MANUAL DE TRANSPARENCIA Y ÉTICA EMPRESARIAL (PTEE) PARA LA PREVENCIÓN DEL RIESGO DE CORRUPCIÓN, OPACIDAD, FRAUDE Y SOBORNO (COFS)

Diagnóstico

Cedimed

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Cedimed está comprometida con el desarrollo de sus negocios a través de un modelo de gestión basado en principios, lineamientos y objetivos socialmente responsables y en cumplimiento de sus valores y principios éticos hace manifiesta su posición de "Cero Tolerancia frente a la corrupción, opacidad, fraude o soborno (COFS)" como una política inquebrantable del quehacer organizacional.

En el Programa de Transparencia y Ética Empresarial, Cedimed compila de manera integral todas las normas internas en materia de prevención y mitigación de los Riesgos de corrupción, opacidad, fraude y soborno, así como los principios y valores éticos establecidos, para llevar a cabo su operación de manera ética, transparente y honesta.

2. OBJETIVOS DEL PROGRAMA DE TRANSPARENCIA Y ETICA EMPRESARIAL

- **Objetivo General:**

Prevenir y mitigar oportunamente los riesgos de COFS, a través de la implementación de las acciones preventivas o correctivas que se consideren necesarias para controlar los factores que los generan.

- **Objetivos Específicos:**

➢ Fomentar el diseño e implementación de controles que faciliten la prevención de riesgos de COFS.
➢ Liderar los procedimientos requeridos para detectar oportunamente posibles situaciones que se materialicen en riesgos COFS.
➢ Reducir el nivel de exposición a riesgos COFS.
➢ Fortalecer la cultura de control interno en la entidad.

3. DEFINICIONES

ADMINISTRACIÓN DE RIESGOS: Cultura, procesos y estructuras que están dirigidas hacia la Administración efectiva de oportunidades potenciales y efectos adversos.

ANÁLISIS DEL RIESGO: Proceso para comprender la naturaleza del Riesgo y determinar su nivel. Proporciona las bases para decidir sobre el tratamiento del Riesgo.

LINEA DE TRANSPARENCIA: Herramienta diseñada para prevenir y detectar eventos COFS, además de monitorear oportunamente las irregularidades que involucren a colaboradores, proveedores, clientes y terceros.

CIBERCRIMEN: Actividades ilícitas que se llevan a cabo para robar, alterar, manipular, enajenar o destruir información o activos (como dinero, valores o bienes desmaterializados) de compañías, valiéndose de herramientas informáticas y tecnológicas.

COFS: Abreviatura de corrupción, opacidad, fraude y soborno.

COLUSIÓN: Acuerdo indebido con otras personas para cometer un ilícito.

CONSECUENCIA: Efectos generados por la ocurrencia de un Riesgo que afecta los

objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento

CORRUPCIÓN: obtención de un beneficio particular por acción u omisión, uso indebido de una posición o poder, o de los recursos o de la información.

CONFLICTO DE INTERÉS: Situación en virtud de la cual una persona (colaborador, prestador de servicio, o tercero vinculado a Cedimed), debido a su actividad se enfrenta a distintas alternativas de conducta con relación a intereses incompatibles, ninguno de los cuales puede privilegiar en atención a sus obligaciones legales o contractuales.

EVENTO: Incidente o situación que ocurre en la empresa durante un intervalo particular de tiempo. Evento presencia o cambio de un conjunto particular de circunstancias.

EVALUACIÓN DEL RIESGO: Proceso de comparación de resultados del análisis del Riesgo con los criterios del Riesgo para determinar si el Riesgo, su magnitud (nivel) o ambos son aceptables o tolerables.

FRAUDE: Cualquier acto ilegal caracterizado por ser un engaño, ocultación o violación de confianza, que no requiere la aplicación de amenaza, violencia o de fuerza física, perpetrado por individuos y/u organizaciones internos o ajenos a la entidad, con el fin de apropiarse de dinero, bienes o servicios.

MONITOREO: Es el proceso continuo y sistemático mediante el cual se verifica la eficiencia y eficacia de una política o de un proceso, mediante la identificación de sus logros y debilidades para recomendar medidas correctivas tendientes a optimizar los resultados esperados.

OPACIDAD: Falta de claridad o transparencia, especialmente en la gestión pública.

PTEE: Abreviatura del Programa de Transparencia y Ética Empresarial.

SEGMENTACIÓN: Es el proceso por medio del cual se lleva a cabo la separación de elementos en grupos homogéneos al interior de ellos y heterogéneos entre ellos. La separación se fundamenta en el reconocimiento de diferencias significativas en sus características.

SOBORNO: Dar dinero o regalos a alguien para conseguir algo de forma ilícita.

- **Tipologías de fraude**

Los fraudes corporativos pueden dividirse en tres categorías principales:

Fraude de estados financieros: Es la deliberada presentación errónea de la situación financiera de la empresa, que se logra de la presentación intencionalmente errónea de cifras o revelaciones o la omisión de las mismas en los estados financieros para engañar a los usuarios de los estados financieros.

Apropiación indebida o malversación de activos: Hurto o utilización indebida de activos de la entidad o bajo responsabilidad de los colaboradores para el beneficio propio o de terceros, generando pérdidas a la entidad. Esta tipología involucra la administración de efectivo, activos fijos y administración de la información de reserva

incluyendo el cibercrimen.

Sustracción de activos:
Se pueden dividir en dos grandes categorías: los que involucran efectivo y los que no involucran efectivo.

Los fraudes con efectivo, que representan hasta un 90% de todas las sustracciones de efectivo, pueden dividirse en tres grandes categorías:

a. *Desembolsos fraudulentos.* Generación de desembolsos para cubrir servicios no prestados, a través de estrategias como: facturación falsa, falsificación de cheques, etc.
b. *Ocultamiento:* Robo de efectivo antes de registrarse en los libros y registros de la organización.
c. *Robo de efectivo:* Robo de efectivo después de registrarse en los libros y registros de la organización.

Corrupción: Los esquemas de corrupción ocurren cuando los funcionarios usan su influencia en una operación de negocios con el fin de obtener algún beneficio para ellos o para otra persona.

Lavado de activos: Toda actividad que pretende dar apariencia de legalidad a dinero de procedencia ilícita.

Incumplimiento de la normativa interna y externa: Actividad ilícita en la cual se identifique incumplimiento de las políticas internas y externas de Cedimed, con el fin de obtener un beneficio personal o para un tercero. Esta tipología puede presentarse en las siguientes situaciones:

- Falsificación o alteración de documentos o registros exigidos por la normatividad interna o externa.
- Infracción a la propiedad intelectual
- Violación de las políticas internas de Cedimed por los colaboradores
- Omisión o impedir la implementación de controles

- **Factores generadores de fraude**

Los factores de riesgo de fraude no necesariamente señalan la existencia de fraude, sin embargo, a menudo están presentes en las circunstancias cuando existe fraude y pueden ayudar a identificar los riesgos de fraude potenciales. Las combinaciones de los siguientes tres factores que se van a mencionar conforman el triángulo de fraude, cada vez que se complete este triángulo se materializa un fraude.

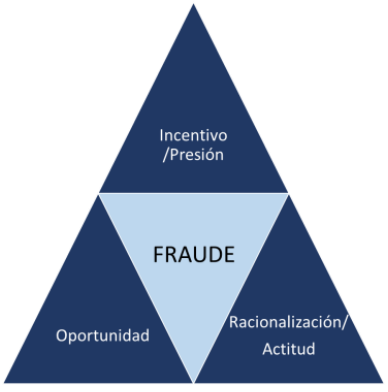


Gráfico No. 2 Triángulo de fraude

i. **Incentivos o presiones:** Las presiones pueden ser reales o percibidas, ejemplos: presiones financieras personales o presiones para lograr objetivos o metas corporativas. Por otra parte, pueden existir incentivos que incrementan la probabilidad de fraude, ejemplos: bonos de la administración estructurados con base en el logro de los objetivos financieros.

ii. **Racionalización:** Racionalización es el proceso mediante el cual la persona que comete fraude legitima o justifica el crimen. A menudo incluye una actitud o un sentimiento de derecho o la creencia de que la empresa puede permitir ello. Ejemplo: Quien comete un fraude puede racionalizar un robo diciendo *la compañía gana millones, perdería solo unos pocos miles y yo realmente necesito el dinero.*

iii. **Oportunidades:** Las oportunidades de cometer fraude se pueden manifestar de diferentes maneras. Puede ser a través de la implementación de controles inadecuados o la elusión de actividades de control o monitoreo. Adicionalmente, la baja percepción de la detección o de las consecuencias sin sentido para comportamientos inapropiados dentro de la organización, genera mayores oportunidades para que ocurra un fraude.

4. MEDIDAS DE CONDUCTA

4.1. Lineamientos Generales

Cedimed cuenta con diferentes políticas y procedimientos encaminados a implementar acciones para el fortalecimiento continuo de una cultura ética, transparente, de lucha contra la corrupción, opacidad, fraude, una gestión antisoborno.

Estos documentos contienen, los principios éticos y valores institucionales, el direccionamiento estratégico, políticas para propender una gestión ética, en la interacción con los diferentes grupos de interés, pautas que guían las relaciones con cada uno de los grupos de interés, pautas de conducta frente a la corrupción, la opacidad, el fraude y la Gestión antisoborno, el tratamiento de las actuaciones ilegales o sospechosas, pautas de comportamiento frente a regalos e invitaciones, entre otros aspectos.

Los lineamientos principales están en los siguientes documentos:

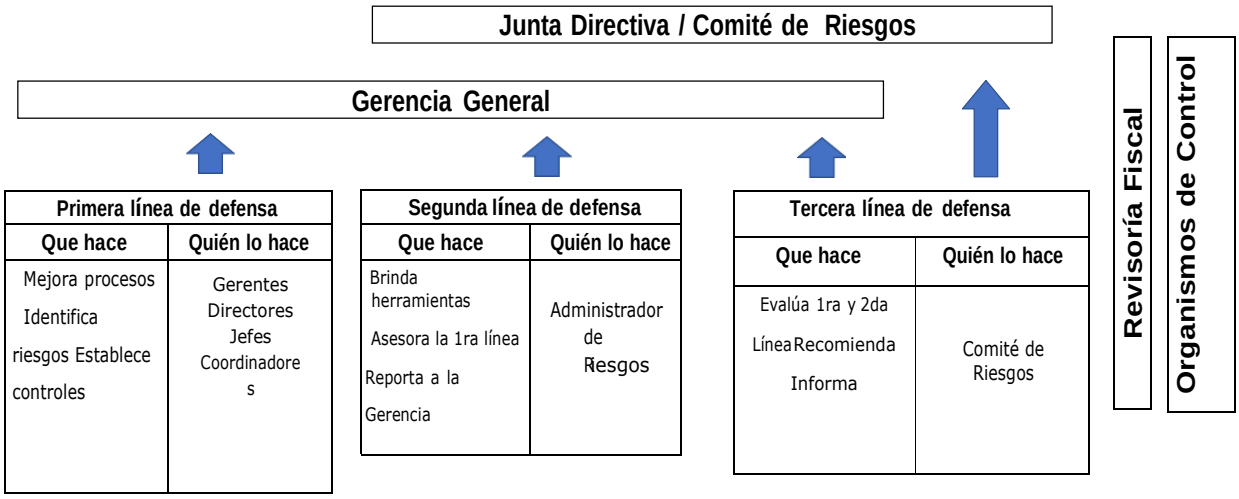
Manual Integral para la gestión del riesgo (M-GR-3)

4.2. Lineamientos Específicos Obligatorios

- Informar sobre actuaciones ilegales o sospechosas de los diferentes grupos de interés en los canales habilitados para ello, incluidos en este documento.
- Proteger y dar uso adecuado de los activos de Cedimed.
- Colaborar con las autoridades competentes.
- Manejar de manera adecuada la información confidencial y privilegiada de la institución.

5. ETAPAS

La Gestión del Riesgo y las Actividades de Control de Cedimed se basan en un modelo de tres líneas de defensa, el cual proporciona una distribución clara de las responsabilidades en cuanto a la gestión de riesgos y definición de controles a efectos de evitar vacíos en la gobernabilidad:



Primera Línea de Defensa: Responsables: Gerentes, Directores, Jefes y Coordinadores

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 Cedimed.

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.

Las funciones de las demás líneas de defensa pueden ser consultadas en el Manual Integral de Gestión de Riesgos (M-GR-3).

5.1. Identificación de riesgos

La identificación de los riesgos está a cargo de los líderes de los procesos (Consultar más detalle en el Manual Integral de Gestión de Riesgos (M-GR-3. Estructura)

Para la adecuada identificación de riesgos, se tendrán en cuenta los siguientes aspectos:

1. Identificación de todos los procesos de Cedimed y las partes interesadas con las que interactúa.

2. La metodología a utilizar para la identificación de los riesgos será la técnica de "Lluvia de ideas" contemplada en la ISO 31010 teniendo en cuenta las siguientes reglas:

Suspender el juicio: Eliminar toda crítica. No se permite ningún comentario crítico a las ideas realizadas. Se anotarán todas las ideas. La evaluación se reserva para después.

Pensar libremente. Pensar fuera de los límites de lo habitual, de lo normal, pueden surgir soluciones nuevas. Algunas ideas no convencionales se transforman en prácticas.

La cantidad es importante. Cuanto mayor sea el número de ideas se tendrá la posibilidad de escoger, adaptar o combinar.

El efecto multiplicador. Los participantes pueden sugerir mejoras de las ideas de los demás o conseguir una idea mejor a partir de otras dos.

3. Para llevar a cabo lo indicado en el punto anterior 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;
- 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.

4. Para nuevos procesos o proyectos debe realizarse la identificación de los riesgos de Riesgo de Corrupción, Opacidad y Fraude. Igualmente aplica para los cambios en los procesos, cuando sea considerado necesario por el (los) líder de dicho proceso.

5.2. Medición de riesgos

En esta etapa se medirán los riesgos por la probabilidad de ocurrencia y su impacto en caso de materializarse. Para llevar a cabo esta etapa se deben tener en cuenta todos los lineamientos de la Política de gestión de riesgos, según el Manual Integral de Gestión de Riesgos.

En esta etapa se determinará el perfil de riesgo inherente (antes de controles)

5.3. Control de riesgos

Cedimed tomará medidas para controlar los Riesgos inherentes a que se ven expuestas con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que se materialicen.

Los controles estarán incluidos en las diferentes políticas y procedimientos de la institución y estarán a cargo de los líderes de los procesos

La metodología para evaluar el diseño y funcionamiento de los controles estará en el documento "Anexo 1 – Definiciones de criterios de riesgo" que hace parte integral del Manual Integral de la Gestión de Riesgos.

En todo caso, dicha metodología tendrá en cuenta los siguientes aspectos:

1. Responsabilidad del control
2. Tipo de Control (Manual / Automático)
3. Naturaleza del control (Preventivo / Detectivo)
4. Frecuencia del control
5. Actividades que componen el control (Documentado / No Documentado)
6. Implementación del Control (Baja / Media / Alta)

La implementación del control hace referencia a la ejecución del control por parte de los responsables. En caso de presentarse observaciones o desviaciones en la ejecución del mismo el líder del proceso deberá implementar las acciones necesarias para que dicho

control opere normalmente y evitar materializaciones de los riesgos.

Cualquier cambio en las políticas y procedimientos deberá quedar documentado en la herramienta habilitada para ello.

En esta etapa se determinará el perfil de riesgo residual (después de controles)

Algunos de los controles que se deben establecer dentro de Cedimed para la prevención del fraude, soborno y corrupción se encuentran los siguientes:

- **Controles estratégicos**
  La alta dirección realizará revisiones de alto nivel a los asuntos de alta criticidad para la organización, tales como:

  ✓ Seguimiento al cumplimiento de la estrategia corporativa.
  ✓ Revisión de los niveles de cumplimiento o avance de los indicadores del Balanced Scorecard.
  ✓ Monitoreo de la efectividad de los sistemas de gestión implementados.

  Adicionalmente, debe garantizar que los sistemas de compensación y los indicadores de gestión no están generando presiones en los funcionarios que los induzcan a cometer acciones fraudulentas.

- **Segregación de funciones**
  Los procesos requieren implementar controles que involucren segregación de funciones, donde un colaborador no tiene control sobre dos o más fases de una operación, lo que permite reducir las oportunidades para que esté en la posición de perpetrar u ocultar errores o fraudes en el curso normal de sus funciones.

- **Controles contables**
  La Dirección Administrativa y Financiera debe garantizar la definición de una política contable y la implementación de los procedimientos necesarios para llevarla a cabo. La política y los procedimientos deben cumplir con los requisitos normativos vigentes y con el marco de información financiera.

  Se debe contar con controles tales como:
  ✓ Monitoreo del procedimiento de pagos a terceros.
  ✓ Cuadres diarios de caja
  ✓ Verificación de registros contables (arqueos, conciliaciones, inventarios, circularizaciones, controles tributarios)

- **Controles de seguridad de la información**
  El Jefe de Sistemas de información, debe velar por la implementación de políticas, procedimientos y controles que garanticen que la información cumpla con los criterios de seguridad (confidencialidad, integridad y disponibilidad), calidad (efectividad, eficiencia y confiabilidad) y cumplimiento de las disposiciones normativas vigentes.

- **Controles del recurso humano**
  La Dirección de Gestión Humana debe garantizar la implementación de controles efectivos en los procesos de selección, vinculación y promoción del recurso humano, tales como:
  ✓ Adecuación de competencias, verificación de antecedentes, visitas domiciliarias, entre otros.
  ✓ Monitoreo de la rotación de personal.

- ✓ Valoración del clima laboral.

- **Controles de los proveedores**
  La Dirección Administrativa y Financiera junto con el Jefe de Compras deben garantizar la implementación de políticas y procedimientos que permitan controlar la contratación de proveedores y monitorear la calidad de sus entregables, entre estos controles se pueden mencionar:

  - ✓ Seguimiento al cumplimiento de las políticas de contratación.
  - ✓ Promover la selección objetiva a través de la definición de criterios de evaluación
  - ✓ Controles de vinculación de acuerdo con los lineamientos establecidos en el Manual Gestión Prevención de Lavado de Activos y de la Financiación del Terrorismo.
  - ✓ Cumplimiento de requisitos relacionados con la administración de la seguridad de la información.
  - ✓ Valorar la gestión realizada por el proveedor. (Evaluación periódica y reevaluación)

- **Controles físicos y patrimoniales**
  La Dirección Administrativa y Financiera debe velar por la implementación y aplicación de controles que permitan garantizar niveles de seguridad adecuados para los activos de Cedimed y mitigar riesgos de fraude relacionados con la sustracción de activos. Dentro de este tipo de controles tenemos:
  - ✓ Seguridad física a las instalaciones administrativas (alarmas, uso de tarjetas de aproximación con registro obligatorio, entre otros)
  - ✓ Inventarios periódicos de insumos y seguimiento a los activos fijos

- **Auditoría de controles**
  Las actividades de control antifraude pueden ser preventivas o detectivas. Los controles preventivos están diseñados para mitigar riesgos de fraude específicos y pueden disuadir que ocurra el fraude, mientras que las actividades detectivas están diseñadas para identificar el fraude si ocurre.

  Los controles detectivos también pueden ser usados para el monitoreo de las actividades con el fin de valorar la efectividad de los controles antifraude y pueden ofrecer evidencia adicional respecto a la efectividad de los programas y controles antifraude.

  El auditor Los integrantes del comité de Riesgos deben probar la efectividad del diseño de los controles, para determinar si son operados como fueron definidos, si los ejecutan colaboradores que poseen las competencias necesarias, si satisfacen los objetivos de control de la organización y si efectivamente pueden prevenir o detectar errores o posibles fraudes.

  Adicionalmente, la auditoría interna realizada por los integrantes del Comité de Riesgos debe tener entre sus responsabilidades, la evaluación de la efectividad del programa antifraude y la comunicación al Representante Legal y Junta directiva de las deficiencias y debilidades detectadas. Los hallazgos y las debilidades deben ser gestionados a través de la implementación de acciones correctivas que se deben documentar en el mapa de riesgos.

- **Denuncias anónimas**
  Cedimed dispone de canales para reportes de situaciones que vayan en contravía de las políticas y procedimientos, el cual debe ser accesible para todos los colaboradores y terceros. Se dará a conocer por la intranet y página web institucional.

  Por su parte, los procedimientos de detección y de investigación de posibles fraudes se deben documentar. Las actualizaciones del Programa Antifraude que el Comité de Riesgos considere no relevantes, es decir, que no modifican la esencia de la política, serán presentadas para aprobación de la Junta Directiva dentro del reporte semestral del Informe de Gestión de Riesgos.

5.4. Monitoreo

Por lo menos semestralmente se efectuará un monitoreo al perfil de riesgo de fraude, soborno y corrupción. Cada líder de proceso, dentro de sus responsabilidades velará porque los controles de su proceso estén funcionando en las periodicidades establecidas y adoptará los correctivos o mejoras a que haya lugar.

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 semestralmente en el Comité de Gerencia.

De llegarse a presentar desviaciones o que se incumplan los indicadores "Meta" por tres períodos consecutivos, 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 Riesgos y Gobierno Corporativo donde se informará los planes de contingencia adoptados respecto de cada escenario extremo presentado.

Adicionalmente, se adopta la herramienta "Ley el primer dígito" o "Ley de Benford" para el análisis de fraude en la organización el cual estará a cargo del comité de Riesgos.

Se llevará un seguimiento mensual en el comportamiento de los datos según la segmentación cargada en el aplicativo que administra los riesgos Sicof, y de acuerdo a las alertas generadas se hará un registro en el formato "Seguimiento Alertas Sicof", con el fin de entablar comunicación e investigación de dichas alertas, generando intervenciones si fuera necesario.

6. ELEMENTOS

6.1. Políticas

La política institucional es de "Cero Tolerancia frente a la Corrupción, la Opacidad y el Fraude y para ello, toma las medidas necesarias con el fin de combatir estos flagelos, buscando permanentemente implementar mecanismos, sistemas y controles adecuados que permitan su prevención, detección y tratamiento.

Para llevar a cabo lo anterior, se adoptan los siguientes lineamientos:

Directores, alta gerencia, colaboradores y/o prestadores de servicios, no participan en ninguna forma de fraude, soborno o práctica de corrupción, directa o indirectamente y toman las medidas necesarias para combatirlos, independientemente de cualquier forma o tipología de la que se trate.

Cedimed establece y promueve dentro de toda la organización, una cultura institucional encaminada a fortalecer la transparencia como valor y principio de toda actuación.

A través del Código de Conducta y Ético del Grupo Quirónsalud se definen las reglas de conducta con el fin de prevenir la promoción de cualquier forma de Corrupción, Opacidad y Fraude, y de manejar adecuadamente el otorgamiento y recepción de regalos, invitaciones y/o favores (hospitalidades).

No mantiene relaciones de ningún tipo con accionistas, directores, colaboradores, prestadores de servicios, proveedores o terceros que hayan sido condenados por actividades ilícitas relacionadas con el fraude, la corrupción o el soborno.

No tolera que sus Directores, y demás colaboradores, y/o prestadores de servicios, proveedores, contratistas y cualquier tercero que tenga relacionamiento con Cedimed, obtengan resultados económicos, comerciales o de cualquier otra índole, a cambio de violar la ley o actuar de manera deshonesta.

Adopta un enfoque preventivo, de tal forma que las vulnerabilidades son minimizadas desde su origen, a través de adecuados criterios de diseño organizacional y programas de transformación cultural.

Segmenta, identifica, mide, controla y monitorea los factores de riesgo relacionados con el Riesgo COFS y, evalúa sistemática y periódicamente, la exposición a los riesgos relacionados con estos delitos, con el fin de implementar medidas administrativas efectivas.

Cedimed tiene a disposición de todos los grupos de interés la línea ética para la recepción y registro de indicios o incidentes por posibles actos indebidos cometidos por parte de sus colaboradores, prestadores de servicios y/o demás grupos de interés (página web – correo: líneaetica@cedimed.com). Además, gestiona de forma oportuna todas las denuncias de actos relacionados con el riesgo de Corrupción, la Opacidad y el Fraude, independientemente de su cuantía o del personal involucrado, garantizando confidencialidad, objetividad, no retaliación, respeto, transparencia, independencia y autonomía de los responsables de las evaluaciones.

Ningún denunciante sufrirá consecuencias negativas por prevenir, rechazar o denunciar actos de esta naturaleza. Cuando sea procedente, Cedimed pondrá en conocimiento de las autoridades competentes toda conducta que contraríe lo previsto en estos

lineamientos e igualmente emprenderá y acompañará las acciones judiciales que sean pertinentes.

Toda persona puede reportar su denuncia de manera anónima si así lo desea. Para los denunciantes que desean aportar sus datos personales en todo momento se garantizará la confidencialidad de la información, para ello, los procesos de investigación o reportes mencionarán, indicarán o insinuarán a la persona denunciante. Correo: líneaetica@cedimed.com administrado por el subgerente de la compañía.

6.2. Procedimientos

Para la adecuada implementación y funcionamiento de las etapas y elementos del Subsistema de Administración del Riesgo COFS Cedimed cuenta con los siguientes procedimientos:

- ***Instrumentación de las diferentes etapas y elementos del SICOF:***
  Programa de Transparencia y Ética Empresarial (PTEE) para la prevención del riesgo de corrupción, opacidad, fraude y soborno (COFS) – (M-GR-1)

- ***Identificación de los cambios y la evolución de los controles, así como del perfil de Riesgo:***
  Manual Integral para la gestión del riesgo (M-GR-3)

- ***Medidas por el incumplimiento del SICOF.***
  Código de Conducta y Ético del Grupo Quirónsalud

- ***Procedimientos y metodologías para identificar, medir, controlar y monitorear los riesgos COFS y Fraude y su nivel de aceptación***
  Manual Integral para la gestión del riesgo (M-GR-3)

- ***Procedimientos y metodologías para implementar y mantener el registro de eventos.***
  El registro de eventos relacionados con el riesgo COFS se efectuará con la misma metodología para el registro de eventos de riesgo operativo y serán registrados en la plataforma tecnológica que Cedimed haya habilitado para este fin.

- ***Procedimientos para reportar sobre posibles casos de corrupción, opacidad o fraude.***
  Canal de denuncias: líneaetica@cedimed.com

6.3. Mecanismos

El Programa de Transparencia y Ética Empresarial (PTEE) para la prevención del riesgo de corrupción, opacidad, fraude y soborno (COFS) de Cedimed está diseñado para establecer cuándo existe una posible actividad de COFS, para ello, cuenta con las siguientes metodologías e indicadores cuantitativos para la oportuna detección de estas posibles actividades:

- Ley de Benford: Es una herramienta estadística que, a través de la aplicación de las frecuencias, demuestra empíricamente que los números tienen un comportamiento regular cuando estos se generan de manera natural. Aplicando esta teoría, se puede inferir que cualquiera de estos conjuntos de datos cuando no se cumpla, se puede afirmar que hay algo anómalo o posible manipulación de la información. Esta herramienta será opcional y será ejecutada desde la Auditoría Interna.

- Indicadores: 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 semestralmente en el Comité de Gerencia.

  De llegarse a presentar desviaciones o que se incumplan los indicadores "Meta" por tres períodos consecutivos, 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.

Cedimed dejará constancia de cada una de las posibles actividades de COFS detectadas, así como del responsable o responsables de su análisis y los resultados del mismo.

6.4. Instrumentos

6.4.1 Señales de Alerta

En la organización y la cultura corporativa:

- Ausencia o debilidad de liderazgo
- Poca independencia entre gobierno y dirección
- Falta de transparencia
- Ausencia de objetivos u objetivos irreales
- Percepción de falta de equidad interna y externa
- Falta de formación y de oportunidades de promoción
- Inexistencia de sistemas de evaluación y reconocimiento
- Controles internos débiles o inexistentes
- Poco respeto a la normativa
- Comité de Riesgos con insuficiente/inadecuada preparación o falta de independencia

En la información financiera:

- Transacciones impropias de la naturaleza de Cedimed
- Inesperadas disminuciones en saldos de tesorería
- Importes elevados en cuentas de gastos a justificar por empleados
- Uso inadecuado de tarjetas de crédito de la empresa
- Pagos de horas extraordinarias poco relacionadas con la actividad
- Oscilaciones no razonables en la ratio compra/venta
- Ventas y otras transacciones con terceros relacionadas/vinculadas
- Ventas de activos, desinversiones por debajo del precio de mercado
- Diferencias importantes con referentes sectoriales

6.4.2 Segmentación de los factores de riesgo

La documentación de la metodología y criterios de segmentación se encuentran en documento separado y hace parte integral de este manual.

Metodología para la segmentación de factores-SICOF (P-PD-1)

6.5. Estructura Y Responsabilidades

6.5.1 Junta Directiva

La Junta Directiva delega al Comité de Riesgos y Gobierno Corporativo las siguientes funciones:

- Definir y aprobar las estrategias y políticas generales relacionadas con el SICOF basado en los informes de los órganos de control.
- Adoptar las medidas necesarias para garantizar la independencia de la persona encargada para la ejecución del SICOF y hacer seguimiento a su cumplimiento.
- Aprobar el Programa de Transparencia y Ética Empresarial (PTEE) para la prevención del riesgo de corrupción, opacidad, fraude y soborno (COFS) y sus actualizaciones.
- Hacer seguimiento y pronunciarse sobre el perfil de COFS de Cedimed.
- Pronunciarse sobre la evaluación periódica del SICOF, que realicen los órganos de control.
- Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SICOF.
- Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que la persona encargada por la entidad para la ejecución del PTEE.
- Conocer los informes relevantes respecto del PTEE, e impartir las órdenes necesarias para que se adopten las recomendaciones y correctivos a que haya lugar.
- Efectuar seguimiento a través de los informes que presente la persona encargada para la ejecución del PTEE, sobre la gestión del mismo en Cedimed y las medidas adoptadas para el control o mitigación de los riesgos más relevantes, por lo menos cada 6 meses.
- Evaluar las recomendaciones relevantes sobre el PTEE, que formule la persona encargada por Cedimed para la ejecución del mismo y los órganos de control interno, adoptar las medidas pertinentes, y hacer seguimiento a su cumplimiento.
- Analizar los informes que presente la persona encargada por Cedimed para la ejecución del PTEE respecto de las labores realizadas para evitar que la entidad sea utilizada como instrumento para la realización de actividades delictivas, actos de COFS y evaluar la efectividad de los controles implementados y de las recomendaciones formuladas para su mejoramiento.

6.5.2 Representante Legal

- Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.
- Adelantar un seguimiento permanente de las etapas y elementos constitutivos del PTEE.
- Designar el área o cargo que actuará como responsable de la implementación y seguimiento del PTEE.
- Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la Administración de este Riesgo implica para la entidad.
- Velar por la correcta aplicación de los controles del Riesgo inherente, identificado y

medido.
- Recibir y evaluar los informes presentados por la persona encargada de la ejecución del PTEE.
- Velar porque las etapas y elementos del PTEE se cumplan.
- Velar porque se implementen los procedimientos para la administración del PTEE.

6.5.3 Administrador del PTEE

Por los conocimientos de los procesos de Cedimed, así como los conocimientos técnicos propios del área, la Junta Directiva designa como encargado de la administración del PTEE al área de auditoría interna de Cedimed. El cumplimiento de sus funciones relacionadas con el PTEE estará a cargo de la Revisoría Fiscal o a través de una evaluación externa.

6.5.3.1 Perfil del Administrador del PTEE

Técnico: Nivel de formación profesional, preferiblemente en áreas de la contaduría o administración con conocimiento en riesgos.

Laborales: Preferiblemente con experiencia en auditoría (interna o externa) o en áreas de gestión de riesgos de cualquier sector de la economía.

6.5.3.2 Incompatibilidades e Inhabilidades del Administrador del PTEE

El Administrador del PTEE, debe tener características de independencia y sin sesgos de las áreas misionales de la institución relacionadas con la prestación de servicios de salud, las áreas encargadas de las negociaciones como son compras, tesorería, facturación, entre otros.

El Administrador del PTEE no puede tener ningún tipo de vínculo por afinidad o consanguinidad con cualquier colaborador dentro la institución.

6.5.3.3 Conflictos de interés

Cualquier situación que genere posibles conflictos de interés por parte del Administrador del PTEE deberá ser informado al Comité de Auditoría, riesgos y gobierno corporativo para que se tomen las decisiones a que haya lugar.

6.5.3.4 Funciones

- Diseñar y someter a aprobación de la Junta Directiva, junto con el Representante Legal, el programa de transparencia y ética empresarial y sus actualizaciones.
- Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.
- Diseñar y proponer para aprobación de la Junta Directiva o quien haga sus veces, la estructura, instrumentos, metodologías y procedimientos tendientes a que Cedimed administre efectivamente sus riesgos de prevención y detección de la Corrupción, la Opacidad y el Fraude, en concordancia con los lineamientos, etapas y elementos mínimos previstos en la normativa vigente.
- Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los Riesgos de COFS.
- Establecer y monitorear el perfil de riesgo de Cedimed e informarlo al órgano correspondiente.
- Desarrollar los modelos de medición del riesgo de COFS, para ello, tendrá en cuenta la

política integral de gestión de riesgos de la institución.

- Desarrollar los programas de capacitación relacionados con la prevención de riesgos COFS.
- Presentar un informe periódico, como mínimo semestral, a la Junta Directiva y al representante legal, sobre la evolución y aspectos relevantes del PTEE, incluyendo, entre otros, una evaluación y análisis sobre la eficiencia y efectividad del PTEE y, de ser el caso, proponer las mejoras respectivas, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.
- Establecer mecanismos para la recepción de denuncias que faciliten, a quienes detecten eventuales irregularidades, ponerlas en conocimiento de los órganos competentes de la institución.
- Informar al máximo órgano social sobre el no cumplimiento de la obligación de los administradores de suministrar la información requerida para la realización de sus funciones.
- Estudiar los posibles casos de COFS, dentro del ámbito de su competencia, para lo cual debe contar con la colaboración de expertos en aquellos temas en que se requiera y elaborar el informe correspondiente para someterlo a consideración del máximo órgano social.
- Informar a las entidades correspondientes los posibles casos de COFS que se lleguen a presentar a través de los canales dispuestos para tal fin.
- Proponer al máximo órgano social programas y controles para prevenir, detectar y responder adecuadamente a los Riesgos de COFS, y evaluar la efectividad de dichos programas y controles.
- Poner en funcionamiento la estructura, procedimientos y metodologías inherentes al PTEE, en desarrollo de las directrices impartidas por el máximo órgano social, garantizando una adecuada segregación de funciones y asignación de responsabilidades.
- Elaborar el plan anual de acción del PTEE y darle estricto cumplimiento.
- Recomendar a la Junta directiva medidas preventivas y/o acciones ante organismos competentes (Judiciales y/o disciplinarlos) para fortalecer el PTEE.
- Velar porque el PTEE se articule con las Políticas de Riesgo adoptada por la junta directiva.
- Velar por el cumplimiento efectivo, eficiente y oportuno del PTEE.
- Garantizar la implementación de canales apropiados para permitir que cualquier persona informe, de manera confidencial y segura, acerca de presuntos incumplimientos del PTEE y posibles actividades sospechosas relacionadas con COF y soborno.
- Verificar la debida aplicación de la política de protección a denunciantes que la institución haya establecido.
- Coordinar el desarrollo de programas internos de capacitación del PTEE.

6.5.4 Líderes de procesos y demás colaboradores

- Identificar y calificar los riesgos propios de su proceso, identificando la causa que los origina y las consecuencias de los mismos.
- Implementar los controles que considere necesario para mitigar los riesgos validando el costo/beneficio de la implementación. El costo de un control no debe ser superior al del riesgo.
- Informar a la auditoría interna sobre posibles situaciones de fraude.

6.6. Órganos De Control

Revisoría Fiscal
Sin perjuicio de las funciones asignadas en otras disposiciones al Revisor Fiscal, éste debe elaborar un reporte al cierre de cada ejercicio contable, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el PTEE.

A su vez, debe poner en conocimiento del Representante Legal los incumplimientos del PTEE, sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

Comité de Riesgos
Por los conocimientos de los procesos de Cedimed, así como los conocimientos técnicos propios del área, la Junta Directiva designa como encargado de la administración del proceso PTEE al comité de riesgos de Cedimed.

El cumplimiento de sus funciones relacionadas con el PTEE estará a cargo de la Revisoría Fiscal o a través de una evaluación externa.

6.7. Documentación

La siguiente información hace parte de la documentación que soporta el PTEE:

- Programa de Transparencia y Ética Empresarial (PTEE) para la prevención del riesgo de corrupción, opacidad, fraude y soborno (COFS).
- Los documentos y registros que evidencien la operación efectiva del SICOF.
- Los informes de la Junta Directiva, el Representante Legal y los órganos de control
- El mapa de Riesgos COFS
- Metodología e instrumentos para la gestión de Riesgos de Corrupción, la Opacidad y el Fraude.
- Políticas establecidas en materia de manejo de información y comunicación, que incluyan mecanismos específicos para garantizar la conservación y custodia de información reservada o confidencial y evitar su filtración.

6.8. Capacitaciones

Cedimed efectuará dos (2) tipos de capacitaciones sobre el COFS/PTEE: 1. Al momento de la vinculación de un nuevo colaborador y 2. Capacitación anual a todos los colaboradores. Cedimed podrá utilizar cualquier metodología que considere conveniente.

Para garantizar el correcto aprendizaje del COFS/PTEE, se contará con proceso de evaluación por cualquier metodología que Cedimed considere conveniente. La constancia de aprobación será mediante la aprobación del 60% del examen.

6.9. Plataforma Tecnológica

Cedimed contará con un aplicativo para administrar los riesgos del PTEE.

6.10. Incumplimiento al Programa de Transparencia y Ética Empresarial

Los incumplimientos a las políticas y procedimientos establecidos en Cedimed para la prevención del riesgo de COFS estarán sujetos a las sanciones establecidas en el Código de Conducta y Ético del Grupo Quirónsalud y a las disposiciones legales vigentes.

6.11. Divulgación de la información

Reportes internos

El comité de Riesgos presentará informes a la Gerencia general y esta a su vez se los presenta a la Junta Directiva de manera semestral.

Reportes externo

El oficial de cumplimiento es el responsable Informar a la Superintendencia Nacional de Salud los posibles casos de Corrupción, Opacidad y Fraude que se lleguen a presentar a través de los canales dispuestos para tal fin.

La política y procedimientos que conforman el programa antifraude son comunicados a todos los niveles de la organización, con el propósito que las conozcan, entiendan y sean conscientes de su importancia. Adicionalmente, se debe involucrar a las partes interesadas externas (clientes, accionistas, entes regulatorios, etc.), cuando se considere necesario.

Para garantizar la oportunidad en la divulgación de la información, Cedimed cuenta con una plataforma tecnológica documental donde todos los colaboradores pueden consultar las políticas y procedimientos.

Los colaboradores deberán firmar su compromiso con el cumplimiento de las políticas, procedimientos y demás documentos relacionados para la prevención del riesgo COFS, al momento de su contratación

7. COLABORACIÓN CON LA JUSTICIA Y AUTORIDADES ADMINISTRATIVAS

Cedimed actuará conforme a lo establecido en la Ley para denunciar situaciones, de las cuales tenga conocimiento o sospecha, relacionadas con el riesgo COFS con las partes con las que interactúa.