Versión: 3
Fecha Última Actualización: 10/12/2018
Aprobado por: Junta Directiva Suramericana S.A
Fecha de Publicación: 20/03/2019
Área Responsable: Vicepresidencia de Tecnología

SEGUROS, TENDENCIAS Y RIESGOS

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

INTRODUCCIÓN Y OBJETIVOS

Suramericana S.A y sus filiales, 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, teniendo en cuenta la confidencialidad, integridad y disponibilidad de la misma, 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 control que regulan nuestras actividades.

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 organización y aplica para Suramericana S.A, sus filiales y subsidiarias.

---

[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 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.

En este documento cuando se haga referencia a *Las Compañías* se habla de Suramericana S.A, sus filiales y subsidiarias.

LINEAMIENTOS GENERALES

1. Esta política general se desarrolla a través de un marco normativo 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 la organización y sus empleados con el marco normativo de seguridad de la información y ciberseguridad de *Las Compañías*.
4. Todas las personas con acceso a la información de *Las Compañías* deberán actuar bajo el marco normativo de seguridad de la información y ciberseguridad.
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 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 de la información y ciberseguridad sea asimilado e incorporado en el accionar de *Las Compañías*.

3. La Alta Gerencia designará una función organizacional adecuada 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 Área de Gobierno de Tecnología desarrollará un sistema de gestión de seguridad de la información[5] 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.
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 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 normativo de seguridad de la información y ciberseguridad.

GOBERNABILIDAD

La aprobación de la presente política está a cargo de la Junta Directiva de SURAMERICANA S.A. Cualquier modificación deberá ser aprobada por estos mismos órganos, siguiendo los lineamientos de Suramericana S.A.

La Vicepresidencia de Tecnología de Suramericana S.A será la instancia responsable del gobierno y la aplicación de esta política.

Este documento se sometió a consideración de la Junta Directiva de **SURAMERICANA S.A**., quien dio su aprobación el **20 de marzo de 2019**, mediante acta número **139**.

[5] Sistema de gestión 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.

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 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 Vicepresidencia de Tecnología de Suramericana S.A 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.

SEGUROS, TENDENCIAS Y RIESGOS

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
24/10/2017	**2**	Beatriz Sepúlveda Jorge Martillo	Reasignación de responsabilidad a la Vicepresidencia de TI
10/12/2018	**3**	Jenny Lorena Giraldo Gallego Gerencia de Gobierno de Tecnología Corporativo	Ajustes y actualización