POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD INDUSTRIAL

SABANA RESOURCES ("SABANA" o la "COMPAÑIA")

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 esta; y a nivel de ciberseguridad industrial, proteger los receptores de riesgo (negocio, reputacional, relacionamiento y seguridad, salud y medio ambiente).

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 industrial.

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. 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 Compañía.

2. DECLARACIÓN DE LA POLÍTICA

2.1. SEGURIDAD DE LA INFORMACIÓN

Sabana 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 confidencialidad, integridad y disponibilidad en el tiempo.

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

La política de Seguridad de la Información & Ciberseguridad Industrial y los lineamientos que la soportan, definen los siguientes principios básicos:

- Generamos una cultura orientada al uso responsable y 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. Sabana establecerá y comunicará los roles, responsabilidades, niveles de autoridad y mecanismos de rendición de cuentas relacionados con la seguridad de la información y la ciberseguridad industrial. Los propietarios de procesos, información, riesgos, plataformas y sistemas industriales serán responsables de identificar, tratar, aceptar y monitorear los riesgos dentro de los niveles autorizados por la Compañía.

- Desde la Gerencia Digital y el área de Seguridad de la Información, desarrollamos en colaboración con todas las áreas de la Compañía, 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. Los riesgos de seguridad de la información y ciberseguridad industrial deberán ser gestionados de acuerdo con el apetito y la tolerancia al riesgo definidos por la Compañía. Toda aceptación de riesgo residual deberá estar documentada, contar con un responsable, incluir una fecha de revisión y ser aprobada por el nivel de autoridad correspondiente. Como resultado se definen e implementan medidas de control y tratamiento que apoyen el logro de los objetivos de la Compañía.

- Promovemos el uso adecuado de los recursos tecnológicos suministrados por Sabana, 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 los 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, Sabana se reserva el derecho de acceder a los activos corporativos y a los servicios tecnológicos proveídos por la Compañía.

- 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.

- Estamos comprometidos con aprovechar las oportunidades que las tecnologías emergentes ofrecen para mejorar nuestra eficiencia, seguridad y sostenibilidad, siempre respetando los valores fundamentales que nos caracterizan como empresa. En este sentido, nos proponemos guiar el uso de estas tecnologías en nuestras operaciones, asegurando que se alineen con nuestra estrategia, objetivos y código de conducta, los cuales están fundamentados en principios de ética, transparencia, privacidad, equidad y supervisión humana. Es fundamental que nuestros usuarios velen por el uso responsable de estas herramientas, garantizando que se empleen de acuerdo con nuestra cultura organizacional y respetando los lineamientos de Seguridad de la Información corporativa para proteger los activos e intereses de la Compañía.

- El uso de Inteligencia Artificial se realizará de manera responsable y segura, asegurando la protección de la privacidad, la mitigación de riesgos asociados a sesgos y la transparencia en los procesos automatizados. Nos orientamos por estándares reconocidos internacionalmente, como ISO 42001, ISO/IEC 23894, ISO 27001 y las normativas de protección de datos aplicables, que sirven como referencia para garantizar buenas prácticas en su adopción. Además, se asegurará la supervisión humana en la toma de decisiones críticas, evitando impactos negativos en la equidad y

asegurando que la tecnología se utilice conforme a los principios éticos y la cultura organizacional de la Compañía.

- Todo el personal vinculado a Sabana —incluyendo directores, funcionarios, empleados (temporales, a término fijo, pasantes o permanentes), consultores, contratistas, subcontratistas, aprendices, personal en asignación temporal, teletrabajadores y cualquier otra persona que preste servicios para la compañía (en adelante, "Personal de Sabana")—, sin importar su ubicación, debe actuar con discreción al referirse a asuntos relacionados con su actividad laboral. Esta precaución es especialmente importante en espacios públicos o en presencia de personas ajenas que no deben tener acceso a información confidencial.

- Los contratistas, subcontratistas o terceros de Sabana Resources, deben cumplir con el A-SCM-CC-007 Anexo de Seguridad de la Información, las cláusulas los acuerdos de confidencialidad y las cláusulas definidas en los contratos. La Compañía podrá realizar una valoración de riesgos y/o evaluaciones a sus proveedores con el objetivo de conocer su ambiente de control con respecto a lo relacionado con Ciberseguridad. Se deberá establecer obligaciones de ciberseguridad, privacidad, continuidad, notificación de incidentes, gestión de subcontratistas, derecho de verificación y devolución o eliminación segura de la información.

- Todos los proyectos que involucren información corporativa, plataformas tecnológicas o sistemas críticos deberán, desde sus etapas tempranas, seguir los lineamientos establecidos en esta política y mantenerse alineados con el proceso de Seguridad de la Información. Esta alineación incluye la incorporación de prácticas y controles definidos para garantizar la protección de los activos, la integridad de la arquitectura y el cumplimiento de los estándares corporativos. Sabana mantendrá inventarios actualizados de información, hardware, software, servicios, identidades, componentes industriales, conexiones, medios y proveedores tecnológicos. Cada activo deberá contar con un propietario, una clasificación, un nivel de criticidad y controles acordes con el riesgo asociado.

- Sabana ha definido mecanismos de monitoreo y control con el fin de minimizar los impactos derivados de incidentes de Seguridad de la Información. Sabana mantendrá capacidades para preparar, detectar, analizar, contener, investigar, comunicar y recuperar incidentes de seguridad de la información y ciberseguridad industrial. Todo Personal de Sabana debe reportar los Incidentes de Seguridad de la Información o Ciberseguridad, eventos sospechosos, incumplimientos normativos y/o el mal uso de activos que este identifique y que puedan afectar a la Compañía.

- Estamos comprometidos con 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 Sabana Resources 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 Sabana Resources ante un evento cibernético. Para el desarrollo de este propósito La Compañía, 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, estándares y buenas prácticas internacionales para mitigar el riesgo cibernético industrial.[1]
- Implementar proyectos de automatización cumpliendo el Gobierno de Sistemas Industriales
- Utilizar nuevas tecnologías tales como inteligencia Artificial en sistemas para de detección de intrusiones, segmentación de red y alertas automatizadas.

3. ALCANCE Y SEGUIMIENTO

Esta política está diseñada para proteger todos los activos de información y la infraestructura crítica de los sistemas de control y automatización en los distintos campos de producción de Sabana. Su aplicación es de obligatorio cumplimiento para todos los empleados, contratistas, subcontratistas o terceros de Sabana Resources indistintamente de su ubicación.

La junta directiva de la Compañía (la "**Junta Directiva**") es el órgano responsable de la aprobación de esta, la cual será revisada por la Gerencia Digital y el área 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, monitoreo y supervisión en cada etapa del ciclo de vida de modelos de Inteligencia Artificial o debido a nuevos requerimientos legales o normativos, que impactan la Seguridad de la Información o la ciberseguridad industrial.

4. CUMPLIMIENTO

Todos los vicepresidentes, directores y gerentes senior son los responsables de asegurar el cumplimiento de la Política de Seguridad de la Información y ciberseguridad industrial al interior de sus equipos.

La Gerencia Digital es la responsable de asegurar el cumplimiento de esta política en la plataforma tecnológica actual e implementación de nuevas tecnologías o soluciones mediante procesos de auditoria o análisis de riesgos.

Ante el incumplimiento, Sabana Resources se reserva el derecho de aplicar medidas disciplinarias y sanciones definidas en la Ley Laboral, Reglamento Interno de Trabajo, Código de Conducta y Ética Corporativa, o lo definido en los términos y condiciones de los contratos establecidos con Personal de Sabana. Ver anexo A

5. VIGENCIA

Esta Política está sujeta a la aprobación de la Junta Directiva de Sabana Resources, quien será responsable de su mantenimiento y revisión periódica.

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

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

Teniendo en cuenta la evolución tecnológica, la facilidad en el manejo de la información y el desarrollo del trabajo colaborativo; la confidencialidad, integridad y disponibilidad de la información toma mayor relevancia y es responsabilidad de cada colaborador de Sabana 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 proporcionadas por Sabana Resources, se deben tener en cuenta como mínimo las siguientes reglas, sin limitarse a ellas:

1. No usar soluciones tecnológicas, sin la previa autorización del área de Seguridad de la Información. Toda licencia o agente de modelos de inteligencia artificial debe estar autorizada por la Compañía y gestionada por el área Digital.
2. Es obligatorio realizar el correcto etiquetado de todo documento generado por medio de la plataforma ofimática para tener el control e inventario de todos los documentos corporativos con su respectiva criticidad.
3. 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.
4. Uso inadecuado de dispositivos externos que puedan poner en riesgo la seguridad de la información tales como USB, discos duros externos.
5. No se permite el préstamo de las claves de acceso a la red o a los sistemas de información corporativos.
6. 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, WeTransfer, One Drive o Google Drive personales.
7. Ser cauteloso frente a correos, portales web de dudosa procedencia, mensajes o redes externas sospechosos o de carácter malicioso que puedan exponer a la Compañía a un ataque cibernético.
8. Los permisos asignados sobre la información corporativa son responsabilidad de cada usuario quien debe garantizar el acceso, protección y uso adecuado de esta información.
9. No se permite compartir información de uso interno y/ o sensible en herramientas de IAcomo ChatGPT, Gemini o similares, los datos usados en estas herramientas deben estar anonimizados para minimizar los riesgos de exposición. La Compañía solamente cuenta con la herramienta Microsoft Copilot autorizada bajo un marco de uso ético.
10. No se permite el uso de herramientas de comunicación unificada (Chat, videoconferencia, llamadas) diferentes al de Microsoft Teams.
11. No se permite el uso del computador corporativo en conexión Wireless públicas o sin contraseña.
12. No se permite realizar descarga de información corporativa en equipos de cómputo personal o no administrado por la organización

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

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.