

Sistema Integrado de Gestión de Riesgos - Definición	Ciclo de gestión de riesgos	Riesgos empresariales y emergentes	Revisión de riesgos	Revisión del riesgo exposición regular	Cultura de riesgo	Auditoría de Riesgos
--	-----------------------------	------------------------------------	---------------------	--	-------------------	----------------------



Sistema de Gestión de Riesgos de Ecopetrol 2022





Sistema Integrado de Gestión de Riesgos - Definición	Ciclo de gestión de riesgos	Riesgos empresariales y emergentes	Revisión de Riesgos	Revisión del riesgo exposición regular	Cultura de riesgo	Auditoría de Riesgos
--	-----------------------------	------------------------------------	---------------------	--	-------------------	----------------------

Todos los empleados de Ecopetrol son responsables de comprender e identificar los riesgos a los que están expuestos en el desempeño de sus funciones y en los procesos en los que participan, y de abordar adecuadamente los riesgos manejables en el desempeño de sus funciones. La gestión de riesgos se realiza de acuerdo con los principios de la empresa, como la integridad y la responsabilidad, y con nuestra declaración cultural.

SISTEMA INTEGRADO DE GESTIÓN DE RIESGOS - SRI

El Sistema Integrado de Gestión de Riesgos de Ecopetrol se define como un conjunto de principios, marco de referencia y proceso que permiten a la organización gestionar los efectos de la incertidumbre en el cumplimiento de los objetivos, maximizar las oportunidades y ayudar a establecer estrategias y tomar decisiones informadas.

La gestión integrada de riesgos en Ecopetrol se adhiere a las normas ISO 31000, COSO 2013 y COSO ERM 2017

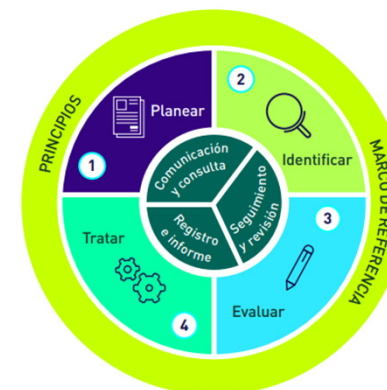
El Sistema Integrado de Gestión de Riesgos (ISR) actúa como la directriz regulatoria general para todos los riesgos gestionados en Ecopetrol y su Grupo, que se encuentran a nivel estratégico, táctico y operativo.



Cada uno de estos niveles tiene diferentes tipologías de riesgo, de acuerdo con las diversas regulaciones y estándares relacionados. Esto significa que los responsables de la gestión de riesgos en la organización deben aplicar métodos particulares de gestión de riesgos en el nivel apropiado de responsabilidad, manteniéndolos dentro de los principios, marcos y procedimientos de gestión de riesgos establecidos en el Sistema Integrado de Gestión de Riesgos.

CICLO DE GESTIÓN DE RIESGOS

El ciclo/proceso de gestión de riesgos se aplica sistemáticamente a todo tipo de riesgos en la organización a nivel estratégico, táctico y operativo, a través de la ejecución de los siguientes pasos:



Ciclo del sistema de gestión de riesgos

- **Plan:** Definición del alcance de las actividades y análisis del contexto interno y externo.
- **Identificar:** Identificación de riesgos basada en los puntos de vista de las personas involucradas y en el análisis de la información.
- **Evaluar:** Análisis de causas y consecuencias. Evaluación según probabilidad e impacto.
- **Tratar:** Selección e implementación de opciones para abordar el riesgo.
- **Comunicación e investigación, Registro e informe, Monitoreo y revisión:** Intercambio de información, retroalimentación, seguimiento continuo y revisión periódica de la exposición al riesgo, documentación y presentación de informes de los resultados de cada etapa del ciclo, Ejemplo: riesgos nuevos o modificados, materialización de riesgos, riesgos potenciales, cambios en las evaluaciones de riesgos, alertas de riesgos y cambios en la exposición al riesgo.

Cualquier cambio en los objetivos de la organización y su entorno interno y externo podría resultar en cambios de riesgo, por lo que el proceso de gestión de riesgos en Ecopetrol refleja la dinámica de la organización.

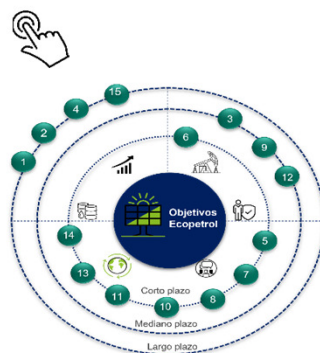


RIESGOS EMPRESARIALES

Relacionado con el riesgo directamente asociado con la estrategia, los objetivos estratégicos y/o el panel de gestión equilibrado de la empresa, representados en el mapa de riesgos de negocio.

Mapa de Riesgos Empresariales Ecopetrol

- 1 Protección e incorporación de recursos y reservas no exitosa.
- 2 Competitividad de activos frente a transición energética.
- 3 Afectación a la sostenibilidad financiera y la generación de valor.
- 4 Subordinadas que no cumplen la promesa de valor.
- 5 Incidentes de interrupción operacional por causas de entorno.
- 6 Transición e incorporación no exitosa de ISA al GE.
- 7 Propagación de epidemias que impactan la operación.
- 8 Eventos HSE por causa operacional.
- 9 Proyectos que no cumplen su expectativa de valor.
- 10 Faltas a la ética y cumplimiento.
- 11 Ciberataques, fuga o pérdida de información.
- 12 Cultura organizacional que no apalanque la estrategia.
- 13 Incumplimiento de compromisos por parte de terceros.
- 14 Afectación a la operación o al gobierno corporativo por cambios geopolíticos, regulatorios o disposiciones de entes de control y del estado.
- 15 Inadecuada gestión frente al cambio climático y agua.



La construcción y actualización del mapa de riesgos del negocio se realiza de manera colectiva, con base en análisis de entorno interno y externo, considerando las tendencias del mercado, los riesgos específicos para las empresas del Grupo Ecopetrol, así como las normas de gestión, puntos de referencia y riesgos de la industria, que normalmente están sujetos a análisis y revisión por índices y radares de sostenibilidad.

La evaluación de estos riesgos se realiza utilizando la Matriz de Evaluación de Riesgos, que contiene los umbrales de aceptación y tolerancia de riesgos, aprobados por el Consejo de Administración.

En 2022 se definieron 61 KRLs y 85 acciones de tratamiento para gestionar las causas o reducir las consecuencias de los riesgos empresariales, asegurando que sean medibles en el tiempo, cuantificables y verificables, lo que asegura su efectividad.

Adicionalmente, cuando tenemos una materialización de riesgos, se definen y ejecutan planes de acción con la participación de los negocios impactados, manteniendo los riesgos dentro de los niveles de tolerancia y aceptación definidos en Ecopetrol..

RIESGOS EMERGENTES

Ecopetrol define los riesgos emergentes como aquellos que se espera que tengan un impacto futuro a largo plazo en la compañía (3-5 años y más) o, en algunos casos, ya han comenzado a impactar a la compañía.

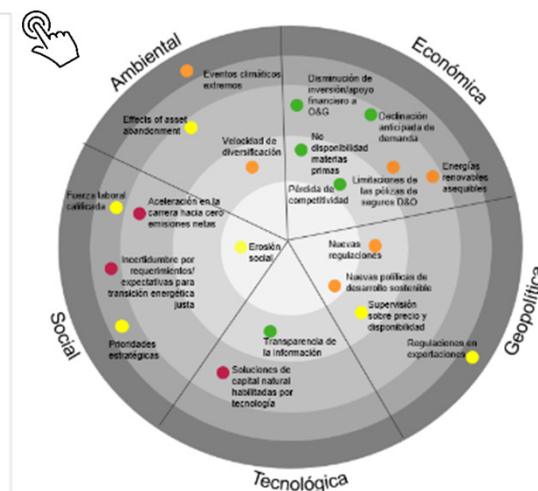
De acuerdo con nuestras definiciones y metodologías, se consideran riesgos emergentes aquellos que cumplen con algunas de las siguientes características: i) El riesgo es nuevo, en desarrollo o aumenta significativamente en importancia. ii) Un riesgo familiar en un contexto nuevo o desconocido o en condiciones de contexto nuevo (reemergente). iii) El posible impacto material, financiero o reputacional del riesgo es a largo plazo y significativo. iv) Es un riesgo externo que surge de eventos externos a la empresa que están fuera de su influencia o control. v) El riesgo y su impacto en la empresa son específicos, y vi) Tiene un alto impacto potencial para Ecopetrol y puede requerir que Ecopetrol adapte su estrategia y/o modelo de negocio.

Impacto potencial:

- Muy Alto
- Alto
- Moderado
- Bajo
- Muy bajo

Horizonte de tiempo:

- Actual – en el contexto de Ecopetrol
- Futuro cercano (1-3 años)
- Futuro previsible (3-5 años)
- Futuro distante (5-10 años)
- Futuro desconocido (10+ años)



Ecopetrol evalúa cada riesgo potencial y define el plan de tratamiento para cada riesgo emergente, que incluye lo siguiente: i) Nuevo riesgo de negocio; ii) Incorporación al riesgo empresarial existente; iii) Monitoreo continuo de riesgos emergentes; o iv) Abandono del riesgo emergente.





Sistema Integrado de Gestión de Riesgos - Definición	Ciclo de gestión de riesgos	Riesgos empresariales y emergentes	Revisión de riesgos	Revisión del riesgo exposición regular	Cultura de riesgo	Auditoría de Riesgos
--	-----------------------------	------------------------------------	---------------------	--	-------------------	----------------------

APETITO DE RIESGO Y TOLERANCIA AL RIESGO

Nuestra primera expresión de apetito de riesgo está inmersa en la estrategia 2040 del Grupo Ecopetrol y es un elemento que considera conceptos relacionados con reputación, sostenibilidad, medio ambiente, cumplimiento, entre otros.

Para el nivel estratégico tenemos algunos riesgos de tolerancia cero, tales como:

- Tolerancia cero a las muertes en el ejercicio de las actividades de la empresa.
- Tolerancia cero a prácticas contrarias a lo establecido en el Código de Ética y Conducta del Grupo Ecopetrol.
- Tolerancia cero a las prácticas en contra de lo establecido en la normativa relacionada con el medio ambiente, la integridad de las personas, las comunidades y otros grupos de interés, entre otros.

Además, existen algunos parámetros estratégicos, financieros y operativos cuantitativos y cualitativos que complementan el apetito de riesgo de la compañía:

- ✓ Parámetros estratégicos de riesgo: Por ejemplo, nuevos productos que se introducirán, productos que se evitarán y enfoque de inversión para gastos de capital.
- ✓ Parámetros de riesgo financiero: Por ejemplo, el nivel máximo aceptable de pérdida o variación en el rendimiento, incluida la variabilidad de las ganancias por acción, el crecimiento / margen del flujo de efectivo libre, las ganancias antes de intereses e impuestos / margen, el rendimiento de los activos, el porcentaje de retorno del EBITDA.
- ✓ Parámetros de riesgo operacional: Por ejemplo, respuesta de sostenibilidad esperada, requisitos ambientales existentes / proyectados, objetivos de seguridad, objetivos de calidad y criterios y concentraciones del cliente.

La tolerancia al riesgo está vinculada al apetito de riesgo de la empresa y es la variación aceptable en el rendimiento del negocio. Describe el rango de resultados aceptables en relación con el logro de un objetivo comercial dentro del apetito de riesgo y se expresa en unidades medibles.

La capacidad de riesgo indica la cantidad máxima que nuestra empresa podría soportar sin afectar su sostenibilidad.

De acuerdo con esto, las zonas de tolerancia y aceptación están representadas en la Matriz de Evaluación de Riesgos de Ecopetrol.

MATRIZ DE EVALUACIÓN DE RIESGOS DE ECOPETROL

La Matriz de Evaluación de Riesgos (RAM) contiene escalas descriptivas de probabilidad de ocurrencia e impactos en dimensiones como personas, medio ambiente, recursos económicos, reputación y clientes.

Según la combinación de probabilidad e impacto, los niveles de riesgo son Muy Alto, Alto, Medio, Bajo y Muy Bajo.

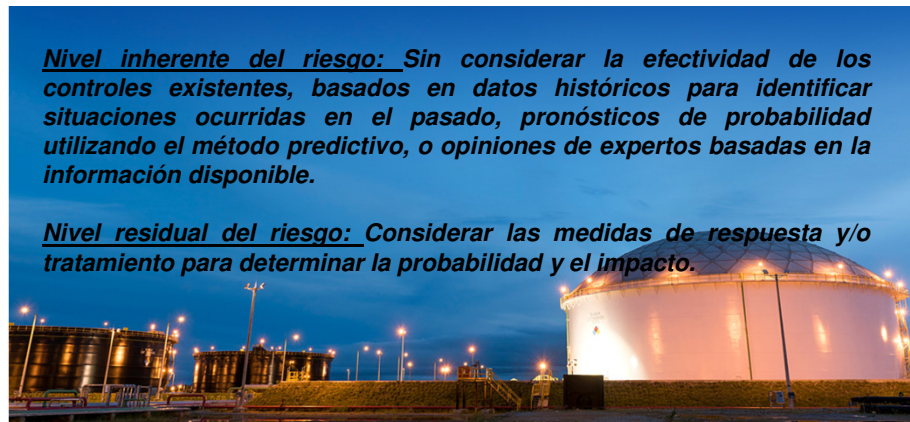
La RAM establece los umbrales indicando las zonas de no tolerancia, tolerancia con controles y aceptación, de la siguiente manera:

- **Zona de no tolerancia** en el que se debe gestionar el riesgo.
- **Zona de tolerancia con controles** en el que el riesgo se gestiona a través de medidas de mitigación.
- **Zona de aceptación** en el que el riesgo es asumido por la empresa.

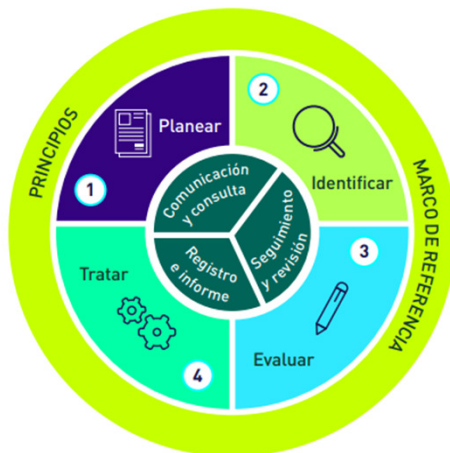
La evaluación de riesgos considera la magnitud de las consecuencias y su probabilidad de ocurrencia, obteniendo información básica para priorizar los riesgos y tomar decisiones con respecto al tratamiento. Esta evaluación del riesgo incluye el cálculo del nivel de riesgo inherente y residual, de acuerdo con las escalas de probabilidad e impactos, y los niveles de tolerancia y aceptación definidos en la Matriz de Evaluación de Riesgos.

Nivel inherente del riesgo: Sin considerar la efectividad de los controles existentes, basados en datos históricos para identificar situaciones ocurridas en el pasado, pronósticos de probabilidad utilizando el método predictivo, o opiniones de expertos basadas en la información disponible.

Nivel residual del riesgo: Considerar las medidas de respuesta y/o tratamiento para determinar la probabilidad y el impacto.



CICLO DE GESTIÓN DE RIESGOS



- **Planear:** definición de alcance de las actividades y análisis de contexto interno y externo.
- **Identificar:** identificación de los riesgos con base en los puntos de vista de las personas involucradas y en el análisis de información.
- **Evaluar:** análisis de causas y consecuencias. Valoración según probabilidad e impacto.
- **Tratar:** selección e implementación de opciones para abordar el riesgo.
- **Comunicación, seguimiento y registro:** intercambio de información, retroalimentación y monitoreo continuo.

El monitoreo de los riesgos de negocio y procesos sirve para identificar alertas, verificar la ejecución de los mitigantes y asegurar acciones frente a las materializaciones reportadas por los responsables, con el fin de mantener los riesgos dentro de los niveles definidos de tolerancia y aceptación. Los resultados relevantes de este seguimiento fueron reportados periódicamente a los Comités Ejecutivo y de Auditoría y Riesgos de acuerdo con la ocurrencia o criticidad de los mismos, mediante informes de gestión en las sesiones mensuales.

El objetivo de revisar el riesgo es verificar permanentemente que los riesgos empresariales identificados, evaluados y tratados están dentro de los niveles tolerables de la empresa de acuerdo con la RAM, con el fin de retroalimentar el ciclo de riesgo del negocio y tomar acciones para asegurar su correcta gestión.

El alcance de esta etapa es el monitoreo y aseguramiento, llevado a cabo permanentemente para identificar alertas de riesgo, verificar la ejecución de factores atenuantes y determinar acciones contra cualquier materialización que surja, con el fin de mantener los riesgos dentro del nivel de tolerancia y aceptación definido. Esto incluye:

- ✓ KRIs y alertas generadas, como métricas utilizadas para proporcionar señales tempranas de aumento de la exposición al riesgo
- ✓ Seguimiento de controles y acciones de tratamiento
- ✓ Análisis de materializaciones de eventos
- ✓ Análisis de posibles cambios en el contexto de riesgo

Este análisis tiene por objeto revisar la exposición al riesgo, en relación con:

- Definir medidas preventivas para evitar la materialización del riesgo y mantener los riesgos dentro de los niveles definidos de tolerancia y aceptación.
- Reevaluar los riesgos en base a la Matriz de Evaluación de Riesgos, de acuerdo con los impactos en el negocio y la probabilidad de ocurrencia.
- Verificar que las medidas de gestión de riesgos se ejecuten correctamente y que se logren los efectos esperados sobre el riesgo.
- Identificar alertas relativas a la posible materialización de riesgos, proponer y ejecutar acciones.
- Analizar los eventos de materialización de riesgos en términos de sus causas, impactos, así como medidas para reducir los impactos y prevenir su recurrencia.



Sistema Integrado de Gestión de Riesgos - Definición	Ciclo de gestión de riesgos	Riesgos empresariales y emergentes	Revisión de riesgos	Revisión del riesgo exposición regular	Cultura de riesgo	Auditoría de Riesgos
--	-----------------------------	------------------------------------	---------------------	--	-------------------	----------------------

FORMACIÓN DE RIESGOS 2022 PARA ADMINISTRADORES NO EJECUTIVOS

Los nueve (9) miembros no ejecutivos del Consejo de Administración reciben capacitación periódica sobre gestión de riesgos. En 2022, los miembros no ejecutivos recibieron educación sobre gestión de riesgos sobre:

i) La junta como actor clave en la supervisión de riesgos; ii) Navegar por las leyes y regulaciones de valores de EE. UU.: Programas de cumplimiento y mitigaciones de riesgos; y iii) Desafíos conscientes para la transformación empresarial hacia un propósito superior (incluye el estudio de diferentes casos con materialización de riesgos); y iv) podcast "Conozca el panorama de riesgos del mundo de O&G", entre otros

Por favor, consulte:

1. Capacitaciones, formaciones y entrenamientos, Informe Integrado de gestión 2022, página 154
<https://files.ecopetrol.com.co/web/esp/cargas/ecopetrol-rigs-2022-esp.pdf>
2. Consejo de Administración en 20F- Informe 2022, páginas 205 - 209
https://www.ecopetrol.com.co/wps/wcm/connect/22a8a7ef-d4ef-46ac-a195-fa7a3acb0e89/22-10205-1_D15.6_Ecopetrol+S.A._20-F.pdf?MOD=AJPERES&attachment=false&id=1650922322313



Nuestra Formación Top en riesgo:

- ¿Qué es la Gestión Integral de riesgos e impactos de HSE?
- Matriz de peligros y riesgos / Barreras y controles para mitigarlos.
- Gestión de riesgos en salud ocupacional.
- Pasos para realizar un análisis de riesgos para la ejecución de un trabajo.
- ¿Qué es un análisis de riesgos para la ejecución de obras?
- Las premisas del análisis de riesgos para la ejecución de obras.
- Roles y responsabilidades en el análisis de riesgos para la ejecución de obras.
- Liderazgo y planificación: Riesgos y controles.
- Métodos para la gestión integral de los riesgos e impactos de HSE.
- Aplicación del método práctico "Y sí" para el análisis de riesgos.

FORMACIÓN DE RIESGOS 2022 PARA ANTIGUOS EMPLEADOS

Ecopetrol ha realizado capacitaciones, relacionadas con el Sistema Integrado de Riesgos, Riesgos de Sostenibilidad y Capacitación especializada en riesgos para empleados en: i) Riesgos emergentes y riesgos Datamart por parte del equipo de GIR (Gestión Corporativa de Gestión Integrada de Riesgos); ii) Conceptos del sistema integrado de gestión de riesgos en las Mesas Redondas de Derechos Humanos; iii) Socialización de la Junta de Riesgos Empresariales del Datamart; iv) Conceptos de gestión de riesgos en términos de amenazas y oportunidades; v) Conceptos de gestión de riesgos en términos de riesgos y oportunidades; entre otros.



34.464 participaciones de trabajadores

Para realizar formaciones en temas de riesgos



65 acciones de formación

En temáticas de riesgos



661 conexiones streaming

En riesgos de sostenibilidad

“En Ecopetrol creemos en la capacitación como un elemento fundamental para fortalecer la cultura del riesgo”





Sistema Integrado de Gestión de Riesgos - Definición

Ciclo de gestión de riesgos

Riesgos empresariales y emergentes

Revisión de riesgos

Revisión del riesgo exposición regular

Cultura de riesgo

Auditoría de Riesgos

AUDITORÍA INTERNA DEL PROCESO DE GESTIÓN DE RIESGOS

PRUEBAS DE GESTIÓN 2022

El Sistema Integrado de Gestión de Riesgos y los Sistemas de Gestión de Control Interno de Ecopetrol cumplen con las normas ISO 31000, COSO (Comité de Organizaciones Patrocinadoras de la Comisión Treadway) y COBIT (Objetivos de Control para la Información y Tecnología Relacionada), así como con las leyes SOX (Sarbanes Oxley Act) y FCPA (Foreign Corrupt and Practices Act) y se rigen por las regulaciones internas aplicables..

ALCANCE DE LA AUDITORÍA

Evaluación del ciclo de gestión de riesgos del proceso mediante la revisión de la adecuación de los riesgos y el diseño y eficacia de los controles que soportan el sistema de control interno sobre la información financiera, tal y como se establece en el marco COSO 2013.



CONCLUSIONES

Con base en los resultados de la evaluación de la efectividad de nuestro control interno sobre la información financiera de acuerdo con los criterios establecidos por el marco COSO 2013, nuestra administración concluyó que nuestro control interno sobre la información financiera era efectivo a partir del 31 de diciembre de 2022.

PLAN DE AUDITORÍA INTERNA 2022

La auditoría interna de Ecopetrol diseña planes de auditoría basados en riesgos, con el fin de determinar las prioridades de la actividad de auditoría interna, consistentes con los objetivos de la Organización de asegurar razonablemente el Sistema de Control Interno de la Compañía y evaluar y proponer acciones de mejora sobre la efectividad del Sistema de Gestión de Riesgos de la Compañía, entre otros. Aquí algunos ejemplos:

Nombre de la auditoría	Alcance del riesgo	Año
Auditoría de gestión ambiental	Identificación y gestión sistemática de los posibles impactos ambientales y riesgos asociados a las actividades de Ecopetrol S.A.	2022
Auditoría de gestión de ciberseguridad	Evaluación de la gestión de riesgos, seguimiento y cumplimiento de los requisitos de ciberseguridad, formación y sensibilización.	2022
Prácticas de gestión y respuesta a la auditoría de incidentes de seguridad de la información	Revisar el estado de las prácticas llevadas a cabo por la organización para mitigar los riesgos de seguridad de la información.	2022

AUDITORÍA EXTERNA DEL PROCESO DE GESTIÓN DE RIESGOS

CALIFICACIÓN DE REASEGURO 2022

Ecopetrol recibió inspecciones de riesgo a la principal instalación industrial en refinación, por parte de un equipo de reaseguros liderado por firmas externas de seguros y auditoría de riesgos, con el fin de identificar oportunidades de mejora en la gestión del riesgo operacional, minimizar la materialización de riesgos que puedan afectar a personas, activos y operaciones.

ALCANCE DE LA AUDITORÍA

Revisión de la gestión de riesgos; Estandarización, implementación y sostenibilidad de prácticas como análisis de riesgos, control de obra y desarrollo de simulacros, mejora de la confiabilidad de los procesos productivos, monitoreo y seguimiento temprano y sistemático de riesgos, plan de inversión y proyectos de crecimiento, planes de capacitación para trabajadores en temas técnicos, e intervención oportuna para cerrar observaciones y recomendaciones de reaseguradores.

CONCLUSIONES

Los resultados colocan a Ecopetrol como un referente en gestión de riesgos, alineado con las mejores prácticas de la industria. Esto tiene un impacto directo en la percepción de las compañías de seguros y los plazos obtenidos durante cada renovación del programa de seguros corporativos del Grupo Ecopetrol. La calificación obtenida es un reconocimiento de clase mundial del proceso de inspección de riesgos.

AUDITORÍA DE CALIDAD 2022

Ecopetrol realiza una auditoría externa para sus sistemas de gestión, con base en los requisitos de las normas ISO y a través del ICONTEC (Organismo Nacional de Normalización de Colombia), considerando como alcance de certificación la exploración y producción de petróleo y gas. Producción de productos refinados y petroquímicos. Comercialización de hidrocarburos, Procesos Administrativos y de Apoyo al Negocio, considerando, entre otros, la norma ISO 9001:2015 con enfoque no solo en los procesos individuales de la organización, sino también en las interacciones de estos procesos, incluyendo sus riesgos y controles.

ALCANCE DE LA AUDITORÍA

La Norma ISO 9001:2015 está orientada hacia un enfoque preventivo que se acentúa con los aspectos referidos a la Gestión de Riesgos, que consisten en reconocer los riesgos (positivos como oportunidades, negativos como riesgos) como dentro de una organización y llevar a cabo las acciones necesarias para evitar que ocurran.

CONCLUSIONES

A partir de 2022, la auditoría externa de Ecopetrol concluyó sobre el proceso de gestión de riesgos, que no tenía incumplimientos contra la norma.



USAMOS NUESTRA ENERGÍA PARA
CONSTRUIR UNA **EMPRESA Y UN PAÍS**
— **DE** TODOS, PARA TODOS —

