POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

SURA COLOMBIA

Gobierno y Arquitectura de TI

Información de responsables

	Fecha (dd/mm/aaaa)	Nombre	Cargo
Elaborado por:	19/05/2016	Kristin Bustos Morón Idárraga David Alberto Garavito Murcia	Analista de Riesgos y Ciberseguridad Analista de Riesgos y Ciberseguridad
Revisado por:	14/04/2025	Juan Felipe Gómez Trujillo	Director Control Interno y Riesgos de TI
Aprobado por:	15/09/2025	Consultoría en Gestion de Riesgos Suramericana S.A.S	Asamblea General de Accionistas

Control de Cambios

Versión	Autor	Descripción del cambio	Fecha
1	Kristin Bustos Morón Idárraga David Alberto Garavito Murcia	Creación y definición de documento	19/05/2016
2	Natalia Álvarez Agudelo Leidy Tatiana Velez Londoño	Reasignación de responsabilidad a Gerencia de Tecnología e incorporación de cumplimiento normativo de la SFC CE007 de 2018	30/01/2019
3	Sandra Milena Castaño Ramírez Christian Soto Parra	Actualización del alcance y elementos generales presentes en el documento Revisión anual	13/10/2023
4	Anibal Alejandro Alvarez Galvis	Actualización de estándares de seguridad (ISO 27001:2022, NIST CSF 2.0). Enfoque más amplio en gestión del riesgo según perfil y contexto. Ajustes al rol de Alta Gerencia, alineado con apetito de riesgo. Refuerzo en actualización y madurez del sistema de gestión.	20/11/2024

Aprobaciones		
Fecha (dd/mm/aaaa)	**Órgano**	**Número de Acta**
18/03/2019	Asamblea General de Accionistas	40
15/09/2025	Asamblea General de Accionistas	57

1. Objetivo

SURA en desarrollo de sus principios: responsabilidad, respeto, transparencia y equidad, determinan la información como uno de los activos más importantes; por lo tanto, declara la seguridad de la información[1] y la ciberseguridad[2] como dos aspectos fundamentales para el logro de sus objetivos estratégicos. En desarrollo de lo anterior, se comprometen con la protección 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 sus partes interesadas[3], procesos y el uso de recursos tecnológicos y de información.

Contempla prácticas exitosas incorporadas a partir de estándares internacionales de seguridad de la información y ciberseguridad[4] que la organización ha seleccionado para su cumplimiento o referencia, así como lineamientos externos definidos por los diferentes entes de vigilancia y control que regulan nuestras actividades.

2. Alcance

Esta Política General de Seguridad de la Información y Ciberseguridad es de cumplimiento obligatorio para todas las partes interesadas que tengan acceso a la información de la

[1] Seguridad de la información: Conjunto de medidas técnicas, organizacionales y legales que permiten a las Compañías asegurar la confidencialidad, integridad y disponibilidad de la información en los procesos y en las tecnologías que la soportan.

[2] Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los activos de información en el ciberespacio que son esenciales para la operación de la organización.

[3] Partes interesadas: Empleados, proveedores, subcontratistas, terceros, clientes, accionistas, asesores, filiales y subsidiarias.

[4] Los estándares internacionales de Seguridad vigentes a la fecha de elaboración de esta política son: ISO 27001:2022 y complementarias, NIST Cybersecurity Framework 2.0.

compañía, con la finalidad de evitar la pérdida, modificación o divulgación no autorizada, acceso no autorizado y proteger la información de todos los riesgos a los que pueda ser expuesta.

3. Aplicabilidad

Aplica para Consultoría en Gestión de Riesgos Suramericana S.A.S, en adelante *La Compañía.*

4. Contenido del documento

LINEAMIENTOS GENERALES

1. Esta política general se desarrolla a través de un marco de actuación de seguridad de la información y ciberseguridad compuesto por directrices, manuales, procesos, procedimientos e instructivos y estándares, entre otros documentos vinculantes que la complementan.
2. Para la gestión adecuada del riesgo de seguridad de la información y ciberseguridad, la compañía se apoyará de metodologías, herramientas, conocimientos, procesos o procedimientos que disminuyan la probabilidad o el impacto de este, de acuerdo con perfil de riesgo, el plan de negocio, la naturaleza, el tamaño, el tipo de información y la complejidad de las actividades que desarrollen, así como con el entorno y los mercados en los que operan.
3. Deberá existir alineación entre los objetivos de la organización y el marco normativo de seguridad de la información y ciberseguridad de La Compañía.
4. Todas las personas con acceso a la información de La Compañía deberán actuar bajo el marco de actuación de seguridad de la información.
5. Todas las personas que acceden a la información de La Compañía son responsables de aplicar los controles necesarios para evitar la pérdida, modificación o divulgación no autorizada, acceso no autorizado y proteger la información de todos los riesgos de seguridad de la información y ciberseguridad a los que pueda ser expuesta.

ROLES Y RESPONSABILIDADES

1. La Junta Directiva, o el órgano que haga sus veces, según corresponda, será la encargada de promover y aprobar los lineamientos frente a la gestión de ciberseguridad y seguridad de la información y los riesgos asociados a estas, incluyéndolos en los planes estratégicos de La Compañía y garantizando la disponibilidad de los recursos que se requieran para el efecto.

2. La Alta Gerencia promoverá una cultura de seguridad de la información y ciberseguridad a todas las partes interesadas, traduciendo la estrategia definida por la Junta Directiva en mecanismos efectivos para que el marco normativo de seguridad sea asimilado e incorporado en el accionar de La Compañía.
3. La Alta Gerencia designará roles y responsabilidades adecuados para la implementación del sistema de gestión de seguridad de la información y la gestión efectiva de los riesgos de seguridad de la información y ciberseguridad, con el personal idóneo y con capacidad decisoria para ejecutar las actividades que se requieran.
4. El rol designado por la Alta Gerencia deberá asegurar que el Sistema de Gestión de Seguridad de la Información y Ciberseguridad responda a las necesidades descritas en el apetito de riesgo y permita alcanzar un nivel de madurez razonable al contexto organizacional, el cual es validado periódicamente por la Alta Gerencia.
5. El rol designado por la Alta Gerencia desarrollará un sistema de gestión de seguridad de la información y velará por mantenerlo actualizado periódicamente de tal forma que se garantice su efectividad, oportunidad y madurez.
6. La Alta Gerencia designará una unidad o función organizacional para la gestión efectiva de los riesgos de seguridad de la información y ciberseguridad.
7. La Unidad o función organizacional deberá:
    a. Reportar de manera semestral a la Junta Directiva y a la Alta Gerencia, los resultados de su gestión, asesorando su toma de decisiones en esta materia.
    b. Actualizarse permanentemente y de manera especializada en materia de Seguridad de la Información y Ciberseguridad.
    c. Desarrollar un sistema de gestión de riesgos de seguridad de la información[5] y ciberseguridad que responda a las necesidades particulares de La Compañía, el cual será revisado y actualizado periódicamente de tal forma que se garantice su efectividad, oportunidad y madurez.
    d. Establecer el programa de formación y cultura en materia de seguridad de la información y ciberseguridad, para La Compañía.
    e. Monitorear y verificar el cumplimiento del marco de actuación de seguridad de la información y ciberseguridad, así como de las obligaciones legales relacionadas.
    f. Sugerir y administrar los presupuestos de seguridad de la información y ciberseguridad.
    g. Realizar las demás actividades que le sean asignadas por la Alta Gerencia.

8. El Área de Riesgos evaluará los riesgos de seguridad de la información y ciberseguridad dentro del sistema de gestión integral de riesgos e informará al

[5] Sistema de gestión de riesgos de seguridad de la información: Es el conjunto de definiciones, herramientas y metodologías que entregan los controles de seguridad, permiten evaluar el riesgo y facilitan la toma de decisiones.

Comité de Riesgos, de la Compañía que cuenten con este órgano de gobierno, sobre el estado de este riesgo, al menos una vez al año.

9. Todas las personas que gestionan información de La Compañía son responsables de acatar, aplicar y verificar el cumplimiento de las definiciones del marco de actuación de seguridad y ciberseguridad

GOBERNABILIDAD

La aprobación de la presente política está a cargo de la Junta Directiva, o el máximo órgano social, según corresponda, de La Compañía y cualquier modificación deberá ser aprobada por estos mismos órganos.

La Gerencia de Tecnología será la instancia responsable del gobierno y la aplicación de esta política.

INSTANCIAS DE DECISIÓN

Las instancias de decisión del marco normativo de seguridad estarán bajo las definiciones de la matriz de delegación de riesgos, el reglamento de trabajo de La Compañía y la normatividad vigente aplicable.

La Compañía maneja información que está legalmente protegida por normas específicas, lo cual podrá acarrear sanciones legales sobre La Compañía o sus grupos de interés.

DIVULGACIÓN

La presente Política será vinculante y deberá ser publicada a todos los grupos de interés, dentro de los sitios definidos por La Compañía.

La Gerencia de Tecnología será la responsable de la administración de esta política y en esa medida gestionará con las áreas involucradas en La Compañía su divulgación, cumplimiento y actualización.

Documento relacionado: Política General de Seguridad de la información y Ciberseguridad de Suramericana S.A.

5. Incumplimiento

La **Política General de Seguridad de la información y** Ciberseguridad es de obligatorio cumplimiento por parte de todos los **empleados, asesores, personal tercerizado y proveedores** que presten servicios a La Compañía. Si un individuo u organización viola las disposiciones descritas en este documento, en el caso de los empleados se

entenderá como una falta grave y si corresponde a vinculaciones de otra naturaleza, se entenderá como incumplimiento a las obligaciones de confidencialidad de información que le asisten, por lo tanto La Compañía se reserva el derecho de tomar las medidas correspondientes, las mismas que podrían incluso conllevar al ejercicio de acciones disciplinarias y legales, a la terminación y/o cancelación de contratos o vínculos contractuales de cualquier naturaleza, según sea el caso, y a que se pretenda la indemnización por los eventuales perjuicios que puedan llegar a causarse como consecuencia de la violación.

El no acatamiento de la política aquí descrita puede hacer vulnerable a La Compañía, exponiéndola a sanciones por parte de los entes de control, pérdidas financieras, de imagen y credibilidad ante sus clientes y accionistas. Por esto el cabal cumplimiento de esta hace parte de las responsabilidades de cada uno de los usuarios de la información de La Compañía.