EPS | sura

Política General de Seguridad de la Información y Ciberseguridad

EPS SURA

Ciberseguridad y Confianza Digital

Elaborado por:	Revisado por:	Aprobado por:
Daniela Hernández Ruiz	Leidy Tatiana Vélez Londoño	Junta Directiva EPS Suramericana S.A.

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 Velez 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	Anibal Alejandro Alvarez 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	Anibal Alejandro Alvarez Galvis	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 ajustan roles y responsabilidades integrando este enfoque. Se amplían definiciones sobre privacidad y protección de datos personales. Se incorpora la responsabilidad de la Alta Gerencia en la definición y revisión del apetito de riesgo en ciberseguridad.	19/04/2026
6	Daniela Hernández Ruiz	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, Se actualiza responsabilidad de Auditoría Interna sobre el programa de ciberseguridad y la alineación del modelo de gobernabilidad con la estructura organizacional vigente.	14/08/2026

Aprobaciones		
Fecha (dd/mm/aaaa)	**Órgano**	**Número de Acta**
28/03/2019	Junta Directiva	215
26/10/2023	Junta Directiva	259
23/05/2025	Junta Directiva	281
29/04/2026	Junta Directiva	293
25/08/2026	Junta Directiva	297

INTRODUCCIÓN Y OBJETIVOS

EPS Suramericana S.A., 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 de las partes interesadas, 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.

[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 prevenir, defender, y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los activos de información y los entornos digitales incluyendo infraestructura de Tecnología de la Información (IT) y Tecnología Operacional (OT), que son esenciales para la continuidad, seguridad y operación de la organización.

3 Grupos de Interés: 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.

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.

Aplica para EPS Suramericana S.A., en adelante La Compañía.

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 (Safety) sobre la confidencialidad de los datos.

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, 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 de metodologías, herramientas, conocimientos, procesos o procedimientos que disminuyan la probabilidad o el impacto de este, 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.

4 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.

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 la 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 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*[5] *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 **Junta Directiva**, o el órgano que haga sus veces, según corresponda, 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 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 a la cadena de suministros, con el personal idóneo y con capacidad decisoria para ejecutar las actividades que se requieran.

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

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 mínimamente semestral y/o de acuerdo con la frecuencia establecida, 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 definida por la Auditoría Interna 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 **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 y si corresponde a vinculaciones de otra naturaleza, se entenderá como incumplimiento a las obligaciones de confidencialidad de información que le asisten, manejos indebidos de plataformas tecnológicas y sistemas de control, por lo tanto La Compañía se reserva el derecho de tomar las medidas correspondientes, las mismas que podrían incluso conllevar al ejercicio de acciones disciplinarias y legales, a la terminación y/o cancelación de contratos o vínculos contractuales de cualquier naturaleza, según sea el caso, y a que se pretenda la indemnización por los eventuales perjuicios que puedan llegar a causarse, **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** como consecuencia de la violación.

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, de imagen y 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 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 sobre La Compañía 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 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,

Junta Directiva EPS Sura S.A.
Acta 297 del 25 de agosto de 2026.