoría y Gobierno Corporativo:

Apoya la inspección y seguimiento de las políticas, procedimientos y controles internos que se establezcan, el análisis de la ejecución de las operaciones de la Clínica, el análisis de las salvedades generadas por el Revisor Fiscal y la revisión periódica de la arquitectura de control de la entidad y del sistema de gestión de riesgos.

Cómite de riesgo:

Encargado de liderar la implementación y desarrollar el monitoreo de la política y estrategia de la gestión de riesgos de la Clínica.

Consecuencia:

Resultado de un suceso que afecta a los objetivos.

Control:

Medida que modifica un riesgo.

Criterio de riesgo:

Términos de referencia respecto a los que se evalúa la importancia de un riesgo.

Líder de proceso:

Persona que tiene la responsabilidad y autoridad para gestionar un riesgo.

Efecto:

Es una desviación, positiva y/o negativa, respecto a lo previsto.

Evaluación del riesgo:

Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su magnitud son aceptables o tolerables.

Evento:

Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

Gestión del riesgo:

Actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Incertidumbre:

Es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un suceso, de sus consecuencias o de su probabilidad.

Mapa de riesgos:

Representación gráfica donde se sitúan cada uno de los riesgos más representativos de la Clínica.

Nivel de Riesgo:

Magnitud de un riesgo o combinación de riesgos, expresados en términos de la combinación de las consecuencias y de su probabilidad.

Objetivos:

Pueden tener diferentes aspectos (tales como financieros, de salud y seguridad, o ambientales) y se pueden aplicar a diferentes niveles (tales como, nivel estratégico, nivel de un proyecto, de un producto, de un proceso).

Perfil de Riesgo:

Es todo el panorama de riesgos de la empresa en el que se refleja la naturaleza y la escala de sus exposiciones al riesgo agregadas y por categorías.

Probabilidad:

Posibilidad de que algún hecho se produzca.

Proceso de gestión del riesgo:

Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

Riesgo:

Efecto de la incertidumbre sobre la consecución de los objetivos.

Riesgo inherente:

Cualquier nivel de riesgo propio de la actividad, cuya evaluación se efectúa sin considerar el efecto de los mecanismos de mitigación y de control.

Riesgo residual:

Es el nivel de riesgo que resulta luego de la aplicación de las medidas de control o mitigación existentes a los riesgos inherentes.

Suceso:

Ocurrencia o cambio de un conjunto particular de circunstancias.

Tratamiento del riesgo:

Proceso destinado a modificar el riesgo.

Valoración del riesgo:

Proceso global que comprende la identificación del riesgo, el análisis del riesgo y la evaluación del riesgo.

5. Principios

Para que la gestión del riesgo sea eficaz, La Clínica cumplirá en todos sus niveles los siguientes principios cuyo propósito es la creación y protección de valor.

- **Es Integrada:** La gestión del riesgo es parte integral de todas las actividades de la Clínica.
- **Es Estructurada y exhaustiva:** Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
- **Se Adapta:** El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
- **Es Inclusiva:** La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- **Es Dinámica:** Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- **Se basa en la mejor información disponible:** Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- **Toma factores humanos y culturales:** El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
- **Mejora continua:** La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

6. Clasificación de los riesgos

La Administración de la Clínica debe gestionar los riesgos que se presenten dentro de su operación, para ello, diseñará políticas y procedimientos para cada uno de ellos basadas en la normativa vigente y en las mejores prácticas.

La clasificación de los riesgos son los siguientes:

Riesgos en Salud

Es el efecto de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios que hubiera podido evitarse. El evento, es la ocurrencia de la enfermedad, traumatismos o su evolución negativa, desfavorable o complicaciones de esta; y las causas, son los diferentes factores asociados a los eventos. De esta manera, se incluyen el marco institucional y el ciclo de gestión de riesgo en salud.

Riesgos Operacional

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

Riesgo Actuarial

Es el efecto que se puede generar por no estimar adecuadamente el valor de los contratos según los diferentes tipos de contratos relacionada con la venta de servicios, de tal manera que estos resulten insuficientes para cubrir las obligaciones futuras que se acordaron.

Riesgo de crédito

Corresponde al efecto que se puede generar como consecuencia del incumplimiento de las obligaciones por parte de sus deudores en los términos acordados (monto, plazo y demás condiciones).

Riesgo de liquidez

Es el efecto que se puede generar por no contar con recursos líquidos para cumplir con sus obligaciones de pago tanto en el corto (riesgo inminente) como en el mediano y largo plazo (riesgo latente).

Riesgo Reputacional

Es el efecto que se puede generar por toda acción propia o de terceros, evento o situación que pueda afectar negativamente el buen nombre y prestigio de la Clínica.

Riesgo de Mercado de Capitales

Es el efecto que se puede generar por un incremento no esperado, de las obligaciones con acreedores tanto internos como externos, o la pérdida en el valor de los activos, por causa de las variaciones en los parámetros del mercado tales como la tasa de interés, la tasa de cambio o cualquier otra variable de referencia que afecte los precios del mercado financiero y asimismo los estados financieros de la Clínica.

Riesgo de Grupo

Es el efeto que se puede generar como resultado de participaciones de capital o actividades u operaciones con entidades que forman parte del mismo grupo empresarial. Este se deriva de la exposición a fuentes de riesgo adicionales a las propias del negocio de la entidad, dentro de las que se encuentran, por ejemplo: i) riesgo de contagio financiero, ii) detrimentos patrimoniales por filtración de flujos o concentración de pasivos y/o; iii) posibles conflictos de intereses, que generen condiciones desfavorables en las transacciones de la entidad.

Riesgo de Fallas de Mercado

Es el efecto que se puede generar por la composición de la estructura del mercado de salud: Mercado monopólico u oligopólico; prácticas de competencia desleal (como lo son la selección de riesgo, barreras de acceso a los servicios, entre otros).

Riesgo de lavado de activos y financiación del terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (FPADM)

Es el efecto que la Clínica puede tener al ser utilizada por organizaciones criminales como instrumento para ocultar, manejar, invertir o aprovechar dineros, recursos y cualquier otro tipo de bienes provenientes de actividades delictivas o destinados a su financiación, o para dar apariencia de legalidad a las actividades delictivas o a las transacciones y fondos de recursos vinculados con las mismas. También se incluye en este riesgo el Riesgo de contagio que es el efecto que la Clínica puede tener, directa o indirectamente, por una acción o experiencia de un vinculado. El vinculado es el relacionado o asociado e incluye personas naturales o jurídicas que tienen posibilidad de ejercer influencia sobre la entidad.

Riesgos de Fraude

Es el efecto que se puede generar por cualquier acto intencional o deliberado de privar los recursos o activos de la Clínica o cualquier actuación, que, sin privar los recursos o activos de la Clínica, sea utilizada para beneficios personales.

Riesgos de Protección de datos personales

Es el efecto que se puede generar por no proteger la información privada y confidencial de las personas naturales con las que interactúa la Clínica.

7. Políticas para la gestión de riesgos

Preservamos la salud y la vida entregando una atención humanizada y de excelencia.

La Clínica se regirá por el modelo de gestión del servicio farmacéutico contenida en las disposiciones legales y de mejores prácticas en la selección de proveedores para la compra de insumos y medicamentos.

La Clínica podrá prestar sus servicios en cualquiera los diferentes mercados existentes basados en la normativa vigente.

- **Riesgos Operacional**
  Generamos confianza al trabajar bajo los más altos estándares de calidad y seguridad para lograr los mejores resultados.

Preservamos la salud y la vida entregando una atención humanizada y de excelencia.

La Clínica se regirá por el modelo de gestión del servicio farmacéutico contenida en las disposiciones legales y de mejores prácticas en la selección de proveedores para la compra de insumos y medicamentos.

La Clínica podrá prestar sus servicios en cualquiera los diferentes mercados existentes basados en la normativa vigente.

- **Riesgo Actuarial**
  Aseguramos los recursos necesarios y suficientes para garantizar la operación eficiente y eficaz de los procesos clínicos y administrativos.

Cada tipo de contrato, para la generación de ingresos, será revisado por la Gerencia Financiera para determinar su viabilidad y rentabilidad.

Periódicamente se generarán y revisarán las rentabilidades de los diferentes contratos de generación de ingresos para determinar el cumplimiento de las metas establecidas.
Periódicamente se generarán y revisarán los reportes de gestión a la atención de pacientes, así como los reportes de peticiones, quejas, reclamos y solicitudes.

- **Riesgo de crédito y Riesgo de Liquidez**
  La Administración debe asegurar, en todo momento, que las atenciones de los pacientes cuenten con las autorizaciones por parte de las aseguradoras.

La Administración debe asegurar la calidad de la facturación y la oportunidad en la radicación de las mismas.

Se evitarán hacer contrataciones con aseguradoras que posean altos indicadores de deterioro financiero. Las atenciones de pacientes que pertenecen a estas aseguradoras se efectuarán solamente para urgencias vitales.

Para aquellos casos donde se requieran atención de pacientes con aseguradoras sin contrato, la administración deberá solicitar las garantías o anticipos respectivos para evitar la no recuperación de la cartera.

Las atenciones a pacientes particulares requerirán anticipo y el monto dependerá del tipo de servicio a prestar. Se exceptúa de lo anterior la atención de urgencias vitales el cual se deberá realizar por mandato de la Ley.

Periódicamente se elaborarán y revisarán los indicadores de morosidad para determinar las acciones a seguir.

- **Riesgo de Mercado de Capitales**
  La Administración requerirá autorización de la Junta Directiva y de Casa Matriz para realizar operaciones o transacciones asociadas a cualquier tipo de tasas o cualquier variable de referencia.

Se exceptúa de lo anterior, los contratos con aseguradoras internacionales para atención de pacientes en la Clínica cuyos pagos se realizarán en las cuentas bancarias de la Clínica en el exterior.

- **Riesgo de Grupo**
  La Administración requerirá autorización de la Junta Directiva y de Casa Matriz para realizar negociaciones de compra o venta de empresas.

Las transacciones realizadas entre empresas del mismo grupo empresarial serán objeto de revelación en las notas a los estados financieros.

- **Riesgo de Fallas de Mercado**

  La Administración procurará no realizar operaciones con entidades que conforman mercado monopólico u oligopólico. La Clínica no participará en prácticas de competencia desleal.

- **Riesgo Reputacional**

  La Administración realizará seguimiento permanente a las redes sociales para determinar comentarios negativos de la Clínica y tomará acciones inmediatas para evitar un mayor impacto.

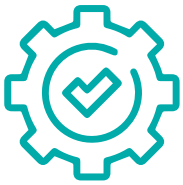
  La Administración atenderá de manera oportuna las peticiones, quejas, reclamos y solicitudes de sus partes interesadas y determinará la causa raíz de los mismos para solucionarlo.

- **Riesgo de lavado de activos y financiación del terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva (FPADM)**

  Las políticas se encuentran definidas en el manual del SARLAFT / FPADM

- **Riesgo de Fraude**

  La Clínica adopta la política “Cero tolerancia frente al fraude, la corrupción y el soborno” tomando las medidas necesarias para combatir estos flagelos, buscando implementar, de forma permanente, mecanismos, sistemas y controles adecuados que permitan su prevención, detección y tratamiento.



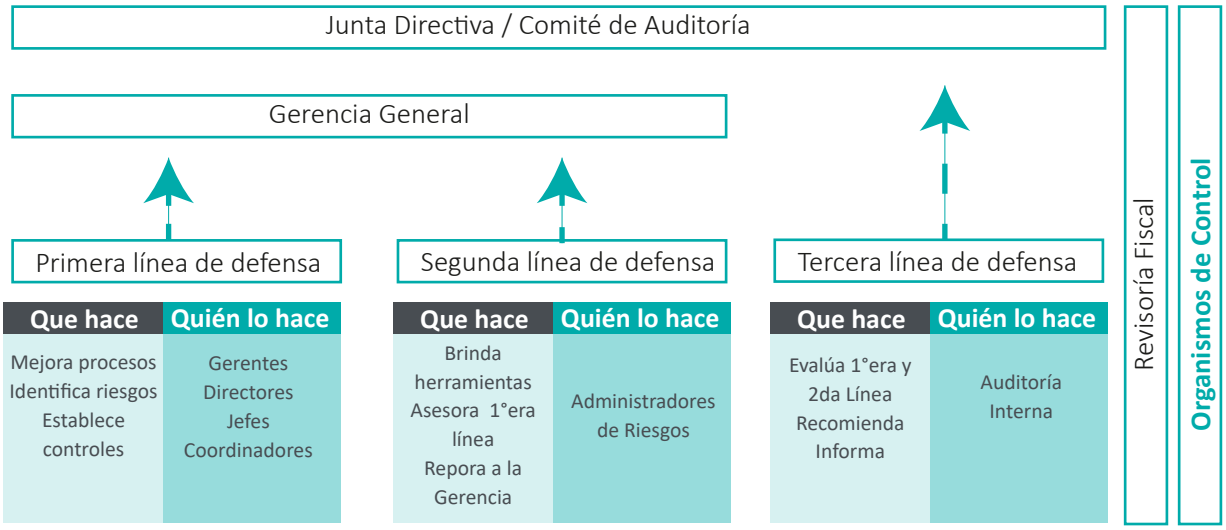
- **Riesgos de Protección de datos personales**

  La Administración debe implementar los controles necesarios para proteger la información privada y confidencial de las partes interesadas con las que interactúa.

8. Estructura, roles y responsabilidades

Estructura:

Como se indicó en el numeral 2 – Terminología, QuirónSalud aplica como parte de su diseño organizativo básico, un modelo de "3 líneas de defensa" (LoD) para estructurar funciones y responsabilidades (accountability) dentro de la empresa. Así, las “3 líneas de defensa” se traducen en:



Primera Línea de Defensa:

Responsable: Directores, jefes

Dentro de sus funciones están la de gestionar los riesgos e implementar acciones correctivas para abordar el proceso y las deficiencias de control, para ello, deben identificar, evaluar, controlar y mitigar los riesgos. Orientan el desarrollo e implementación de políticas y procedimientos internos y aseguran que las actividades sean compatibles con las metas y objetivos de la clínica Imbanaco.

A través de una estructura de responsabilidad en cascada, los colaboradores de nivel medio diseñan e implementan procedimientos detallados que sirven como controles y supervisan la ejecución de estos procedimientos por parte de su personal a cargo. Igualmente realizan el registro de eventos de riesgo presentados en la organización y establecen los planes de acción.

Segunda Línea de Defensa:
Responsable: Administrador de Riesgos

- Las funciones específicas de la segunda línea de defensa son:
- Define la política de gestión del riesgo y da soporte a la primera línea de defensa para la implementación de la política.
- Realiza monitoreo al diseño y ejecución de los controles.

Tercera Línea de Defensa:
Responsable: Auditoría Interna

- La función de control interno, a través de un enfoque basado en el riesgo, proporcionará aseguramiento sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la organización, incluidas las maneras en que funciona la primera y segunda línea de defensa.
- La Gestión del Riesgo de la clínica Imbanaco está soportado en lo siguiente:
- La política de gestión del riesgo que debe ser aprobada por la Junta Directiva.
- La implementación, prueba y mantenimiento de un proceso para administrar la continuidad de

8.1 Junta Directiva

- **Identificar, medir y gestionar** las diversas clases de riesgos (de salud, económicos, reputacionales, de lavado de activos, entre otros), y establecer las políticas asociadas a su mitigación.
- **Aprobar la política de Gestión de Riesgos,** sus modificaciones y actualizaciones.
- **Aprobar el apetito de riesgo,** teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.
- **Garantizar los recursos necesarios** para implementar y mantener en funcionamiento, de forma efectiva y eficiente del sistema de Gestión de Riesgo.
- **Revisar el desempeño de la gestión de riesgos.**

8.2 Comité de Auditoría, Riesgos y Gobierno Corporativo

- **Establecer estrategias para prevenir y mitigar los riesgos en salud.**
- **Identificar, medir, caracterizar, supervisar y anticipar,** mediante metodologías adecuadas, los diversos riesgos (de salud, económicos, operativos, de grupo, lavado de activos, reputacionales, entre otros) asumidos por la entidad, propios de su función en el SGSSS.
- **Hacer seguimiento y evaluar periódicamente el funcionamiento de los Comités internos** de la institución relacionados con asuntos de salud, incluidos los de vigilancia epidemiológica, historias clínicas, infecciones, y farmacia.
- **Velar por el cumplimiento y mejoramiento progresivo de los procesos** y estándares relacionados con la seguridad del paciente.
- **Supervisar los procesos de atención al paciente,** velar por una atención humanizada, y medir y evaluar indicadores de atención (seguimiento y análisis de quejas y reclamos, orientación al usuario, tiempos de espera, etc.).

8.3 Representante Legal

- **Implementar la política aprobada por la Junta Directiva.**
- **Comunicar la política y decisiones adoptadas por la Junta Directiva** a todos y cada uno de los funcionarios dentro de la entidad, quienes en desarrollo de sus funciones y con la aplicación de procesos operativos apropiados deben procurar el cumplimiento de los objetivos trazados por la dirección, siempre sujetos a los lineamientos por ella establecidos.
- **Implementar los diferentes informes, protocolos de comunicación, sistemas de información** y demás determinaciones de la Junta Directiva relacionados con la gestión de riesgos.
- **Fijar los lineamientos tendientes a crear la cultura organizacional de control,** mediante la definición y puesta en práctica de las políticas y los controles suficientes, de tal forma que el personal de todos los niveles comprenda la importancia del control interno e identifique su responsabilidad frente al mismo.
- **Proporcionar a los órganos de control internos y externos,** toda la información que requieran para el desarrollo de su labor.

8.3 Representante Legal

- **Proporcionar los recursos que se requieran** para el adecuado funcionamiento de la gestión del riesgo, de conformidad con lo autorizado por la Junta Directiva.

- **Apoyar y garantizar el efectivo cumplimiento** de las políticas definidas por la Junta Directiva.

- **Adelantar un seguimiento permanente** del cumplimiento de las funciones del Comité de Riesgos u Órgano equivalente, en los casos que aplique, y mantener informada a la Junta Directiva.

- **Conocer y discutir los procedimientos** a seguir en caso de sobrepasar o exceder los límites de exposición frente a los riesgos, así como los planes de contingencia a adoptar respecto de cada escenario extremo.
- **Hacer seguimiento y pronunciarse** respecto de los informes periódicos que presente el Comité de Riesgos u Órgano equivalente sobre el grado de exposición de riesgos asumidos por la entidad y los controles realizados, además de los informes presentados por la Revisoría Fiscal. Lo anterior debe plasmarse en un informe a la Junta Directiva o, quien haga sus veces, y hacer énfasis cuando se presenten situaciones anormales como mínimo en algún riesgo prioritario o existan graves incumplimientos a las políticas, procesos y procedimientos para cada uno de los Subsistemas de Administración de Riesgos.

- **Realizar monitoreo y revisión de las funciones del área de control interno.**

- **Velar porque se dé cumplimiento** a los lineamientos establecidos en el Código de Conducta y Buen Gobierno de la entidad en materia de conflictos de interés y uso de información privilegiada que tengan relación con el Sistema Integrado de Gestión de Riesgos.

- **Vigilar cuidadosamente las relaciones de todas las personas que hacen parte de la entidad** tanto interna como externamente, para identificar y controlar de manera eficiente los posibles conflictos de interés que puedan presentarse.

- **Informar de manera oportuna mediante Oficio a la Superintendencia Nacional de Salud,** acerca de cualquier situación excepcional que se presente o prevea que pueda presentarse como mínimo en el ámbito de la administración de los riesgos prioritarios, de las causas que la originan y de las medidas que se propone poner en marcha por parte de la entidad para corregir o enfrentar dicha situación, si procede.

8.4 Administrador de Riesgos

- Definir los instrumentos, metodologías y procedimientos tendientes a que la Clínica administre efectivamente los riesgos.
- Desarrollar e implementar el sistema de reportes.
- Administrar el registro de eventos de riesgo.
- Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operativo.
- Establecer y monitorear el perfil de riesgo e informarlo al Comité de Riesgos.
- Desarrollar los programas de capacitación relacionados con la gestión del riesgo.
- Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
- Apoyar en el diseño de las metodologías de segmentación, identificación, medición, control y monitoreo de los riesgos a los que se expone la entidad, para mitigar su impacto.
- Sugerir al Comité de Auditoría, Riesgos y Gobierno Corporativo, los ajustes o modificaciones necesarios a las políticas de los diferentes Subsistemas de Administración de Riesgos.
- Proponer al Comité de Auditoría, Riesgos y Gobierno Corporativo, en los casos que aplique, el manual de procesos y procedimientos, a través de los cuales se llevarán a la práctica las políticas aprobadas para la implementación de los diferentes Subsistemas de Administración de Riesgos. Asimismo, velar por su actualización, divulgación y apropiación en todos los niveles de la organización y su operatividad.
- Velar por el adecuado diseño e implementación de los controles a los diferentes riesgos para mitigar su impacto, en todos los niveles de la organización y su operatividad.
- Realizar seguimiento o monitoreo a la eficiencia y la eficacia de las políticas, procedimientos y controles establecidos.
- Apoyar a las áreas en la identificación y evaluación de los límites de exposición para cada uno de los riesgos identificados, y presentar al Comité de Riesgos, en los casos que aplique, las observaciones o recomendaciones que considere pertinentes.

- **Monitorear las condiciones de suficiencia patrimonial y financiera de la entidad,** de acuerdo con la Resolución 3100 de 2019 o las normas que la sustituyan o modifiquen.

- **Velar por el adecuado archivo de los soportes documentales** y demás información relativa al Sistema Integrado de Gestión de Riesgos de la entidad.

- **Participar en el diseño y desarrollo como mínimo de los programas de capacitación** sobre los riesgos identificados y velar por su cumplimiento. Incluir por lo menos los riesgos de los Subsistemas de Administración de Riesgos.

- **Analizar los informes presentados por la Auditoría Interna o quien haga sus veces,** y los informes que presente el Revisor Fiscal para que sirvan como insumo para la formulación de planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.

- **Monitorear e informar al Comité de Auditoría, Riesgos y Gobierno Corporativo,** en los casos que aplique, el avance en los planes de acción y de mejoramiento, para la adopción de las medidas que se requieran frente a las deficiencias informadas, respecto a temas relacionados con el Sistema Integrado de Gestión de Riesgos.

8.4 Auditoría Interna

- **Evaluar periódicamente la efectividad y cumplimiento** de la gestión del riesgo con el fin de determinar las deficiencias y sus posibles soluciones.

- **Informar los resultados de la evaluación de la Gestión** de Riesgos al Comité de Auditoría, al Representante Legal y al Administrador de riesgos.

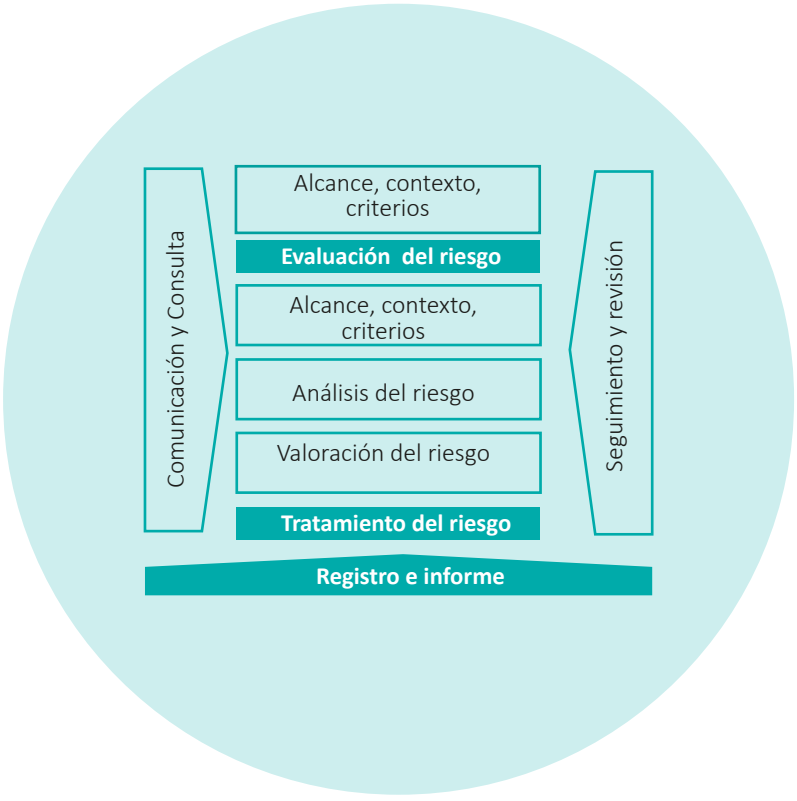
- **Realizar una revisión periódica del registro de eventos de riesgo.**

8.6 Líderes de Procesos

- Conocer y cumplir las políticas y procedimientos correspondientes a la Gestión y Control del Riesgo.
- Identificar los riesgos de los procesos y gestionarlos bajo la metodología que se describe en la presente política.
- Facilitar toda la información que sea necesaria al Administrador de Riesgos y Auditoría Interna de manera que pueda brindar el apoyo necesario para realizar seguimiento a los distintos riesgos.
- Establecer las medidas preventivas y planes de acción más convenientes para tratar el riesgo y conseguir así el perfil de riesgo que la Clínica se ha propuesto.

9.Proceso de gestión del riesgo

El proceso de gestión del riesgo es una parte integrante de la gestión de la Administración y se integra en la cultura y en las prácticas de la Clínica adaptándose a los procesos de negocio de la organización y comprende las siguientes actividades (tomado de la norma ISO 31000 – Gestión del riesgo)



9.1 Comunicación y Consulta

En esta etapa se asistirá a las partes interesadas pertinentes a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo. La consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.

La comunicación y consulta se realizará en todas y cada una de las etapas del proceso de la gestión del riesgo.

9.2 Alcance, contexto y criterios

El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo, para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo.

9.2.1 Alcance

Al interior de la entidad, la gestión del riesgo se aplicará a niveles estratégico, operacionales (procesos), de proyecto u otras actividades que puedan surgir, tomando como consideración entre otros aspectos los objetivos y las decisiones que se necesitan tomar, así como los resultados esperados de las etapas a ejecutar en el proceso.

9.2.2 Contexto Externo e Interno

Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos

En el contexto externo se incluye entre otros aspectos sin limitarse a ellos:

- Entorno social y cultural, político, legal, reglamentario, financiero, tecnológico, económico, natural y competitivo.
- Factores y las tendencias clave que tengan impacto en los objetivos de la organización.
- Relaciones con las partes interesadas externas, sus percepciones y sus valores.

En el contexto interno: Constituye todo aquello al interior de la Clínica que puede influir en la manera en la que una organización gestionará el riesgo. Incluye entre otros aspectos sin limitarse a ellos:

- El gobierno, la estructura, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que se establecen para conseguirlos;
- Las aptitudes, entendidas en términos de recursos y conocimientos (capital, tiempo, personas, procesos, sistemas y tecnologías).
- La cultura de la organización;
- Los sistemas de información, los flujos de información y los procesos de toma de decisiones (tanto formales como informales)

.

9.2.3 Criterios del riesgo

Los criterios del riesgo reflejan los valores, objetivos y recursos de la organización y son coherentes con las políticas y declaraciones acerca de la gestión del riesgo. En el documento "Anexo 1 – Definiciones de criterios de riesgo" se encuentra el nivel de detalle de los criterios tanto del impacto como de la probabilidad.

9.2.4 Apetito / Tolerancia de Riesgo

El apetito/tolerancia al riesgo estará alineado con los límites de la matriz de impacto x probabilidad y por las directrices de Casa Matriz. La organización tratará que el apetito/tolerancia sea categoría "BAJO" en sus riesgos residuales sin embargo, por el modelo de negocio puede estar en otra calificación superior.

9.3 Evaluación del Riesgo: Ciclo General de Gestión de Riesgos

La evaluación del riesgo es el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo. Se llevará a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Utilizará la mejor información disponible, complementada por investigación adicional, si fuese necesario.

9.3.1 Identificación

El propósito de la identificación del riesgo es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a la Clínica lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada.

Para la identificación se deben tener en cuenta los siguientes factores, sin limitarse a ellos así estén o no bajo su control

- Las fuentes de riesgo tangibles e intangibles
- Las causas y los eventos
- Las amenazas y las oportunidades;
- Las vulnerabilidades y las capacidades;
- Los cambios en los contextos externo e interno;
- Los indicadores de riesgos emergentes;
- Las consecuencias y sus impactos en los objetivos;
- Las limitaciones de conocimiento y la confiabilidad de la información;
- Los sesgos, los supuestos y las creencias de las personas involucradas.

9.3.2 Análisis del riesgo: Evaluación y Medición

El propósito del análisis del riesgo es comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo. La Clínica efectuará este análisis de riesgo tanto para el riesgo inherente (calificación del riesgo antes de controles) como para el riesgo residual (calificación del riesgo después de que se ha implementado los controles y se encuentran en funcionamiento).

Realizar el análisis de los riesgos de forma inherente como residual, permitirá determinar la madurez de los controles al interior de la organización.

9.3.2.1. Metodología de calificación de los riesgos

Tanto el riesgo inherente como el riesgo residual se calificarán bajo la metodología "IMPACTO y PROBABILIDAD" los lineamientos para cada calificación estarán descritos en el documento "Anexo 1 – Definiciones de criterios de riesgo"

Impacto	Probabilidad
Severo	Casi seguro
Alto	Probable
Medio	Posible
Bajo	Raro/ Remoto

9.3.2.1 Severidad de los riesgos

Las siguientes son las calificaciones de los niveles de severidad establecidos en la Clínica y las acciones que se deben seguir para cada uno de ellos:

Extremo
Alto
Moderado
Bajo

9.3.2.3 Mapa de riesgos

El mapa de riesgo se construye ubicando en la matriz las calificaciones de la probabilidad y del impacto. El mapa de riesgo para la Clínica es el siguiente:

	1 – Bajo	2 - Medio	3 - Alto	4 - Severo
Reputacional	**Clientes** • Número bajo de reclamaciones (reclamaciones generales o con amenaza de acudir a medios de comunicación).	**Clientes** • Número medio de reclamaciones (sobre un incidente sensible, con amenaza de acudir a medios de comunicación o reclamantes de perfil alto).	**Clientes** • Número alto de reclamaciones. • Caída de puntuaciones NPS en un porcentaje alto.	**Clientes** • Número muy alto de reclamaciones. • Caída de puntuaciones NPS en un porcentaje muy alto. • Caída significativa en la utilización de nuestros productos o servicios.
	Empleados Poco interés, por ejemplo, algunas "charlas en zonas comunes"	**Empleados** Existe un volumen medio de personas que plantean el asunto a sus responsables y/o a través de los canales de comunicación interna.	**Empleados** Existe un volumen alto de personas que plantean el asunto a sus responsables y/o a través de los canales de comunicación interna.	**Empleados** Existe un volumen muy alto de personas de todo QS que demandan medidas correctivas.
	Otros interesados Sin interés	**Otros interesados** Interés medio, p. ej.: • Impacto reputacional a efectos de la autoridad local • Los sindicatos u otros grupos de interés plantean la cuestión informalmente.	**Otros interesados** Interés alto, p. ej.: • Las autoridades demandan una respuesta públicamente. • Los sindicatos u otros grupos plantean el asunto formalmente o públicamente. • Hay socios y proveedores que reconsideran su relación con QS.	**Otros interesados** Interés muy alto, p. ej.: • Impacto reputacional a efectos del Gobierno, que emite observaciones públicas o inicia investigaciones. • Grupos de presión activos. • Socios y proveedores cancelan su relación con QS.
	Medios de comunicación Niveles bajos de cobertura adversa, p. ej.: • Volumen reducido en medios de baja difusión (p. ej., publicación local/regional). • La noticia dura un día. • QS no está en el centro de atención. Es decir, es una más de las empresas implicadas.	**Medios de comunicación** Niveles medios de cobertura adversa, p. ej.: • Volumen medio en medios de baja o mediana difusión (p. ej., publicación local/regional o medio especializados) o cobertura muy reducida en medios de alta difusión. • La noticia dura un par de días. • QS no es el centro de atención o los artículos son descriptivos o muestran nuestros mensajes.	**Medio de comunicación** Niveles altos de cobertura adversa, p. ej.: • Volumen medio o alto en medios nacionales o internacionales de alta difusión (p. e., prensa especializada o medios nacionales, o programas matinales, tertulias radiofónicas, o programas de entretenimiento nocturnos). • La noticia dura varios días. • QS es el centro de atención o el asunto suscita un grado elevado de análisis/comentarios.	**Medio de comunicación** Niveles muy altos de cobertura adversa, p. ej.: • Volumen alto en medios nacionales o internacionales de alta difusión. • Cobertura sostenida durante varios días. • QS es el foco exclusivo de atención y/o es analizada en profundidad (ej: artículos de opinión de analistas de alta difusión).
	Redes sociales Interés bajo, p. ej.: • Contenido negativo compartido por usuarios con pocos seguidores. • Nivel de actividad bajo (me gusta / comparte / comentarios). • El debate en redes sociales no está centrado solo en QS. Es decir, hay otras empresas implicadas o hay otros focos diferentes en la conversación (por ejemplo, sanidad pública vs. sanidad privada).	**Redes sociales** Interés medio, p. ej.: • Contenido negativo compartido por un *influencer*, o un número medio de usuarios con una cantidad baja o media de seguidores. • Nivel de actividad medio (me gusta / comparte / comentarios). • QS está en el centro de los comentarios pero hay otros implicados y hay diferentes focos dentro de la conversación. • Posible riesgo de contagio a los medio de	**Redes sociales** Interés alto, p. ej.: • Contenido negativo compartido por un *influencer*, o por un número medio o alto de usuarios. • Nivel de actividad alto (me gusta / comparte / comentarios). • Creación de un *hashtag*, sitio web (por ejemplo, change.org) o grupo de Facebook críticos hacia QS. • QS está en el centro de los comentarios. • Contagio a los medios de comunicación	**Redes sociales** Interés muy alto, p. ej.: • Contenido negativo compartido por un *influencer*, o por un número alto o muy alto de usuarios. • Nivel de actividad alto o muy alto (me gusta / comparte / comentarios). • Uso frecuente de un *hashtag*, con el nombre de la empresa (Trending Topic), actualización diaria de un sitio web (o alto número de firmas en webs como change.org) o actualización diaria de un

9.3.2.4 Calificación del Riesgo Inherente

Es aquel que puede existir de manera intrínseca en toda actividad. No tiene en cuenta el efecto de los controles.

Las calificaciones las asignará el líder del proceso de acuerdo con el nivel de criticidad de las variables las cuales se encuentran definidas en el documento "Anexo 1 – Definiciones de criterios de riesgo". Los riesgos no se promedian: La calificación estará determinada por la mayor exposición del riesgo en cualquiera de los factores.

9.3.2.5 Calificación del Riesgo Residual

Es el riesgo que resulta tras la aplicación de los oportunos controles que hayan sido considerados por la organización.

La calificación del riesgo residual estará a cargo de cada líder de proceso, después de haber calificado los riesgos inherentes. La calificación del riesgo residual está basada en un juicio cualitativo teniendo en cuenta el diseño y la ejecución de los controles. Los controles para que sean eficaces deben tener las siguientes características tanto en diseño como ejecución:

Responsabilidad del control: Estar asignados a un responsable con una adecuada segregación de funciones

Tipo de Control: Se refiere a si el control es manual o automático. Se considera más fuerte el control cuando es automático.

Naturaleza del control: Preventivo o Detectivo. Se considera más fuerte el control cuando es Preventivo.

Frecuencia del control: Cada cuanto se ejecuta el control. Se considera más fuerte el control si la periodicidad de ejecución es la más apropiada para prevenir el riesgo.

Documentación: Se considera más fuerte el control cuando el mismo se encuentra documentado en una política, procedimiento, etc en la plataforma habilitada para ello.

Los riegos residuales administrativos calificados en “EXTREMO” y “ALTO” serán monitoreados por la Auditoría Interna y presentados en el Comité de Auditoría, Riesgos y Gobierno Corporativo en forma semestral. Para los riesgos asistenciales calificados en esta categoría serán monitoreados por la Dirección de Calidad.

Ejecución del Control: Un control puede estar adecuadamente diseñado, pero sino se ejecuta por parte de los responsables el riesgo tiene más probabilidad de materializarse. Las siguientes serán las calificaciones de la ejecución del control:

Alto:El control está diseñado y funciona eficazmente según lo previsto y puede ser probado y evidenciado.
Medio:El control existe, pero hay deficiencias en su diseño y/o eficacia operativa.
Bajo:El control está establecido, pero es ineficaz, debido a un diseño inadecuado y/o a un funcionamiento incoherente que ha sido identificado o el control no está funcionando.

La evidencia de la ejecución del control estará a cargo del líder del proceso quién deberá demostrar el cumplimiento de los mismos por cualquiera de los mecanismos que considere adecuado.

Un control se considera no satisfactorio cuando no se cumplan todos o alguno de los elementos mencionados anteriormente, para ello, cada líder de proceso deberá tomar las acciones necesarias para garantizar el cumplimiento de estos elementos.

9.3.3 Valoración del Riesgo

El propósito de la valoración del riesgo es apoyar a la toma de decisiones. La valoración del riesgo implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar las acciones a seguir. Al interior de la Clínica las siguientes acciones se deberán realizar según la severidad del riesgo residual:

Extremo	Debe ser puesto en conocimiento de la Gerencia General, la Junta Directiva y el Comité de Auditoría, Riesgos y Gobierno Corporativo y ser objeto de tratamiento inmediato
Alto	Exige la atención del Gerente General y las demás Gerencias, debe ser tratado y monitoreado. Debe ser informado a la Junta Directiva y Comité de Auditoría, Riesgos y Gobierno Corporativo.
Moderado	Debe ser gestionado adecuadamente por los líderes de los procesos y ser objeto de monitoreo continuo. Debe informarse a la Gerencia General.
Bajo	Debe continuar gestionándose con los controles actuales existentes en la organización.

Los líderes de los procesos implementarán los controles necesarios para que sus riesgos residuales sean BAJOS basados en la premisa costo/beneficio donde el control no puede ser más costoso que la materialización del riesgo. No obstante, los riesgos residuales pueden estar en un nivel de severidad mayor justificando los motivos de los mismos.

Los niveles de tolerancia de riesgos estarán determinados por la organización con base en sus indicadores de gestión (KPI) e indicadores de riesgo (KRI) indicados en el numeral 8.5 de esta política.

9.3.3 Tratamiento del Riesgo

El propósito del tratamiento del riesgo es seleccionar e implementar opciones para abordar el riesgo. El tratamiento del riesgo implica un proceso iterativo de:

Las opciones de tratamiento de riesgo son los siguientes:

Tratamiento	Descripción
Evitar	Consiste en no realizar la actividad que genera el riesgo. Evitar supone salir de las actividades que generen riesgos, puede incluir acciones como: • Retirar la fuente de riesgo. • Prescindir de una unidad de negocio, línea de producto o segmento geográfico. • Decidir no emprender nuevas iniciativas/ actividades que podrían dar lugar a riesgos
Reducir	Implica llevar a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez.
Transferir	La probabilidad o el impacto del riesgo se reduce trasladando, o compartiendo el riesgo con uno o varias de las partes. • Adquirir seguros contra pérdidas inesperadas y significativas. • Entrar en sociedad compartida (joint venture). • Establecer acuerdos con otras empresas. • Establecer contratos de servicio • Utilizar instrumentos de mercado de capital. • Tercerizar procesos de negocio.
Aceptar	• Consiste en retener el riesgo para perseguir una oportunidad y establecer un plan apropiado de financiación del riesgo • Provisionar las posibles pérdidas. • Confiar en las compensaciones naturales existentes dentro de un portafolio.

La selección de la opción más apropiada de tratamiento del riesgo implica obtener un análisis de los costos/beneficios.

El tratamiento de los riesgos estará a cargo de cada Líder de proceso y debe ser revisada por cada Gerente del proceso para cumplir con los siguientes objetivos:

- Tener un mejor conocimiento de los controles establecidos y determinar si dichos controles mitigan los riesgos de su proceso.
- Validar que el costo de la implementación de los controles es menor que los beneficios recibidos.
- Adicionar o eliminar nuevos controles o cambiar el tratamiento.

Los planes de tratamiento deben incluir por lo menos los siguientes aspectos:

- Las razones que justifican la selección del tratamiento, incluyendo los beneficios previstos;
- Las personas responsables de la aprobación del plan y de la implementación del plan.
- Las acciones propuestas;
- Las necesidades de recursos, incluyendo las contingencias;
- Las medidas del desempeño y las restricciones;
- Los requisitos en materia de información y de seguimiento; y
- El calendario y la programación.

La aceptación del riesgo estará a cargo del Gerente General y/o de la Junta Directiva según su nivel de criticidad y exposición para la organización.

9.5. Seguimiento y Revisión

El propósito del seguimiento y la revisión es asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso.

La revisión de los riesgos se realiza por lo menos cada año y es realizada por el Administrador de los riesgos, los líderes de los procesos y los órganos de control.

Este manual se revisará anualmente por parte del administrador de riesgos o persona responsable para esta función. Cualquier modificación al mismo debe presentarse al Comité de Auditoría, Riesgos y Gobierno Corporativo para su revisión y aprobación.

Lo anterior no exime a que si antes de esta periodicidad se identifica un riesgo el mismo debe ser analizado con lo indicado en esta política.

Cada líder de proceso implementará indicadores de ejecución (KPI) que tienen como finalidad informar, controlar, evaluar y ayudar a tomar las decisiones y deberán estar alineados a la estrategia de la organización. Para cada indicador se deberá establecer los niveles “Meta” de cumplimiento, así como los niveles de “precaución” y “críticos”. Estos dos últimos niveles serán considerados como señales de alerta (KRI).

Los KPI hacen parte de los pilares estratégicos de la organización y soportan las iniciativas estratégicas. El seguimiento se efectuará mensualmente en el Comité de Gerencia Estratégico y se reportarán a Casa Matriz.

Lo anterior no exime a que si antes de esta periodicidad se identifica un riesgo el mismo debe ser analizado con lo indicado en esta política.

Cada líder de proceso implementará indicadores de ejecución (KPI) que tienen como finalidad informar, controlar, evaluar y ayudar a tomar las decisiones y deberán estar alineados a la estrategia de la organización. Para cada indicador se deberá establecer los niveles "Meta" de cumplimiento, así como los niveles de "precaución" y "críticos". Estos dos últimos niveles serán considerados como señales de alerta (KRI).

Los KPI hacen parte de los pilares estratégicos de la organización y soportan las iniciativas estratégicas. El seguimiento se efectuará mensualmente en el Comité de Gerencia Estratégico y se reportarán a Casa Matriz.

De llegarse a presentar desviaciones o que se incumplan los indicadores "Meta", los líderes de los procesos se deben establecer planes de contingencia para intervenir y tratar los diferentes riesgos, teniendo en cuenta la variabilidad de los riesgos identificados, con el propósito de ajustar las desviaciones lo más pronto posible.

Cada líder será responsable y establecerá los plazos, periodicidad, reportes de avance y de evaluaciones periódicas sobre las estrategias seleccionadas.

Los incumplimientos a los límites serán presentados en el Comité de Auditoría, Riesgos y Gobierno Corporativo donde se informará los planes de contingencia adoptados respecto de cada escenario extremo presentado.

El proceso de seguimiento y revisión abarcan todos los aspectos del proceso de gestión del riesgo, con la finalidad de:

• Asegurar que los controles son eficaces y eficientes tanto en su diseño como en su utilización.

• Obtener la información adicional para mejorar la valoración del riesgo.

• Analizar y sacar conclusiones de los sucesos (incluyendo los cuasi-accidentes), cambios, tendencias, éxitos y fallos.

• Detectar los cambios en el contexto interno y externo, incluidos los cambios en los criterios de riesgo y en el propio riesgo, que puedan requerir la revisión de los tratamientos de riesgo y de las prioridades.

• Identificar los riesgos emergentes.

9.6. Registro e informe

La alta dirección de la Clínica proporcionará comunicaciones específicas y orientadas que se dirigirán a las expectativas de comportamiento y las responsabilidades del personal, incluyendo una clara exposición de su filosofía y enfoque de gestión de riesgos, su delegación y autoridad.

9.6.1 Divulgación de la Información Interna

Como resultado del monitoreo y control de cada uno de los riesgos identificados y especialmente los prioritarios, la Clínica elaborará reportes semestrales como mínimo, que permitan establecer el perfil de riesgo de éstas.

Asimismo, al cierre del ejercicio contable informará sobre el cumplimiento de las políticas, los límites establecidos y su grado de cumplimiento, el nivel de exposición a los diferentes riesgos a los que se ven expuestas las entidades que incluya los prioritarios y la cuantificación de los efectos de la posible materialización de estos sobre la salud de la población de su área de influencia, las utilidades, el patrimonio y el perfil de riesgo de la Clínica.

Estos informes serán presentados al Representante Legal, a la Junta Directiva y los líderes de los procesos involucrados, los cuales deben quedar plasmados en acta donde se socialicen estos informes.

9.6.1 Divulgación de la Información Externa

El Representante Legal, en el informe de gestión anual incluirá en las notas a los estados financieros un apartado sobre la gestión adelantada en materia de administración de los diferentes subsistemas de gestión de riesgos el contendrá un resumen de su situación en materia de la administración de dichos riesgos con información cualitativa y cuantitativa.

En la información cualitativa se informará sobre los objetivos, estrategias y filosofía en la gestión de riesgos y los controles implementados en cada uno para mitigarlos, así como los cambios potenciales en los niveles de riesgo, cambios materiales en las estrategias y límites de exposición para cada uno de los Subsistemas de Administración de Riesgos.

En la información cuantitativa sobre la gestión integral de los riesgos se informará el resultado de la políticas y metodologías internas aplicadas prevaleciendo el carácter privilegiado, confidencial o reservado de la información.

9.6.3 Capacitaciones

La comunicación sobre procesos y procedimientos estará alineada con la cultura deseada, la cual se reforzará en todo momento. Para lograr lo anterior la Clínica contará con una estrategia de capacitación sobre el sistema de Gestión de Riesgos.

La estrategia de capacitación se basa en el plan para la comunicación y consulta de cada paso del proceso de gestión de riesgo. El mismo abarca tanto las partes interesadas internas como externas.

10. Procesos y procedimientos para la gestión de riesgos

La Clínica establecerá los procesos y procedimientos para instrumentar la Política de Gestión de Riesgo, para ello, cada subsistema de gestión de riesgos contará con documentación en forma separada de este manual y que hace parte integral del mismo.

Esta documentación contendrá como mínimo los siguientes aspectos: Implementación de las diferentes etapas del ciclo general de riesgos y los elementos específicos.

• Dar los lineamientos para garantizar el efectivo y oportuno funcionamiento de los Subsistemas de Administración de Riesgos, para adoptar oportunamente los correctivos necesarios.

• Definir las acciones a seguir en caso de incumplimiento de los límites fijados y los casos en los cuales se deban solicitar autorizaciones especiales.

•Determinar los informes internos y externos, que permitan la toma de decisiones de manera oportuna en todas las instancias de la organización.

11. Documentación

Las etapas del ciclo general de riesgos y los elementos específicos de los diferentes Subsistemas de Administración de Riesgos estarán soportados en documentos y registros, garantizando la integridad, oportunidad, trazabilidad, confiabilidad y disponibilidad de la información allí contenida.

Esta documentación contendrá como mínimo lo siguiente:

• Las políticas para la administración de cada uno de los riesgos.
• Las metodologías y procedimientos para la identificación, medición, control y monitoreo de los riesgos identificados. A su vez, el establecimiento de los niveles de aceptación y límites de exposición.
• La estructura organizacional que garantice el desarrollo de cada uno de los Subsistemas de Administración de Riesgos y que, a su vez, fortalezca el Sistema Integrado de Gestión de Riesgos.
• Los roles y responsabilidades de quienes participan en la gestión de los diversos riesgos identificados, especialmente los prioritarios.
• Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos de cada uno de los Subsistemas de Administración de Riesgos.
• Roles, responsabilidades y acciones de los órganos de control interno frente a cada uno de los Subsistemas de Administración de Riesgos.
• Las estrategias de capacitación y divulgación de cada uno de los Subsistemas de Administración de Riesgos.

Igualmente hacen parte de la documentación:

• Las actas de la Junta Directiva, donde conste la aprobación, ajustes o modificaciones a las políticas de los Subsistemas de Administración de Riesgos.
• Los instructivos o manuales que contengan los procesos y procedimientos a través de los cuales se llevan a la práctica las políticas aprobadas para cada uno de los Subsistemas de Administración de Riesgos.
• El Código de Conducta y Buen Gobierno.
• Los informes presentados por la Junta Directiva, el Representante Legal y el Comité de Auditoría, Riesgos y Gobierno Corporativo. Entre estos debe encontrarse un reporte sobre el cumplimiento de los límites y del nivel de exposición de los diferentes riesgos establecidos por la entidad, particularmente los prioritarios.
• Los informes presentados por los órganos de control, sobre el funcionamiento y resultados de la implementación de cada uno de los Subsistemas de Administración de Riesgos.
• Las actas de Junta Directiva en donde conste la presentación del informe del Comité de Riesgos y del Revisor Fiscal, en los casos que aplique.
• Las constancias de las capacitaciones impartidas a todos los empleados, socios, directivos, administradores y cualquier otra persona que tenga vinculación con la entidad sobre el Sistema Integrado de Gestión de Riesgos, con el fin de asegurar que sean entendidas e implementadas en todos los niveles de la organización.
• Los documentos y registros que evidencien el funcionamiento oportuno, efectivo y eficiente de cada uno de los Subsistemas de Administración de Riesgos.
• Las metodologías, parámetros, fuentes de información y demás elementos utilizados para la medición de cada uno de los riesgos.
• El procedimiento a seguir en caso de incumplimiento a los límites preestablecidos en cada uno de los Subsistemas de Administración de Riesgos.

12. Infraestructura tecnológica

La Clínica dispondrá y utilizará la infraestructura tecnológica y los sistemas necesarios para garantizar el funcionamiento efectivo, eficiente y oportuno del Sistema Integrado de Gestión de Riesgos para generar informes confiables. Contará con un soporte tecnológico acorde con sus actividades, operaciones, riesgos asociados y tamaño que le permita centralizar la información relacionada con la gestión de riesgos el cual debe ser validado por lo menos una vez al año.

13. Vigencia

La última actualización fue aprobada el 17 de agosto de 2022 en el Comité de Auditoría, Riesgos y Gobierno Corporativo mediante acta # 19.