Oleoducto Central S.A. (Ocensa) reconoce que la seguridad y privacidad de la información y la ciberseguridad son factores estratégicos clave para proteger los activos de información, garantizar la continuidad del negocio y mantener la confianza de clientes, socios, autoridades y otras partes interesadas**.**

La organización reafirma su compromiso de gestionar estos aspectos de manera integral, rigurosa y alineada con las mejores prácticas y como manifestación de este compromiso, establece y adopta la presente política de Seguridad de la información y ciberseguridad como una directriz corporativa, para proteger los activos de información, ciberactivos, sistemas tecnológicos y operaciones críticas mediante la implementación de controles efectivos, fortaleciendo la cultura de seguridad, garantizando el cumplimiento normativo y construyendo un entorno cibernético seguro, resiliente y confiable.

NUESTRO COMPROMISO

Esta política establece un marco integral que guiará las acciones para proteger la confidencialidad, integridad y disponibilidad de activos de información y ciberactivos, basada en los siguientes principios rectores a través de los cuales OCENSA se compromete a:

1. Gobierno
Establecer un modelo robusto para la gestión de la seguridad de la información, la privacidad y la ciberseguridad, el cual estará respaldado por la alta dirección e integrado con la estrategia corporativa. Este compromiso se traduce en la asignación de responsabilidades claras, recursos adecuados y mecanismos de supervisión eficaces que permitan asegurar una gestión transversal, efectiva y sostenible de la seguridad en todos los niveles de la organización.

2. Enfoque basado en riesgos
Gestionar la seguridad con base en la identificación, evaluación y tratamiento sistemático de los riesgos que puedan afectar sus activos de información y ciberactivos. Esta gestión de riesgos será continua, adaptable a los cambios del entorno y orientada a minimizar impactos sobre la operación, la reputación y el cumplimiento, permitiendo priorizar acciones y proteger lo que es verdaderamente crítico para la sostenibilidad del negocio.

3. Protección de la Información y el ambiente tecnológico
Proteger la información, sistemas y recursos tecnológicos mediante controles técnicos, procedimentales y organizacionales efectivos que garanticen su confidencialidad, integridad, disponibilidad y privacidad. Este compromiso incluye la identificación, clasificación y salvaguarda de los activos según su nivel de criticidad.

4. Garantizar el cumplimiento normativo y regulatorio
Cumplir con las normativas legales, regulatorias y contractuales aplicables en materia de seguridad de la información, privacidad y protección de datos personales, ciberseguridad, continuidad operativa y otros requisitos específicos del sector. Este compromiso incluye el monitoreo constante del entorno regulatorio, la implementación de controles para garantizar la conformidad y el fortalecimiento de la cultura organizacional basada en la ética y la responsabilidad.

5. Ciberresiliencia y continuidad
Desarrollar e implementar capacidades de ciberresiliencia que le permitan anticiparse, responder y recuperarse de posibles incidentes de seguridad, fallas operativas o desastres tecnológicos. Este compromiso se materializa en la formulación de planes de recuperación ante desastres y pruebas periódicas que aseguren la estabilidad operativa y la protección de los procesos críticos ante cualquier eventualidad.

6. Cultura y corresponsabilidad

Fomentar una cultura de seguridad y corresponsabilidad entre todos los colaboradores, contratistas y terceros, promoviendo comportamientos seguros, éticos y alineados con las políticas establecidas. Este compromiso se refleja en estrategias permanentes de formación, sensibilización y comunicación que permitan construir un entorno donde la seguridad sea entendida como una responsabilidad compartida.

7. Seguridad desde el diseño

Integrar la seguridad y la privacidad desde las fases más tempranas de diseño y desarrollo de procesos, servicios y soluciones tecnológicas. Este compromiso incluye adoptar prácticas seguras de desarrollo, configuración y gestión de sistemas, con un enfoque preventivo que reduzca vulnerabilidades y promueva la protección proactiva de la información en todo su ciclo de vida.

8. Seguridad de la cadena de suministro

Establecer lineamientos para la gestión de riesgos relacionados con terceros y la cadena de suministro, promoviendo prácticas que contribuyan a preservar la seguridad de la información y la continuidad del negocio. Esto incluye la adopción de medidas razonables para conocer y mitigar posibles impactos derivados de las relaciones con proveedores, contratistas y aliados, alineando su gestión con los principios de seguridad definidos por la organización.

9. Uso ético y responsable de la tecnología

Impulsar el uso ético, transparente y responsable de tecnologías digitales, incluyendo aquellas emergentes como inteligencia artificial, IoT y automatización, garantizando que su adopción esté alineada con los valores corporativos, el respeto por los derechos fundamentales y la seguridad de la información. Este compromiso promueve la confianza digital y el desarrollo tecnológico sostenible, asegurando que la innovación no comprometa la seguridad ni la privacidad.

10. Ciclo de mejora continua

Aplicar el principio de mejora continua en todos los aspectos relacionados con la gestión de la seguridad, la privacidad y la ciberseguridad. A través de revisiones periódicas, auditorías, análisis de desempeño e incorporación de aprendizajes, se buscará fortalecer de forma constante el modelo de gestión, adaptándolo a los cambios tecnológicos, organizacionales y del entorno de amenazas.

Todos los empleados, contratistas y proveedores de Ocensa deben conocer, aplicar, divulgar y velar por el cumplimiento de esta política

APLICABILIDAD

La presente política, además de los manuales, procedimientos o documentos derivados o complementarios a ésta, aplican a toda la organización y son de obligatorio cumplimiento para todo colaborador de la compañía, proveedores, contratistas, terceros, o cualquier persona que gestione o tenga acceso ocasional o permanente a los activos de información de Ocensa y/o a los recursos tecnológicos.

El incumplimiento o violación a estas políticas o lineamientos derivados serán sancionados de acuerdo con el Reglamento Interno de Trabajo, las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

SEGUIMIENTO, REVISIÓN Y RESPONSABLES DE LA POLÍTICA

La presente política y demás documentos asociados se revisarán acorde a lo establecido en el ESTANDAR DE PUBLICACIÓN Y ACTUALIZACIÓN DE DOCUMENTOS o si ocurren cambios normativos, organizacionales y de contexto, para asegurar su continua idoneidad, eficiencia y pertinencia.

El seguimiento a la implementación de la política y su revisión estará a cargo de la Dirección de servicios corporativos y en cabeza de la Gerencia de Tecnología, Soluciones e Innovación.

CONTROL DE ACTUALIZACIONES

VERSIÓN	FECHA	DESCRIPCIÓN
0	03/10/2016	Elaboración del documento
N/A	12/05/2020	En cumplimiento del **ESTÁNDAR CONTROL DE INFORMACIÓN DOCUMENTADA GDI-STD-002** se obtiene como respuesta con el ID 1040 que el presente documentó **Si Requiere Actualización**.
1	26/08/2025	Cambio nombre del documento y actualización general del mismo

Yulieth Angarita Claro Gerente Tecnología, Soluciones e Innovación (E) **Revisó**	Alberto Holguin Holguin Director de servicios corporativos **Aprobó**