1. OBJETIVO GENERAL

Asegurar el conocimiento de todo el personal de la organización, terceros, contratistas, proveedores y todas aquellas personas que tengan acceso a la información de Enlace Operativo, de las directrices y mecanismos que se deben cumplir y utilizar para proteger los activos de información de la Compañía y de sus clientes, con el propósito de preservar la integridad, confidencialidad y disponibilidad de la información, garantizando la viabilidad y sostenibilidad del negocio en el largo plazo.

2. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- Desarrollar el negocio bajo unas condiciones razonables de seguridad y de administración de la información.

- Promover una cultura permanente en seguridad de la información en todos los niveles y con partes interesadas, que permita incrementar los controles, identificar riesgos e incidentes y garantizar la confidencialidad, integridad y disponibilidad de la información.

- Cumplir los requisitos legales y de seguridad de la información aplicables al Core del negocio.

- Minimizar los riesgos de los procesos misionales de la organización.

- Garantizar la continuidad del negocio frente a incidentes.

3. ALCANCE

La Política de la información aplica a:

- Todos los empleados de la compañía.

- Todos los activos de información durante su ciclo de vida, incluyendo creación, adquisición, distribución, transmisión, almacenamiento y/o eliminación; en todas sus formas: física, electrónica, intangible, impresa, escrita, reproducida y hablada; y en todos los ambientes en los cuales ésta reside, para asegurar que los activos de información que se encuentran en lugares externos (otros países y ciudades, proveedores de servicios, asesores, etc.) estén sometidos a controles equivalentes para su protección.

- Todas las terceras partes, contratistas o proveedores, que manejen información relevante para el negocio.

- La política se da a conocer a todas las instancias anteriores o cualquier parte interesada que manipule, intercambié o comparta información con la compañía.

4. INTRODUCCIÓN

ENLACE OPERATIVO consciente de la importancia de proteger los activos de información que soportan la operación y continuidad del negocio frente a los riesgos que puedan afectar su seguridad, establece políticas, responsabilidades y procedimientos de seguridad donde se definen los lineamientos y directrices a seguir.

Es por ello por lo que ENLACE OPERATIVO declara la seguridad de la información y la ciberseguridad como dos aspectos fundamentales para el logro de sus objetivos estratégicos. En desarrollo de lo anterior, la alta dirección se compromete con la protección, mejora continua y el aseguramiento de la información que gestionan física y digitalmente de las partes interesadas, teniendo en cuenta la confidencialidad, integridad y disponibilidad de esta, a través de los procesos y el uso de recursos tecnológicos y de información.

El presente documento describe la Política General de Seguridad de la Información y Ciberseguridad en ENLACE OPERATIVO, la cual se basa en estándares, buenas prácticas y normativas aplicables. Esta política es definida y aprobada por la Gerencia de Producto y TI, y es la base para definir la metodología de riesgos, implantación de controles y toma de decisiones de Seguridad de la Información y Ciberseguridad.

---

[1] Entiéndase por partes interesadas o Stakeholders: Clientes, Proveedores, Asesores, Accionistas, Miembros de Junta, Comité de Auditoría de Junta, Revisoría Fiscal, Entes Reguladores (Ministerio de la Protección Social, Ministerio de Comercio, Industria y Turismo, Superintendencia Financiera de Colombia), Gobierno Nacional, Gremios, Competencia, Grupo SURA.

5. POLÍTICAS GENERALES

- Los empleados son responsables de garantizar la implementación de las directrices de seguridad de información (sensible, personal y confidencial de todas las partes) y de cumplir con las responsabilidades asignadas frente a las mismas en todo momento, tanto internamente como de cara a proveedores y clientes.

- Todas las partes interesadas son responsables de implementar los controles de seguridad definidos, garantizando la confidencialidad, integridad y disponibilidad de la información y activos de información que le sean asignados. Por lo tanto, es responsabilidad del líder, al interior de ENLACE OPERATIVO, de dicho contrato, garantizar la divulgación de esta información y validar la aplicación de estas políticas por los terceros a su cargo.

- Cada líder de proceso es responsable de garantizar la implementación de las Políticas de Seguridad de la información con su grupo de colaboradores, realizar seguimiento y establecer los correctivos que sean necesarios para preservar la seguridad de los activos de información asignados.

- La información que se almacena y transporta por medios electrónicos o físicos debe adecuarse a los modelos de seguridad definidos para la misma.

- El Plan de Continuidad de Negocio es implementado, monitoreado y analizado permanentemente por parte del Comité de Administración de Crisis (CAC) o en su defecto el Comité de Continuidad (CC).

- Todas las terceras partes son responsables de informar a su líder directo o al responsable del proceso respectivo los eventos o incidentes de seguridad, ciber amenazas y/o ciberataques que se presenten, para establecer las acciones necesarias que disminuyan la probabilidad de ocurrencia de estos en los procesos críticos del negocio.

- Todos los empleados deben dar cumplimiento a lo establecido en la cláusula de Seguridad de la información y los lineamientos de seguridad de la información estipulados desde la contratación. Cualquier incumplimiento en la protección de datos sensibles de nuestros empleados, clientes, proveedores o cualquier otro tercero a la que podamos tener acceso, se interpondrán sanciones de acuerdo con lo establecido por el Reglamento interno de trabajo y/o establecido por la ley de Protección de datos.

- Todos los empleados de la Compañía que laboren en instalaciones de terceros (clientes) se acogerán a las políticas definidas, planes de emergencia, planes de continuidad y temas relacionados con seguridad de la información y salud en el trabajo que estén establecidos en dichas instalaciones, según lo descrito en la guía Gestión de la Continuidad de Negocio, cumpliendo a su vez con la política de seguridad de ENLACE OPERATIVO, teniendo en cuenta que los temas o conceptos que no sean regulados o exigidos por el cliente, pero estén normados o definidos por ENLACE OPERATIVO, deberá cumplir la política más estricta.

- La Política de Seguridad de la Información, los lineamientos se basan en el estándar ISO 27001 (anexo A), circular externa 007 de 2018 y demás prácticas de seguridad adoptadas por la Compañía, teniendo en cuenta los diferentes objetivos, dominios y controles necesarios y aplicables a nuestra organización.