CONTROL DE CAMBIOS			
Act.	**Fecha**	**Páginas**	**Descripción**
01	2022.nov.29	-	Lanzamiento.

TABLA DE CONTENIDO

1 OBJETIVO

Proporcionar a los miembros de la Auditoría Interna de Coosalud EPS S.A. una metodología de consulta y aplicación que describa las principales normas, procesos y procedimientos para la práctica de las actividades de auditoría interna.

Específicamente, este manual busca el logro de los siguientes objetivos:

- Documentar una metodología para la práctica de la auditoría interna que ayude a la Auditoría Interna de Coosalud EPS S.A. al aseguramiento independiente y objetivo de la efectividad del gobierno corporativo, la gestión de riesgos y el control interno bajo las prácticas internacionales de auditoría interna.
- Establecer un método de trabajo estándar para el desarrollo de las actividades de la Auditoría Interna.
- Formalizar los procesos de comunicación eficaz y efectiva con los dueños de los procesos, la Administración y el Comité de Contraloría Interna.
- Propender porque las auditorías internas se desarrollen con calidad, mediante una adecuada planificación y programación de las actividades, la aplicación de procedimientos para la obtención y análisis de las evidencias, así como para la comunicación de los resultados y la eficiente administración y asignación de recursos.
- Contribuir al posicionamiento de la Auditoría Interna como una instancia de aseguramiento y consulta que genere valor a Coosalud EPS S.A.

2 REQUISITOS LEGALES

El presente Manual de Función de Auditoría Interna de Coosalud EPS, se rige por el marco normativo establecido en las normas internacionales para el ejercicio profesional de la Auditoría Interna así:

- Normas sobre atributos (1000 al 1322)
- Normas sobre desempeño (2000 al 2600) emitidas por el Instituto de Auditores Internos (IIA - The Institute of Internal Auditors)
- Circular 007 de 2017 de la Superintendencia Nacional de Salud - Instrucciones Generales para la implementación de mejores prácticas Organizacionales.
- Código de conducta y buen gobierno de Coosalud EPS S.A.
- Circular 004 de 2018 de las Superintendencia Nacional de Salud - Instrucciones generales relativas al código de conducta y buen gobierno organizacional, el Sistema Integrado de Gestión de Riesgos y a sus subsistemas de administración de riesgos
- Estatuto de Auditoría Interna de Coosalud EPS S.A.

3 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 entidad y la encarga de idear, ejecutar y controlar los objetivos y estrategias de la misma. También se incluye en la Alta Gerencia el Auditor interno.

Arquitectura de Control: Concepto integral que agrupa todo lo relacionado con el ambiente de control, gestión de riesgos, sistemas de control interno, información, comunicación y monitoreo. Permite a la entidad contar con una estructura, unas políticas y unos procedimientos ejercidos por toda la organización (desde la Junta Directiva y la Alta Gerencia, hasta los propios empleados), los cuales pueden proveer una seguridad razonable en relación con el logro de los objetivos de la empresa.

Asamblea General: Reunión colectiva de los miembros del Máximo Organo Social, que puede darse de manera ordinaria o extraordinaria, según lo establece el Código de Comercio o la norma que regule cada tipo especial de entidad y los estatutos de la entidad.

Conflicto de interés: Se considera que existe un conflicto de interés cuando por una situación de control, influencia directa o indirecta entre entidades, personas naturales o jurídicas; se realicen operaciones, transacciones, decisiones, traslado de recursos, situaciones de ventaja, mejoramiento en la posición de mercado, competencia desleal, desviaciones de recursos de seguridad social, o cualquier situación de hecho o de derecho que desequilibre el buen funcionamiento financiero, comercial o de materialización del riesgo al interior del sector. Estos desequilibrios tienen su fundamento en un "interés privado" que motiva a actuar en contravía de sus obligaciones y puede generar un beneficio personal, comercial o económico para la parte que incurre en estas conductas.

Directores: Son los miembros de la Junta Directiva u órganos equivalentes según la figura jurídica de que se trate.

Empresas off-shore: Empresas creadas en centros financieros con un nivel impositivo muy bajo. También conocidas como "paraísos fiscales".

Grupos de interés: Todas aquellas personas que, por su vinculación con la entidad, tienen interés en esta, a saber: el público en general, miembros del Máximo Órgano Social, empleados, proveedores de bienes y servicios, afiliados, clientes, usuarios, autoridades económicas y tributarias, autoridades de regulación, inspección, vigilancia y control, y otros actores identificados como grupos de interés por la entidad, si los llegase a tener.

Grupo Empresarial: Se entiende como la conformación de grupo empresarial de acuerdo al artículo 28 de la Ley 222 de 1995, siempre que las categorías de matriz, filial y subsidiaria a las que hace referencia el Código de Comercio para establecer el vínculo de subordinación, incluyan a sociedades civiles como las entidades sin ánimo de lucro, asociaciones mutuales, cooperativas y otras entidades propias del sector de la salud.

Hallazgo material: Un hecho económico es material cuando, debido a su naturaleza o cuantía, su conocimiento o desconocimiento, teniendo en cuenta las circunstancias de su entorno, puede alterar significativamente las decisiones económicas de los usuarios de la información. Al preparar estados financieros, la materialidad se debe determinar en relación con el activo total, el pasivo total, el pasivo corriente, el capital de trabajo, el patrimonio o los resultados del ejercicio, según corresponda.

Independiente: Se entiende por independiente, aquella persona que en ningún caso sea:

- Empleado o directivo de la EPS, la EMP o el SAP o de alguna de sus filiales, subsidiarias o controlantes, incluyendo aquellas personas que hubieren tenido tal calidad durante el año inmediatamente anterior a la designación, salvo que se trate de la reelección de una persona independiente.
- Miembros del Máximo Órgano Social que directamente o en virtud de convenio dirijan, orienten o controlen la mayoría de los derechos de voto de la entidad o que determinen la composición mayoritaria de los órganos de administración, de dirección o de control de la misma.
- Socio o empleado de asociaciones o sociedades que presten servicios de asesoría o consultoría a la EPS, la EMP o el SAP o a las entidades que pertenezcan al mismo Grupo Empresarial del cual forme parte esta, cuando los ingresos por dicho concepto representen para aquellos, el veinte por ciento (20%) o más de sus ingresos operacionales.
- Empleado o directivo de una fundación, asociación o sociedad que reciba donativos importantes de la EPS, la EMP o el SAP. Se consideran donativos importantes aquellos que representen más del veinte por ciento (20%) del total de donativos recibidos por la respectiva institución.
- Administrador de una entidad en cuya Junta Directiva participe un Representante Legal (Principal o Suplente) de la EPS, la EMP o el SAP.
- Persona natural que reciba directamente de la EPS, la EMP o el SAP alguna remuneración diferente a los honorarios como miembro de la Junta Directiva, del Comité de Contraloría Interna o de cualquier otro Comité creado por la Junta Directiva

Junta Directiva: Es el máximo órgano colegiado encargado de la dirección de la entidad. Sus miembros se conocen como Directores. Lo aquí dispuesto para la Junta Directiva y sus Directores se entiende dicho para el Consejo de Administración de las cooperativas y sus consejeros, respectivamente. Para efectos de la presente Circular, en cuanto a las cajas de compensación familiar, las disposiciones sobre las Juntas Directivas aplican para los Comités de Dirección de EPS. Tal denominación puede variar según la figura jurídica de la que se trate.

Matriz: Sociedad que ostenta el control o el poder de decisión sobre otra u otras llamadas filiales (si se trata de un control directo) o subsidiaria (si es por intermedio de sus propias subordinadas). Ver articulo 260 y siguientes del Código de Comercio, el Capítulo V de la Ley 222 de 1995 y demás normas que lo modifiquen o adicionen.

Máximo Órgano Social: Es el máximo órgano de gobierno de la entidad. Es la Asamblea General o quien haga sus veces y puede variar su denominación según la figura jurídica de la que se trate. Para esta Circular se llamarán "miembros del Máximo órgano Social" o "miembros" al accionista, en el caso de una sociedad comercial por acciones, al socio en las sociedades comerciales con cuotas o partes de interés, al miembro en una mutual, al cooperado en una cooperativa, al afiliado en caso de una caja de compensación familiar que cuenta con autorización para operar programas de salud, o por cualquier denominación que se adopte de acuerdo a la naturaleza jurídica de la respectiva entidad.

Su principal función es velar por el cumplimiento de los objetivos misionales de la entidad, mediante la realización de Asambleas, que pueden darse de manera ordinaria o extraordinaria, según lo establece el Código de Comercio o la norma que regule cada tipo especial de entidad y los estatutos de la entidad.

Miembro Minoritario: Aquel miembro del Máximo Órgano Social que por su reducida participación en el capital social o en la propiedad de la entidad no tiene capacidad de controlar directa o indirectamente a la entidad ni de

influir en la toma de decisiones, o aquel definido como tal de acuerdo con los estatutos de la entidad o de las normas vigentes,

Miembro Significativo: Aquel miembro del Máximo Órgano Social que por sí solo o en virtud de acuerdo con otros miembros, es titular de derechos de voto que igualan o superan un determinado limite (fijado en el 5% del total de derechos de voto) y cuya participación tenga una finalidad estable.

Miembros: También referenciado como miembros del Máximo Órgano Social. Este término es utilizado en la presente Circular con el fin de identificar al accionista, en caso de una sociedad comercial por acciones, al socio en las sociedades comerciales con cuotas o partes de interés, al miembro en una mutual, al cooperado en una cooperativa, al afiliado en caso de una caja de compensación familiar que cuenta con autorización para operar programas de salud, o a cualquier denominación que se adopte de acuerdo a la naturaleza jurídica de la respectiva entidad.

Partes Vinculadas: Siguiendo la Norma internacional de Contabilidad (NIC) No 24:
"Una parte se considera vinculada con la entidad si dicha parte:

(a) directa, o indirectamente a través de uno o más intermediarios:
(i) controla a, es controlada por, o está bajo control común con, la entidad (esto incluye dominantes, dependientes y otras dependientes de la misma dominante);
(ii) tiene una participación en la entidad que le otorga influencia significativa sobre la misma; o
(iii) tiene control conjunto sobre la entidad;
(b) es una asociada (según se define en la NIC 28 Inversiones en Entidades Asociadas) de la entidad;
(c) es un negocio conjunto, donde la entidad es uno de los partícipes (véase la NIC 31 Intereses en Negocios Conjuntos):
(d) es personal clave de la dirección de la entidad o de su dominante;
(e) es un familiar cercano de una persona que se encuentre en los supuestos (a) o (d);
(f) es una entidad sobre la cual alguna de las personas que se encuentra en los supuestos (d) o (e) ejerce control, control conjunto o influencia significativa, o bien cuenta, directa o indirectamente, con un importante poder de voto; o
(g) es un plan de prestaciones post-empleo para los trabajadores, ya sean de la propia entidad o de alguna otra que sea parte vinculada de esta."

Participación significativa: Se considerará participación significativa en una entidad, aquella equivalente al cinco por ciento (5%) o más del capital o de las acciones en circulación, según su naturaleza jurídica.

Presidente Ejecutivo: Posición individual dentro de la entidad que responde ante la Junta Directiva. El Presidente Ejecutivo es el máximo responsable del Giro Ordinario de la entidad y a él reportan de forma directa la mayoría de los miembros de la Alta Gerencia. Quien actúa como Representante Legal Principal o Titular de la sociedad. Tal denominación puede variar según la figura jurídica de la que se trate.

Propuesta de Acuerdo: Texto preparado por la Junta Directiva que acompaña a cada uno de los puntos incluidos en la Agenda de la Asamblea General. La Propuesta de Acuerdo describe literalmente la cuestión que la Junta Directiva

somete a la votación de los miembros del Máximo Órgano Social y puede incluir una sugerencia de la Junta Directiva a los miembros sobre el sentido de voto.

Sistema de Control Interno (SCI): Conjunto de principios, procedimientos y mecanismos de verificación y evaluación establecidos por la Junta Directiva u órgano equivalente, la Alta Gerencia y demás funcionarios de una entidad aseguradora del sistema de salud colombiano, para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos: (i) La efectividad, la seguridad y la eficiencia de las operaciones, (ii) La confiabilidad y la transparencia de la información de salud y financiera, (iii) El cumplimiento de las leyes y normas que sean aplicables a la entidad, (iv) El salvaguardar los recursos de la entidad, y, (v) El seguimiento y verificación de lo relacionado con las normas vigentes en materia de garantía de la calidad.

El Sistema de Control Interno se fundamenta principalmente en las definiciones, principios y metodologías del COSO (Committee of Sponsoring Organizations of the Treadway Commission), en particular de COSO I, COSO Il y COSO III, los cuales son complementarios.

Usuario: Es toda persona natural a la que la entidad le garantiza el acceso a servicios de salud mediante el aseguramiento.

4. LA AUDITORIA INTERNA

4.1. DEFINICIÓN DE LA AUDITORIA

El Instituto de Auditores Internos de los Estados Unidos define la auditoría interna como “La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.”.

La auditoría interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, la auditoría interna clásica se ha venido ocupando fundamentalmente del Sistema de Control Interno, es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera. Se ha centrado en el terreno administrativo, contable y financiero.

La necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la dirección. Con anterioridad, el control lo ejercía directamente la dirección de la empresa por medio de un permanente contacto con sus mandos intermedios, y hasta con los empleados de la empresa. En la gran empresa moderna esta peculiar forma de ejercer el control ya no es posible hoy día, y de ahí la emergencia de la llamada auditoría interna.

La Auditoría Interna debe funcionar como una actividad concebida para agregar valor y mejorar las operaciones de una organización, así como contribuir al cumplimiento de sus objetivos y metas; aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y dirección.

El objetivo de la Auditoría interna es asistir a los miembros de la organización, descargándoles de sus responsabilidades de forma efectiva. Con este fin les proporciona análisis, valoraciones, recomendaciones, consejos e información concerniente a las actividades revisadas. Incluye la promoción del control efectivo a un costo razonable.

La Auditoría Interna tiene la misión de mejorar y proteger el valor de la organización proporcionando aseguramiento, visión y asesoramiento objetivo basado en riesgos.

La nueva auditoría ya no comprende sólo los controles tradicionales, sino que en la búsqueda de proteger los activos de la organización audita el cumplimiento de normativas (sean estas internas o externas), políticas, directrices y principios fundamentales de gestión moderna de empresas, su función en todo caso es la de verificar la existencia de dichos controles y los mismos sean correctamente llevados a cabo. En el caso de los procesos administrativos y productivos deberá contarse con auditores capacitados debidamente en dichas áreas y sus informes tendrán un enfoque netamente de asesoramiento.

Ahora bien, de acuerdo con otra definición, la auditoria es una actividad que tiene por objetivo fundamental examinar y evaluar la adecuada y eficaz aplicación de los sistemas de control interno, velando por la preservación de la integridad del patrimonio de una entidad y la eficiencia de su gestión económica, proponiendo a la dirección las acciones correctivas pertinentes.

Las auditorías internas, denominadas en algunos casos auditorías de primera parte, se realizan por, o en nombre de, la propia organización para la revisión por la dirección y otros fines internos, y puede constituir la base para la declaración de conformidad de una organización.

Las auditorías externas incluyen lo que se denomina generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras Independientes y externas, tales como las que proporcionan la certificación/registro de conformidad con las Normas ISO 9001 o ISO 14001.

4.2. PRINCIPIOS DE LA AUDITORIA

De acuerdo con lo establecido en los principios para la profesión y práctica de la Auditoría Interna, declarados por el Instituto de Auditores Internos (IIA), el personal de la Gerencia de Auditoría Interna de Coosalud EPS debe preservar:

- Integridad: La integridad de los auditores internos establece confianza y, consiguientemente, provee la base para confiar en su juicio.

- Objetividad: Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir por sus propios intereses o por las otras personas.

- Confidencialidad: Los auditores internos respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización a menos que exista una obligación legal o profesional para hacerlo.

- Competencia: Los auditores internos aplican el conocimiento, aptitudes y experiencia necesarios al desempeñar los servicios de auditoría interna.

4.3. ALCANCE DE LA AUDITORIA

La Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de Coosalud Entidad Promotora de Salud S.A., ayudándola a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

El alcance de la auditoria es una labor coordinada con Presidencia Ejecutiva, Vicepresidencias, Director Nacional de Auditoria, Gerentes Regionales y de Sucursales, se define a partir de las necesidades de la empresa y quedará plasmado en el Plan de Auditoria Anual.

4.4. ACTIVIDADES DE LA DIRECCIÓN DE AUDITORÍA INTERNA

La Función de Auditoría Interna es la encargada de la planeación, ejecución y comunicación de las actividades de aseguramiento y consultoría a los diferentes procesos de Coosalud Entidad Promotora De Salud E.P.S.

La Dirección de Auditoría Interna Coosalud Entidad Promotora De Salud S.A. debe evaluar y contribuir a la mejora de los procesos de gobierno, gestión de riesgos y control, utilizando un enfoque sistemático disciplinado y basado en riesgos en el desarrollo de los Servicios de Aseguramiento o de Consultoría; en consecuencia, el alcance de las evaluaciones que realiza auditoría interna a los sistemas, procesos, etc., tendrán en cuenta la evaluación del funcionamiento íntegro del SCI: ambiente de control, gestión de riegos, actividades de control, información y comunicación, actividades de monitoreo.

4.4.1. Actividades de Aseguramiento

Corresponden a las actividades realizadas por los auditores internos, como un proceso de evaluación objetiva de evidencias, para expresar una opinión o conclusión independiente respecto de una operación, función, proceso,

sistema u otro asunto. Dichas actividades se realizan dando estricto cumplimiento de las normas internacionales de auditoría interna.

4.4.2. Actividades de Consultoría

Corresponde a las actividades de asesoramiento y consulta, que pueden realizar los auditores internos en las que tenga las habilidades, capacidad y experiencia necesarias; siempre y cuando, no asuma responsabilidad de gestión, de tal manera que no quebrante su objetividad e independencia. Estas actividades están dirigidas a mejorar los procesos de gobierno, gestión de riesgos y actividades de control. Las actividades de consultoría se realizan de acuerdo con su plan de trabajo y con los requerimientos de la Administración. Las siguientes son algunas posibles categorías de actividades de consultoría que se podrá realizar:

- Consultorías formales: Planificadas y sujetas a un acuerdo escrito.
- Consultorías informales: Actividades rutinarias, tales como la participación en comités permanentes, proyectos de tiempo limitado, reuniones o el intercambio rutinario de información.
- Consultorías especiales: Participación en un equipo de fusión y adquisición o de conversión de un sistema; opinión acerca de un asunto específico.

A continuación, se desarrollan las actividades de aseguramiento y consultoría sobre los elementos de Gobierno, Riesgos y Control:

	Aseguramiento	Consultoría
Gobierno	▪ Evaluar ambiente ético. ▪ Evaluar la eficacia de las estrategias, tácticas y comunicaciones. ▪ Trabajos especiales. ▪ Comunicaciones con grupos de interés. ▪ Informar sobre la eficacia del Sistema de Control Interno.	▪ Promover la cultura ética y el cumplimiento de las políticas corporativas. ▪ Brindar asesoramiento sobre las formas de mejorar las prácticas de gobierno. ▪ Asesorar sobre la autorregulación y autogestión.
Riesgo	▪ Brindar aseguramiento sobre la evaluación de los riesgos. ▪ Brindar aseguramiento de que los riesgos son correctamente evaluados. ▪ Evaluar los procesos de la gestión de riegos. ▪ Revisar el tratamiento de los riesgos clave.	▪ Capacitar sobre gestión de riesgos. ▪ Facilitar, identificar y evaluar los riesgos, actividad realizada con salvaguarda.

	▪ Identificación y valuación de los riesgos de fraude.	
Control	▪ Brindar aseguramiento de la fiabilidad e integridad de la información financiera y operativa. ▪ Evaluar la eficacia y eficiencia de operaciones. ▪ Brindar aseguramiento sobre los controles de protección de activos. ▪ Evaluar el cumplimiento de la normatividad legal. ▪ Evaluar la seguridad de los sistemas de TI. ▪ Evaluar el cumplimiento de las actividades establecidas en los procedimientos.	▪ Promover la cultura de control en Coosalud E.P.S. S.A. ▪ Facilitación y capacitación en temas como: autocontrol, eficacia y efectividad de los controles, etc.

5. GOBIERNO

El Gobierno Coosalud E.P.S. S.A. se define como un sistema que combina políticas, procesos y estructuras definidas por su Junta Directiva y la Administración con el fin de informar, dirigir, gestionar y vigilar sus actividades para el logro de sus objetivos y proteger los intereses de sus stakeholders (accionistas, empleados, clientes, proveedores, Estado, etc.), bajo el cumplimiento de las normas legales, estándares y prácticas reconocidas.

La Junta Directiva como principal gestor del gobierno corporativo, junto con la Administración como responsable de la eficacia del proceso de gobierno, han definido e implementado diferentes estrategias, estructuras, políticas y procedimientos con el fin de:

- Promover la ética y los valores dentro de la entidad.
- Asegurar la gestión y responsabilidad eficaz en el desempeño de la entidad.
- Comunicar la información de riesgos y controles a las áreas respectivas de la entidad.
- Coordinar las actividades y la comunicación entre la Junta Directiva, la Revisoría Fiscal, la Dirección de Auditoría Interna y la Administración.

Coosalud E.P.S.S.A es responsable por la veracidad de la información puesta a disposición de conformidad con las directrices emanadas por la alta dirección y en cumplimiento de las normas regulatorias de obligatorio cumplimiento. De igual manera son responsables de la información presupuestal, financiera y contractual entregada para la ejecución de la auditoria.

5.1. Actividades de Aseguramiento sobre Gobierno

La Función de Auditoría Interna evaluará y dará las recomendaciones apropiadas para mejorar la eficacia del proceso de gobierno corporativo con el fin de que se logren sus objetivos, para lo cual evaluará el diseño, la implantación y eficacia de los objetivos, programas, prácticas y actividades de Coosalud E.P.S. S.A. relacionados con la ética, la interacción con los grupos de interés, y el cumplimiento de la gestión de los colaboradores conforme a las políticas, normas, procedimientos y reglamentos definidos por la Junta Directiva y la Administración. El marco de referencia utilizado será la normatividad establecida por la medida de mejores prácticas de gobierno organizacional de la Circular Externa 007 de 2017 Circular Externa 004 de 2018 y Circular Externa 008 de 2018 de la Superintendencia Nacional de Salud, en lo relacionado con el Ambiente de Control.

La Función de Auditoría Interna evaluará la documentación de gobierno en los Estatutos, el Código de Buen Gobierno, la Política de Control Interno, el Código de Conducta y Ética, y las políticas y procedimientos de recursos humanos, y los demás que considere pertinentes. Los siguientes son algunos aspectos de los procesos de gobernanza en las prácticas de gobierno de la Junta Directiva y de Coosalud E.P.S. S.A. que Auditoría Interna debe evaluar:

Prácticas de gobierno de la Junta Directiva.

- Estructura de la Junta Directiva y sus Comités, estatutos, funciones y responsabilidades, procesos, y presentación de informes.
- Actividades de la Junta: periodicidad de reuniones, documentos de las reuniones, actas e informes, acciones de seguimientos, pronunciamientos y cumplimiento normativo.
- Cumplimiento de las funciones de la Junta Directiva como: objetivos, estrategias, estructura, planes operativos y presupuestos, gestión de riesgos, la ética, medición del desempeño y de los resultados, compensación, políticas y procedimientos.
- Órganos de control internos y externos.
- Responsabilidades de la Junta Directiva u órgano equivalente definidas en la Circular Externa 008 de 2018 de la Superintendencia Nacional de Salud.

Prácticas de gobierno de Coosalud E.P.S. S.A.

- Definición de principios básicos que rigen a la entidad.
- Desarrollo de estrategias, planes operativos y presupuestos, estructuras organizativas, y los comités de Administración.
- Asignación de autoridad y responsabilidades.
- Definición de conductas, código de ética, incluyendo los conflictos de interés, el trato justo, la protección y el uso adecuado de los activos, información privilegiada, mecanismos de reporte confidencial sobre posibles infracciones (líneas telefónicas), y las acciones disciplinarias.
- Sistema de gestión de riesgos que incluya el control, la gestión del riesgo de fraude, y el gobierno de TI.
- Cumplimiento de la normatividad legal, reglamentos y códigos que se han adoptado.
- Sistema de comunicación en todas las direcciones (hacia arriba, abajo, y a través de la entidad).
- Procesos que garanticen una comunicación efectiva con los accionistas y partes interesadas.
- Gestión de personal, selección, desarrollo, retención y planificación de la sucesión.

- Políticas de responsabilidad y sostenibilidad de la entidad.
- Seguimiento y medición del desempeño a los funcionarios.
- Mecanismo de compensación y compensación variable.

5.1.1. Actividades de Aseguramiento sobre el Ambiente Ético (Valores, Cultura, Filosofía)

La Función de Auditoría Interna debe evaluar periódicamente como mínimo, el cumplimiento de las disposiciones contempladas en el Código de Buen Gobierno Corporativo y el Código de Ética y Conducta, así como la eficacia de sus estrategias, tácticas, comunicaciones y demás procesos para alcanzar el nivel deseado de cumplimiento legal y ético.

Así como otras actividades de gobierno, la ética puede ser evaluada como parte de un examen amplio de Gobierno o como un proyecto independiente que contribuya a la evaluación general de gobierno, o se pueden integrar en las auditorías que se centran más directamente en las operaciones de negocios o actividades de apoyo.

La Función de Auditoría Interna debe, entre otros, evaluar la eficacia de los siguientes aspectos de la cultura ética de Coosalud E.P.S. S.A.:

- Código de ética formal, aprobado, comunicado, con declaraciones claras y comprensibles, incluyendo los procedimientos que regulan el fraude y la corrupción, comportamientos no aceptados e ilegales.
- Comunicaciones frecuentes y demostraciones de actitudes y comportamientos éticos esperados por los empleados, proveedores y clientes.
- Estrategias explícitas para apoyar y mejorar la cultura ética con programas regulares para actualizar y renovar el compromiso de Coosalud E.P.S. S.A con una cultura ética.
- Mecanismos definidos para el reporte confidencial de supuestas infracciones al Código de ética y conducta, políticas, fraudes y demás acciones de mala conducta.
- Declaraciones periódicas de los empleados sobre conflicto de intereses, la aceptación del Código de ética y conducta, y su compromiso de cumplimiento.
- Procesos para asegurar el cumplimiento de las disposiciones del Código de Buen Gobierno y el Código de Ética y conducta, investigaciones sobre posibles infracciones, comunicación adecuada de hallazgos, etc.
- Persona o área a quien se puede acudir para pedir asesoría sobre cómo tratar o informar un problema ético.
- Capacitaciones sobre ética a todos los empleados y proveedores clave.
- Encuestas a empleados, proveedores y clientes para evaluar el clima ético de Coosalud E.P.S. S.A.
- Verificación regular de referencias y antecedentes como parte de los procedimientos de contratación de empleados.

5.1.2. Actividades de Aseguramiento sobre Gobierno de Riesgos de Fraude

La Función de Auditoría Interna constituye un mecanismo eficaz en el tratamiento del fraude; los auditores internos pueden ayudar a la Administración a determinar si Coosalud E.P.S. S.A. tiene controles internos adecuados y fomenta un ambiente de control adecuado que prevenga el riesgo de fraude. Las actividades de aseguramiento del riesgo de fraude se pueden abordar bajo diferentes enfoques en la realización de sus actividades:

- Actividades de Auditoría Interna sobre gestión del fraude. Esto incluye evaluar las políticas, las prácticas de sensibilización, la gestión de la Junta Directiva y de la Administración al respecto (ambiente de control), así como las prácticas relacionadas, tales como la evaluación de riesgos, la evaluación de la idoneidad de los controles preventivos y de detección en la gestión del riesgo de fraude dentro del nivel de tolerancia de Coosalud E.P.S. S.A., gestión de incidentes, investigaciones y mecanismos de recuperación. La Auditoría Interna debe asignar recursos a las actividades relacionadas con el fraude en coordinación con otros riesgos de Coosalud E.P.S. S.A.

- Auditoría para detectar la probabilidad de fraude probando procesos de alto riesgo, con la intención de buscar los indicadores de fraude dentro de Coosalud E.P.S. S.A., y con las relaciones comerciales externas.

- Teniendo en cuenta el fraude como parte de cada auditoría. Por ejemplo, una lluvia de ideas sobre el riesgo de fraude, la evaluación de los controles de fraude, el diseño de los procedimientos que tengan en cuenta el riesgo de fraude, o la evaluación de los errores para determinar si podría ser un indicio de fraude. Los resultados acumulativos pueden ofrecer una perspectiva de si los programas de gestión de riesgos y la sensibilización de la Administración se han aplicado con eficacia en toda Coosalud E.P.S. S.A.

Las actividades de aseguramiento para la detección de riesgo de fraude se pueden hacer a través de técnicas de análisis de datos, para lo cual la Administración garantizará el acceso a todos los sistemas de TI, así como a toda la información (confidencial o no) de sus colaboradores, clientes y proveedores.
Coosalud E.P.S. S.A, se compromete a poner en conocimiento de posibles irregularidades o fraudes que comprometan a la gerencia, contratistas o funcionarios que desempeñan funciones claves dentro del negocio y que puedan afectar de forma importante los resultados de las operaciones.

5.1.3. Actividades de Aseguramiento sobre el Gobierno de la Seguridad de la información

El Gobierno de TI consiste en el direccionamiento, la estructura organizacional y los procesos que aseguran que la tecnología de la información de Coosalud E.P.S. S.A. sostiene y apoya las estrategias y los objetivos estratégicos, para la prestación de servicios los diferentes grupos de interés de la entidad, en condiciones de seguridad, calidad y cumplimiento. Por esta razón, Coosalud E.P.S. S.A. debe establecer, desarrollar, documentar y comunicar políticas de tecnología y definir los recursos, procesos, procedimientos, metodologías y controles necesarios para asegurar su cumplimiento La responsabilidad sobre la seguridad de la información corresponde a la Junta Directiva, la Administración y líderes de cada proceso

- Junta Directiva: Define las estrategias de Coosalud E.P.S. S.A. establece y supervisa las políticas relacionadas con la gestión de tecnología de la información, la seguridad de la información. Define la cultura de seguridad corporativa.
- Administración: Es responsable de definir políticas de seguridad de la información, mediante la ejecución de un programa que comprenda, entre otros, el diseño, implantación, divulgación, educación y mantenimiento de las estrategias y mecanismos para administrar la seguridad de la información. Asegura que las políticas y directrices sobre seguridad de la información son comprendidas por Coosalud E.P.S. S.A. y destina recursos suficientes para la seguridad de la información, promueve el objetivo de seguridad de la información y fomenta la mejora y el éxito continuo.
- Líderes de cada proceso: Contribuyen al diseño e implementación de las actividades de seguridad de la información; revisan y monitorean los controles de seguridad de la información; y definen los requisitos de seguridad de la información. Son los encargados de asegurar la gestión y la verificación diaria de los procesos y controles de TI.

La Función de Auditoría Interna evaluará que las políticas, procedimientos y estrategia de seguridad de la información establecidas por la Administración de Coosalud E.P.S. S.A. cumplan con los requerimientos establecidos por la SFC. Con el fin de evaluar el diseño y eficacia de los controles en respuesta a los riesgos dentro del gobierno de Coosalud E.P.S. S.A., las operaciones y los sistemas de información, sobre la confiabilidad e integridad de la información (financiera y operativa), corresponderá a la Función de Auditoría Interna evaluar el ambiente del control de la información, incluyendo la comprensión, adopción y la efectividad; validar los esfuerzos sobre seguridad de la información y comparar las prácticas actuales con los estándares de la industria. Igualmente, evaluará si la gestión de la tecnología de información de la Coosalud E.P.S. S.A. apoya las estrategias y objetivos de la organización.

Evaluará entre otros siguientes aspectos:

La Función de Auditoría Interna entre otros asuntos, debe evaluar los siguientes aspectos relacionados con el Gobierno de TI:

- Plan estratégico de tecnología, el cual debe estar alineado con el Plan estratégico de Coosalud E.P.S. S.A.
- La Infraestructura de tecnología.
- Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico, en lo aplicable a la entidad.
- Administración de proyectos de sistemas.
- Administración de la calidad.
- Adquisición de tecnología.
- Adquisición y mantenimiento de software de aplicación.
- Instalación y acreditación de sistemas.
- Administración de cambios.
- Administración de servicios con terceros.
- Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.

- Continuidad del negocio.
- Seguridad de los sistemas.
- Educación y entrenamiento de usuarios.
- Administración de los datos.
- Administración de instalaciones.
- Administración de operaciones de tecnología.
- Documentación

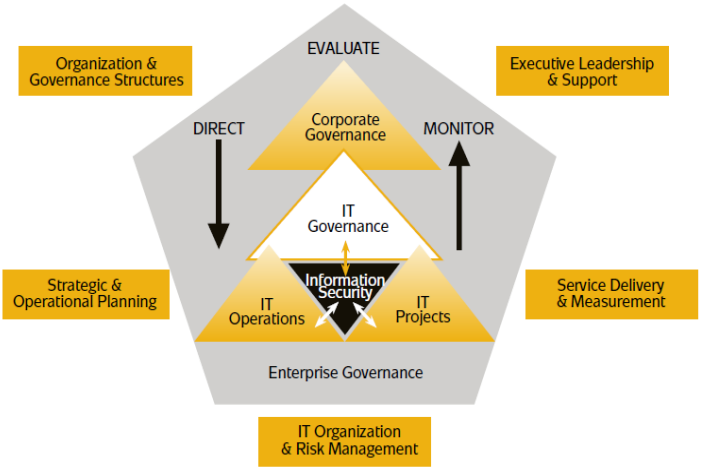
5.1.4. Actividades de Aseguramiento del Gobierno de TI

Un Gobierno de TI efectivo, ayuda a garantizar que TI soporte las metas de negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociadas a TI. El Gobierno de TI implica la gestión de las operaciones y proyectos de TI para asegurar la alineación entre estas actividades y las necesidades de Coosalud E.P.S. S.A. definidas en su plan estratégico. El gobierno de TI incluye procesos y controles que ayudan a la entidad a gestionar mejor su entorno de TI y el equilibrio general del perfil de riesgos de Coosalud E.P.S. S.A., en el apetito de riesgo y los niveles de tolerancia.

Para que el gobierno de TI sea efectivo debe estar compuesto por los siguientes componentes: estructuras de gobierno y organización; liderazgo ejecutivo y soporte técnico; planificación estratégica y operacional; entrega y medición de servicios y, organización y gestión de riesgos de TI.

La siguiente grafica relaciona los componentes que conforman las áreas de control de gobierno de TI[1].

La Función de Auditoría Interna evaluará la estructura de gobierno de TI y la capacidad de alcanzar resultados positivos para Coosalud E.P.S. S.A. y formular recomendaciones para mejorar la eficiencia y la eficacia de la función de TI; específicamente, evaluará si el gobierno de TI apoya las estrategias y objetivos de la entidad, genera valor y da cumplimiento a los requerimientos regulatorios para los controles de TI en áreas como privacidad, seguridad e integridad en el ambiente de control de Coosalud E.P.S. S.A.. En este sentido, con el objetivo de desarrollar una auditoría eficaz, la Función de Auditoría Interna podrá ejecutar tanto auditorías de gestión como auditorías de cumplimiento. Las



[1] Figura tomada de Global Technology Audit Guide (GTAG®) 17, Auditing IT Governance del IIA.

auditorías de cumplimiento se centrarán en el cumplimiento de los requisitos regulatorios externos y las políticas y procedimientos internos. Entre tanto, las auditorías de desempeño corresponderán a realizar análisis y evaluación más profunda en cuanto a lo que impulsa el rendimiento de Coosalud E.P.S. S.A.

5.2. Actividades de Consultoría sobre Gobierno

La Función de Auditoría Interna podrá desarrollar actividades de consultoría sobre las formas de mejorar las prácticas de gobierno, dependiendo de los temas que considere relevantes, o por petición exclusiva de la Administración o el Comité de Auditoría de Junta Directiva. Igualmente, a través de los comités de los que hace parte el Gerente de Auditoría o cualquier otro miembro, puede dar opiniones o asesorar sobre temas específicos. Dentro de las actividades de consultoría se resaltan las siguientes: promover la cultura ética y el cumplimiento de las políticas corporativas, brindar asesoramiento sobre las formas de mejorar las prácticas de gobierno, asesorar sobre la autorregulación y autogestión sobre temas de TI, etc.

5.2.1. Consultoría sobre la cultura ética y el cumplimiento de políticas corporativas

Los grupos de interés Coosalud E.P.S. S.A. deben estar comprometidos con la cultura ética de la entidad; el Código de Conducta y Ética y el Código Gobierno Corporativo constituyen declaraciones formales de los valores de la entidad, el comportamiento esperado de sus colaboradores y terceras partes, las estrategias para mantener una cultura alineada con sus compromisos legales, éticos y sociales. Por lo tanto, forman parte de una herramienta de obligatoria observancia para consulta de todos los colaboradores.

La Función de Auditoría Interna debe asumir un rol activo en apoyo de la cultura ética, dada su posición y su nivel de confianza e integridad y sus habilidades para convertirse en defensor eficaz de la conducta ética. Los miembros de la Gerencia de Auditoría Interna tienen la competencia y capacidad para solicitar a los miembros de Coosalud E.P.S. S.A. en cualquier nivel jerárquico a cumplir con las responsabilidades legales, éticas y sociales de la organización.

5.2.2. Asesoría de gobierno sobre políticas y mecanismos antifraude

Aunque la Junta Directiva y la Administración son los responsables de definir estrategias antifraude, la Función de Auditoría Interna, por petición de la Administración o del Comité de Auditoría de Junta Directiva, puede desempeñar una función clave en el asesoramiento sobre la definición e implementación de políticas y prácticas antifraude que incluyen la sensibilización, la prevención y los programas de detección.

Los servicios de consultoría de gobierno también ayudarán a identificar y evaluar el riesgo de fraude y determinar la idoneidad de los mecanismos de control para la revisión de procesos, nuevos proyectos corporativos o aplicaciones informáticas.

De otro lado, la Función de Auditoría Interna podrá desempeñar un rol de investigación de las sospechas de riesgos de fraude interno o externo.

6. RIESGOS

El riesgo se puede definir como una circunstancia, evento, amenaza, acto u omisión, que al presentarse pueda impedir el logro de los objetivos estratégicos y/o la implementación de las estrategias formuladas por la Administración. La gestión sobre los riesgos se realiza por parte del área de Riesgos y los Líderes responsables de los procesos de la organización.

La Función de Auditoría Interna podrá realizar actividades de aseguramiento sobre el sistema de gestión de riesgo, con el fin de evaluar su eficacia y contribuir a su mejoramiento. Igualmente, podrán realizar actividades de consultoría, siempre que éstas no afecten su independencia ni su objetividad.

A continuación, se relacionan las principales actividades que la Función de Auditoría Interna podrá o no realizar frente a la Gestión de Riesgos Empresariales (ERM por sus siglas en inglés):[2]

Roles principales de la Auditoría Interna respecto al ERM	Roles legítimos de la auditoría interna realizados con salvaguarda *	Roles que la Auditoría Interna No debe realizar
▪ Brindar aseguramiento sobre procesos de gestión de riesgo. ▪ Brindar aseguramiento de que los riesgos son correctamente evaluados. ▪ Evaluación de los procesos de gestión de riesgo. ▪ Evaluación de reporte de riesgos claves. ▪ Revisión del manejo de los riesgos claves.	▪ Facilitación, identificación y evaluación de riesgos. ▪ Entrenamiento a la gerencia sobre respuesta a riesgos. ▪ Coordinación de actividades de ERM. ▪ Consolidación de reportes sobre riesgos. ▪ Mantenimiento y desarrollo del marco de ERM. ▪ Defender el establecimiento del ERM. ▪ Desarrollo de estrategias de gestión de riesgo para aprobación de la junta	▪ Establecer el apetito de riesgo. ▪ Imponer procesos de gestión de riesgo. ▪ Manejar el aseguramiento sobre los riesgos. ▪ Tomar decisiones en respuesta a los riesgos. ▪ Implementar respuestas a riesgos a favor de administración. ▪ Responsabilidad de la gestión.

(*) La Función de Auditoría Interna puede ampliar su participación en el ERM, aplicando las siguientes condiciones:

[2] Fuente: Declaración de Posición del IIA. El Rol de la Auditoría Interna en la Gestión del Riesgo Empresarial. Septiembre de 2004.

- Debe estar claro que la gerencia mantiene la responsabilidad de la gestión de riesgo.
- La naturaleza de la responsabilidad de auditoría interna debe ser documentada en los estatutos de auditoría y aprobado por el Comité de Auditoría.
- Auditoría interna no debe gestionar ningún riesgo en favor de la Administración.
- Auditoría interna debe proveer consejo, motivar y soportar las decisiones realizada por la dirección, en vez de tomar decisiones de riesgo por ellos mismos.
- Auditoría Interna tampoco puede brindar aseguramiento objetivo en ninguna parte del marco de ERM de la cual es responsable. Tal aseguramiento debe ser provisto por otra parte sustancialmente calificada.
- Cualquier trabajo más allá de las actividades de aseguramiento debe reconocerse como una asignación de consultoría y la implementación de normas relativas a tales asignaciones deben seguirse.

6.1. Actividades de Aseguramiento sobre Riesgos

Para determinar si el sistema de gestión de riesgos es eficaz, la Función de Auditoría Interna debe evaluar si:

- Los objetivos de Coosalud E.P.S. S.A. apoyan su misión y están alineados con la misma.
- Los riesgos significativos (claves) están identificados y evaluados.
- Existen planes de tratamiento apropiados al riesgo que alinean los riesgos con la aceptación de riesgos por parte de Coosalud E.P.S. S.A.
- Se capta información sobre riesgos claves, permitiendo al personal, la dirección y la Junta Directiva cumplir con sus responsabilidades, y se comunica dicha información oportunamente a través de la Coosalud E.P.S. S.A.

Para tal fin, la Función de Auditoría Interna podrá realizar evaluaciones (actividades de aseguramiento) al sistema como tal, o a través de las evaluaciones que se realizarán a los diferentes sistemas y procesos de Coosalud E.P.S. S.A. El resultado de dichos trabajos, analizado conjuntamente, proporcionará un entendimiento del sistema de gestión de riesgos de la entidad y su eficacia.

La Función de Auditoría Interna evaluará las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de Coosalud E.P.S. S.A., con relación a lo siguiente:

- Logro de los objetivos estratégicos.
- Fiabilidad de integridad de la información financiera y operativa.
- Eficacia y eficiencia de las operaciones y programas.
- Protección de activos.
- Cumplimiento de leyes, regulaciones, políticas, procedimientos y contratos.

Asimismo, la Función de Auditoría Interna evaluará la posibilidad de ocurrencia de fraude y cómo Coosalud E.P.S. S.A. gestiona el riesgo de fraude.

6.1.1. Actividades de Aseguramiento sobre el Sistema de Gestión de Riesgos

El sistema de gestión de riesgos es un proceso estructurado, consistente y continuo a través de Coosalud E.P.S. S.A. para identificar, evaluar, decidir sobre las respuestas a los riesgos clave e informar sobre las oportunidades y amenazas que afectan el logro de sus objetivos. La Función de Auditoría Interna evaluará dicho sistema con el fin de obtener evidencia suficiente y apropiada para determinar que los objetivos clave de los procesos de gestión de riesgos se hayan cumplido, con el fin de formarse una opinión sobre la adecuación de dichos procesos. Al obtener esta evidencia, la Función de Auditoría Interna podrá tener en cuenta los siguientes procedimientos de auditoría:

- Investigar y revisar desarrollos, tendencias e información actualizada del sector económico correspondiente a los negocios de Coosalud E.P.S. S.A., y otras fuentes apropiadas de información, con el fin de determinar los riesgos y exposiciones que puedan afectar a Coosalud E.P.S. S.A. y los procedimientos de control relacionados que se utilizan para afrontar, vigilar y reevaluar aquellos riesgos.
- Revisar las políticas corporativas, las actas de la Junta Directiva y del Comité de Auditoría de Junta Directiva, con el fin de determinar las estrategias de negocio de Coosalud E.P.S. S.A., su filosofía y metodología de gestión de riesgos, su inclinación al riesgo, y su aceptación de riesgos.
- Revisar informes previos de evaluación de riesgos emitidos por la Administración, la revisoría fiscal y otras fuentes.
- Entrevistar a la Administración con el fin de determinar los objetivos de las unidades de negocio, los riesgos relacionados, y las actividades de mitigación de riesgos y vigilancia de controles.
- Asimilar información con el fin de evaluar independientemente la eficacia de la mitigación de riesgos, vigilancia, y comunicación de riesgos y actividades de control asociadas.
- Evaluar la adecuación de las líneas de reporte para las actividades de vigilancia del riesgo.
- Revisar la adecuación y oportunidad de la información sobre los resultados de la gestión de riesgos.
- Revisar la integridad del análisis de gestión de riesgos y las acciones tomadas por parte de la Administración para remediar los problemas identificados en los procesos de gestión de riesgos, y sugerir mejoras.
- Determinar la eficacia de los procesos de autoevaluación de la Administración mediante observaciones, pruebas directas del control y los procedimientos de vigilancia, pruebas de la información utilizada en actividades de vigilancia y otras técnicas apropiadas.
- Revisar los problemas relacionados con el riesgo que puedan indicar debilidad en las prácticas de gestión de riesgos y, si corresponde, comentarlos con la Administración y el Comité de Auditoría de Junta Directiva.

6.1.2. Actividades de Aseguramiento sobre Sistemas de Administración de Riesgos

La Función de Auditoría Interna debe evaluar cómo la administración de Coosalud E.P.S. S.A. realiza la identificación, gestión, seguimiento, valoración y definición de apetito y tolerancia de los riesgos estratégicos y de procesos, teniendo en cuenta las siguientes categorías:

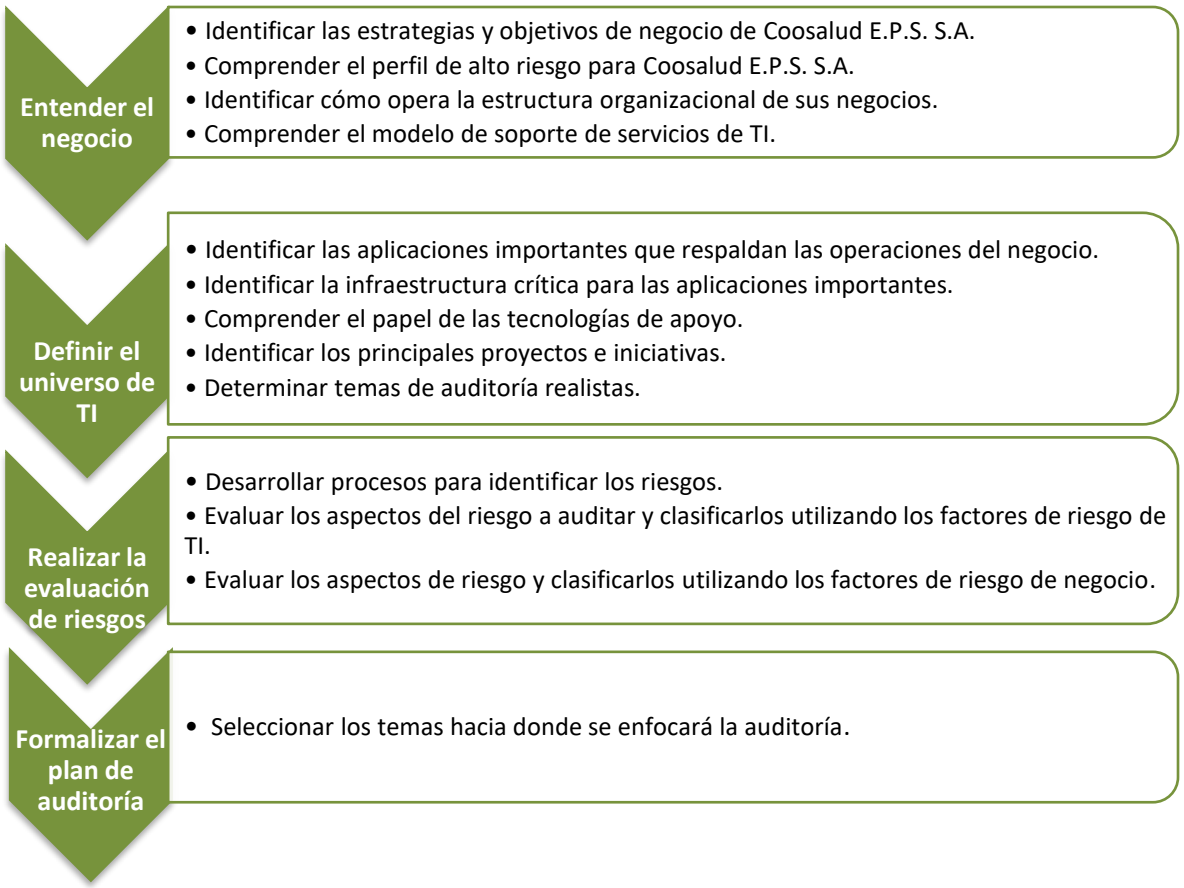
I. Riesgo en Salud.
II. Riesgo Actuarial.
III. Riesgo de Crédito.
IV. Riesgo de Liquidez.

V. Riesgo de Mercado de Capitales.
VI. Riesgo Operacional.
VII. Riesgo de Fallas de Mercado de Salud.
VIII. Riesgo de grupo.
IX. Riesgo Reputacional.
X. Riesgo de Lavados de Activos y Financiación del Terrorismo. (Circular Externa 009 de 2016).

6.1.3. Actividades de Aseguramiento sobre Gestión de Riesgos de TI

La Función de Auditoría Interna deberá considerar los riesgos de TI en la planeación de sus actividades, con el fin de ayudar a la Administración en el monitoreo y control de la correcta ejecución de las actividades que minimizan los riesgos de TI. Para tal fin, deberá identificar los objetivos de Coosalud E.P.S. S.A., su estrategia, los activos de información y los sistemas o recursos de información que generalmente almacenan, usan o manipulan los activos claves (Hardware, software, base de datos, redes, instalaciones, personas, etc.).

Para la definición del plan anual de Auditoría Interna en lo relacionado a TI, se deberá realizar las siguientes actividades:



Para un eficaz trabajo de auditoría se tendrán en cuenta los siguientes aspectos:

- Las fallas de la tecnología representan un riesgo que debe ser evaluado, gestionado y auditado, si representa un riesgo clave para Coosalud E.P.S. S.A.
- Los controles clave deben ser identificados como el resultado de una evaluación de arriba hacia abajo de los riesgos del negocio, tolerancia al riesgo y análisis de controles necesarios para gestionar o mitigar los riesgos de negocio.
- Los riesgos del negocio se ven mitigados por una combinación de controles manuales y automáticos.

6.2. Actividades de Consultoría sobre Riesgos

La Función de Auditoría Interna por solicitud de la Administración, la Junta Directiva, el Comité de Auditoría de Junta Directiva, o como resultado de la evaluación al sistema de gestión de riesgos de Coosalud E.P.S. S.A., o por iniciativa propia, podrá ayudar mediante consultoría en la identificación, evaluación, e implementación de metodologías de gestión de riesgos y controles, con el fin de mejorar el sistema de gestión de riesgos.

La Función de Auditoría Interna deberá tener en cuenta que las actividades de consultoría no afecten su independencia y objetividad, y no deberá asumir ninguna responsabilidad de la gestión de riesgo.

Algunas actividades de consultoría que puede desempeñar la Función de Auditoría Interna son:

- Poner a disposición de Coosalud E.P.S. S.A. las herramientas y técnicas de gestión utilizadas para analizar los riesgos y controles.
- Ser un líder para crear una cultura de gestión de riesgos en Coosalud E.P.S. S.A., aprovechando su experiencia en la gestión y control de riesgos y su conocimiento global de Coosalud E.P.S. S.A.
- Asesorar a través de talleres, entrenamiento de Coosalud E.P.S. S.A en el riesgo y el control y la promoción del desarrollo de un lenguaje común, el enfoque y el entendimiento.
- Actuar como punto central para la coordinación, seguimiento e información sobre los riesgos.
- Apoyar a la Administración en el asesoramiento sobre la mejor forma de mitigar el riesgo.

7. CONTROL

El control es cualquier medida adoptada por la Junta Directiva, la Alta Gerencia y demás partes interesadas, con el fin de mitigar los riesgos y aumentar la probabilidad de que se alcancen los objetivos y metas establecidas por Coosalud E.P.S. S.A. Es responsabilidad de la Alta Gerencia planear, organizar y dirigir la realización de acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y las metas.

7.1. Actividades de Aseguramiento sobre Control

La Función de Auditoría Interna mediante sus actividades de aseguramiento, deberá asistir a Coosalud E.P.S. S.A. en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua. La Función de Auditoría Interna deberá:

- Evaluar la adecuación y eficacia de los controles en respuesta a los riesgos del gobierno, operaciones y sistemas de información de la organización, respecto a:

  - Logro de los objetivos estratégicos de la organización.
  - Fiabilidad e integridad de la información financiera y operativa,
  - Eficacia y eficiencia de las operaciones y programas,
  - Protección de activos, y
  - Cumplimiento de leyes, regulaciones, políticas, procedimientos y contratos.

- Evaluar las políticas y procedimientos que propicien que los empleados de todos los niveles de Coosalud E.P.S. S.A. cuenten con los conocimientos, habilidades y conductas necesarios para el desempeño de sus funciones.

- Evaluar si la estructura organizacional permite soportar el alcance del SCI de Coosalud E.P.S. S.A., y que están definidos claramente los niveles de autoridad y responsabilidad, precisando el alcance y límite de los mismos.

7.1.1. Actividades de Aseguramiento sobre TI

La Función de Auditoría Interna, dentro de sus actividades de aseguramiento de TI, deberá:

- Garantizar un nivel básico suficiente de conocimientos de auditoría de TI en los auditores.
- Incluir la evaluación de las TI en sus procesos de planificación.
- Evaluar si el gobierno de TI en la organización sostiene y apoya las estrategias y objetivos.
- Identificar y evaluar las exposiciones al riesgo relacionadas con los sistemas de información de Coosalud E.P.S. S.A.
- Evaluar los controles que responden a los riesgos en los sistemas de información de Coosalud E.P.S. S.A.
- Considerar las técnicas de auditoría basadas en la tecnología de uso, según corresponda.

Para cumplir con estas responsabilidades la auditoría interna deberá:

- Evaluar controles generales, que rigen para todas las aplicaciones de sistemas y ayudan a asegurar su continuidad y operación adecuada. Dentro de éstos se incluyen aquellos que se hagan sobre la administración de la tecnología de información, su infraestructura, la administración de seguridad y la adquisición, desarrollo y mantenimiento del software.
- Evaluar controles de aplicación, los cuales incluyen pasos a través de sistemas tecnológicos y manuales de procedimientos relacionados, se debe concentrar en la suficiencia, exactitud, autorización y validez de la captura y procesamiento de datos.

- Evaluar controles sobre limitaciones de acceso a las distintas áreas de la organización, de acuerdo con el nivel de riesgo asociado a cada una de ellas, teniendo en cuenta tanto la seguridad de los empleados de Coosalud E.P.S. S.A. como de sus bienes, de los activos de terceros que administra y de su información.

La Función de Auditoría Interna definirá una estructura formal para hacer frente a los controles de TI dentro del sistema general de los controles internos. La estructura para evaluar los procesos de TI debe comprender los siguientes pasos[3]:

Estructura de la Auditoría de TI	
Entendimiento de los controles de TI	Gobierno - Gestión - Técnica
	Aplicaciones generales
	Prevención, Detección Corrección
	Información – Seguridad
Importancia de los controles de TI	Fiabilidad y Eficacia
	Ventaja Competitiva
	Legislación y Regulación
Roles y Responsabilidades	Gobierno
	Gestión
	Auditoría
Basado en el Riesgo	Análisis de Riesgos
	Respuesta a los Riesgos
	Baseline Controls
Monitoreo y Técnicas	Marco de control
	Frecuencia
Aseguramiento	Metodologías
	Comité de Auditoría Interface

7.1.2. Actividades de Aseguramiento sobre Seguridad de la Información

La falta de protección de la información confidencial por medio de controles adecuados puede tener consecuencias significativas para Coosalud E.P.S. S.A., lo cual puede afectar la reputación de las personas y de la organización, exponer a Coosalud E.P.S. S.A. a riesgos que tengan consecuencias legales, y disminuir la confianza de clientes, proveedores y colaboradores. Los riesgos asociados con la privacidad de la información comprenden a la privacidad personal (física y psicológica); la privacidad del espacio (libertad de vigilancia); la privacidad de las comunicaciones

[3] Estructura propuesta por el IIA: Global Technology Audit Guide (GTAG®) 1. marzo de 2012.

(libertad de vigilancia); y la privacidad de la información (obtención, uso y revelación de información personal por parte de terceros). La información personal se refiere generalmente a información que puede estar asociada con un individuo determinado, o que tiene características de identificación que cuando se combina con otra información puede asociarse a un individuo en particular. Puede incluir cualquier información fáctica o subjetiva, registrada o no, en cualquier formato o medio.

El control eficaz sobre la protección de la información personal es un componente esencial de los procesos de gobierno, gestión de riesgos y control de Coosalud E.P.S. S.A. La Administración es responsable de identificar los riesgos principales para Coosalud E.P.S. S.A. e implementar procesos de control apropiados que reduzcan esos riesgos. Esto incluye establecer el enfoque de privacidad necesario para Coosalud E.P.S. S.A. y vigilar su implementación.

La Función de Auditoría Interna deberá contribuir al buen gobierno y a la gestión de riesgos evaluando la adecuada identificación de riesgos efectuada por la dirección con respecto a sus objetivos de privacidad, y la adecuación de los controles establecidos para reducir esos riesgos a un nivel aceptable. La Función de Auditoría Interna tiene la capacidad de evaluar el enfoque de privacidad de Coosalud E.P.S. S.A. e identificar los riesgos significativos, así como efectuar recomendaciones apropiadas para reducirlos.

La Función de Auditoría Interna identificará los tipos de información obtenida por Coosalud E.P.S. S.A. que se consideren personal o privada, lo apropiado de las mismas, la metodología de recolección utilizada, y si el uso que hace Coosalud E.P.S. S.A. de esa información es el que corresponde a lo que se pretende y a la legislación aplicable.

Dada la naturaleza altamente técnica y legal de los problemas de privacidad, la Función de Auditoría Interna ha de tener los conocimientos y competencias apropiadas para realizar una evaluación de los riesgos y controles del enfoque de control de la organización.

Al realizar dicha evaluación de la gestión del enfoque de privacidad de Coosalud E.P.S. S.A., se tendrá en cuenta lo siguiente:

- Las leyes, regulaciones y políticas referidas a la privacidad definidas por el gobierno.
- Se asesorará para determinar la naturaleza exacta de las leyes, regulaciones y otras normas y prácticas aplicables a Coosalud E.P.S. S.A.
- Se apoyará con especialistas en tecnología de la información para determinar que los controles sobre la seguridad informática y la protección de datos existan y sean revisados y evaluados regularmente respecto de su adecuación.

7.1.3. Actividades de aseguramiento sobre controles de aplicación

Los controles de aplicación son los controles que pertenecen al ámbito de los procesos de negocio individuales o sistemas de aplicación, incluyendo edición de datos, la separación de funciones de negocios, equilibrio de los totales de procesamiento, registro de transacciones reportes de error, etc. Por lo tanto, el objetivo de los controles de aplicación es garantizar que:

- Los datos registrados sean exactos, completos, autorizados, y correctos.
- Los datos se procesan según lo previsto en un período de tiempo aceptable.
- Los datos almacenados son exactos y completos.
- Los resultados son precisos y completos.
- Se mantiene un registro para rastrear el proceso de almacenamiento de datos, desde la entrada hasta la salida.

La Función de Auditoría Interna debe identificar los sistemas críticos y realizar evaluaciones a los controles de aplicación con el fin de asegurar que su objetivo para el cual fueron diseñados se está cumpliendo. Se debe tener en cuenta lo siguiente:

- **Áreas de control en los sistemas de información:** Contempla los procedimientos para administrar la seguridad de información durante el proceso de transferencia de datos entre las aplicaciones y los sistemas donde se soportan los procesos de negocio.

- **Área de control en la plataforma tecnológica:** Contempla el ambiente de control a nivel de base de datos, servidores, sistemas operativos, y sistemas de redes y comunicaciones; que, a su vez, soportan a los sistemas de información y, por ende, las operaciones del negocio.

- **Análisis de vulnerabilidades:** Contempla la ejecución de pruebas de vulnerabilidad en la plataforma tecnológica asociada con los sistemas de información, servidores de aplicaciones, bases de datos que tienen impacto en las operaciones del negocio.

7.2. Actividades de Consultoría sobre Control

La Función de Auditoría Interna por su nivel dentro de Coosalud E.P.S. S.A. y por sus habilidades y conocimientos sobre controles, podrá desarrollar actividades de consultoría en temas de ambiente de control y actividades de control, procesos de control relacionados con cultura de control y autoevaluación de control.

7.2.1. Actividades de Consultoría sobre Cultura de Control

La Función de Auditoría Interna puede desempeñar actividades de consultoría a la Administración en temas de cultura organizacional que fomentan en todos los empleados de Coosalud E.P.S. S.A.: principios, valores y conductas orientadas hacia el control; esto con el fin de que la entidad cuente con personal competente e inculquen en Coosalud E.P.S. S.A. un sentido de integridad y concientización sobre el control.

Con el propósito de fomentar una cultura de autocontrol en Coosalud E.P.S. S.A., el equipo de Auditoría Interna podrá definir agendas de capacitación y sensibilización relacionadas con:

- Marco de control interno – COSO/COBIT.
- Marco de control interno establecido por la SFC.

- Marco Integrado de Control Interno "COSO" Committee of Sponsoring Organizations of The Treadway Commission.
- Requerimientos esenciales de control: Normas básicas del Sistema de Control Interno y Políticas de Seguridad de Sistemas.
- Principios rectores de Control: Definición de normas, políticas y procedimientos, Segregación de funciones y responsabilidades, Documentación, Supervisión y revisión, Oportunidad del Control, etc.

7.2.2. Actividades de Consultoría sobre Autoevaluación

Según las prácticas profesionales recomendadas para el ejercicio de la actividad de Auditoría Interna, han definido la autoevaluación de control como un proceso, a través del cual la Administración y el personal clave de Coosalud E.P.S. S.A. evalúan el sistema de control interno, para proveer una seguridad razonable en el logro de los objetivos de negocio. La autoevaluación de control debe ser utilizada para evaluar controles básicos (ética, liderazgo, competencia, comunicación, moral, trabajo en equipo, confianza), así como controles tradicionales (manuales de políticas, procedimientos, regulaciones, leyes, normas).

El rol del equipo de Auditoría Interna en los procesos de Autoevaluación de control es servir de facilitador usando su experiencia y conocimiento para guiar a la Administración y demás personal en el proceso de evaluación de los riesgos, así mismo, debe coordinar el proceso, planeando y consolidando los resultados.

8. EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO (SCI)

Se entiende por SCI el conjunto de políticas, principios, normas, procedimientos y mecanismos de verificación y evaluación establecidos por la Junta Directiva, la Administración y demás funcionarios de Coosalud E.P.S. S.A. para proporcionar un grado de seguridad razonable en cuanto a la consecución de los siguientes objetivos:

- Prevenir y mitigar la ocurrencia de fraudes, originados tanto al interior como al exterior de Coosalud E.P.S. S.A.
- Realizar una gestión adecuada de los riesgos.
- Aumentar la confiabilidad y oportunidad en la Información generada por Coosalud E.P.S. S.A.
- Dar un adecuado cumplimiento de la normatividad y regulaciones aplicables a Coosalud E.P.S. S.A.

Como función de Auditoría Interna deberá asistir a Coosalud E.P.S. S.A. en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua, sin perjuicio de la autoevaluación y el autocontrol que corresponden a cada funcionario de Coosalud E.P.S. S.A.

La Función de Auditoría Interna una vez al año deberá informar a la Administración y al Comité de Auditoría de Junta Directiva, sobre la efectividad del sistema de control interno. Para ello, la Auditoría Interna deberá soportarse en el resultado de las actividades de aseguramiento que realizó durante el último año, además de pruebas adicionales que considere pertinentes.

Para la evaluación sobre la efectividad del sistema de control interno se tendrá en cuenta lo establecido por la Superintendencia Nacional de la Salud y la metodología definida por la Auditoria Interna.

9. TIPOS DE AUDITORIAS

9.1.1. Auditorias Programadas de Evaluación

Son las auditorias integrales que se realizan en el Nivel Nacional y/o las Sucursales para determinar el cumplimiento de las políticas directrices y normas generales. Este tipo de visita de inspección cobra vital importancia en la medida en la que levanta información sobre identificación de riesgos potenciales, fallas y debilidades en la alineación de los procesos estratégicos, por fallas en los procesos operativos y de control.

9.1.2. Auditorias de Seguimiento

Son las auditorias enfocadas especialmente al seguimiento de los procesos críticos con fallas o compromisos de ajuste. Generalmente se realizan sobre áreas específicas para verificar el cumplimiento de las recomendaciones anteriores, sobre la evaluación de indicadores de gestión, o para la verificación de resultados.

9.1.3. Auditorias Especiales

Son acciones de contingencias sobre la detección imprevista de irregularidades en la gestión del servicio o de los recursos. Este tipo de auditoría es netamente investigativa y su objeto es establecer las dimensiones de un siniestro, el compromiso de la empresa y las responsabilidades de suceso.

9.1.4 Auditorias Continuas

Son las inspecciones realizadas por los auditores internos que tendrán como objetivo velar por el cumplimiento de todos los procesos y procedimientos en el trabajo.

10. DESCRIPCIÓN DE LAS ACTIVIDADES DE LA AUDITORIA

ACTIVIDADES	QUIEN	CUANDO	COMO	DONDE	PARA QUÉ
Planeación de la Auditoría					
Preparación del programa de auditorias	▪ Outsourcing auditoría interna ▪ Dirección Nacional de Auditoría interna	Anual	Se realiza la priorización de procesos según el mapa de procesos y en alineación con los objetivos	Plan general de auditoría interna	Organizar y priorizar la ejecución de la auditoria

			estratégicos de la compañía.		
Selección del equipo auditor	▪ Outsourcing auditoría interna	Anual	Se verifica el proceso que se va auditar y de acuerdo a la extensión y área se define el equipo requerido	Plan general de auditoría interna	Determinar según las necesidades del proceso el auditor que va a realizar la auditoría
Definir objetivos, alcance, criterios y viabilidad	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Al inicio de cada auditoria	Verificando en la caracterización del proceso a auditar	Se describe en la carta de inicio de auditoria	Determinar el alcance según la arquitectura del proceso y sus particularidades y comunicar al líder el objetivo, alcance y criterios en la auditoria de su proceso.
Contacto inicial con auditado	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Al inicio de cada auditoria	Carta de inicio de auditoría y reunión de apertura	Se notifica mediante correo electrónico donde se envía adjunta la carta de inicio y se establece fecha de reunión	Comunicar al auditado los objetivos, metodología, alcance y tiempos de ejecución.
Revisión de los documentos a auditar	▪ Outsourcing auditoría interna	Al inicio de cada auditoria	Por medio de la intranet de Coosalud se descarga la documentación requerida	Intranet Coosalud	Tener conocimiento previo del proceso a auditar
Preparación del plan de auditorias	▪ Outsourcing auditoría interna ▪ Dirección Nacional de	Al inicio de cada auditoria	De acuerdo con el proceso se definen los tiempos para cada fase	Se identifica en la carta de inicio las fechas de cada fase	Dar conocimiento al líder del proceso y al equipo de auditoria los tiempos definidos para cada fase, así

	auditoría interna				poder finalizar en los tiempos establecidos
Asignación de las tareas al equipo auditor.	▪ Outsourcing auditoría interna	Al inicio de cada auditoria	Según el proceso y subprocesos se definen las actividades para el grupo auditor	Se documenta en el plan de pruebas	Definir las actividades que realizará el equipo auditor y las fechas de cierre para cada una de ellas.
Preparación de los documentos de trabajo	▪ Outsourcing auditoría interna	Al inicio de cada auditoria	De acuerdo con el proceso se define los documentos a verificar	Documentos internos	Alistamiento de la documentación requerida para la auditoria
Ejecución de la Auditoría					
Reunión de apertura	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Al inicio de cada auditoria	Se define fecha para reunión de manera virtual o presencial	Virtual o presencial	Presentar al equipo auditor, el objetivo de la auditoría, metodología y resolver inquietudes iniciales que surgen de la revisión de documentación disponible. Aclarar dudas.
Comunicación durante la auditoria	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Durante la auditoria	Mediante correo electrónico o por medio del Director Nacional de auditoría interna, si no hay respuesta oportuna se deriva solicitud a la Secretaria General	Correo electrónico	Entendimiento del proceso, solicitud y entrega de la información solicitada.
Recopilación y verificación de información	▪ Dirección Nacional de	Durante la auditoria	Se realiza la solicitud	Se dispondrá de sharepoint	Mantener la información

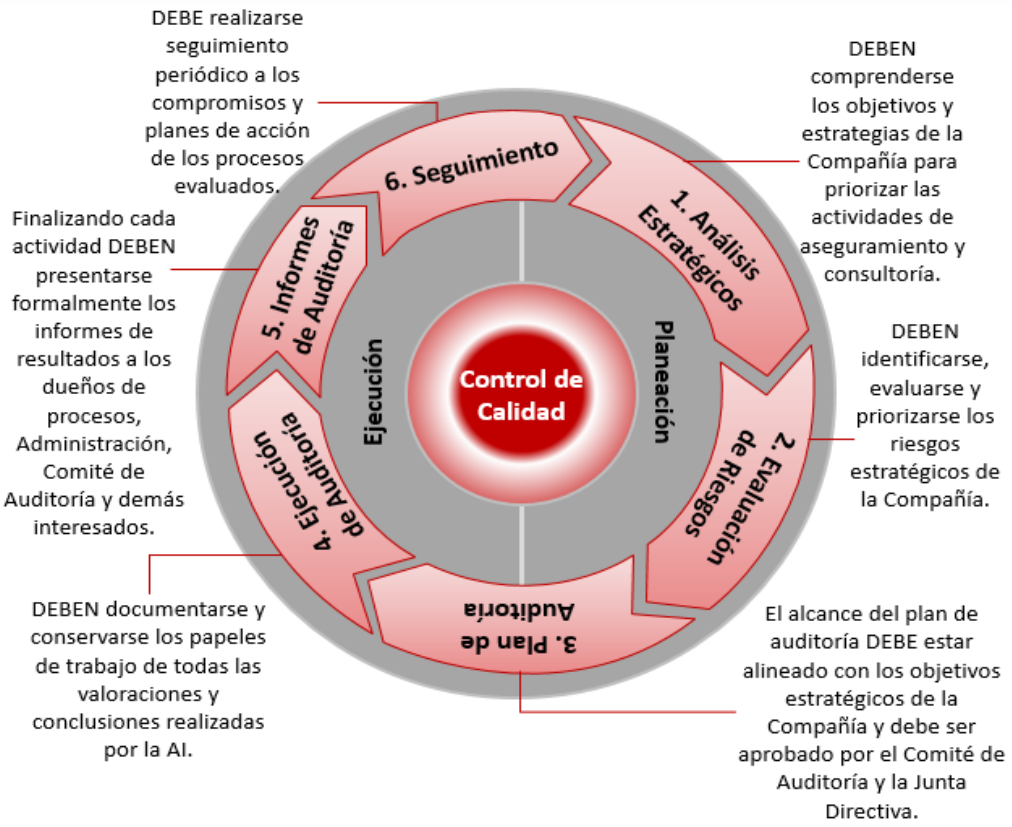
	auditoría interna ▪ Outsourcing auditoría interna		mediante correo electrónico de lo requerido. En caso de no cumplir con la completitud, se solicitará de forma inmediata la información faltante para su remisión el mismo día.	o drive para el ingreso de los documentos requeridos	requerida en un lugar seguro y disponible para la auditoria. El líder proceso contará con 3 días hábiles para el envío de la información en el caso de no enviarla se entenderá que no se cuenta con esta.
Notificación de hallazgos	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Durante la auditoria	Mediante el informe detallado	Se envía por correo electrónico	Validar los hallazgos con el líder del proceso quien contara con 2 días hábiles para generar observaciones
Preparación de las conclusiones	▪ Outsourcing auditoría interna	Durante la auditoria	A partir de los papeles de trabajo y según la validación de hallazgos	Papeles de trabajo	Para poder dar un resultado a la prueba generada
Preparación del Informe de Auditoría					
Preparación del informe de auditoría de cada auditor.	▪ Outsourcing auditoría interna	Finalizando la auditoria	De acuerdo con los hallazgos identificados	En el formato definido	Presentación de los resultados de la auditoria
Presentación del Informe de auditoría ante la oficina de control interno	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Finalizando la auditoria	Presentación del informe definido	Reunión definida entre las partes	Recibir recomendaciones del informe a presentar
Análisis de la Información por parte del jefe de control interno	▪ Dirección Nacional de auditoría interna	Finalizando la auditoria	Por medio del envío de correo electrónico del	Informe detallado	Para verificar que se abarquen todos los puntos requeridos

			informe detallado		
Presentación del informe preliminar ante el líder del proceso	▪ Outsourcing auditoría interna	Finalizando la ejecución de la auditoria	Reunión para la presentación	Informe detallado definitivo posterior a la validación de hallazgos	Conocimiento del resultado final
Presentación de evidencias correspondientes a las observaciones del informe	▪ Líder del proceso	Finalizando la ejecución de la auditoria	Mediante correo electrónico	Informe detallado preliminar a los 2 días hábiles de envío por la auditoría interna	Subsanar o validar los hallazgos identificados a los que haya lugar
Presentación del Informe de Auditoría					
Entrega del informe al Director Nacional de Auditoria	▪ Outsourcing auditoría interna	Una vez se finaliza la auditoria	Mediante correo electrónico	Se dispone por correo electrónico	Revisión y posterior distribución por el Director Nacional de Auditoria
Distribución del informe a los Vicepresidentes	▪ Dirección Nacional de auditoría interna ▪ Outsourcing auditoría interna	Una vez se finaliza la auditoria	Mediante correo electrónico	Desde el área de auditoría interna se realiza la distribución por correo electrónico	Conocimiento del resultado final y establecer los planes de mejora para los hallazgos
Envío De planes de mejoramiento	▪ Vicepresidentes del área auditada	Una vez se finaliza la auditoria	Mediante correo electrónico	En los formatos establecidos	Dar a conocer los planes de mejoramiento definidos por el área que subsanen los hallazgos.
Revisión de los planes de mejoramiento	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	Una vez se finaliza la auditoría.	Por medio de correo electrónico se envían las observaciones dentro del mismo formato si hay lugar	Se realiza en el formato establecido para este fin.	Corregir los planes de mejora que no cumplan con la subsanación de los hallazgos establecidos

Consolidación del informe definitivo	▪ Outsourcing auditoría interna	Una vez se obtiene las observaciones y planes de mejoramiento	Por correo electrónico	En el informe preliminar enviado y formato establecido	Dar cierre al informe detallado definitivo para presentar
Socialización del informe definitivo	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna ▪ Líder del proceso	Finalización de la auditoria	Mediante presentación del informe ejecutivo	Presencial o virtual	Conocimiento de los resultados de la auditoría realizada
Evaluación y control del proceso de auditoría					
Seguimiento a los planes de mejoramiento.	▪ Outsourcing auditoría interna ▪ Dirección Nacional de auditoría interna	De acuerdo con la frecuencia acordada entre las partes	Verificando la ejecución de los planes de mejora en los formatos establecidos	Vía correo electrónico o share point	Dar seguimiento al cumplimiento y ejecución de los planes de mejoramiento definidos
Evaluación y Verificación del desempeño del equipo auditor	▪ Outsourcing auditoría interna	Al finalizar la auditoria	Encuesta de satisfacción definida	Vía correo electrónico	Identificar las oportunidades de mejora del equipo auditor
Análisis de la ejecución del proceso de auditorias	▪ Outsourcing auditoría interna	Al cierre de la auditoria	Análisis de la actividad realizada	Formato especifico	Definir como estuvo nuestro proceso de auditoria

11 DESCRIPCIÓN DEL PROCESO DE AUDITORÍA

La metodología Auditoría Interna se compone de dos módulos (Planeación y Ejecución), los cuales se descomponen en seis fases, como se muestra en la siguiente gráfica y se desarrollan en los próximos capítulos.



12 PROCEDIMIENTOS Y ACTIVIDADES DE LA AUDIORÍA INTERNA

12.1 Fase Planeación

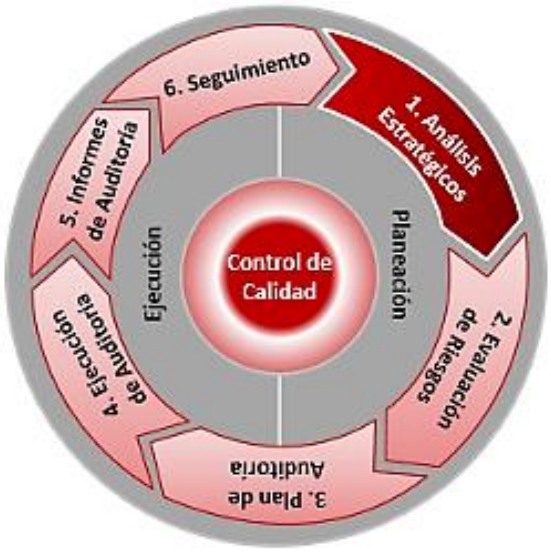
En esta fase se verifican las necesidades de la organización alineado a sus objetivos estratégicos para iniciar la construcción del plan de auditoría, teniendo en cuenta el objetivo y alcance definido.

12.1.1.1 Análisis Estratégico

Objetivos

Proporcionar un marco para la Función de Auditoría Interna que ayude a identificar los eventos que tienen relevancia Coosalud E.P.S. S.A., y además que ayude a comprender los asuntos y fuerzas externas que lo afectan. También que le permita identificar los objetivos estratégicos, y proporcionar una comprensión de cómo la organización responde a los desafíos que impiden el logro de estos objetivos.

De los resultados de este análisis y de la información recopilada, se identifican riesgos que pueden afectar el logro de los objetivos estratégicos Coosalud E.P.S. S.A. y que serán tenidos en cuenta durante la Fase de Evaluación del Riesgo.



En esta fase el equipo de Auditoría Interna debe comprender los objetivos y estrategias de Coosalud E.P.S. S.A. para priorizar las actividades de aseguramiento y consultoría, teniendo en cuenta los siguientes aspectos:

- Análisis de Información sobre Antecedentes
- Compresión de los Objetivos y Estrategias

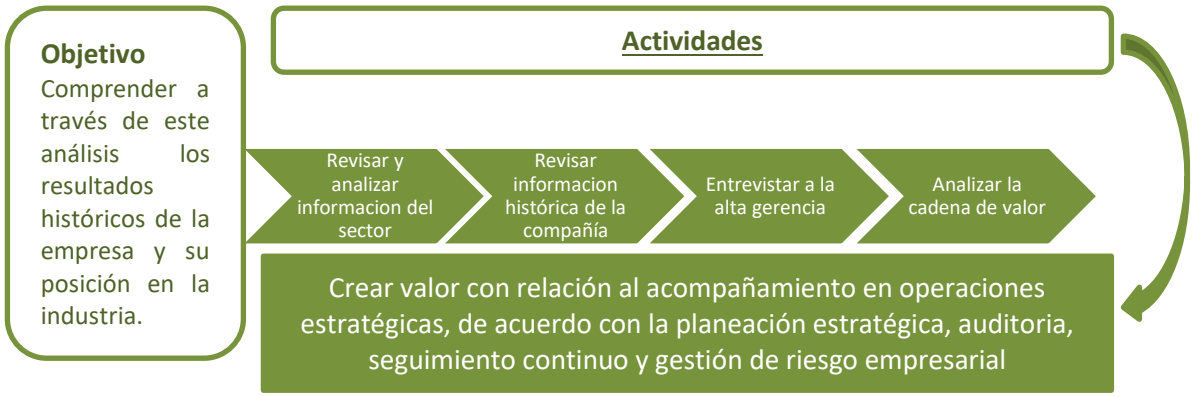
El propósito de esta Fase es garantizar que las actividades de aseguramiento cubren adecuadamente Coosalud E.P.S. S.A. Para ello es necesario conocer cómo responde La entidad a las fuerzas externas tales como: entorno económico, social, mercado, legal y tecnológico, factores específicos del sector financiero, y cualquier otro en el que se desarrolle Coosalud E.P.S. S.A.

El análisis estratégico provee a la Auditoría Interna un marco para comprender los objetivos y estrategias de Coosalud E.P.S. S.A. y luego considerar los riesgos que pueden afectar el logro de dichos objetivos.

12.1.1.2 Analizar la Información sobre Antecedentes

La documentación para analizar por la Auditoría sobre antecedentes incluye: estructura organizacional, visión, misión, valores, objetivos y estrategias, así como información del sector.

Las actividades que se llevan a cabo son las siguientes, las cuales deben estar documentadas por la Auditoría Interna y a disposición para su permanente consulta, revisión y actualización:

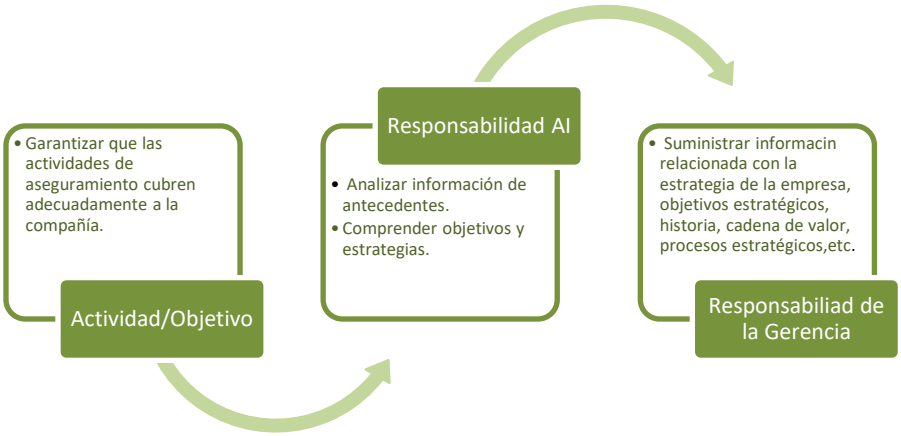


12.1.1.3 Comprender los Objetivos y Estrategia

Una vez que la Auditoría Interna ha analizado, documentado y comprendido la información sobre antecedentes, se encuentra preparada para entender hacia donde se dirige Coosalud E.P.S. S.A. y podrá enfocarse en sus actividades de aseguramiento y asesoría dando prioridad a los procesos, proyectos o actividades del negocio que facilitan el logro de las estrategias y objetivos, así como los que representan riesgos de negocio más importantes. De esta manera, las actividades de aseguramiento y asesoría se realizarán con un enfoque basado en riesgos.

La Auditoría Interna debe desarrollar la Fase 1, por lo menos una vez al año según los cambios del negocio, actualizar y reflejar su análisis acorde a los objetivos y planes estratégicos de Coosalud E.P.S. S.A.

Las principales responsabilidades de la Auditoría Interna y de las partes interesadas son:



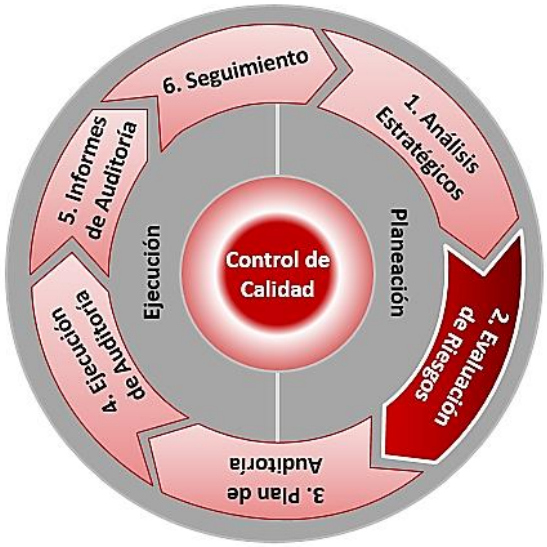
12.1.2 Evaluación de riesgos estratégicos

Objetivos

En la evaluación de riesgos se identifican riesgos estratégicos relacionados con los objetivos y estrategias de Coosalud E.P.S. S.A. y se evalúa en qué medida estos riesgos ponen en peligro el cumplimiento de los objetivos estratégicos.

Es importante tener en cuenta que la evaluación de riesgos es una actividad que normalmente es impulsada por cambios importantes del perfil de riesgo en Coosalud E.P.S. S.A.

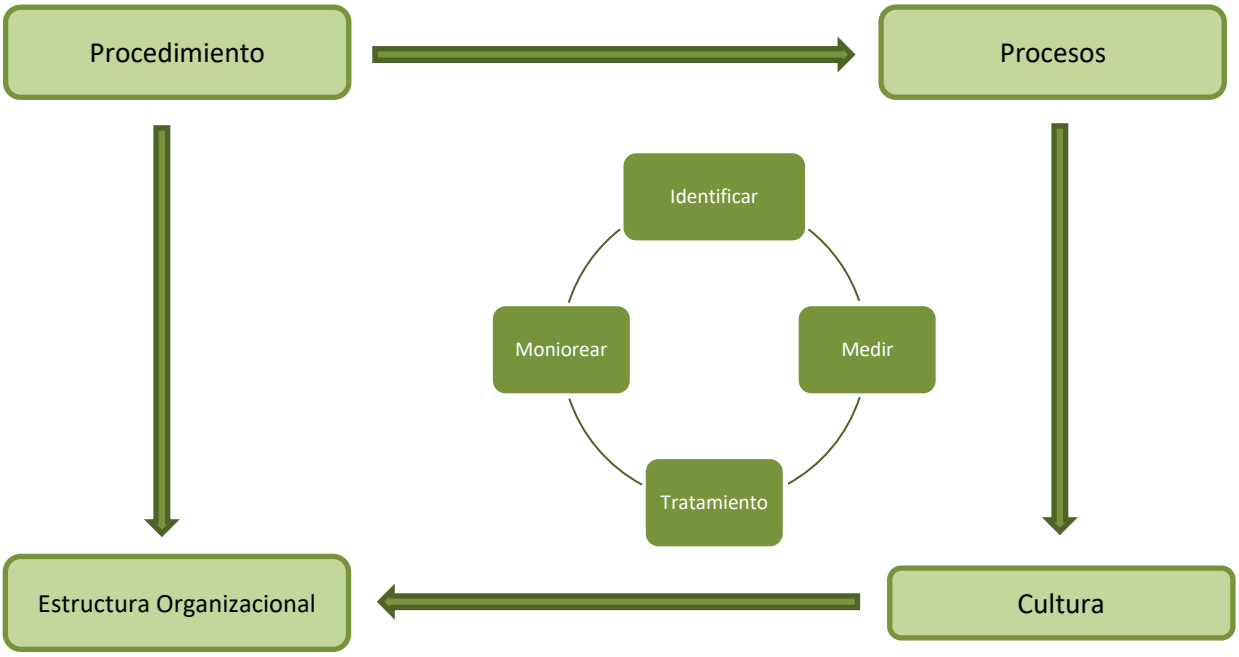
Se deben realizar programas de monitoreo que permitan identificar eventos que desencadenen la necesidad de actualizar la evaluación de riesgos, como: reestructuración, lanzamiento de nuevos productos y cambios en el dueño del proceso.



Como se indica en la Fase de Análisis Estratégico, la identificación de los objetivos estratégicos y las estrategias se produce a través de reuniones con la Alta Gerencia y en la comprensión de las fuerzas externas, aspectos relacionados con la industria y las actividades de Coosalud E.P.S. S.A.

12.1.2.1 Definición de los Riesgos Estratégicos

La definición de riesgos estratégicos será responsabilidad de la Gerencia Comercial, quien deberá considerar la metodología definida para la identificación, valoración, tratamiento y monitoreo de los riesgos estratégicos de Coosalud E.P.S. S.A. El equipo de Auditoría Interna también deberá tener en cuenta esta metodología en el entendimiento que realice de los riesgos estratégicos.



12.1.2.2 Asociación de Riesgos Estratégicos a Procesos

La ejecución de esta Fase está a cargo del equipo de Auditoría Interna; aquí se explica de manera detallada los pasos a seguir para asociar los objetivos estratégicos de la empresa con los riesgos estratégicos y con sus procesos. Estos elementos se constituyen en componentes claves en el diseño y construcción del Plan de Auditoría.

12.1.2.2.1 Asociación de Objetivos Estratégicos con Riesgos Estratégicos

Con base en los riesgos estratégicos de Coosalud E.P.S. S.A., la Auditoría Interna debe valorar aquellos riesgos que en caso de materializarse podrían afectar el cumplimiento de dichos objetivos. La valoración del nivel de riesgo se da en términos de probabilidad e impacto, así:

Criterios para evaluar el impacto						
Puntaje	**Clasificación**	**Finanzas**	**Operaciones**	**Cumplimiento**	**Estratégico**	
		EBITDA	**Alcance**	**Legal/Regulatorio**	**Reputacional**	**Recurso Humano**
5	Catastrófica	5%	Perdida de participación en el mercado del 5% Perdida de información crítica y/o confidencial irrecuperable Destrucción parcial o total de las instalaciones y/o equipos Incumplimiento por encima del 10% en alcance, calidad y costo de los proyectos estratégicos	Intervención de Coosalud E.P.S. S.A., o sus aliados estratégicos por incumplimientos legales	Pérdida de confianza y credibilidad de Coosalud E.P.S. S.A., a nivel nacional e internacional. Cubrimiento prolongado de medios de prensa nacionales y/o internacionales. Daño irreparable al nombre Coosalud E.P.S. S.A.,	Perdida de una o más vidas humanas y/o generación de incapacidad total y permanente por accidente o enfermedad profesional de algún colaborador de Coosalud E.P.S. S.A.,
4	Mayor	4%	Perdida de participación en el mercado del 4% Fallas tecnológicas que generen un incremento de 25% al 30% de la carga operativa o reprocesos de Coosalud E.P.S. S.A. Incumplimiento por encima del 8% en alcance, calidad y costo de los proyectos estratégicos	Sanciones económicas por incumplimiento de las normas establecidas por los entes reguladores	Pérdida de confianza y credibilidad de Coosalud E.P.S. S.A., a nivel nacional o local. Cubrimiento prolongado de medios de prensa regionales. Atención de medios de prensa nacionales. Afectación al nombre Coosalud E.P.S. S.A., reparable en el mediano plazo.	Afecta de forma general la salud propiciando incapacidad temporal de los colaboradores de Coosalud E.P.S. S.A., incluyendo enfermedades ocupacionales

3	Moderado	3%	Perdida de participación en el mercado del 3% Fallas tecnológicas que generen un incremento de 15% al 25% de la carga operativa o reprocesos de Coosalud E.P.S. S.A. Incumplimiento por encima del 6% en alcance, calidad y costo de los proyectos estratégicos	Demandas o sanciones relacionadas con la atención en salud prestada en Coosalud E.P.S. S.A.,	Pérdida de confianza de los grupos de interés regulatorios o de gobierno. Cubrimiento prolongado de medios de prensa regionales. Atención de medios de prensa nacionales. Afectación al nombre Coosalud E.P.S. S.A., reparable en el mediano plazo.	Afecta de forma general la salud de los colaboradores de Coosalud E.P.S. S.A., sin propiciar incapacidad temporal. Otras lesiones que producen tiempo perdido
2	Menor	2%	Perdida de participación en el mercado del 2% Fallas tecnológicas que generen un incremento de 6% al 14% de la carga operativa o reprocesos de Coosalud E.P.S. S.A. Incumplimiento por encima del 6% en alcance, calidad y costo de los proyectos estratégicos	Demandas o sanciones relacionadas con el incumplimiento de las normas aplicables a Coosalud E.P.S. S.A.,	Pérdida de confianza por parte de varios grupos de interés, excluyendo los regulatorios o de gobierno. Cubrimiento de medios de prensa locales. Paros o protestas de grupos de interés locales.	Afecta levemente la salud de algunos colaboradores de Coosalud E.P.S. S.A., sin embargo, no genera incapacidad temporal, incluyendo casos de primeros auxilios y de tratamiento médico

1	Insignificante	1%	Perdida de participación en el mercado del 3% Fallas tecnológicas que generen un incremento menor al 5% de la carga operativa o reprocesos de Coosalud E.P.S. S.A., Incumplimiento por encima del 2% en alcance, calidad y costo de los proyectos estratégicos	No generan demandas ni sanciones económicas y/o administrativas	Pérdida de confianza por parte de algún grupo de interés, excluyendo los regulatorios o de gobierno.	No afecta la salud de los colaboradores de Coosalud E.P.S. S.A., y no genera incapacidad temporal. Atención en el lugar de trabajo y no afecta rendimiento laboral

Criterios para evaluar la probabilidad			
Nivel	**Criterio**	**Descripción**	**Frecuencia**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez en los últimos 5 años
3	Posible	El evento podrá ocurrir en algún momento	Al menos una vez en los últimos 2 años
4	Probable	Es probable que suceda el evento en la mayoría de las circunstancias	Al menos una vez en el último año
5	Casi seguro	Se espera que suceda el evento en la mayoría de las circunstancias	Más de una vez al año

Posteriormente se debe elaborar la matriz de asociación de objetivos estratégicos a los riesgos estratégicos, la cual debe contener:

- Código de identificación - Nomenclatura
- Nombre y descripción del riesgo.
- Objetivo estratégico afectado.

Objetivos Estratégicos	
Id	**Descripción**
O1	**Dar Valor al Sistema:** Con el aumento de años de vida saludable de los afiliados priorizando la morbimortalidad infantil, gestantes y las enfermedades crónicas como el cáncer.
O2	**Dar Valor al Afiliado:** A través de la seguridad, oportunidad, accesibilidad, integralidad y humanización de la atención.
O3	**Dar Valor al accionista:** Por medio del crecimiento sostenido de la compañía, la eficiencia operacional, la habilitación financiera, el reconocimiento de los grupos de interés y EBITda positivo.

Asociación de Riesgos Estratégicos a Objetivos Estratégicos con su Correspondiente Valoración de Riesgo Residual

Nomenclatura	Riesgo	Objetivo Estratégico Afectado	Nivel de Riesgo Residual	Calificación	
R1	Inapropiada gestión del riesgo de la salud de los afiliados a Coosalud EPS que impacte los años de vida saludables	1, 2, 3	Medio	2	
R2	Inoportunidad en la atención de los servicios de salud que deterioren el estado de salud de los afiliados de Coosalud EPS	1,2,3	Medio	2	
R3	Barreras de acceso que limiten el acceso a la atención de los afiliados	1.2	Medio	2	Medio
R4	Falta de integralidad en la atención que deterioro el estado de salud de los afiliados	2	Bajo	1	Bajo
R5	Servicio deshumanizado por parte de los colaboradores de Coosalud y sus prestadores de atención	1.2	Medio	2	
R6	Fallas en los protocolos de seguridad de la atención de los afiliados de Coosalud por parte de los prestadores de servicios de salud	1.2	Bajo	1	
R7	Estancamiento del crecimiento de la compañía que impacte su punto de equilibrio	3	Bajo	1	
R8	Ineficiencia operacional en los procesos de Coosalud EPS	1,2,3	Medio	2	
R9	Perdidas económicas de Coosalud EPS	3	Medio	2	

3
2
1

Una vez valorados los riesgos (subriesgos), estos se priorizan de acuerdo con la combinación de la probabilidad e impacto (Severidad Subriesgo).

12.1.2.2.2 Relación de Riesgos Estratégicos con Procesos

Se construye una lista ordenada por macroprocesos, indicando la totalidad de los procesos y subprocesos que los conforman; adicionalmente, se listan todos los riesgos previamente calificados de acuerdo con lo indicado en el paso anterior y se registra la calificación de nivel de riesgo (Severidad Subriesgo) en la casilla del proceso que el riesgo impacta el logro de los objetivos, el siguiente es el ejemplo:

Tipo de Procesos	Macroproceso	Proceso (Unidad Auditable)	Ponderación	Total	Riesgos Estratégicos									Resultado Priorización
					R1	R2	R3	R4	R5	R6	R7	R8	R9	
Estratégico	Gestión Integral del Riesgo	Gestión Integral del Riesgo	5.4%	30	4	3	3	3	2	4	4	4	3	**30**
Misional	Gestión de la población	Análisis de mercado	4.8%	27	1	4	3	4	3	2	4	2	4	**27**
Misional	Gestión de la población	Afiliación y registro	4.5%	25	3	4	3	2	2	2	3	2	4	**25**
Misional	Gestión de la población	Gestión del ingreso	4.7%	26	2	4	2	3	3	2	4	2	4	**26**
Misional	Gestión de la población	Prestaciones económicas	4.1%	23	2	3	2	2	2	3	3	2	4	**23**
Misional	Gestión de la protección de la salud	Gestión del riesgo en salud	5.9%	33	4	4	4	4	4	4	3	3	3	**33**
Misional	Gestión de la protección de la salud	Gestión de la calidad de los servicios de salud	5.6%	31	4	3	3	4	3	4	3	4	3	**31**
Misional	Gestión de la protección de la salud	Gestión de la oportunidad	5.2%	29	4	4	4	2	4	3	2	3	3	**29**
Misional	Gestión de la protección de la salud	Gestión del acceso	5.9%	33	3	5	5	3	4	2	4	3	4	**33**
Apoyo	Apoyo	Gestión Estratégica	5.2%	29	3	3	3	2	2	4	4	4	4	**29**
Apoyo	Apoyo	Gestión reputacional y de comunicaciones	5.6%	31	3	4	4	4	4	4	3	2	3	**31**
Apoyo	Apoyo	Gestión financiera	4.3%	24	2	2	2	2	2	2	4	3	5	**24**
Apoyo	Apoyo	Medición, análisis y mejora	5.0%	28	2	3	3	3	3	3	3	5	3	**28**
Apoyo	Apoyo	Gestión de la experiencia del usuario	6.1%	34	4	4	4	4	4	4	3	4	3	**34**
Apoyo	Apoyo	Gestión del talento humano	4.3%	24	2	2	2	2	4	2	3	4	3	**24**
Apoyo	Apoyo	Gestión de TICS	4.7%	26	3	2	4	3	2	2	3	4	3	**26**
Apoyo	Apoyo	Gestión administrativa	4.5%	25	2	3	3	3	3	2	3	2	4	**25**
Apoyo	Apoyo	Gestión jurídica	4.3%	24	3	2	3	2	2	3	3	3	3	**24**
Apoyo	Apoyo	Gestión del egresgo	5.0%	28	3	3	3	3	3	2	4	3	4	**28**
Apoyo	Apoyo	Gestión contable	5.0%	28	3	3	3	3	3	2	4	3	4	**28**
														0
														0
														0
														0
														0
														0
														0
			100%	**558**	**57**	**65**	**63**	**58**	**59**	**56**	**67**	**62**	**71**	

Se obtiene una calificación total por proceso la cual indica la exposición al riesgo de cada proceso, así como ponderación de la participación porcentual de cada proceso en todo el Universo de Auditoría.

Finalmente se clasifica el resultado de la ponderación de acuerdo con la escala de calificación para el atributo Participación en Riesgos estratégicos.

12.1.2.2.3 Análisis y Priorización de los Procesos Por Evaluar

De lista de las unidades auditables que conforman el Universo de Auditoría se califica cada uno de los Atributos definidos según al conocimiento de Coosalud E.P.S. S.A. y se calcula la ponderación final en la columna "Calificación". El siguiente es un ejemplo del formato ***F3 - Análisis y Priorización de los Procesos a Evaluar***:

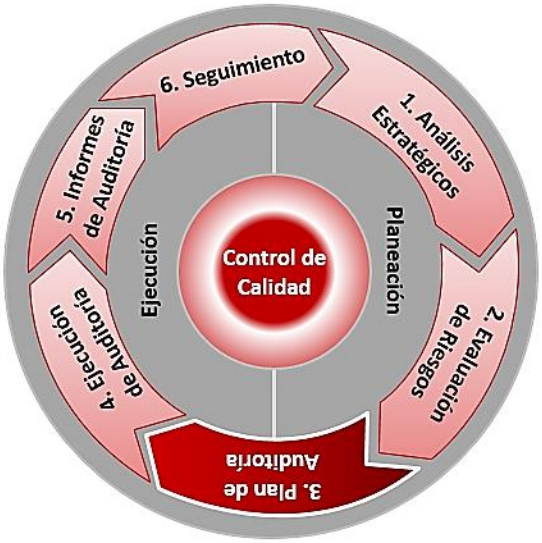
Criterios de valoración de Macro/ procesos/ a evaluar			Impacto del proceso en los objetivos y riesgos estratégicos	Resultados de la Última Auditoria	Tiempo Transcurrido desde la Ultima Evaluación	Expectativas Alta Dirección - Procesos Críticos	Expectativas Facilitadores de Control Interno	Normatividad y Regulación Sobre los Procesos	Cambios de Organización y/u Operativos	Calificación
Tipo de Proceso	Macroproceso	Proceso	25%	15%	15%	15%	15%	10%	5%	Total
Apoyo	Apoyo	Gestión contable	7	7	7	7	7	7	5	**6.90**
Misional	Gestión de la protección de la salud	Gestión de la calidad de los servicios de salud	7	5	7	7	7	7	5	**6.60**
Apoyo	Apoyo	Gestión financiera	5	7	7	7	7	7	7	**6.50**
Apoyo	Apoyo	Gestión del egreso	7	5	7	7	7	5	5	**6.40**
Misional	Gestión de la protección de la salud	Gestión de la oportunidad	7	5	7	7	7	5	5	**6.40**
Apoyo	Apoyo	Medición, análisis y mejora	7	5	7	7	7	5	3	**6.30**
Misional	Gestión de la población	Prestaciones económicas	5	7	7	7	7	5	5	**6.20**
Estrategico	Estrategico	Gestión Estratégica	7	5	7	7	7	3	3	**6.10**
Misional	Gestión de la población	Gestión del ingreso	5	5	7	7	5	5	3	**5.50**
Misional	Gestión de la protección de la salud	Gestión del riesgo en salud	7	5	1	7	5	7	7	**5.50**
Apoyo	Apoyo	Gestión de la experiencia del usuario	7	7	1	7	3	7	5	**5.40**
Misional	Gestión de la población	Análisis de mercado	5	5	7	7	3	3	3	**5.00**
Misional	Gestión de la protección de la salud	Gestión del acceso	7	5	1	7	3	5	7	**5.00**
Apoyo	Apoyo	Gestión reputacional y de comunicaciones	5	3	7	7	3	5	3	**4.90**
Apoyo	Apoyo	Gestión jurídica	5	5	3	7	3	7	3	**4.80**
Misional	Gestión Integral del Riesgo	Gestión Integral del Riesgo	7	5	1	7	3	5	3	**4.80**
Misional	Gestión de la población	Afiliación y registro	5	7	1	7	3	5	3	**4.60**
Apoyo	Apoyo	Gestión del talento humano	5	3	1	7	3	5	5	**4.10**
Apoyo	Apoyo	Gestión de TICS	5	3	1	7	3	5	5	**4.10**
Apoyo	Apoyo	Gestión administrativa	3	3	1	7	5	5	5	**3.90**

Posteriormente se organiza la Calificación Total desde el mayor valor al menor, de forma que cada subproceso quede priorizado en todo el universo auditable.

12.1.2.2.4 Plan de auditoría

Objetivos

El Plan de Auditoría Interna constituye el ámbito de trabajo de la Auditoría Interna, su alcance y amplitud deberán estar en línea con las necesidades de Coosalud E.P.S. S.A. y la evaluación de riesgos realizada por la Gerencia de Planeación Corporativa. La aprobación del plan estará a cargo del Comité de Auditoría y de la Junta Directiva, así como las modificaciones que se realicen al plan inicial.



El Plan de Auditoría basado en riesgos, permite identificar las prioridades de la actividad de Auditoría Interna y alinearse con las metas de Coosalud E.P.S. S.A.

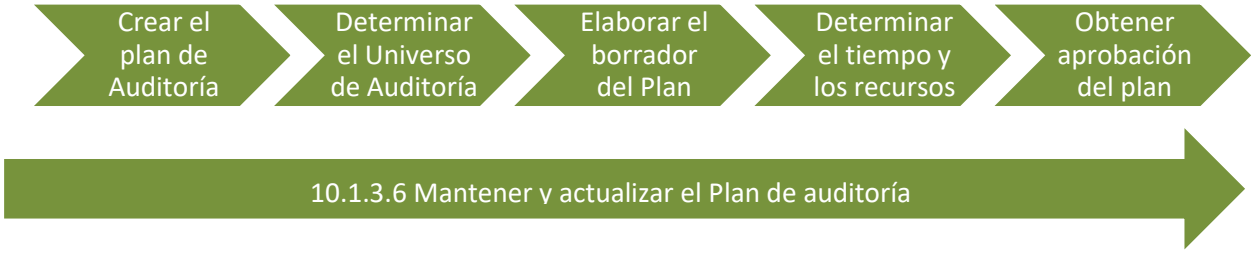
El Plan de Auditoría Interna indica los parámetros generales, los recursos y el alcance de los trabajos de Auditoría Interna, incluye controles internos o funciones que deben revisarse y la forma en que se llevará a cabo el plan, adicionalmente se debe establecer un proceso continuo para evaluar, actualizar y mantener el plan conforme a los cambios que pueda tener Coosalud E.P.S. S.A. los riesgos, las operaciones, los programas, los sistemas y los controles.

El plan se elabora anualmente y tiene una revisión semestral desviaciones, en caso de ser necesario realizar ajustes se notificará al Comité de Auditoría de la Junta Directiva para su aprobación.

El Plan de auditoría deberá ser aprobado por el Comité de Auditoría de la Junta Directiva, dejando evidencia en el acta del mes inmediatamente siguiente a su presentación. El Comité de Auditoría podrá solicitar ajustes al plan de acuerdo con las necesidades de la Junta Directiva.

Cuando la Auditoría Interna no cuente con el recurso necesario o idóneo para la ejecución de su trabajo, esta podrá apoyarse en consultores externos, teniendo en cuenta que esto podría mejorar los procesos de gestión de Riesgo, Control y Gobierno de Coosalud E.P.S. S.A.

A continuación, se presentan las principales actividades a desarrollar para elaborar el Plan de Auditoría**:**



Detalle:

Crear el plan de Auditoría

Teniendo en cuenta los resultados de la Fase 2, el desarrollo del Plan de Auditoría se focalizará en los riesgos que tienen un mayor impacto y probabilidad, concentrándose en los principales riesgos empresariales, asegurando tener en cuenta toda la información pertinente. Estos riesgos se deben alinear con los procesos de negocio que serán prioritarios para evaluar y que serán incluidos en el Plan.

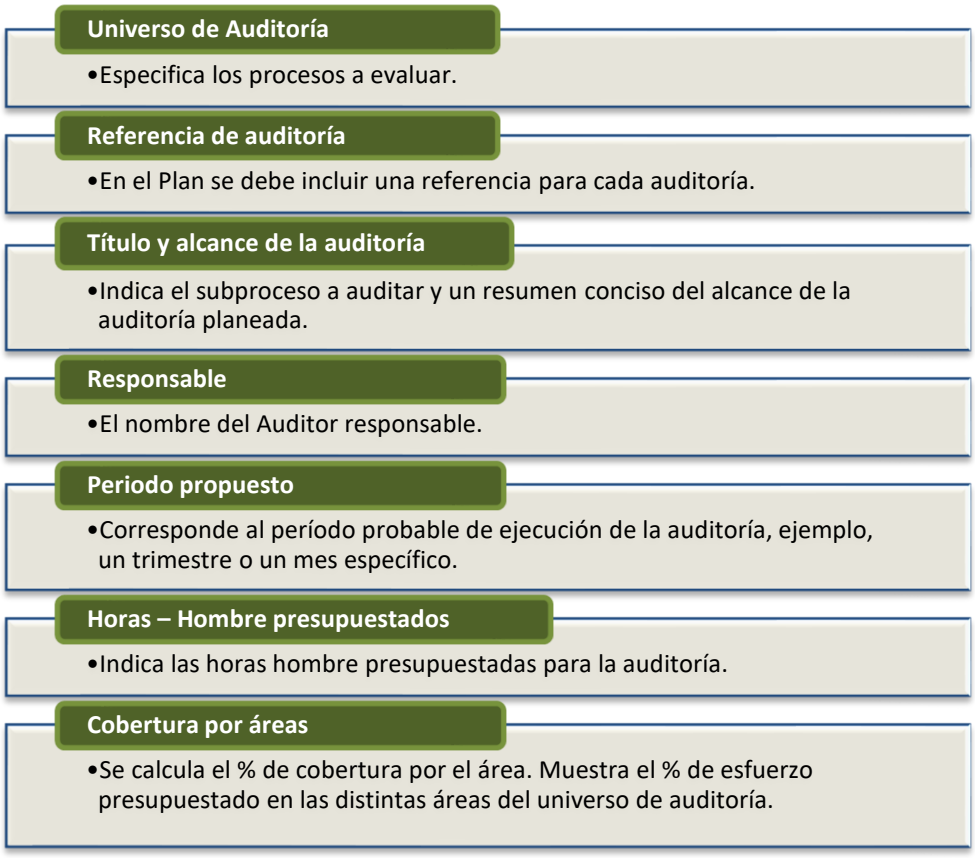
Determinar el Universo de Auditoría

Consiste en determinar los procesos del negocio y proyectos a ser incluidos en el Plan alineados a los riesgos de mayor impacto y mayor probabilidad que pueden afectar el logro de los objetivos estratégicos de Coosalud E.P.S. S.A. con dichos procesos y proyectos:

En la definición del Plan se tiene en cuenta otra información que permite la priorización de actividades que complemente el análisis de riesgos de Coosalud E.P.S. S.A y que incluya criterios de evaluación propios de Auditoría Interna como:

- Tiempo transcurrido desde la última evaluación
- Cambios de organización y/u operativos
- Complejidad administrativa y operativa
- Rotación del personal
- Resultados de la última auditoría
- Materialidad en los estados financieros
- Resultado de monitoreo de controles financieros y operativos
- Criticidad de Riesgos Residuales - Mapa de riesgo del proceso
- Se ha solicitado auditoría al proceso por las partes interesadas.
- Normatividad y regulación sobre los procesos

Los resultados del análisis y priorización de actividades se tendrán en cuenta para realizar una clasificación en actividades de consultoría y aseguramiento, según correspondan a la naturaleza del trabajo de Auditoría Interna.



Se preparará un cronograma detallado por actividades (Auditoría de procesos, auditorías especiales, seguimiento de planes de acción, pruebas permanentes o recurrentes sobre operaciones o informaciones puntuales y consultoría a procesos) y responsables a efectuar las auditorías en Project o Excel para su seguimiento y control.

Elaborar el borrador del Plan

El Plan de Auditoría Interna define el tiempo y los recursos necesarios para lograr las actividades propuestas y proporciona una base para que la Auditoría Interna lleve a cabo la supervisión del progreso y el rendimiento del equipo.

Dadas las limitaciones de recursos y tiempo, el Comité de Auditoría de Junta Directiva puede decidir dónde centrar sus esfuerzos durante el período de evaluación y qué aplazar hasta los próximos años.

Obtener aprobación del Plan

La Gerencia de Auditoría debe presentar el Plan de Auditoría al Comité de Auditoría de Junta Directiva para su aprobación. A su vez, este podrá solicitar la ejecución de determinados proyectos de aseguramiento y consultoría a áreas y/o procesos de interés para él, incluso si estos proyectos no se encuentran identificados como de alta prioridad en el mapa de riesgos.

Mantener y actualizar el Plan de Auditoría

El Plan de Auditoría debe ser dinámico. Una vez aprobado por el Comité de Auditoría, puede ajustarse en el tiempo por diversos factores y cambios internos y externos. Cualquier modificación al mismo debe ser aprobada por el Comité de Auditoría.

12.2 Fase de ejecución

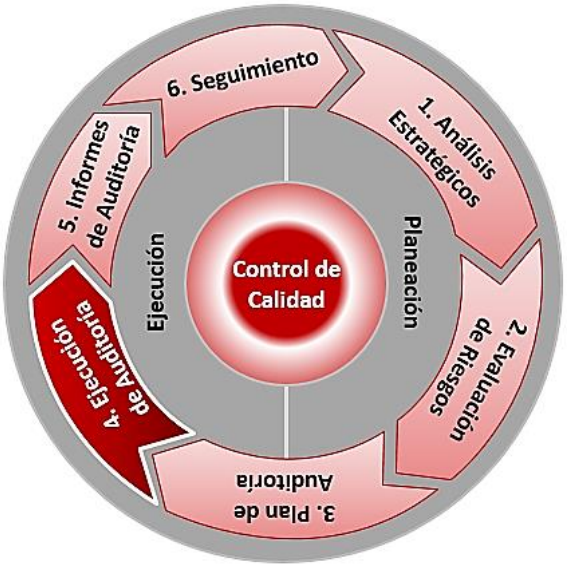
En esta fase se realizarán las actividades propias de la auditoria, de acuerdo con el plan de auditoría y dentro de los tiempos establecidos, los cuales podrían variar debido a las demoras que se puedan presentar para las reuniones de entendimiento, entrega de información y validaciones de hallazgos.

12.2.1 Ejecución de Auditoría

Objetivos

La ejecución de las actividades de la Auditoría Interna resultado del conocimiento adquirido a través del análisis estratégico, la gestión y evaluación de riesgos y la planificación de la Auditoría Interna.

Durante esta fase, la metodología se centra en proporcionar conclusiones y oportunidades de mejora de rendimiento para Coosalud E.P.S. S.A.



Esta fase se centra en la ejecución de actividades de aseguramiento a los diferentes procesos, identificar oportunidades de mejora, y generar recomendaciones que ayuden al mejoramiento continuo de los procesos y que agreguen valor a Coosalud E.P.S. S.A. De acuerdo con el plan anual de auditoría aprobado por el Comité de Auditoría de Junta Directiva, se ejecutarán los trabajos de aseguramiento a cada proceso. En dicha planeación se debió contemplar los objetivos, tiempo y asignación de recursos.

Las actividades que se deben realizar en esta fase son:

- Entendimiento y análisis del proceso
- Preparar carta de alcance
- Diligenciar reporte de declaración de conflictos de interés de los auditores
- Analizar riesgos y controles del proceso
- Elaborar el programa de aseguramiento
- Ejecutar el programa de aseguramiento
- Recolectar la evidencia
- Definición de planes de mejora y compromisos por parte de los dueños de proceso
- Supervisión del trabajo de auditoría interna (Esta actividad es transversal a toda la actividad de aseguramiento).

A continuación, se presenta el detalle de las actividades que debe llevar a cabo el equipo de Auditoría Interna durante esta fase:

12.2.1.1 Entendimiento y Análisis del Proceso

El entendimiento del proceso se realiza a través de entrevistas, lecturas de políticas y manuales de procedimientos y discusiones con la Gerencia (responsable del proceso) y demás personas claves del desarrollo del proceso.

Para el entendimiento del proceso a evaluar, se requiere documentarlo (si no está documentado) o identificar entre otros los siguientes atributos: objetivos del proceso, alcance, entradas, salidas, herramientas utilizadas, responsables, factores críticos de éxito, indicadores y los procedimientos asociados a ellos. El entendimiento del proceso puede realizarse a través de una prueba de recorrido.

Se dará comunicación del inicio de la auditoria mediante la carta en el formato correspondiente la cual será dirigida al líder del proceso bajo el conocimiento del Director Nacional de auditoría interna, donde se indicará la necesidad de programación de la reunión de apertura y entendimiento requerido para la auditoria, se contará con 3 días hábiles para recibir respuesta con la programación definida.

12.2.1.2 Análisis e identificación de Riesgos y Controles

Esta actividad corresponde al análisis de los riesgos y controles asociados al proceso, proyecto o actividad que se evaluará, producto de la actividad de Entendimiento y Análisis. El análisis de riesgos y controles permitirá precisar las pruebas de auditoría a realizar, haciendo énfasis en los riesgos claves y en aquellos riesgos que tengan mayor magnitud.

12.2.1.3 Programa de Auditoría Interna

De acuerdo con el análisis de riesgos y controles efectuado, se identificarán los controles claves que serán objeto de prueba y se elaborará el Programa de Auditoría Interna. En dicho programa se incluirá el objetivo de la evaluación, el alcance, los recursos asignados, el cronograma, el objetivo del proceso, proyecto o actividad que se evaluará, y las pruebas que se ejecutaran. Igualmente, el programa de trabajo incluirá las metodologías a utilizar, tales como auditoría basada en tecnología y técnicas de muestreo.

El Programa de Auditoría será elaborado por el Auditor de proceso y el Auditor de TI y deberá estar aprobado por el Gerente de Auditoría Interna, con el fin de proporcionar una seguridad razonable de que se alcancen los objetivos del trabajo y se mantengan la objetividad del auditor interno

Se deberá tener en cuenta los siguientes aspectos cuando se vaya a elaborar el Programa de Auditoría:

Pruebas bien diseñadas
¿Cuál es el objetivo de la prueba?
¿Qué control se va a comprobar en la prueba?
¿La prueba debe enfocarse solo al monitoreo del cumplimiento del control o se debe profundizar en la parte sustantiva de la prueba?
¿La prueba logra el objetivo?
¿Existe alguna situación de riesgo identificada en el entendimiento del proceso que no tiene implementado un control que amerite realizar una prueba sustantiva para asegurar que no se haya materializado el riesgo asociado?
¿Existe una prueba más rápida que ofrezca la misma fiabilidad?
¿Hay alguna prueba en la que se pueda comprobar más de un control?
¿Son los datos sobre los que está haciendo las pruebas fiables? ¿Cómo puede comprobarlo?
¿Cuál es su justificación para el tamaño de su muestra y el método de selección?
¿De qué población está seleccionada su muestra? ¿Es completa?
¿Su muestra abarca un periodo de tiempo adecuado? ¿La definición de la prueba es clara, precisa, completa y facilita su documentación (evidencia) con relación al objetivo de la misma prueba?

12.2.1.4 Ejecución del Programa

La Ejecución del Programa consistirá en realizar las pruebas de diseño y eficacia a los controles que se seleccionaron para probar, así como las pruebas sustantivas determinadas en el programa. Los procedimientos de ejecución deben ser estructurados de tal forma que proporcionen evidencia que permita satisfacer los objetivos de la evaluación.

A partir de este análisis se determinará la necesidad de solicitud de información o soportes requeridos para la ejecución de las pruebas definidas, por lo que se realizará solicitud de información al líder del proceso mediante correo electrónico donde se dará como tiempo establecido 3 días hábiles para su entrega.

Las pruebas realizadas se deben documentar detalladamente y de manera clara, de tal manera que una persona que no ejecutó el trabajo, al inspeccionarlo entienda el trabajo que se llevó a cabo, qué se observó y a qué conclusiones se llegó a partir de las observaciones hechas.

Las conclusiones y valoraciones del equipo de auditoría deberán estar debidamente respaldadas por la ejecución completa y correcta del trabajo de campo y la documentación de los resultados. Para tal fin, es necesario que se conserven todos los papeles de trabajo. Entre otros, a continuación, se describen algunos papeles de trabajo que se deben conservar:

Contenido y conservación de Papeles de Trabajo
Presentación de Reunión de Inicio de la Auditoría
Comunicación de Inicio de la Auditoría
Análisis y entendimiento de los procesos a evaluar
Programa de auditoría
Desarrollo de pruebas
Resumen de hallazgos
Comunicación de los dueños de proceso de los planes de acción incluidos en el informe final
Borradores de informes
Informe final

12.2.1.5 Recolección de Evidencia

Esta actividad consiste en la recolección de la documentación con la información que soporte los hallazgos y dejar evidencia valida, suficiente y confiable de los mismos, con el fin de que cada hallazgo esté debidamente soportado. El propósito de la actividad de Recolección de Evidencia es aportar soporte y respaldo a cada una de las observaciones, conclusiones y recomendaciones del equipo de Auditoría Interna.

El propósito de la documentación de los papeles de trabajo consiste en:

Propósito de los Papeles de trabajo
Ayudar en la planificación, ejecución y revisión de los trabajos

Propósito de los Papeles de trabajo
Proporcionar el soporte principal a los resultados del trabajo
Documentar si los objetivos del trabajo se han alcanzado
Soportar la precisión e integridad del trabajo realizado
Suministrar una base para el programa de aseguramiento y mejora de calidad de la actividad de auditoría interna
Facilitar las revisiones de terceras partes

Los principales aspectos que se deberán considerar en el desempeño del trabajo y que permitirán recolectar información relevante son:

Aspectos sobre la información a recolectar
Se debe dar prevalencia a la información objetiva sobre la subjetiva.
Los documentos proporcionan evidencia fuerte, entre tanto las opiniones soportan evidencia débil.
Las opiniones expertas o informadas prevalecen sobre las opiniones con información sin sustento.
La evidencia directa es aquella que utiliza fenómenos medibles, o información científica, para sustentar una hipótesis.
La información obtenida de sistemas de control interno fuertes prevalece sobre la información proveniente de sistemas de control interno débiles.
La información de partes externas o que proviene de forma independiente de los procesos evaluados prevalece sobre la información interna del proceso.
La información obtenida de muestras estadísticas técnicamente proporciona evidencia fuerte, mientras que la información obtenida de muestras no estadísticas proporciona evidencia débil.
La información corroborada prevalece sobre la información no corroborada
La información preparada oportunamente prevalece sobre la información preparada después del tiempo requerido

Deberá existir formatos En los formatos en los que se pueda documentar las pruebas y evidencias que soportan los hallazgos identificados.

12.2.1.6 Plan de Mejoramiento y Compromisos

Como resultado del trabajo de auditoría se identificarán hallazgos u oportunidades de mejora, para lo cual el equipo de auditoría deberá formular recomendaciones. Corresponderá a los dueños del proceso, proyecto o actividad que se evalúe, dar respuesta y comentarios a cada uno de éstas, y establecer compromisos y medidas pertinentes, con las fechas de realización y el responsable, con el fin de subsanar la debilidad observada.

La Dirección de Auditoría Interna realizará seguimiento a los planes de acción, con el fin de asegurar su implementación efectiva y oportuna.

Los hallazgos deberán ser presentados de la siguiente manera:

- **Criterio**: Norma, ley, política o procedimiento relacionado con el proceso evaluado.
- **Condición**: Situación actual presentada en el proceso evaluado (observación)
- **Causa**: Situación que origina la condición presentada
- **Riesgo:** Posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos.
- **Efecto**: Situación que se origina por la condición presentada.
- **Recomendación**: Acciones claras encaminadas a mejorar los procesos y a disminuir las causas.
- **Acción de Mejoramiento:** Son las acciones establecidas por la Alta Gerencia para superar la situación, indicando al responsable y fecha de su implementación.

12.2.1.7 Supervisión del Trabajo de Auditoría Interna

Todos los trabajos de Auditoría Interna serán supervisados por el Gerente de Auditoría Interna y el Auditor Senior, con el fin de asegurar que se alcancen los objetivos, la calidad del trabajo y el desarrollo personal. La supervisión de cada trabajo es un proceso permanente que abarca desde la planeación hasta la emisión del informe final, de igual manera se realiza sobre el seguimiento de acciones de mejoramiento definidas por la Administración.

La supervisión del trabajo de auditoría debe realizarse:

- Durante la planeación de cada proyecto de auditoría para garantizar que el programa de auditoría satisfaga el alcance de la misma.
- Al finalizar cada prueba contemplada en el programa de auditoría.
- Durante la elaboración del borrador del informe.
- Los seguimientos de las acciones de mejoramiento que debe implementar la Administración sobre los hallazgos de auditoría informados.

Objetivos de la supervisión del trabajo de Auditoría Interna
Asegurar que los auditores designados posean en conjunto los conocimientos, técnicas y otras competencias requeridas para desempeñar el trabajo.
Proporcionar instrucciones adecuadas durante la planificación y aprobar el programa de trabajo.
Asegurar que se complete el programa de trabajo aprobado, a menos que se justifiquen y autoricen modificaciones.
Determinar que los papeles de trabajo soporten adecuadamente las observaciones, conclusiones y recomendaciones del trabajo.
Asegurar que las comunicaciones del trabajo sean precisas, objetivas, claras, concisas, constructivas y oportunas.
Asegurar que se cumplan los objetivos del trabajo.

Proporcionar oportunidades para que se desarrollen los conocimientos, técnicas y otras competencias de los auditores internos.

Con el fin de que se logre un desempeño eficaz de la actividad de auditoría interna es importante que se tenga en cuenta algunas prácticas de control interno que sirven de orientación y guía:

- Categorías de Control
- Pruebas de Evaluación de Controles y Deficiencias de Control
- Técnicas de Pruebas de Controles
- Control de Fraude

Se presentará una guía que le permitirá al Equipo de Auditoría Interna a comprender las actividades para tener en cuenta para el aseguramiento de procesos, en especial, aquellas involucradas en la fase de Ejecución.

12.2.1.8 Política de acceso y retención de papeles de trabajo

De acuerdo con la Norma Internacional para el Ejercicio de la Profesional de la Auditoría Interna “2330”, el Gerente de Auditoría es el funcionario encargado de autorizar el acceso a los registros del trabajo, previa aprobación de la alta gerencia o de los asesores legales antes de dar a conocer tales registros a terceros, según corresponda.

Los papeles de trabajo podrán ser examinados por las entidades estatales y por los funcionarios de la Rama Jurisdiccional en los casos previstos en las Leyes. Dichos papeles están sujetos a reserva y deberán conservarse por un tiempo no inferior a cinco (5) años, contados a partir de la fecha de su elaboración, estarán en poder del Outsourcing de auditoría interna, en caso de requerirlos se deberá realizar el flujo de aprobaciones definidos por el Outsourcing.

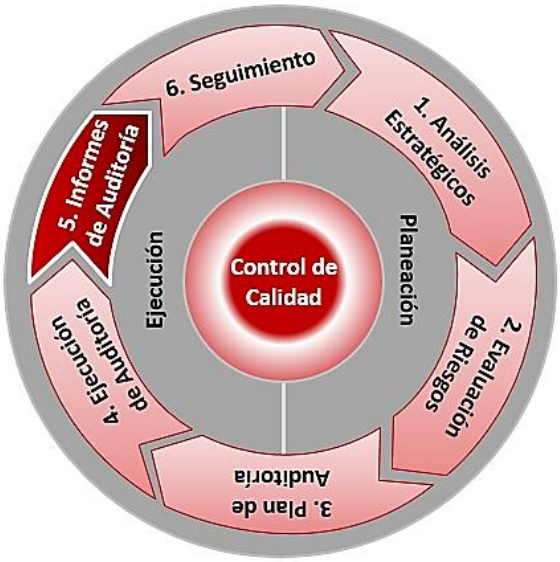
12.2.1.9 Informes

Objetivos

Los informes de Auditoría Interna generan valor a Coosalud E.P.S. S.A. de manera oportuna, clara, constructiva, concisa, bien recibida y aceptada.

El objetivo principal de la presentación de informes es comunicar los resultados de la labor de Auditoría Interna, ayudando así a los cambios que contribuyan al logro de objetivos.

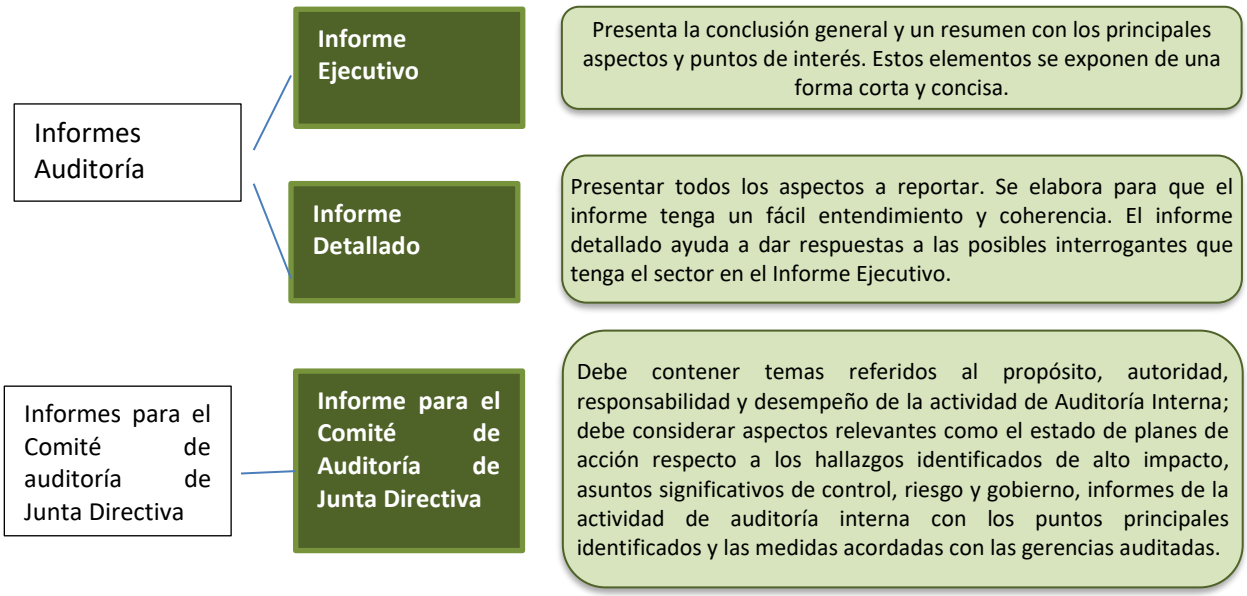
Los informes deben presentarse formalmente en reuniones con el Comité de Auditoría, Altos Directivos, los dueños de procesos, y otras partes interesadas del proceso de Auditoría.



12.2.1.10 Informe de Auditoría Interna

El informe de Auditoría Interna es el medio que tiene la Administración y las partes interesadas, para evaluar la calidad del trabajo de la Gerencia de Auditoría Interna, por lo tanto, es necesario tomar un tiempo adecuado para preparar y redactar los informes.

La presentación de los informes se realiza a través de documentación formal y reuniones con la Administración, los responsables de procesos y otras partes interesadas en los trabajos de Auditoría Interna, con el fin de asegurar la calidad de las conclusiones y recomendaciones. Se presentarán los siguientes informes:



Las siguientes son algunas pautas que deberán tener en cuenta los Auditores Internos al redactar los informes de auditoría:

Pautas para tener en cuenta al redactar informes de auditoría
¿Quiénes son los destinatarios?
¿Quiénes van a leer el informe y qué desean saber?
¿Es fácil de leer?, es decir: ¿Es correcta la gramática?, ¿Se han utilizado frases cortas e indicadores (uso de títulos y subtítulos)?
¿Los mensajes que se comunican son claros?, es decir: ¿Son claras las conclusiones y las medidas a tomar?
¿El contenido expone claramente el impacto y las consecuencias de los problemas o las conclusiones? ¿Hay una conclusión principal sobre el proceso evaluado?
¿Contiene de manera concreta el alcance, las observaciones y las medidas que se hayan acordado con los responsables de los procesos o la Administración?
¿Se incluye un plan de acción claro que se haya acordado con la Administración, donde se definan los responsables y los plazos de ejecución (facilitando así su seguimiento)?

Debe existir un formato que tendrá que ser observado por el equipo de Auditoría Interna para presentar los resultados de sus evaluaciones, y se deberá indicar la calificación del informe de acuerdo con la siguiente escala:

Puntaje	Madurez de los procesos de la sucursal	Solidez Controles	Número de hallazgos encontrados en la sucursal
	Promedio Probabilidad por Impacto	Promedo Solidez	No. Hallazgos en rojo
1	° = 25 ; > 20	0 a 0,9	más de 5
2	° > 15 ; < 19	1 a 1,9	más de 4
3	° > 10 ; < 14	2 a 2,9	más de 3
4	° > 9 ; < 5	3 a 3,9	más de 2
5	° > 4 ; = 0	4 a 5	más de 1
Peso porcentual	**25%**	**25%**	**50%**

Evaluación General del Control Interno		
Semaforización	Ponderación	Resultado
	1 al 3	**Insatisfactorio** Alto riesgo, alto impacto, requiere atención urgente
	4 al 7	**Requiere Mejora** Riesgo moderado, impacto moderado, requiere atención, debe resolverse a corto plazo
	8 a 10	**Satisfactorio** Bajo riesgo, baja prioridad

12.2.1.11 Informe de gestión y resultado de la evaluación sobre la eficacia del SCI

Al cierre de cada ejercicio, la Gerencia de Auditoría Interna debe presentar un informe de su gestión y su evaluación sobre la eficacia del sistema de control interno, incluyendo todos sus elementos. El informe incluirá por lo menos lo siguiente:

Contenido Informe de gestión y evaluación del SCI
Título
Identificación de los temas, procesos, áreas o materias objeto del examen, el periodo y criterios de evaluación, y la responsabilidad sobre la información utilizada, precisando que la responsabilidad del auditor interno es señalar los hallazgos y recomendaciones sobre los sistemas de control interno y de administración de riesgos.
Especificación respecto a que las siguientes evaluaciones se realizaron de acuerdo con la regulación, las políticas definidas por la junta directiva u órgano equivalente y mejores prácticas de auditoría sobre el particular:
▪ Evaluación de la confiabilidad de los sistemas de información contable, financiera y administrativa.
▪ Evaluación sobre el funcionamiento y confiabilidad del sistema de control interno.
Mencionar las limitaciones que encontraron para realizar sus evaluaciones, tener acceso a información u otros eventos que puedan afectar el resultado de las pruebas realizadas y las conclusiones.
Relación de las recomendaciones formuladas sobre deficiencias materiales detectadas, mencionando los criterios generales que se tuvieron en cuenta para determinar la importancia de las mismas.
Resultados del seguimiento a la implementación de las recomendaciones formuladas en informes anteriores.
Identificación, nombre y firma, ciudad y fecha de elaboración.

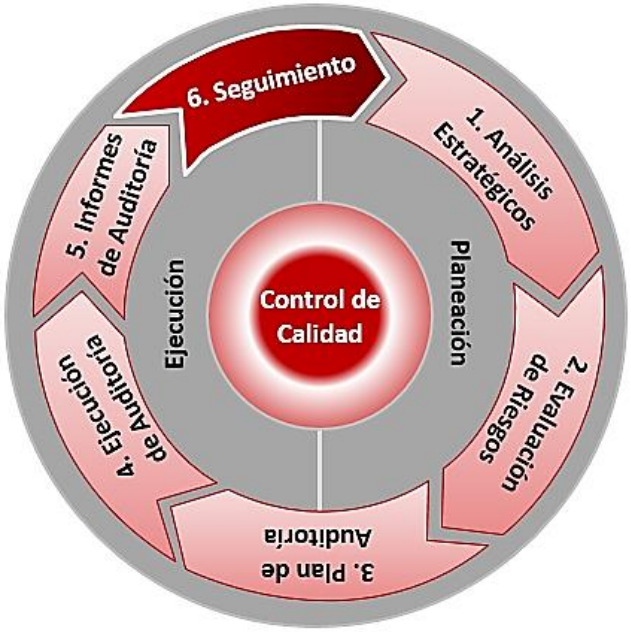
La calificación al cierre del ejercicio de la evaluación del SCI será dada de acuerdo con la siguiente escala:

Valor	Categoría	Descripción
5	**Sistema de control interno efectivo y en constante actualización**	Los procesos se han refinado hasta un nivel de mejor práctica; se basan en los resultados de mejoras continuas.
4	**Sistema de control interno efectivo**	Los procedimientos se han estandarizado, documentado y difundido a través del entrenamiento. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo mejora constante y proporcionan buenas prácticas
3	**Sistema de control interno por mejorar**	Se han desarrollado los procesos hasta el punto que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar
2	**Sistema de control interno débil**	Existe evidencia de que la EPS ha reconocido que los problemas existen y requieren ser resueltos.
1	**Sistema de control interno insuficiente**	Carencia completa de cualquier proceso reconocible.

12.2.1.12 Seguimiento

Objetivos

El asegurar que el trabajo de la AI produce los resultados adecuados para Coosalud E.P.S. S.A. es el objetivo primordial de la fase de seguimiento, es decir, verificar que se ponen en práctica las medidas acordadas con la Gerencia sobre los hallazgos y observaciones informadas por la AI.



Esta fase se realizará con base en la siguiente información:

- Observaciones y hallazgos de la AI, planes de acción de la gerencia, tiempos límites de implementación de las recomendaciones, y personas responsables
- Respuesta de la Gerencia sobre el estatus de los planes de acción y fechas de implementación actualizadas, si aplica.
- El seguimiento permite vigilar la disposición de los resultados comunicados a la AI, asegura que las acciones de la Gerencia hayan sido implantadas eficazmente o que la Alta Gerencia haya aceptado el riesgo de no tomar medidas.

  La periodicidad para realizar el seguimiento depende de la evaluación final del proceso, proyecto o actividad la cual está ligada al resultado de la evaluación de los controles. Es decir, el seguimiento dependerá de los siguientes resultados como evaluación final.

Estado de evaluación del plan de acción	Descripción	Colorimetría
Cumplido	Los soportes aportados evidencian un cierre de la totalidad de las acciones propuestas	**Verde**
No cumplido	Los soportes aportados no evidencian un cierre de la totalidad de las acciones propuestas	**Rojo**
Reprogramado	Las acciones propuestas no han iniciado en la fecha señala por falta de autorización, aprobación o recursos para su implementación	**Gris**
Cancelado	Las acciones propuestas no son aplicables o ejecutables al interior de la organización por falta de autorización, aprobación o recursos para su implementación	**Amarillo**

Esta fase se realizará con base en la siguiente información:

- Observaciones y hallazgos del equipo de AI, planes de acción de la gerencia, tiempos límites de implementación de las recomendaciones y responsables.
- Respuesta de la gerencia sobre el estatus de los planes de acción y fechas de implementación actualizadas.
- Observaciones y hallazgos de la AI.

Adicionalmente en esta sección se presentan los siguientes aspectos:

- **Planes de mejora:** Son las acciones para realizar en acuerdo con la Alta Gerencia y las personas responsables de los procesos. Esto para resolver las situaciones reportadas en los informes, con el fin de mitigar los riesgos identificados
- El equipo de Auditoría Interna debe evaluar las actividades desarrolladas para la resolución de los problemas comparándolas con el plan de acción, así:

  1) Determinar los hallazgos que deben ser monitoreados.

  2) Evaluar la razonabilidad de las acciones desarrolladas por la Gerencia.

  3) Evaluar si las acciones implementadas van dirigidas hacia solucionar y mejorar los hallazgos originales, es decir erradicar las causas que lo originan.

  4) Confrontar las respuestas y actualizar el estatus del plan de acción

- **Gestión frente a los planes de mejora:** Para verificar y realizar un mayor seguimiento a los planes de mejora se deben implementar los siguientes indicadores para medir el grado de implementación y el nivel de respuesta de los dueños de proceso.

  5) Acciones Implementadas/ Compromisos Adquiridos: mide la gestión de la administración frente a los hallazgos presentados

  6) Fecha de implantación / Fecha Compromiso: mide el nivel de respuesta a las fechas de compromiso

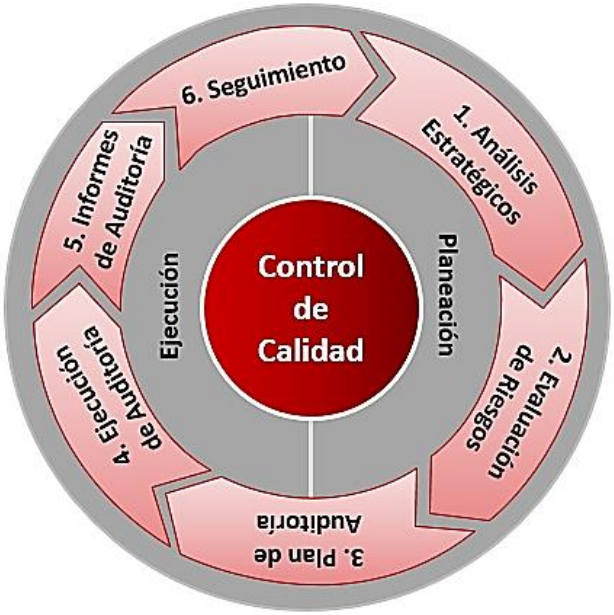
  7) Acciones canceladas / Compromisos adquiridos: mide el porcentaje de acciones que no fueron implementadas

El ***Informe de seguimiento a planes de mejora*** debe ser observado por el equipo de Auditoría Interna para presentar los resultados obtenidos en el seguimiento a la gestión de los dueños de proceso en la implementación de los planes de mejora.

12.2.2 Control de Calidad

Objetivos

La AI debe desarrollar y mantener un proceso de control de calidad y mejora que cubra todos los aspectos de la actividad de AI, evaluando su eficiencia y eficacia e identificando oportunidades de mejora.



El propósito del programa de calidad y mejora es ayudar a la actividad de AI a agregar valor y mejorar las operaciones de la organización y a proporcionar aseguramiento de que la actividad de control cumple con su misión y ayuda a la Función de AI:

- Supervisar el desarrollo e implementación de los procedimientos de control interno, administrar y mantener la guía metodológica de AI.
- Ayudar en el proceso general de programación de trabajos de aseguramiento y el control de tiempos correspondiente.
- Supervisar la capacitación y desarrollo del equipo de AI.
- Supervisar los sistemas de estadísticas y mediciones de control posevaluación y otras encuestas.
- Supervisar y administrar la obtención de información y la preparación de los informes periódicos resumidos por parte de la actividad de auditoría para la Administración.
- Administrar y mantener la base de datos integral de seguimiento de las recomendaciones y planes de acción resultantes de los trabajos de aseguramiento.

El programa de calidad y mejora incluye los siguientes aspectos:

12.2.2.1 Encuesta de satisfacción

Este documento debe ser enviado y diligenciado por las Gerencias y Direcciones evaluadas, una vez el equipo de AI termine su trabajo de aseguramiento. El propósito de la encuesta es obtener retroalimentación que permita mejorar la actividad de auditoría en los siguientes aspectos:

- Desempeño técnico y profesional del equipo de AI.
- Calidad y satisfacción del servicio.
- Relaciones con los dueños del proceso evaluado.

12.2.2.2 Indicadores de Gestión de la Función de Auditoría Interna

El propósito de los indicadores es medir la gestión realizada por la Función de AI y proveer información sobre cómo la actividad genera a Coosalud E.P.S. S.A. un entorno de mejora continua.

Las principales mediciones en las que la Dirección de AI puede focalizarse son:

- El costo total de la Función de AI y su relación con:

  - Los costos, activos y ventas de Coosalud E.P.S. S.A.
  - La cantidad de informes emitidos

- La satisfacción de las Gerencias evaluadas con el trabajo realizado:

  - Reunión de inicio
  - Relación del equipo de AI con la Gerencia y Direcciones y personal responsable del proceso evaluado.
  - Cumplimiento del alcance establecido
  - Utilidad de las recomendaciones

- Aportes al Gobierno Corporativo

  - Cantidad de reuniones al año y presentaciones de resultados a la Alta Gerencia

- Logro de metas:

  - Porcentaje de cumplimiento del Plan Anual de Auditoría Interna
  - Porcentaje implementado de recomendaciones

- Calidad del personal de AI:

- Cantidad de Personas con experiencia específica en la industria
- Porcentaje de personas con certificaciones relacionados con control interno

➢ Mejora de los procesos de AI:

- Implementación de la guía metodológica
- Uso de herramientas tecnológicas
- Estado actual de la Función de Auditoría Interna respecto a las perspectivas de posicionamiento, proceso y gente.

Los indicadores deben ser diligenciados por la Dirección de AI.

12.2.2.3 Evaluaciones del programa de Calidad y Mejora

La actividad de AI debe adoptar un proceso para supervisar y evaluar la eficacia general del programa de calidad. Este proceso debe incluir tanto evaluaciones internas como externas.

✓ Evaluaciones Internas:

Las evaluaciones internas, también conocidas como revisión interna o autoevaluación deben ser parte integrante de la supervisión del día a día, revisión y medición de la actividad de AI. Las evaluaciones internas deben incluir:

- Revisiones continúas del desempeño de la actividad de AI.
- Revisiones periódicas mediante autoevaluación o a través de integrantes de los procesos de la organización.

Estas evaluaciones están usualmente incorporadas a las políticas y procedimientos rutinarios utilizados para gestionar la actividad y deben ser realizados por medio de procesos y herramientas tales como:

- La supervisión del trabajo
- Listas de verificación (*checklists*) y otros medios para proporcionar aseguramiento de que se están cumpliendo los procedimientos adoptados por la actividad de AI.
- Retroalimentación de los clientes de AI y otras partes interesadas.
- Presupuestos de proyectos y sistemas de control de tiempos

✓ Evaluaciones Externas

Las evaluaciones externas de aseguramiento de calidad deben realizarse, al menos, una vez cada cinco años por un revisor o equipo de revisión competente e independiente, externo a Coosalud E.P.S. S.A.

Estas evaluaciones deben cubrir las actividades de consultoría y aseguramiento desempeñadas por el equipo de AI. Dentro de las evaluaciones externas se destaca:

- Que se evalúe e indique la calidad de la actividad de AI y aportar recomendaciones para las mejoras apropiadas.
- Que todos los esfuerzos de evaluación y mejora de calidad incluyan la modificación de recursos, tecnología, procesos y procedimientos en forma apropiada y oportuna, según lo indicado por las actividades de vigilancia y evaluación
- Que, a fin de proporcionar responsabilidad y transparencia, la Gerencia de AI comparta los resultados de las evaluaciones externas y si corresponde, de las evaluaciones internas de programas de calidad con las diversas partes interesadas en la actividad, como por ejemplo la Alta Gerencia.

12.2.2.4 Reporte sobre el Programa de Calidad

La Dirección de AI debe comunicar los resultados de las evaluaciones externas a la Presidencia

Algunos de las formas como se deben comunicar los resultados por la Dirección de Auditoría Interna a la Presidencia, son los siguientes:

- ✓ Al finalizar una evaluación externa, el equipo de revisión debe emitir un informe formal que contenga una conclusión sobre la evaluación de calidad y mejora de la actividad de AI.
- ✓ El informe también debe considerar el cumplimiento de las políticas y normas aplicables e incluir las recomendaciones de mejora apropiadas
- ✓ El informe debe ser remitido a la persona u organización que solicitó la evaluación.

La Dirección de Auditoría Interna debe preparar un plan de acción por escrito en respuesta a los comentarios y recomendaciones significativos contenidos en el informe de la evaluación externa, y es responsable de realizar un seguimiento adecuado del mismo.

12.2.2.5 Auditorias especiales

La Dirección de Auditoría Interna, por solicitud expresa del Comité de Auditoría y/o la Administración, podrá realizar trabajos especiales, incluso contratar a un auditor externo para realizarla, siguiendo los lineamientos definidos por esta Gerencia.

12.2.2.6 Documentación

Toda la información de la auditoría deberá ser soportada, sea en medio físico o en medio magnético y estas deberán reposar en los archivos de la oficina de control interno a nivel nacional.
Los documentos correspondientes a informes, matrices de riesgo, anexos de evidencias o soportes relacionados a los resultados de la auditoria se dispondrán en un share point o drive de Coosalud para su debida consulta.

12.2.2.7 Acuerdos de niveles de servicio y plan de comunicaciones

Se definen tiempos para las actividades relacionadas con la ejecución de la auditoría interna

1. Tiempo de apertura de las auditorias por parte del Outsourcing será máximo un día hábil posterior al tiempo definido en el Plan de Auditoria
2. Una vez enviada la carta de inicio se contará con 1 día hábil para definir la fecha de la reunión de inicio, en esta reunión se definirá la fecha de reunión de entendimiento
3. Solicitud de información o soportes por el Outsourcing se contará con 2 días hábiles posterior a la reunión de entendimiento, se precisa que si es requerida segundas solicitudes se realizarán durante la ejecución de la auditoria.
4. La entrega de información o soportes por el líder del proceso tendrá como máximo 3 días hábiles a partir del correo de solicitud
5. Se realizará la notificación de hallazgos al área auditada la cual contará con 2 días hábiles para emitir observaciones pertinentes.
6. Una vez el Outsourcing presenta el informe preliminar al área auditada, contarán con 3 días hábiles para enviar soportes o evidencias y observaciones.
7. La formulación de los planes de mejora deberá ser emitidos por el área máximo 3 días hábiles de haber sido solicitado por el Outsourcing de auditoría.
8. Las observaciones realizadas por el Outsourcing a los planes de mejora deberán ser corregidas en un tiempo de 2 días hábiles.
9. La entrega informe final se realizará a los 2 días hábiles de haber recibido los planes de acción corregidos.

Plan de comunicación:

Comunicación	Responsable	Propósito / Lugar	Método de entrega/ Frecuencia	Lista de Distribución
Inicio del proyecto	Interventora del contrato	Informar a todos los interesados el inicio del proyecto.	Vía correo electrónico	Cargos directivos y dueños de proceso
Solicitud de información	Por parte del Outsourcing, la solicitará siempre el Gerente o Supervisor de proceso.	Corresponde a información del cliente adicional a la pactada inicialmente.	Se hará vía e-mail desde el correo del Outsourcing del Coordinador del proyecto	Se enviará a Directivos y dueños de proceso
Citación a Reunión	Por parte del Outsourcing, la solicitarán el Senior del proyecto.	Corresponde a la información soporte de la AI	Vía correo electrónico	Sponsor Coosalud EPS
Informes y reuniones para validación	Por Outsourcing, el Supervisor o Senior del proyecto y por Coosalud, los dueños de proceso.	Validar los informes de cada capítulo evaluado.	Previa coordinación entre equipo KPMG y dueños de proceso, y mediante envío por correo electrónico.	Envío inicial a los directivos y posteriormente a los dueños de procesos
Envío de entregables	Por Outsourcing, los enviará el Coordinador del Proyecto.	Reportar los resultados finales de la AI.	Medio impreso y carta remisoria, una vez se haya realizado la revisión del Gerente, Supervisor y Socio del proyecto.	Sponsor Coosalud EPS

12.2.2.8 Entrega de producto conforme

Se cuenta con una fase de pre-validación del informe detallado y hallazgos, durante esta fase, se podrán hacer aclaraciones y subsanaciones debidamente soportadas por evidencias, las cuales se podrán allegar por este medio, así como también enviar las dudas y/o observaciones que tenga al respecto. Si llegase a existir alguna controversia que no se pueda solucionar mediante estos acercamientos se podrá incluir una observación en el aparte de "comentarios de la administración" sobre los diferentes puntos de vista si así se requiere.

Para esta fase se dispondrá de un plazo de 3 días hábiles, según nuestros acuerdos de servicio, de no recibir respuesta antes de esta fecha se darán por avalado los hallazgos, se procederá a emitir el informe y a solicitar los planes de mejora correspondientes para finalmente hacer entrega del informe final.

Una vez culminada las fases de entendimiento, evaluación, validación y establecimiento de planes de mejora correspondientes al proceso auditado, por medio del presente comunicado, se comparte la versión final del informe de la auditoría realizada, así como también, el flujograma elaborado por el proceso con los riesgos y controles identificados por la auditoría.
Si no se reciben comentarios u observaciones con respecto a la información enviada se dará por aceptados los informes.