POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Servicios de Salud IPS Suramericana S.A.S.

Ciberseguridad y Confianza Digital

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

Elaborado por:	Revisado por:	Aprobado por:
Daniela Hernández Ruiz	Leidy Tatiana Veléz Londoño	Asamblea General de accionistas Servicios de Salud IPS Suramericana S.A.S.

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 Vélez 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	Aníbal Alejandro Álvarez 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
5	Daniela Hernández Ruiz	Se actualiza el objetivo de la política incorporando tecnologías de la información (IT) y tecnologías de la operación (OT). Se incluye lineamiento para la gestión del riesgo de ciberseguridad en la cadena de suministro. Se actualizan los roles y responsabilidades de gobierno de la seguridad de la información y ciberseguridad, incorporando la gestión del apetito de riesgo por parte de la Alta Gerencia, la formalización de la función de Ciberseguridad, la actualización de la responsabilidad de Auditoría Interna sobre el programa de ciberseguridad y la	14/08/2026

		alineación del modelo de gobernabilidad con la estructura organizacional vigente.	

Aprobaciones		
Fecha (dd/mm/aaaa)	**Órgano**	**Número de Acta**
13/02/2019	*Asamblea General de Accionistas*	*123*
15/03/2024	*Asamblea General de Accionistas*	*53*
15/09/2025	*Asamblea General de Accionistas*	*59*
17/09/2026	*Asamblea General de Accionistas*	*62*

INTRODUCCIÓN Y OBJETIVOS

Servicios de Salud IPS Suramericana S.A.S, en desarrollo de sus principios de responsabilidad, respeto, transparencia y equidad, determina que la información es uno de sus activos estratégicos más importantes; por lo tanto, declara la seguridad de la información y la ciberseguridad como dos aspectos fundamentales para el logro de sus objetivos estratégicos. En desarrollo de lo anterior, se compromete con la protección y el aseguramiento de la información de las partes interesadas que gestiona en medios físicos y digitales, teniendo en cuenta su confidencialidad, integridad y disponibilidad, a través de sus grupos de interés, procesos y recursos tecnológicos y de información.

Contempla prácticas exitosas incorporadas a partir de estándares internacionales de seguridad de la información y ciberseguridad[1] *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.*

ALCANCE

Esta Política General de Seguridad de la Información y Ciberseguridad es de cumplimiento obligatorio para todos los grupos de interés que tengan acceso a la información y/o plataformas tecnológicas de la compañía, con la finalidad de evitar la indisponibilidad, la pérdida, acceso, modificación o divulgación no autorizados, y así proteger la información y el adecuado funcionamiento de todos los dispositivos, de los riesgos a los que pueda ser expuesta en las tecnologías de la información (IT) y las tecnologías de la operación (OT), priorizando en estos últimos la continuidad del servicio y la integridad física de las personas sobre la confidencialidad de los datos.

Aplica para Servicios de Salud IPS Suramericana S.A.S, en adelante La Compañía.

LINEAMIENTOS GENERALES

1. *Esta política general se desarrolla a través de un* ***Marco Normativo de Seguridad de la Información y Ciberseguridad****, compuesto por directrices,*

1 Los estándares internacionales de Seguridad vigentes a la fecha de elaboración de esta política son: ISO 27001:2022, ISO 27002, ISA IEC 62443, HIPAA, CIS, NIST 800-82, Cybersecurity Framework 2.0 y complementarias.

manuales, metodologías, procesos, procedimientos, instructivos, estándares, entre otros documentos vinculantes que la complementan. 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 Compañía se apoyará en metodologías, herramientas, conocimientos, procesos o procedimientos que disminuyan la probabilidad o el impacto de este, de acuerdo con el perfil de riesgo, el plan de negocio, la naturaleza, el tamaño, el tipo de información y la complejidad de las actividades que desarrolle, así como con el entorno y los mercados en los que opere.*
3. *La organización deberá implementar controles específicos para la gestión del riesgo de seguridad de la información y ciberseguridad en la **cadena de suministro (incluye IT/OT)**, asegurando que los proveedores, contratistas y terceros cumplan con los estándares definidos por La Compañía 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 la protección de datos personales de La Compañía.*
5. *La Compañía 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[2] en materia de ciberseguridad y seguridad*

[2] Como mínimo el apetito de riesgo es revisado anualmente y/o por demanda con base en las amenazas, riesgos y el contexto organizacional.

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

2. *La **Junta Directiva**, o el órgano que haga sus veces, será la encargada de promover, revisar 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.*
3. *La **Alta Gerencia** promoverá una conciencia en seguridad de la información y ciberseguridad en todos los grupos de interés, 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 La Compañía.*
4. *La **Alta Gerencia** designará una unidad o función organizacional con 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 (IT y OT), incluyendo los relacionados con 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 como unidad o función organizacional para la seguridad de la información y ciberseguridad** deberá:*
    a. *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.*
    b. *Desarrollar un Sistema de Gestión de Seguridad de la Información 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.*
    c. *Reportar como mínimo semestralmente o con la frecuencia que se establezca, a la Junta Directiva y a la Alta Gerencia, los resultados de su gestión, asesorando su toma de decisiones en esta materia.*
    d. *Actualizarse permanentemente y de manera especializada en materia de seguridad de la información y ciberseguridad.*

e. *Establecer el programa de formación y cultura en materia de seguridad de la información y ciberseguridad (incluye IT/OT).*
f. *Monitorear y verificar el cumplimiento del Marco Normativo de Seguridad de la Información y Ciberseguridad, así como de las obligaciones legales relacionadas.*
g. *Sugerir y administrar los presupuestos de seguridad de la información y ciberseguridad.*

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 de La Compañía o la instancia competente, 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 establecida en su planeación anual, la cual es dinámica, de acuerdo con la evaluación basada en riesgos que realice de este tema.*
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, y las definiciones complementarias de privacidad y protección de datos personales y demás normas internas y externas aplicables al manejo de la información.*

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*** *y, en general, de* ***todos los grupos de interés*** *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; si corresponde a vinculaciones de otra naturaleza, se entenderá como incumplimiento de las obligaciones de confidencialidad de la información, así como manejo indebido de*

plataformas tecnológicas y sistemas de control. Por lo tanto, La Compañía se reserva el derecho de tomar las medidas correspondientes, que podrían conllevar el ejercicio de acciones disciplinarias y legales, la terminación y/o cancelación de contratos o vínculos contractuales de cualquier naturaleza, según sea el caso, y la solicitud de indemnización por los eventuales perjuicios causados, ***especialmente cuando dichos incumplimientos pongan en riesgo la disponibilidad de servicios críticos de salud o la integridad física de las personas y de la infraestructura operativa****.*

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 y reputacionales, así como pérdida de 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.

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.

El rol designado por la Alta Gerencia será la instancia responsable del gobierno y la aplicación de esta política.

INSTANCIAS DE DECISIÓN

Las instancias de decisión del Marco Normativo de Seguridad de la Información y Ciberseguridad 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 para La Compañía o sus grupos de interés.

DIVULGACIÓN

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

El rol designado por la Alta Gerencia será el 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. (Oficina Corporativa)*

Aprueba:

Asamblea General de Accionistas Servicios de Salud IPS Suramericana S.A.S.

Acta 62 del 17 de Septiembre de 2026.