Versión: 7
Fecha Última Actualización: 28/10/2024
Aprobado por: Comité de Riesgos / Junta Directiva Suramericana S.A.
Fecha de Publicación:22/11/2024
Área Responsable: Vicepresidencia de Gestión de la Estrategia y Tecnología

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

INTRODUCCIÓN Y OBJETIVOS

Suramericana S.A y sus filiales y subsidiarias, en desarrollo de sus principios: Responsabilidad, Respeto, Transparencia y Equidad, determinan la información como uno de los activos estratégicos 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 esta, a través de sus grupos de interés[3], procesos y el uso de recursos tecnológicos y de información.

Toma como referencias 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

[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] Grupos de interés: 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, ISO 27002, NIST Cybersecurity Framework 2.0 y complementarias.

Esta Política General de Seguridad de la Información y Ciberseguridad es de cumplimiento obligatorio para todos los grupos de interés[5] que tengan acceso a la información de la organización, con la finalidad de evitar la indisponibilidad, la pérdida, modificación o divulgación no autorizada, el acceso no autorizado y así proteger la información de todos los riesgos a los que pueda ser expuesta. Aplica para Suramericana S.A, sus filiales y subsidiarias.

En este documento cuando se haga referencia a SURAMERICANA S.A. 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, procesos, procedimientos, instructivos, estándares, etc. Los cuales deben ser definidos y aplicados de acuerdo con la clasificación de la información de la compañía.
2. Para la gestión adecuada del riesgo de seguridad de la información y ciberseguridad, la organización se apoyará de metodologías, herramientas, conocimientos, procesos o procedimientos que disminuyan la probabilidad e impacto de estos, 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, el riesgo de seguridad de la información y ciberseguridad, el marco normativo de seguridad de la información y ciberseguridad, y Marco de actuación de gestión de información de *Suramericana*.

ROLES Y RESPONSABILIDADES

[5] Son aquellos grupos que tienen responsabilidad, influencia, cercanía, dependencia y representación. Estos son establecidos conforme a las definiciones de reputación y marca organizacionales.

1. La Alta Gerencia 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 Suramericana y garantizando la disponibilidad de los recursos que se requieran para el efecto.
2. La Alta Gerencia promoverá una conciencia de seguridad de la información y ciberseguridad a todos los grupos interesados, traduciendo la estrategia de la compañía en mecanismos efectivos para que el marco normativo de seguridad de la información y ciberseguridad sea asimilado e incorporado en el accionar de *Suramericana*.
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 anualmente por la Alta Gerencia.
5. El rol designado por la Alta Gerencia desarrollará un sistema de gestión de seguridad de la información[6], el cual deberá ser actualizado periódicamente de tal forma que se garantice su efectividad, oportunidad y madurez.
6. 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.
7. El Área de Auditoría Interna evaluará los controles de seguridad de la información y ciberseguridad e incluirá dentro de su plan de trabajo los aseguramientos sobre aspectos clave que se requieran. La periodicidad de estos aseguramientos será definida por la Auditoria Interna en su planeación anual, la cual es dinámica, de acuerdo con la evaluación basada en riesgos que realice de este tema.

[6] 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.

8. Todos los Grupos de Interés que accedan a información de la compañía son responsables de acatar los lineamientos definidos dentro 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 Gestión de la Estrategia y Tecnología será la responsable de la administración de esta política y en esa medida gestionará con las áreas involucradas en SURAMERICANA S.A. su divulgación, cumplimiento y actualización una vez al año
Este documento se sometió a consideración de la Junta Directiva de SURAMERICANA S.A., quien dio su aprobación el *21 de Noviembre de 2024, mediante acta número 202.*

DIVULGACIÓN Y ACTUALIZACIÓN

La presente Política se divulgará a todos los grupos de interés, y se actualizará de acuerdo con los cambios organizacionales, disposiciones legales u otros aspectos que puedan afectar los lineamientos aquí descritos.

Versión: 7
Fecha Última Actualización: 28/10/2024
Aprobado por: Comité de Riesgos / Junta Directiva Suramericana S.A.
Fecha de Publicación:22/11/2024
Área Responsable: Vicepresidencia de Gestión de la Estrategia y Tecnología

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
03/04/2020	4	Jorge Martillo Gerencia de Gobierno de Tecnología Corporativo	Revisión anual
14/02/2022	5	Flavio Gallego Gerencia de Servicios Estratégicos – Vicepresidencia TI Corporativo. Luis Felipe Villegas Gerencia de Riesgos Operacionales Corporativo.	Revisión Anual
19/10/2023	6	Carolina Panesso Gestión de Información Gerencia de Tecnología y focos estratégicos Kristin Bustos Gerencia de Riesgos Operacionales Corporativo.	Revisión Anual

		Carlos Andrés Valencia Gerente de Gobierno y planeación de Tecnología – Rol Ciberseguridad Asesoró: Felipe Cossio Auditoría Corporativo	
28/10/2024	7	Carlos Andrés Valencia Gerente de Gobierno y planeación de Tecnología – Rol Ciberseguridad Kristin Bustos Gerencia de Riesgos Operacionales Corporativo Asesoraron: Sebastián Arango Alzate, Auditoría Corporativo Sandra Yaneth García, Especialista en Cumplimiento y Transformación Legal	Revisión anual