Versión: 2
Fecha Última Actualización: 30/01/2019
Aprobado por: Junta Directiva o quien haga sus veces de las siguientes sociedades; Seguros Generales Suramericana S.A, Seguros de Vida Suramericana S.A, EPS y Medicina Prepagada Suramericana S.A., Servicios de salud IPS Suramericana S.A., Fondo Mutuo de Inversión de Empleados Suramericana "Fondosura", Consultoría en Gestión de Riesgos Suramericana S.A.S, Diagnóstico y Asistencia Médica S. A. S-Dinámica S.A., Operaciones Generales Suramericana S.A.S., Inversiones Suramericana Colombia S.A.S., y Servicios Generales Suramericana S.A.S
Fecha de Publicación: 30/01/2019
Área Responsable: Gobierno y Arquitectura de Tecnología

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

INTRODUCCIÓN Y OBJETIVOS

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[3], teniendo en cuenta la confidencialidad, integridad y disponibilidad de la misma, a través de los 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.

[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] Estándares internacionales de Seguridad: Conjunto de Marcos de Referencia como COBIT5, ISO 27001, ISO 27002, ISO 27032, NIST, ISF – Information Security Forum. – De este estándar si tenemos algo implementado?, agregaría más fácil 27032 que es la de ciberseguridad

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 compañía y aplica para Seguros Generales Suramericana S.A, Seguros de Vida Suramericana S.A,., EPS y Medicina Prepagada Suramericana S.A., Servicios de salud IPS Suramericana S.A., Fondo Mutuo de Inversión de Empleados Suramericana "Fondosura", Consultoría en Gestión de Riesgos Suramericana S.A.S, Diagnóstico y Asistencia Médica S. A-Dinámica S.A.S, Operaciones Generales Suramericana S.A.S. Inversiones Suramericana Colombia S.A.S. y Servicios Generales Suramericana S.A.S, en adelante *Las Compañías*.

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. Se deberán establecer procesos y procedimientos para la adecuada gestión del riesgo de seguridad de la información y ciberseguridad, contemplando las etapas de prevención, protección y detección, respuesta y comunicación, y recuperación y aprendizaje.
3. Deberá existir alineación de los indicadores y metas comerciales de *Las Compañías* y sus empleados con el marco de actuación de seguridad de la información y ciberseguridad.
4. Todas las personas con acceso a la información de *Las Compañías* deberán actuar bajo el marco de actuación de seguridad de la información.
5. Todas las personas que acceden a la información de *Las Compañías* 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 la seguridad de la información y la gestión de los riesgos de seguridad de la información y ciberseguridad, incluyéndolos en los planes estratégicos de *Las Compañías* 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 *Las Compañías*.
3. La Alta Gerencia designará una unidad o función organizacional para la gestión efectiva de los riesgos de seguridad de la información y ciberseguridad.
4. 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 *Las Compañías*, 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 *Las Compañías*..
    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

[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.

5. 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 Comité de Riesgos, de aquellas Compañías que cuenten con este órgano de gobierno, sobre el estado de este riesgo, al menos una vez al año.
6. Todas las personas que gestionan información de *Las Compañías* 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 *Las Compañías* 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 *Las Compañías* y la normatividad vigente aplicable.

Las Compañías manejan información que está legalmente protegida por normas específicas, lo cual podrá acarrear sanciones legales sobre *Las Compañías* 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 *Las Compañías.*

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

Versión: 2
Fecha Última Actualización: 30/01/2019
Aprobado por: Junta Directiva o quien haga sus veces de las siguientes sociedades; Seguros Generales Suramericana S.A, Seguros de Vida Suramericana S.A, EPS y Medicina Prepagada Suramericana S.A., Servicios de salud IPS Suramericana S.A., Fondo Mutuo de Inversión de Empleados Suramericana "Fondosura", Consultoría en Gestión de Riesgos Suramericana S.A.S, Diagnóstico y Asistencia Médica S. A. S-Dinámica S.A., Operaciones Generales Suramericana S.A.S., Inversiones Suramericana Colombia S.A.S., y Servicios Generales Suramericana S.A.S
Fecha de Publicación: 30/01/2019
Área Responsable: Gobierno y Arquitectura de Tecnología

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

APROBACIONES			
COMPAÑÍA	**FECHA**	**ÓRGANO**	**NÚMERO DE ACTA**
Seguros de Vida	Enero 30 de 2019	Junta Directiva	No. 1955
Seguros Generales	Enero 30 de 2019	Junta Directiva	No. 2574

CONTROL DE CAMBIOS			
FECHA	**VERSIÓN**	**AUTOR**	**DESCRIPCIÓN DEL CAMBIO**
19/05/2016	**1**	Kristin Bustos Morón Idárraga David Alberto Garavito Murcia	Creación y definición de documento
30/01/2019	**2**	Natalia Alvarez Agudelo Leidy Tatiana Velez Londoño	Reasignación de responsabilidad a Gerencia de Tecnología e incorporación de cumplimiento normativo de la SFC CE007 de 2018