POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Vicepresidencia de Negocio y Tecnología

Suramericana S.A.

Elaboración y responsabilidad
Carlos Andres Valencia - Gerente de Capacidades de Tecnología
Leidy Tatiana Vélez Londoño – Especialista de Ciberseguridad

Revisión
Kristin Bustos Morón – Gerente de Riesgos Operacionales
Paola Andrea Galeano – Director de Gestión de riesgos
Diana Carolina Restrepo Carvajal – Analista de Diseño organizacional
Maria Camila Guio Minotas – Analista Legal, Gestión Ética y Cumplimiento
Asesoró: Sebastián Arango Alzate – Director de Auditoría de TI Regional

Aprobación
Junta Directiva de Suramericana S.A.

Versión		
V8	Revisión y actualización anual de la política	19 de marzo 2026

Documentos relacionados

INTRODUCCIÓN Y OBJETIVOS

Suramericana S.A y sus filiales y subsidiarias (En adelante, conjuntamente llamadas "SURAMERICANA", "La Compañía" y/o "La Organización"), 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 que la seguridad de la información[1] y la ciberseguridad[2] son dos aspectos fundamentales para el logro de sus objetivos estratégicos. En desarrollo de lo anterior, se comprometen con la protección y garantía de la seguridad de la información que gestionan 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

Esta Política General de Seguridad de la Información y Ciberseguridad aplica a Suramericana S.A, sus filiales y subsidiarias y es de cumplimiento obligatorio para todos los grupos de interés que tengan acceso a la información de la organización, con 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] Para efectos de esta política, se entiende por grupos de interés, con independencia del nivel jerárquico y forma de contratación a todos los empleados, proveedores, subcontratistas, intermediarios de seguros (asesores, corredores, agencias, brokers, etc), administradores/directores (miembros de la alta gerencia y Junta Directiva), clientes, accionistas y otros que tienen responsabilidad, influencia, cercanía, dependencia y representación, conforme a las definiciones de reputación y marca organizacionales.

[4] Los estándares internacionales de Seguridad vigentes a la fecha de elaboración de esta política son: ISO 27001:2022, ISO 27002, CIS, NIST Cybersecurity Framework 2.0 y complementarias.

finalidad de evitar la indisponibilidad, la pérdida, acceso, modificación o divulgación no autorizados, y así proteger la información de todos los riesgos a los que pueda ser expuesta en las tecnologías de la información (IT), y las tecnologías de la operación (OT).

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, entre otros. 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. La organización deberá implementar controles específicos para la gestión del riesgo de seguridad de la información y ciberseguridad en la **cadena de suministro**, asegurando que los proveedores, contratistas y terceros cumplan con los estándares definidos por Suramericana y/o los marcos internacionales o lineamientos aplicables según el tipo de relación contractual.
4. 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, el Marco de actuación de gestión de información y la privacidad y protección de datos personales de *Suramericana*.
5. La Organización deberá definir los lineamientos para la protección y el aseguramiento de la información que no repose en medios digitales y que sea de su propiedad o esté bajo su custodia.

ROLES Y RESPONSABILIDADES

1. La **Alta Gerencia** será la responsable de definir, aprobar y revisar periódicamente el *apetito de riesgo* en materia de ciberseguridad y seguridad de la información,

asegurando su alineación con los objetivos estratégicos y el plan de negocio de la organización.

2. La **Alta Gerencia** será la encargada de promover y aprobar los *lineamientos* frente a la gestión de ciberseguridad y seguridad de la información incluyéndolos en los planes estratégicos de Suramericana y garantizando la disponibilidad de los recursos que se requieran para el efecto.
3. 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*.
4. La **Alta Gerencia** designará roles y responsabilidades adecuados para la *implementación del sistema de gestión de seguridad de la información y ciberseguridad* y la gestión efectiva de los riesgos de seguridad de la información y ciberseguridad, incluyendo los relacionados a la cadena de suministro, con el personal idóneo y con capacidad decisoria para ejecutar las actividades que se requieran.
5. 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, las normas externas y el entorno de la Organización y permita alcanzar un nivel de madurez razonable al contexto organizacional, el cual es validado anualmente por la Alta Gerencia.
6. El **rol designado por la Alta Gerencia** desarrollará un sistema de gestión de seguridad de la información[5], el cual deberá ser actualizado periódicamente de tal forma que se garantice su efectividad, oportunidad y madurez.
7. 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.
8. 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

[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.

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.

9. **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, y las definiciones complementarias de privacidad y protección de Datos Personales y demás normas internas y externas aplicables al manejo de la información.

GOBERNABILIDAD

La aprobación de la presente política está a cargo de la Junta Directiva de SURAMERICANA S.A. Cualquier modificación deberá ser aprobada siguiendo esta definición, los lineamientos de gobierno corporativo de **SURAMERICANA S.A.** y su Directriz de estructura normativa.

Cada filial tendrá la responsabilidad de elaborar, aprobar, difundir y revisar regularmente sus normas internas locales siguiendo los criterios establecidos en esta norma.

DIVULGACIÓN Y ACTUALIZACIÓN

La presente norma interna se divulgará a todos los equipos de Suramericana, sus filiales y subsidiarias, y se actualizará anualmente y los cambios organizacionales, disposiciones legales u otros aspectos que eventualmente puedan afectar los lineamientos aquí descritos.

Esta política será publicada en el sitio de normas interno de Suramericana y en los lugares dispuestos por cada una de las compañías a quienes se les aplique esta norma.

El responsable de la administración y cumplimiento de estos lineamientos será la Vicepresidencia de Negocio y Tecnología de Suramericana .