POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

TI-P-001

1 OBJETIVO

Proteger los activos de información de TI/TO del Oleoducto de los Llanos Orientales S.A. y Oleoducto Bicentenario de Colombia S.A.S, gestionando y asegurando los principios generales que preservan la confidencialidad, integridad y disponibilidad de la información, mediante la definición de políticas de obligatorio cumplimiento.

2 ALCANCE

La política de seguridad de la información y ciberseguridad aplica sin limitación y es de obligatorio cumplimiento por todos los colaboradores de las compañías, proveedores, contratistas y terceros que cuenten con acceso a los activos de información de TI/TO.

3 POLÍTICA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Compañías reconocen la importancia de la seguridad de la información y la ciberseguridad al igual que el valor de su información como uno de los activos más importantes, así la necesidad de que los diferentes procesos gestionen la información y los activos de información de manera segura alineados a las mejores prácticas de seguridad de la información y ciberseguridad para contribuir con el cumplimiento de los objetivos estratégicos organizacionales y todas las partes interesadas.

Para garantizar el cumplimiento del presente documento de deben adoptar conductas y buenas prácticas de seguridad de la información y ciberseguridad por parte de los colaboradores de las compañías, proveedores y contratistas que en el ejercicio de sus funciones generen, procesen, transporten y almacenen información en los diferentes servicios, plataformas tecnológicas y de operación, preservando la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información;

Por lo anterior en las compañías debe velar por:

1. El cumplimiento de los requisitos y principios de Seguridad, Privacidad de la Información y Ciberseguridad.

2. Proteger los activos de información TI/TO.

3. Administrar, gestionar y mitigar los riesgos asociados a seguridad de la información y Ciberseguridad en los diferentes procesos.

4. Establecer y divulgar las directrices, normas, Políticas, Estándares, Procedimientos e Instructivos de Seguridad de la Información y Ciberseguridad, generando compromiso en todos los procesos y colaboradores, proveedores y contratistas.

5. Fortalecer la cultura de seguridad de la información y ciberseguridad de todos los colaboradores, proveedores y contratistas que interactúen con los activos de información TI/TO.

6. Garantizar los requisitos de Seguridad, Privacidad de la Información y Ciberseguridad en el plan de continuidad del negocio frente a incidentes de Seguridad, Privacidad de la Información y Ciberseguridad.

7. Implementar medidas de seguridad necesarias para prevenir, mitigar, y disminuir los impactos de la materialización de posibles amenazas o ataque cibernéticos.

8. Trabajar como apoyo en la cooperación con entidades públicas y privadas en la gestión de la seguridad de la información, ciberseguridad y ciberdefensa.

9. Apoyar la continuidad del negocio, la innovación tecnológica y la aplicación de las mejore prácticas de seguridad, garantizando el cumplimiento de los requisitos legales y reglamentarios, orientados a la mejora continua.

10. Procurar por generar mejora continua en las actividades de seguridad de la información y ciberseguridad en los diferentes procesos de las compañías.

4 PRINCIPIOS

En las compañías nos comprometemos a la gestión adecuada la seguridad de la información y la ciberseguridad, mediante la adopción de los siguientes principios por parte de todos los colaboradores, proveedores y contratistas, con acceso a la información, infraestructura tecnológica y de operación de las Compañías**:**

- **Estamos comprometidos a tratar la información con el debido cuidado**, normalmente utilizamos información contenida en documentos, mensajes de correo y sistemas de información. Esta información debe estar disponible para aquellos que la requieren, pero no para quienes no estén autorizados. La protección de nuestra información es un deber de todos.

- **Estamos comprometidos a ser precavidos al comunicarnos**, compartiendo la información que hace parte del trabajo diario, sin embargo, la información también puede brindar una ventaja competitiva importante. Por esta razón, es importante actuar con precaución a la hora de comunicarse a través de cualquier canal de comunicación (conversaciones personalmente o por teléfono, comunicación escrita por chat, documentos físicos o electrónicos, redes sociales, eventos presenciales o virtuales, entre otros)

- **Nuestra identidad es un preciado bien**, para que no seamos responsables de las acciones realizadas por otros, no permitimos que roben nuestra identidad. Para ello no se comparte y se protege las contraseñas, dispositivos de identificación y autenticación.
  Si alguien diferente a usted tiene acceso a estos medios de identificación, tendrá acceso a su información, aplicaciones y podrá actuar en su nombre.

- **Estamos comprometidos en cuidar y proteger los dispositivos,** para realizar nuestro trabajo requerimos usar dispositivos electrónicos, como el computador de escritorio o portátil y el teléfono inteligente. Estos aparatos nos permiten acceder a información y aplicaciones. Por lo tanto, es muy importante que funcionen adecuadamente, que no sean manipulados, que no puedan ser utilizados por otras personas no autorizadas y que no tengan software no autorizado y/o malicioso.

- **El orden es primordial en el sitio de trabajo**, el lugar de trabajo en la oficina y su espacio de trabajo virtual deben permanecer ordenados, esto permitirá identificar con que información cuenta y garantizar la confidencialidad de esta.

- **Estamos comprometidos a Ser precavidos durante los desplazamientos o trabajando fuera de las instalaciones de la compañía,** cuando abandone las instalaciones protegidas de las Compañías, incluso al trabajar en casa, los documentos y los dispositivos portátiles como el computador o el móvil inteligente que se lleve consigo, se encuentran expuestos a mayores riesgos, por lo que requieren de una protección especial.

- **Estamos comprometidos en reportar cualquier incidente o evento sospechoso,** si a pesar de las medidas de seguridad, sucede algún incidente no deseado u observa algún evento o comportamiento sospechoso, es necesario notificarlo tan pronto como pueda con el fin de tomar las medidas que permitan limitar los posibles daños e impedir la repetición del incidente.

- **Estamos comprometidos a solicitar o aprobar únicamente los accesos requeridos para cumplir con las funciones** y cada colaborador, contratista y tercero debe tener acceso exclusivamente a la información que requiere para poder cumplir con las responsabilidades asignadas o para las cuales fue contratado.

- **Estamos comprometidos en evitar conflictos de segregación funcional,** controlando que una persona tenga total control sobre más de una responsabilidad dentro del sistema, que le permita realizar algún tipo de fraude o cometer algún tipo de error de manera intencional o desprevenida.

- **Nos comprometemos a colaborar activamente con los procesos de monitoreo y control, para lograr que nuestra información esté debidamente asegurada**, debemos monitorear de forma continua el cumplimiento de nuestras políticas procedimientos, y de los principios que acá describimos.

5 POLITICAS ESPECIFICAS DE SEGUIRDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Políticas de seguridad de la información y ciberseguridad definidas en las compañías, las cuales son de estricto cumplimiento por todos los colaboradores, proveedores y contratistas que tengan acceso a la información e infraestructura tecnología, así:

5.1 Política de Control de Acceso

Definir las pautas generales para asegurar un acceso seguro y controlado a la información de Las Compañías, impidiendo los accesos no autorizados.

5.2 Política de Asignación de Contraseñas

Implementar la seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización, usando claves fuertes y como mínimo 2MFA.

5.3 Política de Respaldo de información

Definir las pautas generales para garantizar en Las Compañías la ejecución, preservación, mantenimiento y verificación de copias de respaldo de la información.

El respaldo de la información busca reducir los impactos de los riesgos generados por la pérdida de información y es un mecanismo para soportar los planes de contingencia, recuperación ante desastres y atención a incidentes de seguridad de la información adoptados por Las Compañías.

5.4 Política de Eliminación y Destrucción de Medios

Asegurar la disposición final segura de todos los elementos o dispositivos que contengan información de Las Compañías, cuando se den de baja o sean reutilizados.

5.5 Política Transferencia de Información

Mantener la seguridad de la información cuando se autoriza el intercambio de esta dentro de Las Compañías y con cualquier entidad externa

5.6 Política de Adquisición, Desarrollo y Mantenimiento de Software

Asegurar que el software sea adquirido con los controles de seguridad requeridos en la protección de la integridad y confidencialidad de la información.
Asegurar que únicamente Gerencia de Innovación y Transformación Digital adquiere software y/o aprueba cualquier compra relacionada.

5.7 Política de Gestión de Cambios

Garantizar que los cambios sobre la infraestructura de tecnología de información, los servicios por terceras partes, políticas, controles y comunicaciones en Las Compañías se realicen e implementen adecuadamente siguiendo políticas estándar.

5.8 Política de Uso de correo Electrónico

Definir las pautas generales para asegurar una adecuada protección de la información de Las Compañías cuando se usa el servicio de correo electrónico por parte de los usuarios autorizados.

5.9 Política de Uso de Servicios de Acceso a Internet.

Definir las pautas generales para asegurar una adecuada protección de la información de Las Compañías en el uso del servicio de Internet por parte de los usuarios autorizados.

5.10 Política de Antimalware

Definir las pautas generales para asegurar una adecuada protección de la información de Las Compañías contra software malicioso.

5.11 Política Uso de Dispositivos Móviles

Garantizar la seguridad de la información cuando se utilizan dispositivos móviles en las Instalaciones de Las Compañías o cuando se usan para tener acceso a sistemas de información o servicios de procesamiento de información, aunque no se encuentren dentro de instalaciones de ODL.

5.12 Política de Uso Aceptable de Activos

Definir las pautas generales para asegurar un adecuado uso y administración de los activos informáticos de Las Compañías por parte del personal a cargo de su administración.

5.13 Política Escritorio y Pantalla limpia

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida o daño de la información disponible de los puestos de trabajo durante y fuera del horario trabajo normal de los empleados, contratistas y terceros que prestan sus servicios a Las Compañías.

5.14 Política de Seguridad de Proveedores

Seguridad de la información para relaciones con proveedores, contratistas y terceros Mantener la seguridad de la información y los servicios de procesamiento de información a los cuales tienen acceso los proveedores, contratistas o terceros que prestan sus servicios a Las Compañías.

5.15 Política Tratamiento de Datos Personales

En cumplimiento a lo dispuesto en la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 de 2013 sobre protección de datos personales, las compañías establecen la política de tratamiento de datos personales con el propósito de que todas las personas puedan conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en las bases de datos o archivos a cargo de las compañías.

5.16 Política de Teletrabajo

Esquema acordado formalmente entre el empleado y el empleador para trabajar en un ligar diferente a la oficina, pero garantizando con los mínimos principios de seguridad.

5.17 Política de Seguridad en la Nube

La correcta implementación de servicios de información en la Nube reducirá el riesgo de que se presenten incidentes de seguridad que afecten a las compañías y generen un daño irreparable.

5.18 Política de Gestion de Riegos de Seguridad de la Información

Orientado a gestionar de manera eficaz los riesgos de seguridad de la información asociados a los activos de información en los diferentes procesos.

5.19 Política de Uso de Controles Criptográficos

Permite la adopción de algoritmos criptográficos fuertes y que aún no son vulnerables.

5.20 Política de Incumplimiento de la Política de Seguridad de la Información y Ciberseguridad

Acciones correctivas, disciplinarias o legales en caso del incumplimiento de las políticas de seguridad de la información y ciberseguridad.

El detalle de los lineamientos se encuentra en el Manual de Políticas de Seguridad de la Información y Ciberseguridad TI-M-003

6 ESTRUCTURA DE GOBIERNO

A continuación, describimos la estructura de gobierno de seguridad de la información y ciberseguridad definida por las Compañías:

6.1 JUNTA DIRECTIVA - COMITÉ DE AUDITORÍA

- Supervisa la adecuada gestión de riesgos de seguridad de la información y ciberseguridad.

6.2 PRESIDENTE

- Aprueba la política de seguridad de la información y ciberseguridad TI-P-001.

6.3 GERENTE DE INNOVACIÓN & TRANSFORMACIÓN DIGITAL

- Revisa y aprueba las políticas y las funciones generales en materia de seguridad de la información y ciberseguridad descritas en el Manual de Políticas de Seguridad de la Información y Ciberseguridad TI-M-003.
- El área de operación y ciberseguridad se ejecutan los lineamientos definidos.

6.4 LÍDERES O DUEÑOS DE PROCESO

Asegurar el conocimiento y cumplimiento de las políticas, procedimientos y directrices de seguridad de la información y ciberseguridad, por parte de terceros contratados que cuentan con acceso a la infraestructura tecnológica de las Compañías, para lo cual debe:

- Asegurar que en los documentos contractuales se incluyan la obligatoriedad de cumplir con las políticas, directrices y requerimientos de seguridad de la información establecidas por las Compañías.
- Asegurar que los terceros son informados y entrenados en los aspectos de seguridad relevantes de acuerdo con la labor que van a cumplir y el nivel de acceso que tendrán a la información de las Compañías.
- Asegurar la identidad de las personas a quienes les será dado acceso a las instalaciones y la información de las Compañías.
- Documentar y aprobar los privilegios de acceso que se asignarán a los usuarios.
- Retirar los privilegios de acceso asignados a los terceros, de manera inmediata cuando ya no los requieran para cumplir con sus funciones.

6.5 LIDER DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Monitorear que los dueños de proceso y gestores de contratos vigilen y hagan cumplir las políticas, procedimientos y directrices de seguridad de la información y ciberseguridad, por parte de terceros contratados.
- Proponer buenas prácticas de seguridad y ciberseguridad para los diferentes componentes de la infraestructura tecnológica.

6.6 COLABORADORES, CONTRATISTAS Y TERCEROS

Todos los colaboradores, contratistas y terceros con acceso a la información de las Compañías son responsables de:

- Cumplir de manera obligatoria con las políticas y directrices establecidas por las Compañías en materia de seguridad de la información y Ciberseguridad.

El detalle de los responsables se encuentra en el Manual del Sistema de Gestión Seguridad de la Información.

7 DOCUMENTO RELACIONADOS

TI-M-003 Manual Sistema de Gestión de Seguridad de la Información.

8 TABLA DE VERSIONES Y CAMBIOS

Versión	Fecha	Cambios
1	**19/12/2012**	Creación del documento
2	**01/12/2014**	Se actualiza el documento
3	**23/03/2018**	Se actualiza el documento
4	**18/12/2020**	Se actualiza el documento
5	**07/10/2022**	Se actualiza el objetivo, el alcance y la descripción de la política
6	**10/04/2023**	Se actualiza la política para dar alcance a TO y la inclusión de políticas adicionales.

Elaboró	Revisó	Aprobó
DS WASR DocuSigned by: William Garzon C62EBB29666D495... **William Garzón Hernández** Especialista de Operaciones e Infraestructura Digital	DocuSigned by: Gustavo Adolfo Cordoba Ortiz 2F1AB3DDEBB7488... **Gustavo Adolfo Córdoba Ortiz** Gerente de Innovación & Transformación Digital	DocuSigned by: 61871B8C54E44F0... **Alejandro Pinzón Pinzón** Presidente
10/04/2023	**10/04/2023**	**10/04/2023**