POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD INDUSTRIAL

FRONTERA ENERGY Y SUBSIDIARIAS ("FRONTERA" o la "CORPORACIÓN")

1. ANTECEDENTES

La Política de Seguridad de la Información y Ciberseguridad Industrial (la "**Política**") es un marco de actuación que tiene como objetivo, a nivel de seguridad de la información, proteger la información estratégica y los activos relacionados con la creación, procesamiento, almacenamiento, transmisión, eliminación o destrucción de la misma; y a nivel de ciberseguridad industrial, proteger los receptores de riesgo (negocio, reputacional, relacionamiento y seguridad, salud y medio ambiente).

La necesidad de interconexión entre los dispositivos electrónicos industriales y los sistemas de información empresarial, así como la adopción en los Sistemas de Control y Automatización Industrial (IACS) de tecnologías abiertas de uso común en ambientes de Tecnologías de la Información (IT), generan nuevos riesgos de ciberseguridad que hace algún tiempo no existían. Las consecuencias de la materialización de estos riesgos podrían provocar no solo pérdida de producción con impactos financieros, sino también impactos ambientales y afectación a la salud de las personas. Lo anterior tiene una incidencia directa en el cumplimiento de objetivos estratégicos y continuidad operativa de la Organización.

Los activos de la información incluyen, pero no se limitan a: procesos, información (electrónica, física y cualquier otro tipo de información que provenga de medios no convencionales), personas, hardware, software, propiedad intelectual, bases de datos, servicios, información no estructurada y sistemas de control.

2. DECLARACIÓN DE LA POLÍTICA

2.1. SEGURIDAD DE LA INFORMACIÓN

Frontera reconoce la información como un activo de vital importancia para el negocio, permitiendo el logro de sus objetivos y manteniendo su ventaja competitiva, por lo tanto, se deben generar los mecanismos necesarios para protegerla garantizando su integridad en el tiempo.

La información, a través de su ciclo de vida, debe estar disponible, sin ambigüedad y catalogada de manera consistente de acuerdo con su valor, importancia y con la privacidad que demanda su naturaleza.

La política de Seguridad y los Lineamientos que la soportan, definen los siguientes principios básicos:

- Generamos una cultura orientada al uso seguro de la información y de los medios que la soportan por parte de los empleados, contratistas y terceros, a través del fortalecimiento del conocimiento y del desarrollo de competencias que permitan mitigar los riesgos de ciberseguridad; así como, el fortalecimiento de las capacidades técnicas necesarias.

- Desde la Gerencia Senior de ITS y la Gerencia de Seguridad de la Información, desarrollamos en colaboración con todas las áreas de la Corporación, procesos de gestión de riesgos que nos permitan identificar y evaluar las diferentes amenazas y vulnerabilidades a las que puede estar expuesta la información, incluyendo la plataforma tecnológica y los sistemas de control industrial. Como resultado se definen e implementan medidas de control y tratamiento que apoyen el logro de los objetivos de la Corporación.

- Promovemos el uso adecuado de los recursos tecnológicos suministrados por Frontera, los cuales deben ser utilizados únicamente para cumplir con la finalidad para la cual han sido asignados; dichos recursos deberán ser utilizados de tal forma que se protejan derechos de autor y propiedad intelectual y en ningún caso podrán ser utilizados para cualquier actividad ilegal o que no estén en línea con nuestros valores corporativos. Adicionalmente, Frontera se reserva el derecho de acceder a los activos corporativos y a los servicios tecnológicos proveídos por la Corporación.

- Cumplimos con todas las leyes, regulaciones y requisitos contractuales, así como con los lineamientos internos establecidos para el manejo de la información confidencial y/o información personal garantizando su integridad, confidencialidad y acceso solo a personal autorizado.

- Todos los directores, funcionarios, empleados (temporales, término fijo o permanentes), consultores, contratistas, subcontratistas, aprendices, staff de asignación temporal, tele-trabajadores, pasantes, o cualquier otra persona que trabaje para Frontera (En adelante "**Personal de Frontera**") , indistintamente de su ubicación, deben mantener discreción al momento de hablar acerca de su actividad laboral en Frontera, especialmente al encontrarse en sitios públicos o rodeados de personas que no deben tener acceso a este tipo de información.

- Para la prestación de servicios de los contratistas, subcontratistas o terceros de Frontera Energy, deben cumplir con el A-SCM-CC-007 ANEXO de Seguridad de la Información y las cláusulas de confidencialidad definidas en los contratos.

- Los proyectos desarrollados por la Corporación, que afecten la seguridad de la información o las plataformas tecnológicas o de misión crítica, desde sus etapas iniciales, deben incluir la evaluación de aspectos relacionados con la arquitectura de seguridad de la información siguiendo los lineamientos definidos.

- Frontera tiene definidos mecanismos de monitoreo y control con el fin de minimizar los impactos derivados de incidentes de Seguridad de la Información. Todo Personal de Frontera

debe reportar los Incidentes de Seguridad de la Información o Ciberseguridad, eventos sospechosos, incumplimientos normativos y el mal uso de activos que este identifique y que puedan afectar a la Corporación.

- Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, impulsado por la Alta Dirección.

2.2. CIBERSEGURIDAD INDUSTRIAL

En Frontera Energy estamos comprometidos con la ciberseguridad industrial con el fin de proteger los receptores de riesgo (negocio, reputacional, relacionamiento y seguridad, salud y medio ambiente) frente a las potenciales consecuencias que pueden ocasionar los Sistemas de Control y Automatización Industrial (IACS) de los procesos industriales de Frontera Energy ante un evento cibernético. Para el desarrollo de este propósito Frontera Energy, establece esta política para definir los objetivos que debe seguir el Programa de Ciberseguridad Industrial, los cuales se describen a continuación:

- Asegurar la efectividad de la gestión del riesgo cibernético industrial, mitigando el riesgo y manteniéndolo en un estado aceptable.
- Crear y mantener una cultura sólida del riesgo cibernético industrial.
- Aplicar normas internacionales para mitigar el riesgo cibernético industrial.[1]
- Implementar proyectos de automatización cumpliendo el Gobierno de Sistemas Industriales

3. ALCANCE Y SEGUIMIENTO

La presente política tiene como alcance la protección de todos los activos de información y de la infraestructura de misión crítica de los diferentes campos de producción de Frontera, con el fin de garantizar que los riesgos de Seguridad de la Información y de Ciberseguridad sean gestionados de forma estructurada y adaptable a los cambios del entorno tecnológico y de negocio. Así mismo, esta política es de obligatorio cumplimiento para todo el personal, contratistas, subcontratistas o terceros de Frontera indistintamente de su ubicación.

La junta directiva de la Corporación (la "**Junta Directiva**") es el órgano responsable de la aprobación de la misma, la cual será revisada por la Gerencia de Seguridad de la Información a intervalos programados para identificar oportunidades de mejora. Revisiones no programadas serán llevadas a cabo como consecuencia de cambios relevantes en las prácticas de negocio, cambios en la infraestructura tecnológica y/o en el proceso industrial, o debido a nuevos requerimientos legales o normativos, que impactan la Seguridad de la Información o la ciberseguridad industrial.

4. CUMPLIMIENTO

Ante el incumplimiento, Frontera Energy se reserva el derecho de aplicar medidas disciplinarias y sanciones definidas en la Ley Laboral, Reglamento Interno de Trabajo, Código de Conducta y

[1] *Normas internacionales corresponden a la aplicación de ISA / IEC -62443 Industrial Cybersecurity.*

Ética Corporativa, o lo definido en los términos y condiciones de los contratos establecidos con Personal de Frontera. Ver anexo A.

Todos los vicepresidentes, Directores y Gerentes Senior son los responsables de asegurar el cumplimiento de la Política de Seguridad de la Información al interior de sus equipos.

5. VIGENCIA

Esta Política está sujeta a la aprobación de la Junta Directiva de Frontera, quien será responsable de su mantenimiento y revisión periódica. La revisión más reciente de esta Política fue aprobada el 5 de diciembre de 2023.

ANEXO A. REGLAS CLAVES PARA EL CUMPLIMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta la evolución tecnológica, la facilidad en el manejo de la información y el desarrollo del trabajo colaborativo; la confidencialidad e integridad de la información toma mayor relevancia y es responsabilidad de cada colaborador de Frontera evitar riesgos que puedan impactar a la organización en su reputación o en la pérdida de información.

Recordamos que como usuarios de la información y de las plataformas tecnológicas proveídas por Frontera, se deben tener en cuenta como mínimo las siguientes reglas:

1. No usar soluciones tecnológicas que requieran licenciamiento, sin la previa autorización de ITS. Toda licencia debe estar autorizada por la compañía y gestionada por ITS.
2. No entregar o publicar, bajo ningún concepto, información confidencial o de uso interno de la compañía a terceros sin la debida aprobación. Por ejemplo, bases de datos con información personal, proyectos en curso, información financiera reservada, imágenes corporativas, entre otros.
3. Uso inadecuado de dispositivos externos que puedan poner en riesgo la seguridad de la información tales como USB, discos duros externos.
4. No se permite el préstamo de las claves de acceso a la red o a los sistemas de información corporativos.
5. No compartir espacios virtuales de trabajo con personal no autorizado. Así mismo, se prohíbe almacenar información de manera local en los equipos corporativos y compartir información en nubes personales tales como Dropbox, One Drive y Google Drive personales.
6. Ser cauteloso frente a correos, páginas, mensajes o redes externas que puedan exponer a la compañía a un ataque cibernético.

7. Los permisos asignados sobre la información corporativa son responsabilidad de cada usuario quien debe garantizar el acceso y uso adecuado de esta información.

Para el cumplimiento de las reglas relacionadas anteriormente, todo colaborador cuenta con el apoyo de la Gerencia de Seguridad de la Información, quienes guiarán en la gestión de las mismas.

No obstante, por lo anterior, recordamos que estas reglas son de obligatorio cumplimiento y su no atención puede generar la aplicación de medidas disciplinarias y sanciones, definidas en la Ley Laboral, en el Reglamento Interno de Trabajo y en el Código de Conducta y Ética Corporativa.