HOJA DE CONTROL DE CAMBIOS

Versión	Fecha	Cambios realizados en el documento
1	Enero -2016	Emisión de la primera versión del documento. Resolución No. 2016004.
2	Mayo-2018	Revisión anual de la Política de Seguridad de la Información Institucional y actualización del código del documento de PCA.16. DR.01 por PCA.01.02. DR.01. Acta No. 00481.
3	Octubre-2020	Revisión anual de la Política de Seguridad de la Información Institucional. Acta No. 00691.
4	Octubre-2022	Revisión anual de la Política de Seguridad de la Información Institucional. Se incluye los Lineamientos 4.6 y 4.7, se modifica el punto 5.6. Cambio de código de PCA.01.02.DR.01 a PCA.04.01.DR.01.
5	Agosto - 2023	Revisión anual de la Política de Seguridad de la Información Institucional. Actualización de formato. Se modifica en el numeral 4.1 del apartado Lineamientos considerando la serie de normas 27000 y no únicamente 27001.
6	Mayo - 2024	Revisión anual de la Política de Seguridad de la Información Institucional. Actualización integral del documento en función del Acuerdo Ministerial 2024-0003 - EGSI v3.
7	Junio - 2025	Revisión anual de la Política de Seguridad de la Información Empresarial, aprobada por el Comité de Seguridad de la Información en sesión de 15 de mayo de 2025, conforme se evidencia del Acta de la Segunda Reunión Ordinaria (2025). Se modifica el Punto dos “Alcance” por “Ámbito de Aplicación”. Se incluye el Punto 4 “Principios de Seguridad de la Información” y se modifica la numeración de todo el documento a partir de dicho punto. Se incluye en el punto 6 “Definición de términos” los conceptos de “Información”, “Seguridad de la Información” y se modifica el concepto de “Propietario de información” Se incluyen las reglas 7.30 hasta la 7.33 Se modifican las reglas 8.19, 8.20, 8.21 y 8.23 del apartado “Subgerencia de Tecnologías de la Información y Comunicaciones”. Se incluye la regla 8.29 en el apartado Subgerencia de Logística y Abastecimiento Se modifica el apartado “Subgerencia de Planificación y Control de Gestión” por “Jefatura de Seguridad y Transparencia de la Información”, de este apartado se modifican las reglas 8.37, 8.38, 8.39, 8.40, 8.41 y se incluye la regla 8.43. Se incluye la regla 8.49 del apartado “Jefatura de PMO Empresarial” Se eliminan las reglas 7.46 y 7.47 del apartado “Oficial de Seguridad de la Información” y se modifica las reglas 8.50 y 8.52 Se incluye el apartado 9. Cumplimiento de Normativa. En todo el documento se modifica la frase “Comité de Seguridad y Trasparencia de la Información” por “Comité de Seguridad de la Información”.

“Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado.”

8	Septiembre 2026	Revisión y actualización integral de la Política Empresarial de Seguridad de la Información, aprobada por el Comité de Seguridad de la Información en su Segunda Reunión Ordinaria de 2026. Se reorganiza la estructura del documento. Se incorporan principios y objetivos específicos relacionados con la protección de datos personales y la privacidad. Se actualiza el apartado de definiciones, incorporando nuevos conceptos asociados a protección de datos personales, custodia de información, anonimización, tratamiento de datos personales e inteligencia artificial. Se reestructuran los lineamientos dejando 4 generales y se agrupan otros según los siguientes ámbitos: gestión de riesgos, clasificación y protección de la información, capacitación y cultura organizacional, gestión de incidentes, gestión de accesos, gestión de vulnerabilidades, tecnologías emergentes, servicios en la nube, gestión con terceros, protección de datos personales y escritorio limpio. Se definen responsabilidades específicas para el Comité de Seguridad de la Información, la Jefatura de Seguridad y Transparencia de la Información, el Oficial de Seguridad de la Información y se incorpora además al Delegado de Protección de Datos Personales. Se actualizan y redefinen las responsabilidades de las unidades organizacionales, incorporando controles relacionados con ciberseguridad, gestión de vulnerabilidades, servicios en la nube, protección de datos personales y gestión de terceros. Se actualizan los apartados de cumplimiento normativo, restricciones y prohibiciones. En todo el documento se actualiza la terminología y contenido para incluir expresamente la protección de datos personales como parte integrante del Sistema de Gestión de Seguridad de la Información (SGSI).

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

1. Introducción

La Empresa Pública de Hidrocarburos del Ecuador EP PETROECUADOR reconoce a la información y a los datos personales como activos estratégicos indispensables para el cumplimiento de su misión, visión y objetivos empresariales; por lo tanto, se compromete a protegerlos durante todo su ciclo de vida, garantizando la confidencialidad, integridad, disponibilidad y, cuando corresponda, la privacidad de la información y de los datos personales que trata.

Para este fin, la empresa implementa y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) y adopta medidas organizativas, técnicas, físicas y legales orientadas a prevenir accesos no autorizados, pérdida, alteración, divulgación o destrucción de la información y de los datos personales, promoviendo el cumplimiento de la normativa vigente y la gestión adecuada de los riesgos asociados.

2. Ámbito de aplicación

La *"Política de Seguridad de la Información Empresarial"* es un eje transversal de cumplimiento y aplicación obligatoria en los procesos de la empresa, para todo el personal de la EP PETROECUADOR y agentes externos que, en el ejercicio de sus funciones o actividades, accedan, procesen, almacenen, transmitan o administren información y/o datos personales de la EP PETROECUADOR.

Su aplicación abarca todos los procesos institucionales, activos de información, sistemas tecnológicos, infraestructuras, medios físicos y digitales, así como todas las etapas del ciclo de vida de la información y de los datos personales: recolección, registro, organización, almacenamiento, uso, consulta, transmisión, transferencia, conservación, archivo y eliminación.

3. Objetivo de la política

Establecer los principios, lineamientos y controles necesarios para gestionar la seguridad de la información y la protección de los datos personales tratados por la EP PETROECUADOR, con el fin de garantizar su confidencialidad, integridad, disponibilidad y privacidad, mediante la implementación de controles preventivos, detectivos y correctivos basados en la gestión de riesgos; el cumplimiento legal y regulatorio; y, la mejora continua de los procesos institucionales.

4. Principios de Seguridad de la Información y Protección de Datos Personales

- **Confidencialidad**: La información debe ser accesible solo a las personas autorizadas y con una necesidad legítima de conocerla.
- **Cumplimiento Legal**: La empresa cumplirá con la legislación ecuatoriana sobre protección de datos personales, derechos de propiedad intelectual y demás normativas relacionadas con la seguridad de la información.
- **Defensa en profundidad**: La empresa adoptará un enfoque mediante múltiples capas de seguridad para garantizar un análisis exhaustivo y la detección de posibles intrusiones.
- **Disponibilidad**: La información debe estar disponible para los usuarios autorizados cuando sea necesario para su operación y toma de decisiones.
- **Finalidad y minimización**: La recopilación, uso, almacenamiento y demás actividades de tratamiento de datos personales se realizarán únicamente para fines específicos,

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

legítimos y previamente definidos, limitándose a los datos estrictamente necesarios para cumplir dichos fines

- **Integridad**: La información debe mantenerse precisa, completa y actualizada, evitando alteraciones no autorizadas.
- **Mínimo privilegio:** Se otorgarán únicamente los permisos y niveles de acceso esenciales e indispensables para que el usuario pueda llevar a cabo sus actividades designadas, minimizando la superficie de riesgo.
- **Necesidad de saber:** La asignación de accesos estará limitada a la información específica que sea estrictamente indispensable para la ejecución de las tareas o funciones del cargo, evitando la exposición innecesaria a datos no requeridos.
- **Protección de datos personales**: La empresa incorporará medidas técnicas, organizativas, jurídicas y administrativas orientadas a garantizar la protección de datos personales desde la concepción de procesos, servicios, sistemas y proyectos.
- **Responsabilidad proactiva**: La empresa implementará mecanismos de gobernanza, control y supervisión que permitan prevenir riesgos, asegurar el cumplimiento normativo y demostrar la eficacia de las medidas adoptadas para la protección de la información y los datos personales.
- **Segregación de funciones**: Se prohíbe la concentración de funciones críticas o que generen potencial conflicto de interés en una misma persona. La separación de funciones se implementará como un control clave para reducir el riesgo de fraude, corrupción, errores intencionales o no intencionales, y abusos de privilegios en los procesos críticos. Por ejemplo, un usuario no debe tener permisos para registrar y aprobar simultáneamente una misma transacción o proceso.

5. Objetivos de Seguridad de la Información

- Gestionar los riesgos de seguridad de la información y protección de datos personales asociados a los procesos, activos de información y recursos tecnológicos de la EP PETROECUADOR.
- Proteger la confidencialidad, integridad, disponibilidad y, cuando corresponda, la privacidad de la información y de los datos personales tratados por la EP PETROECUADOR, mediante la implementación de controles adecuados.
- Fortalecer las capacidades institucionales para la prevención, detección, respuesta y recuperación frente a incidentes de seguridad de la información y eventos que afecten datos personales.
- Promover una cultura organizacional de seguridad de la información y protección de datos personales, fortaleciendo la concientización, capacitación y cumplimiento de las responsabilidades asignadas.
- Garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad de la información y protección de datos personales.

6. Compromiso

La Gerencia General, reconoce a la información empresarial y a los datos personales tratados por la EP PETROECUADOR como activos estratégicos fundamentales para el cumplimiento de los objetivos estratégicos empresariales, por lo que mantiene el compromiso de cumplir y hacer cumplir los principios de confidencialidad, integridad, disponibilidad y protección de datos personales observando en todo momento las leyes, políticas y normativa vigente, mediante la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) empresarial.

7. Definición de términos

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

Activo de información: Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños en un sistema u organización.

Anonimización: Proceso mediante el cual los datos personales son transformados de forma irreversible para impedir la identificación directa o indirecta de una persona natural, utilizando técnicas que eliminan o modifican los elementos identificativos, de manera que el titular de los datos no pueda ser identificado por ningún medio razonablemente disponible.

Confidencialidad: Se garantiza que la información sea accesible solo a aquellas personas autorizadas a su acceso.

Custodio de información: Responsable de garantizar la confidencialidad, integridad y disponibilidad del activo de la información. Puede actuar en función de sus atribuciones o bajo encargo del propietario de información.

Dato personal: Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

Documento digital: Es el documento que resulta de la digitalización de un documento físico.

Documento electrónico: Documento que se genera a través de un sistema o proceso electrónico.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a sus recursos cuando éstos lo requieran.

IA: Inteligencia artificial

Información: Conjunto de datos con valor para la empresa. Pueden ser generados, recibidos, procesados, almacenados, transmitidos o conservados por la EP PETROECUADOR en cualquier formato o medio. Constituye un activo estratégico que debe ser protegido durante todo su ciclo de vida para garantizar su confidencialidad, integridad, disponibilidad.

Incidente de seguridad de la información: Evento único o serie de eventos inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información.

Integridad.: Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.

Privacidad: Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.

Propietario de información: Titular o responsable de proceso de cada área administrativa u operativa que tiene la responsabilidad sobre la información bajo su ámbito de gestión y que establece los requisitos de clasificación, acceso, protección, conservación y tratamiento de dicha información, garantizando su adecuada protección durante todo su ciclo de vida. En el

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

caso de la información generada en comités y otros cuerpos colegiados, se entenderá como propietario a quien presida el mismo.

Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Es la preservación de la confidencialidad, integridad, disponibilidad de la información mediante un conjunto de medidas preventivas y reactivas sobre los activos de información en el marco de la gestión pública, a fin de garantizar la protección de la información crítica y el cumplimiento de las leyes, normativas y regulaciones aplicables a las entidades del sector público.

Sistema de información: Conjunto de aplicaciones, servicios, activos de tecnologías de la información u otros componentes que manejan información.

Tecnologías de la información (IT por sus siglas en inglés): Conjunto de activos, sistemas y servicios tecnológicos destinados al tratamiento de la información, incluyendo su generación, procesamiento, almacenamiento, transmisión, intercambio y protección, con el fin de apoyar la gestión administrativa, operativa y estratégica de la empresa.

Tecnologías operativas (OT por sus siglas en inglés): Conjunto de activos, sistemas y servicios tecnológicos destinados a supervisar, controlar, automatizar y proteger procesos operacionales, infraestructura crítica y activos físicos de la empresa, garantizando la seguridad, continuidad y confiabilidad de las operaciones.

Tercero: Persona o entidad fuera de la EP PETROECUADOR que requiere acceso a información empresarial.

Tratamiento de datos personales: Cualquier acción realizada sobre datos personales, independientemente del medio utilizado, destinada a su gestión, utilización, conservación, intercambio, protección o eliminación.

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

8. Lineamientos generales

8.1. Las disposiciones previstas en este documento son de aplicación obligatoria para todo el personal de la EP PETROECUADOR y para usuarios externos vinculados con la empresa. Su aplicación abarca la ejecución de los procesos empresariales y la prestación de servicios a nivel nacional e incluye tanto el ámbito de tecnologías de la información (IT), como de tecnologías operativas (OT).

8.2. La empresa mantendrá un Sistema de Gestión de Seguridad de la Información y emitirá la normativa complementaria necesaria para su implementación y mejora continua.

8.3. La EP PETROECUADOR considerará la seguridad informática como un mecanismo de protección para la información, que permita controlar o evitar las amenazas cibernéticas, las cuales ponen en riesgo la información que es procesada, transmitida y almacenada por medios digitales.

8.4. Todo aplicativo desarrollado internamente o implementado por un tercero deberá contar con la designación de un administrador funcional y un administrador técnico.

Se establecen los siguientes lineamientos de acuerdo con temas específicos relacionados con la seguridad de la información:

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

GESTIÓN DE RIESGOS

8.5. La seguridad de la información y la protección de datos personales en la EP PETROECUADOR estarán basadas en un enfoque de gestión de riesgos que permita identificar, evaluar, tratar y monitorear amenazas y vulnerabilidades que puedan afectar los objetivos empresariales.
8.6. La EP PETROECUADOR realizará evaluaciones de impacto en protección de datos personales cuando el tratamiento pueda implicar riesgos elevados para los derechos y libertades de los titulares.
8.7. En todo tipo de proyecto que se desarrolle dentro de la EP PETROECUADOR y durante todo su ciclo de vida, se incorporarán criterios de seguridad de la información, garantizando la protección de la información y el tratamiento de los riesgos asociados, de conformidad con las políticas institucionales, el SGSI y la normativa vigente.

CLASIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

8.8. La EP PETROECUADOR realizará la clasificación de la información de acuerdo con la normativa vigente y requisitos legales determinados por entes de control. La información podrá ser clasificada como pública, confidencial o reservada y, cuando así lo reciba, conservará la clasificación de información que provenga de otra institución.
8.9. Los propietarios y custodios de información física y digital deberán gestionar e implementar controles y/o medidas de protección proporcionales al tipo de información.
8.10. La clasificación de información como reservada no podrá invocarse para negar el acceso a la información requerida por autoridades judiciales, órganos de control o demás entidades legalmente competentes en el ejercicio de sus atribuciones, ni en los casos relacionados con presuntas violaciones de derechos humanos, de conformidad con la normativa vigente.

CAPACITACIÓN, COMUNICACIÓN Y CULTURA ORGANIZACIONAL

8.11. La EP PETROECUADOR comunicará y difundirá la Política de Seguridad de la Información Empresarial y sus actualizaciones a todos los servidores, trabajadores y personal que acceda a la información institucional, mediante los canales oficiales de comunicación y los mecanismos de capacitación, inducción, sensibilización y concientización que se establezcan para tal efecto.
8.12. La EP PETROECUADOR promoverá una cultura de seguridad de la información y protección de datos personales mediante programas continuos de capacitación, concientización y comunicación para todo el personal de la EP PETROECUADOR y agentes externos.

USO DE ACTIVOS DE INFORMACIÓN

8.13. La información generada, procesada, almacenada o transmitida mediante los recursos tecnológicos institucionales asignados al personal de la EP PETROECUADOR constituye un activo de información de la empresa y deberá ser utilizada exclusivamente para fines autorizados. La EP PETROECUADOR establecerá controles para el uso de equipos, aplicaciones, medios de almacenamiento y registros de auditoría, así como para el desarrollo, adquisición e implementación de soluciones tecnológicas.
8.14. Las transacciones y operaciones ejecutadas en los sistemas propios o de terceros deben mantener registros de trazabilidad (logs) que identifiquen las acciones y errores generados por los diferentes funcionarios de las distintas unidades orgánicas y de negocio, garantizando su integridad, inalterabilidad y conservación.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

8.15. Al término de la relación laboral o ante movimientos internos de personal, la información institucional bajo responsabilidad del trabajador deberá ser transferida formalmente a su nivel de supervisión o al servidor designado utilizando los instrumentos de control aplicables, garantizando su integridad, disponibilidad y continuidad operativa. La devolución de activos institucionales, servicios, credenciales y recursos tecnológicos, así como la revocación de accesos correspondientes, se realizará conforme a los procedimientos institucionales vigentes.

GESTIÓN DE INCIDENTES

8.16. Todo evento, debilidad o incidente de seguridad de la información o de protección de datos personales deberá ser reportado oportunamente al Oficial de Seguridad de la Información y gestionado conforme a los procesos y procedimientos de respuesta a incidentes de la EP PETROECUADOR.
8.17. Todo incidente que comprometa los datos personales deberá ser evaluado para determinar la necesidad de notificación a la Autoridad de Protección de Datos Personales y a los titulares afectados conforme la normativa vigente.
8.18. Ante un evento o incidente de seguridad de la información detectado en caso de ser requerido, las unidades orgánicas y de negocio darán acceso a la Jefatura de Seguridad y Transparencia de la Información a los registros de auditoría de los sistemas informáticos e información custodiada por el personal de la empresa en dispositivos de almacenamiento, computadores u otros medios.
8.19. Cuando un evento o incidente de seguridad de la información o de protección de datos personales pueda afectar simultáneamente la continuidad operativa, la seguridad y salud de las personas, las instalaciones o la capacidad institucional de respuesta ante emergencias, su gestión deberá coordinarse con las áreas competentes, conforme a las políticas y/o procesos institucionales aplicables.

GESTIÓN DE ACCESOS

8.20. El acceso a los activos de información de la EP PETROECUADOR será otorgado bajo los principios de necesidad de saber, mínimo privilegio y segregación de funciones, manteniendo mecanismos que aseguren la autenticación, autorización y trazabilidad de las actividades realizadas.
8.21. El administrador funcional de las aplicaciones empresariales será responsable de definir, mantener y revisar los roles y perfiles de acceso conforme a las necesidades del negocio, así como aprobar o validar su asignación a los usuarios de los sistemas institucionales, en observancia de la normativa vigente.

ENTREGA, TRANSFERENCIA Y CUSTODIA DE INFORMACIÓN

8.22. La entrega, transferencia, conservación y custodia de la información institucional deberán realizarse conforme a las disposiciones legales, regulatorias y procedimientos internos aplicables, garantizando la continuidad de su administración y protección.
8.23. La información confidencial que sea compartida por las diferentes unidades orgánicas y de negocio de la EP PETROECUADOR con otras instituciones del Estado o terceros autorizados deberá estar amparada por los correspondientes instrumentos legales, convenios de intercambio de información o acuerdos de confidencialidad que garanticen su adecuada protección, a excepción de los requerimientos efectuados por autoridades administrativas, legislativas o judiciales.
8.24. La información clasificada como reservada únicamente podrá ser compartida cuando exista habilitación legal expresa, competencia institucional que lo autorice o disposición derivada del acto de clasificación correspondiente, observando las restricciones

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

establecidas en la Ley Orgánica de Transparencia y Acceso a la Información Pública, normativa aplicable y demás disposiciones vigentes.

GESTIÓN DE VULNERABILIDADES

8.25. La empresa implementará procesos de identificación, evaluación, tratamiento y monitoreo de vulnerabilidades técnicas, aplicando controles de seguridad proporcionales al riesgo antes de la puesta en producción de activos tecnológicos y durante su ciclo de vida. La gestión de vulnerabilidades deberá ejecutarse, considerando análisis de criticidad y exposición al riesgo. Para los activos críticos será realizada por lo menos una vez al semestre y para otros activos, al menos una vez al año. Este análisis será realizado preferentemente con mecanismos externos.
8.26. Previo al paso a producción de cualquier sistema informático o componente propio o de un tercero, se deberá realizar un análisis de vulnerabilidades. No se autorizará la liberación a producción de soluciones que presenten vulnerabilidades críticas o altas.

TECNOLOGÍAS EMERGENTES Y SERVICIOS EN LA NUBE

8.27. El uso de tecnologías de inteligencia artificial deberá realizarse de forma responsable, ética y segura, respetando la normativa aplicable, los derechos de las personas, la propiedad intelectual y los principios de seguridad de la información y protección de datos personales.
8.28. La información empresarial clasificada como reservada o confidencial, no podrá ser almacenada, procesada o respaldada en nubes públicas ni herramientas de inteligencia artificial no aprobadas por la empresa.
8.29. Está prohibido el uso de inteligencia artificial en actividades que contravengan la normativa o representen riesgos inaceptables para los derechos fundamentales, la seguridad o la dignidad de las personas.
8.30. El entrenamiento de modelos de inteligencia artificial con información institucional deberá contar con un informe del Comité Técnico de Transformación Digital que incluya la validación del Oficial de Seguridad de la Información y del Delegado de Protección de Datos Personales en el ámbito de sus competencias previo a la aprobación por parte de la Gerencia General.
8.31. Todo servicio en la nube deberá incorporar mecanismos que garanticen la continuidad del negocio, la recuperación de la información y la gestión segura de los datos al finalizar la prestación del servicio.
8.32. La utilización de servicios en la nube para almacenar, procesar, respaldar o gestionar información institucional deberá contar con la autorización del propietario de la información y cumplir los requisitos de seguridad de la información, protección de datos personales, gestión documental y demás normativa aplicable, considerando los resultados del análisis de riesgos y el criterio técnico de las áreas competentes cuando corresponda.

GESTIÓN CON TERCEROS

8.33. Los contratos, convenios o acuerdos suscritos con terceros deberán incluir cláusulas relacionadas con la seguridad de la información y protección de datos personales.
8.34. En los procesos de adquisición de bienes o servicios tecnológicos que involucren el almacenamiento, procesamiento y transmisión de información, se deberá observar que se lo realice con proveedores que garanticen el cumplimiento de estándares de seguridad y protección, especialmente para aquellos clasificados como confidenciales o reservados, así como que ofrezcan garantías adecuadas para el tratamiento de datos personales.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

PROTECCIÓN DE DATOS PERSONALES

8.35. La EP PETROECUADOR garantizará que el tratamiento de datos personales se realice de conformidad con la normativa vigente, aplicando principios de licitud, finalidad, minimización, confidencialidad, seguridad y responsabilidad proactiva, así como medidas proporcionales al nivel de riesgo del tratamiento.

8.36. Los datos personales, especialmente aquellos considerados sensibles deberán ser tratados mediante medidas de seguridad y confidencialidad acordes con su nivel de riesgo. Estas medidas podrán incluir controles de acceso restringido, registros de trazabilidad, conservación segura, transferencia controlada, anonimización y eliminación segura, entre otras.

8.37. Los datos personales deberán conservarse únicamente durante el tiempo necesario para cumplir las finalidades del tratamiento y obligaciones legales aplicables, garantizando posteriormente su eliminación, anonimización o bloqueo seguro de acuerdo con la normativa de gestión documental vigente.

ESCRITORIO LIMPIO

8.38. El personal de la EP PETROECUADOR deberá mantener medidas de protección física que eviten la exposición no autorizada de información y activos institucionales en las áreas de trabajo, manteniendo escritorios limpios y pantallas de los equipos libres de información sensible cuando no se encuentren en uso. Los documentos, credenciales, dispositivos y demás activos deberán almacenarse de forma segura para evitar accesos no autorizados.

9. Gobernanza en seguridad de la información y protección de datos personales

El Comité de Seguridad de la Información es el órgano que ejerce la gobernanza en seguridad de la información en la EP PETROECUADOR, su funcionamiento será regulado a través de un Reglamento y contemplará en su conformación, además de los lineamientos establecidos en el Esquema Gubernamental de Seguridad de la Información, la participación de diferentes unidades orgánicas y de negocio.

La Subgerencia de Planificación y Control de Gestión presidirá el Comité de Seguridad de la Información.

La Jefatura de Seguridad y Transparencia de la Información será encargada de coordinar la implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo la gestión de riesgos, la implementación de controles y el cumplimiento de la normativa interna aplicable.

El Oficial de Seguridad de la Información ejercerá funciones de supervisión, seguimiento y asesoramiento en materia de seguridad de la información, monitoreando el cumplimiento de la presente política, informando al Comité de Seguridad de la Información sobre el estado de la seguridad de la información y escalando oportunamente los riesgos e incidentes que puedan afectar a la organización.

El Oficial de Seguridad de la Información ejercerá sus funciones con independencia funcional respecto de las áreas operativas y tecnológicas responsables de la ejecución de controles, teniendo acceso directo al Comité de Seguridad de la Información y a la Gerencia General para el escalamiento de riesgos críticos.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

El Delegado de Protección de Datos Personales ejercerá las actividades establecidas en la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás normativa aplicable. El delegado actuará de manera coordinada con el Oficial de Seguridad de la Información en los aspectos relacionados con la protección de datos personales y la gestión de incidentes que involucren datos personales.

Los responsables de procesos, propietarios de información, custodios y servidores en general, son responsables de proteger la información y los datos personales bajo su control, así como de cumplir las disposiciones establecidas en la presente política y la normativa relacionada.

10. Roles y responsabilidades

Para la aplicación de la presente política, además de las atribuciones establecidas en el Manual Orgánico de la EP PETROECUADOR y de la normativa vigente, se determinan las siguientes responsabilidades:

Gerencia General

10.1. Liderar el cumplimiento del Sistema de Gestión de Seguridad de la información de la organización.
10.2. Asignar los recursos necesarios para el mantenimiento del Sistema de Gestión de Seguridad de la información (SGSI), previo al análisis realizado por el Comité de Seguridad de la Información.
10.3. Aprobar la Política de Seguridad de la Información Empresarial y cualquier cambio a la misma, así como las recomendaciones presentadas por el Comité de Seguridad de la Información.
10.4. Promover la difusión, apoyo y cumplimiento de lo establecido en la presente política.
10.5. Designar un Oficial de Seguridad de la Información (OSI).

Comité de Seguridad de la Información

10.6. Velar por la aplicación de la presente política.
10.7. Revisar la Política de Seguridad de la Información Empresarial previo a la aprobación de la Máxima Autoridad.
10.8. Revisar el estado de los riesgos, incidentes, indicadores y planes de tratamiento de seguridad de la información y protección de datos personales.
10.9. Revisar y recomendar a la Gerencia General la aprobación de normativa interna en materia de seguridad de la información.

Jefatura de Seguridad y Transparencia de la Información

10.10. Gestionar el Sistema de Seguridad de la Información (SGSI), coordinar la definición de normativa y lineamientos generales para la gestión de la seguridad de la información empresarial, y realizar controles y evaluaciones internas que permitan verificar el correcto funcionamiento del SGSI empresarial y de sus procedimientos relacionados.
10.11. Evaluar el cumplimiento y eficacia de los controles de seguridad de la información, así como coordinar la evaluación interna del Sistema de Gestión de Seguridad de la información (SGSI) de forma periódica.
10.12. Informar a las unidades competentes sobre incumplimientos identificados en materia de seguridad de la información y protección de datos personales, para la adopción de las acciones correspondientes.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

10.13. Asesorar y coordinar la identificación y gestión de riesgos de seguridad de la información y de protección de datos personales de la EP PETROECUADOR, para lo cual, mantendrá actualizada la metodología de gestión de riesgos.
10.14. Gestionar la preparación, detección, evaluación y respuesta ante la ocurrencia de incidentes de seguridad de la información empresarial en coordinación y apoyo de las unidades orgánicas y de negocio de la EP PETROECUADOR.
10.15. Determinar los procedimientos de evaluación de vulnerabilidades previos a la puesta en producción de sistemas informáticos, verificando que las soluciones no presenten vulnerabilidades críticas o altas antes de su liberación.
10.16. Elaborar y presentar al Comité de Seguridad de la Información indicadores, riesgos, incidentes y el estado general del Sistema de Gestión de Seguridad de la Información.
10.17. Coordinar la revisión y actualización de la Política de Seguridad de la Información Empresarial, con la finalidad de realizar ajustes necesarios de mejora al menos una vez al año y cuando se produzcan cambios significativos a nivel operativo, legal, tecnológico, económico en el entorno de la EP PETROECUADOR.

Oficial de Seguridad de la Información

10.18. Asesorar y coordinar con el equipo técnico designado por el Comité de Seguridad de la Información, la ejecución periódica de la metodología de gestión de riesgos de seguridad de la información.
10.19. Coordinar e informar al Comité de Seguridad de la Información de las acciones de recuperación de los servicios tecnológicos cuando se presenten incidentes de seguridad de la información de prioridad crítica que afecten la continuidad de las operaciones de la empresa o una vez que haya sido declarado un evento de crisis.
10.20. Supervisar el cumplimiento de la presente política y reportar al Comité de Seguridad de la Información los incumplimientos, riesgos relevantes y oportunidades de mejora identificados.
10.21. Realizar el seguimiento al estado de los riesgos, incidentes, planes de tratamiento y acciones correctivas asociadas a la seguridad de la información.
10.22. Coordinar con el Delegado de Protección de Datos Personales los aspectos relacionados con incidentes, riesgos y medidas que involucren datos personales.

Delegado de Protección de Datos Personales

10.23. Asesorar a la EP PETROECUADOR en el cumplimiento de la Ley Orgánica de Protección de Datos Personales, su Reglamento General y demás normativa aplicable en materia de protección de datos personales.
10.24. Supervisar el cumplimiento de las políticas, procedimientos, controles y demás instrumentos relacionados con la protección de datos personales dentro de la empresa.
10.25. Emitir recomendaciones respecto de los riesgos asociados al tratamiento de datos personales y promover la adopción de medidas que permitan proteger los derechos y libertades de los titulares.
10.26. Asesorar a las unidades orgánicas y de negocio en la aplicación de los principios de protección de datos personales y en la implementación de medidas de privacidad desde el diseño y por defecto.
10.27. Coordinar con el Oficial de Seguridad de la Información la gestión de incidentes que involucren datos personales, así como las acciones de mitigación correspondientes.
10.28. Participar en la revisión de evaluaciones de impacto en protección de datos personales cuando la naturaleza, alcance o finalidad del tratamiento pudiera representar un riesgo elevado para los derechos y libertades de los titulares.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

10.29. Actuar como punto de contacto y coordinación con la Superintendencia de Protección de Datos Personales en los asuntos relacionados con sus competencias.
10.30. Asesorar en la atención de solicitudes para el ejercicio de los derechos de los titulares de datos personales, de conformidad con la normativa vigente.
10.31. Elaborar y presentar informes a la Gerencia General y al Comité de Seguridad de la Información sobre el estado de cumplimiento en materia de protección de datos personales.

Procuraduría

10.32. Brindar asesoría jurídica a los propietarios de información durante el proceso de clasificación de información, cuando se requiera determinar la aplicación de disposiciones legales, restricciones de acceso, criterios de confidencialidad, reserva o protección de datos personales, de conformidad con la normativa vigente.
10.33. Emitir criterios jurídicos respectos de la aplicación de las categorías de información pública, confidencial y reservada, cuando se requiera para su adecuada gestión y protección.
10.34. Revisar y emitir criterios jurídicos sobre los contratos, convenios, acuerdos de confidencialidad e instrumentos de intercambio de información que involucren el tratamiento o transferencia de información institucional.
10.35. Asesorar a las unidades organizacionales respecto de los requerimientos de información formulados por autoridades judiciales, organismos de control y demás entidades competentes, verificando su apego al marco jurídico aplicable.

Subgerencia de Tecnologías de la Información y Comunicación

10.36. Implementar y determinar las medidas de ciberseguridad producto del análisis de riesgos de seguridad de la información, con la finalidad de proteger la integridad, disponibilidad y confidencialidad de la información digital almacenada en la infraestructura tecnológica.
10.37. Gestionar los niveles de acceso e identidad lógica de acuerdo con las necesidades de los propietarios de la información o procesos.
10.38. Identificar, evaluar y gestionar el tratamiento a los riesgos de ciberseguridad a los que se encuentre expuesta la infraestructura tecnológica a fin de minimizar la ocurrencia de un ataque digital a la infraestructura y servicios tecnológicos de la empresa.
10.39. Implementar las medidas técnicas preventivas ante amenazas cibernéticas que permitan detectar, proteger, responder y recuperar los sistemas de información e información digital frente a incidentes de ciberseguridad.
10.40. Establecer metodologías para el desarrollo seguro de aplicativos informáticos, así como los estándares y medidas de seguridad para dicha ejecución.
10.41. Aplicar los mecanismos correspondientes para eliminar o enmascarar datos, previo al uso de la información en ambientes no productivos. Estos datos deben ser identificados por el propietario de la información.
10.42. Aprobar técnicamente la adquisición, desarrollo, construcción, adaptación o adopción de soluciones de software destinadas al uso institucional; verificar que cumplan con los requerimientos tecnológicos, de seguridad de la información, interoperabilidad y arquitectura institucional; garantizar la realización de las pruebas funcionales, técnicas y de seguridad antes de su paso a producción; y coordinar la obtención de las autorizaciones o avales ante los organismos competentes requeridos por la normativa vigente.
10.43. Desarrollar los procedimientos que permitan fortalecer de manera continua la gestión de vulnerabilidades técnicas, basándose en los análisis de riesgos identificados en la empresa y/o la ocurrencia de un incidente de seguridad con apoyo de los usuarios

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

funcionales de los sistemas empresariales. Así también establecerá criterios técnicos para determinar la clasificación de vulnerabilidades: críticas, altas, medias y bajas.

10.44. Definir la estrategia de modelo de servicio a implementar en la nube (IaaS, SaaS, PaaS) en conjunto con las áreas requirentes en función de las necesidades de operación, seguridad y requisitos legales.

Subgerencia de Logística y Abastecimiento

10.45. Mediante la Jefatura de Gestión Documental y Archivo, administrar funcionalmente los sistemas y herramientas tecnológicas que soportan la gestión documental institucional; elaborar y mantener la normativa, lineamientos e instrumentos archivísticos de su competencia, alineados con el SGSI empresarial; y custodiar los instrumentos de control, inventario y catastros documentales institucionales, garantizando su integridad, disponibilidad y protección.

10.46. Establecer y mantener los lineamientos para la organización, identificación, codificación, etiquetado, custodia, conservación y protección de documentos físicos, digitales y electrónicos que conforman los archivos de gestión y el archivo central institucional, de conformidad con la normativa vigente.

10.47. Establecer los lineamientos y controles para la transferencia, intercambio y entrega de información física y digital a las partes interesadas internas y externas que se encuentren al amparo de contratos, convenios o acuerdos que regulen su intercambio.

10.48. Establecer mecanismos contractuales que obliguen a los contratistas y proveedores a reportar oportunamente incidentes que comprometan la información institucional, de conformidad con los procedimientos de gestión de incidentes de la empresa.

Subgerencia de Talento Humano

10.49. Verificar los antecedentes y asegurar la idoneidad de todos los candidatos a ocupar cargos en la empresa teniendo en cuenta la norma legal vigente y ética aplicable a fin de minimizar riesgos de seguridad de la información.

10.50. Establecer los mecanismos para concientizar, formar y educar al personal sobre las responsabilidades, reglas y obligaciones de seguridad de la información aplicables.

10.51. Formalizar, comunicar y socializar los procesos disciplinarios aplicables al personal que incumplan las directrices de seguridad de la información establecidas en este documento y demás normativa aplicable, conforme a la normativa legal vigente.

10.52. Coordinar con la Subgerencia de Tecnologías de la Información y Comunicación y la Jefatura de Seguridad Física la implementación de mecanismos automatizados para controlar los procesos de vinculación, movimientos y desvinculación del personal, a fin de minimizar los riesgos asociados al uso inadecuado de accesos lógicos y físicos, roles asignados y manejo de la información.

10.53. Definir, comunicar y socializar al personal de la empresa las responsabilidades y deberes con relación a la seguridad de la información, incluso aquellas que siguen siendo válidas aún después de la terminación de la relación laboral.

10.54. En coordinación con Tecnologías de la Información y Comunicación, definir las condiciones y restricciones para las actividades de trabajo a distancia, considerando los requisitos de seguridad física del entorno, seguridad de las comunicaciones y la sensibilidad de la información física o digital.

10.55. Coordinar con la Jefatura de Seguridad y Transparencia de la Información, la definición de criterios para preservar la confidencialidad, integridad y disponibilidad de la información y la protección de los datos personales y la privacidad de los titulares en las diferentes responsabilidades que se asignen a los trabajadores de la EP PETROECUADOR.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

Jefatura de Imagen y Comunicación

10.56. Gestionar los mecanismos institucionales de comunicación y apoyar la difusión de información relacionada con la seguridad de la información cuando corresponda.
10.57. Elaborar, mantener actualizado y realizar el seguimiento oportuno del plan de comunicación ante incidentes de seguridad de la información, con criterios diferenciados dependiendo de su naturaleza e impacto.

Jefatura de Seguridad Física

10.58. Determinar y mantener las medidas de seguridad físicas perimetrales y del entorno a la empresa, incluidos los diferentes sitios donde se encuentra el personal para evitar el acceso físico no autorizado, el daño y la interferencia a la información de la empresa.
10.59. Identificar las instalaciones críticas y monitorearlas de acuerdo con los riesgos identificados en el ámbito de competencia de seguridad física.

Niveles de supervisión, dirección y máximas autoridades de unidades orgánicas y de negocio.

10.60. Las autoridades de las unidades orgánicas y de negocio, deberán promover con su equipo de trabajo el cumplimiento de la presente política y demás normativa interna a fin de proteger la información empresarial que se encuentra bajo su custodia.
10.61. Los responsables de los macroprocesos, procesos y subprocesos de la empresa deberán identificar los riesgos de seguridad de la información y gestionar su tratamiento en los procesos incluyendo aquellos que tengan interacción con proveedores o terceros.
10.62. Los responsables de los macroprocesos y procesos deberán implementar y mantener dentro de su normativa, procesos y procedimientos, las reglas y controles necesarios para proteger la información física y digital bajo su custodia, así como los datos personales que gestionen, de conformidad con las políticas institucionales vigentes.
10.63. Las jefaturas inmediatas son responsables de verificar el buen uso de la información asociada a los procesos y servicios bajo su responsabilidad, por parte del personal de la institución y personal externo autorizado a su cargo (proveedores nacionales o internacionales, pasantes o consultores).
10.64. Los propietarios de los activos de información serán los responsables de identificar, registrar y mantener actualizado el inventario de los activos de información a su cargo, de conformidad con la metodología institucional establecida para la gestión y clasificación de la información, con el apoyo técnico y metodológico de la Jefatura de Seguridad y Transparencia de la Información y la Procuraduría.
10.65. Los propietarios de activos de información serán responsables de gestionar la clasificación de la información acorde a la normativa vigente; y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

Administradores de contratos, Prosecretario de Directorio, Secretarios de Comité y otras figuras ad hoc

10.66. Custodiar los expedientes generados en el ejercicio de sus roles, preservando su disponibilidad, integridad y confidencialidad.

Personal de EP PETROECUADOR

Son obligaciones de todo el personal de la EP PETROECUADOR:

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

10.67. Conocer y cumplir las disposiciones descritas en la presente política, así como las leyes y normativa conexa

10.68. Tomar conocimiento de las comunicaciones emitidas en materia de seguridad de la información y de asistir o realizar los cursos de capacitación que se pongan a disposición.

10.69. Utilizar las cuentas de usuario, perfiles de acceso y demás recursos tecnológicos asignados únicamente para el cumplimiento de sus funciones y asignaciones de trabajo y serán responsables de su utilización y seguridad.
Dar cumplimiento a las normas, procesos y procedimientos establecidos en la empresa referentes al adecuado uso y manejo de la información, a fin de mantener las salvaguardas necesarias para proteger la información tanto física como digital que soporta sus operaciones.

11. CUMPLIMIENTO DE NORMATIVA

11.1. La EP PETROECUADOR se compromete a cumplir con todas las normativas legales y regulaciones aplicables en materia de seguridad de la información, entre las que se incluyen:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Código Orgánico Integral Penal
- Ley de Seguridad Pública y del Estado
- Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP)
- Ley Orgánica de Protección de Datos Personales
- Ley Orgánica para el Fortalecimiento de la Ciberseguridad
- Reglamento General de la Ley Orgánica de Telecomunicaciones
- Normas de Control Interno - CGE
- Esquema Gubernamental de Seguridad de la Información (Acuerdo Ministerial 2024 - 0003)
- Estándares nacionales o internacionales, como la NTE INEN ISO/IEC 27000, y cualquier otra normativa o ley relacionada que regule la seguridad de la información y protección de los datos personales en el sector público.

12. RESTRICCIONES Y PROHIBICIONES

12.1. El uso de los activos de información, infraestructura tecnológica y recursos físicos provistos por la EP PETROECUADOR está estrictamente limitado al cumplimiento de las funciones laborales asignadas. Se prohíbe explícitamente a los trabajadores de la empresa:

- Utilizar los recursos institucionales para almacenar, procesar, promover o difundir contenido que configure un delito, conductas discriminatorias, apuestas o actividades contrarias al Código de Ética y al Reglamento Interno de la EP PETROECUADOR, incluyendo el envío de texto difamatorio, ofensivo, intimidatorio o injurioso contra la honra de las personas.
- Intentar evadir, desactivar, alterar o vulnerar las medidas de seguridad, privilegios de acceso, firewalls o configuraciones de control lógico implementadas en los equipos y aplicaciones de la empresa.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

- Ejecutar, instalar, almacenar o transferir software no autorizado o cualquier tipo de código malicioso que ponga en riesgo la confidencialidad, integridad o disponibilidad de la infraestructura tecnológica.
- Emplear el correo electrónico institucional u otros canales oficiales de comunicación para el envío de mensajería masiva no autorizada (spam), propaganda comercial, gremial, proselitismo político o cadenas de datos ajenas al giro del negocio de la EP PETROECUADOR.
- Retirar, transferir, copiar o distribuir documentos y activos de información digitales o físicos sin contar con la debida justificación y aprobación del propietario de la información.
- Acceder, registrar o utilizar cuentas de correo o credenciales de acceso institucional ajenas, así como registrar la dirección de correo corporativa en plataformas digitales de acceso público que no tengan relación estricta con la actividad laboral que desempeña.
- Está prohibido el uso de IA para la toma de decisiones con impacto significativo sobre personas, así como en actividades que representen una amenaza clara para los derechos fundamentales, la seguridad o la dignidad de las personas.

13. EXCEPCIONES Y SANCIONES

13.1. Los sistemas heredados que no permitan implementar integralmente los controles de seguridad definidos podrán operar bajo una excepción formalmente aprobada, mientras se ejecuten las acciones para su actualización, reemplazo o mitigación de riesgos.

13.2. Los controles establecidos en la presente política podrán exceptuarse cuando una disposición legal, orden judicial o requerimiento formal emitido por autoridad competente establezca un tratamiento distinto de la información.

13.3. El incumplimiento de la presente política por parte de los trabajadores de la EP PETROECUADOR podrá dar lugar a la aplicación del régimen disciplinario, debiéndose aplicar el debido proceso establecido en la Norma Interna de Talento Humano.

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."

ACTA DE APROBACIÓN

RESPONSABLE(S)	FIRMA(S)
APROBADOR(ES) *Responsable del Macroproceso o su delegado, conforme resolución vigente y/o acta de designación de responsables de procesos.* El(Los) suscrito(s) aprueba(n) este documento para su formalización y publicación en la Normativa Interna de Gestión.	Validar únicamente en FirmaEC. Firmado electrónicamente por: SEBASTIAN JOSE MAAG PARDO **Cargo:** Gerente General Validar únicamente en FirmaEC. Firmado electrónicamente por: CRISTIAN OSWALDO HIDALGO FALLAIN **Cargo:** Subgerente de Planificación y Control de Gestión
ELABORADOR(ES) Y REVISOR(ES) DEL ÁREA(S) USUARIA(S) *Delegado(s) del Responsable del Proceso o su delegado* El(Los) suscrito(s) dejan constancia de la elaboración y/o revisión de este documento para su formalización y publicación en la Normativa Interna de Gestión.	Validar únicamente en FirmaEC. Firmado electrónicamente por: LUIS ANDRES ANDRADE CORRALES **Cargo:** Jefe de Seguridad y Transparencia de la Información (Oficial de Seguridad de la Información) Validar únicamente en FirmaEC. Firmado electrónicamente por: JUAN FRANCISCO YEPEZ SALAZAR **Cargo:** Analista de Seguridad de la Información
REVISIÓN LEGAL *Área Legal* El(Los) suscrito(s) deja(n) constancia del asesoramiento a los responsables de los macro procesos y procesos en la legislación aplicable vigente. De acuerdo con la Norma de Control Interno número 200-06: "*Competencia profesional*", emitida por la Contraloría General del Estado, sin que se pueda extender su participación sobre el análisis o validación de aspectos técnicos o económicos. La revisión efectuada se limita a las modificaciones solicitadas por el área requirente, conforme consta en la hoja de control de cambios; y, a las responsabilidades señaladas en el Proceso ASE.01 Gestión de Asuntos Jurídicos; y, ASE.PR.01 Requerir y Actualizar Procesos, Procedimientos y/o Documentos Relacionados.	Validar únicamente en FirmaEC. Firmado electrónicamente por: GABRIELA ABIGAIL MEJIA CABRERA **Cargo:** Jefe de Asesoría y Normas Laborales Validar únicamente en FirmaEC. Firmado electrónicamente por: MARIA JOSE TRUJILLO JARAMILLO **Cargo:** Abogado de Relaciones Laborales
REVISIÓN METODOLÓGICA *Área de Gestión por Procesos* El(Los) suscrito(s) deja(n) constancia de la revisión de los aspectos metodológicos de la Gestión por Procesos. De acuerdo con la Norma de Control Interno número 200-06: "*Competencia profesional*", emitida por la Contraloría General del Estado, sin que se pueda extender su participación sobre el análisis o validación de aspectos técnicos o económicos.	Validar únicamente en FirmaEC. Firmado electrónicamente por: MIRYAN ARACELY CANIZARES REATEGUI **Cargo:** Jefe de Gestión por Procesos Validar únicamente en FirmaEC. Firmado electrónicamente por: JAEL ANDREA TORRES VALENZUELA **Cargo:** Analista de Gestión por Procesos

"Este documento es de propiedad exclusiva de EP PETROECUADOR. Se prohíbe su uso no autorizado."