POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

ALIANZA MEDELLÍN ANTIOQUIA EPS S.A.S SAVIA SALUD EPS, reconoce la importancia de gestionar la información de manera responsable y segura. Por ello, es de carácter obligatorio avanzar en la implementación de un Modelo de Seguridad y Privacidad de la Información (MSPI) que establezca un marco de confianza para todos los afiliados, colaboradores y proveedores.

Proteger la información es esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos. Por ello, se busca desarrollar mecanismos que permitan identificar y gestionar de manera sistemática los riesgos asociados a la seguridad de la información, minimizando el impacto sobre nuestros activos y respondiendo de manera efectiva a las necesidades de los diferentes grupos de interés.

Este compromiso está alineado con la misión y visión de SAVIA SALUD EPS, así como con el cumplimiento de la normatividad vigente aplicable, con el fin de fortalecer las capacidades de protección y seguridad de la información, construyendo una base sólida que respalde las labores diarias en beneficio de todos los involucrados.

PROYECCIÓN DE LA POLÍTICA

1. Base Legal

La implementación de la política de Seguridad de la Información de SAVIA SALUD EPS se fundamenta en el cumplimiento de los lineamientos y obligaciones legales vigentes establecidos para el adecuado manejo de la información. Por lo anterior, la presente política se fundamenta en las siguientes normas:

En primer lugar, la **LEY 1273 DE 2009** o Ley de Delitos Informáticos: Por medio de la presente se modifica la Ley 599 de 2000 (Código Penal) al tipificar y sancionar las conductas que atenten contra la seguridad y la confidencialidad de los sistemas de información, los datos y las comunicaciones, por lo tanto, se configura como el principal instrumento legal fundamental en Colombia para prevenir y sancionar las eventuales conductas delictivas en el entorno digital.

Posteriormente, la **LEY 1581 DE 2012** o Ley de Protección de Datos Personales: Regula el tratamiento de la información personal en las empresas privadas y entidades públicas. Busca garantizar el derecho fundamental de 'Habeas Data', es decir, el derecho que tiene cada persona para conocer, actualizar y rectificar la información que se haya recolectado en bases de datos o archivos.

Anudado a lo anterior, el **DECRETO 1377 DE 2013** profundiza la normativa de Protección de Datos Personales, estableciendo los principios y derechos generales del 'Habeas Data', en otras palabras, el Decreto complementa las pautas y las directrices concretas para que las entidades como SAVIA SALUD EPS cumplan con las obligaciones establecidas en la Ley 1581 de 2013.

Para finalizar, la normativa internacional en la norma **ISO/IEC 27001:2022**, proporciona una implementación y un mantenimiento al Sistema de Gestión de Seguridad de la Información (SGSI), es un marco estratégico y sistemático que obliga a las empresas y entidades establecer herramientas que permitan proteger proactivamente la confidencialidad, integridad y disponibilidad de la información.

Se concluye que, existe un marco jurídico y normativo completo diseñado para la protección integral de la información. Constituyendo tres pilares fundamentales, en primer lugar, la prevención y sanción penal

(Ley 1273 de 2009), en segundo lugar, la protección de datos personales (Ley 1581 de 2012 y el Decreto 1377 de 2013) y, por último, la gestión de la seguridad (ISO/IEC 27001:2022).

2. Justificación de la política

La definición de esta política de Seguridad de la Información en SAVIA SALUD EPS responde a la necesidad de garantizar un manejo adecuado, confiable y seguro de la información en todos los niveles de la organización. La información es uno de los activos más valiosos, ya que su integridad, confidencialidad y disponibilidad son esenciales para el cumplimiento de la misión y la visión institucional.

Riesgos asociados a la ausencia de la política

Sin una política clara y estructurada, Savia Salud EPS podría enfrentar riesgos significativos, tales como:

- **Vulneración de datos personales:** Que podría resultar en sanciones legales, daños a la reputación y pérdida de confianza por parte de los afiliados, colaboradores y proveedores.
- **Ciberataques:** Que pueden comprometer la continuidad del servicio y generar pérdidas económicas y operativas.
- **Fallas en la gestión de riesgos:** Incapacidad para identificar y mitigar de manera oportuna los riesgos asociados a la Seguridad de la Información.
- **Desconocimiento normativo:** Falta de cumplimiento con la legislación aplicable, lo cual puede derivar en sanciones administrativas o judiciales.

Ventajas de la implementación de la política

La implementación de esta política en el marco del Sistema de Gestión de la Información permitirá a Savia Salud EPS:

- **Fortalecer la confianza** de los grupos de interés al garantizar la protección de sus datos personales y sensibles.
- **Prevenir incidentes de seguridad** a través de la identificación y gestión proactiva de riesgos.
- **Asegurar el cumplimiento normativo**, evitando sanciones legales y reforzando el compromiso con las regulaciones locales e internacionales.
- **Optimizar procesos internos**, promoviendo una cultura de seguridad y responsabilidad en el manejo de la información.
- **Resguardar la continuidad operativa**, minimizando impactos negativos derivados de incidentes relacionados con la seguridad de la información.

Esta política es una herramienta fundamental para proteger los activos de información de Savia Salud EPS, y garantizar la sostenibilidad operativa y fortalecer su relación con los afiliados y demás grupos de interés.

3. Objetivo de la política

Garantizar la protección integral de los activos de información de Savia Salud EPS frente a amenazas internas y externas, deliberadas o accidentales, mediante el cumplimiento de las leyes y regulaciones aplicables, la gestión sistemática de riesgos, y la promoción de una cultura organizacional basada en la

concienciación y formación en seguridad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos para todos los grupos de interés.

4. Alcance

Esta política se aplica a todos los colaboradores, contratistas, practicantes, afiliados, consultores y personal externo. Su alcance se extiende a todos los activos de información de Savia Salud EPS, en cualquiera de sus formatos (digital, físico o verbal), y abarca el ciclo de vida completo de la información, desde su creación hasta su eliminación. Esto incluye, de manera enunciativa mas no limitativa, el acceso y uso de los sistemas de información, documentos, canales de comunicación, equipos de cómputo, redes y demás recursos tecnológicos de la organización.

5. Condiciones generales

Para la aplicación efectiva de la Política de Seguridad de la Información de Savia Salud EPS, se establecen las siguientes pautas, que servirán como criterios para auditorías internas y externas:

- **Cumplimiento Normativo:** Todos los procesos relacionados con la gestión de información deben cumplir con las leyes, regulaciones y normativas aplicables, incluyendo la Ley 1581 de 2012, el Decreto 1377 de 2013, y otras disposiciones nacionales e internacionales pertinentes.
- **Clasificación y Control de Información:** La información debe ser clasificada según su nivel de sensibilidad (pública, confidencial o restringida) y tratada en conformidad con los controles establecidos para cada categoría.
- **Gestión de Riesgos:** Se debe realizar de manera periódica una identificación, evaluación y tratamiento de los riesgos asociados a la seguridad de la información, documentando las acciones implementadas para mitigar dichos riesgos.
- **Acceso Controlado:** El acceso a los sistemas, aplicaciones y recursos de información debe estar limitado a los usuarios autorizados, con privilegios asignados en función de sus roles y responsabilidades, garantizando el principio de mínimos privilegios.
- **Concienciación y Capacitación:** Todos los colaboradores deben participar en programas de formación y concienciación sobre seguridad de la información, para garantizar un manejo adecuado y seguro de los datos.
- **Gestión de Incidentes:** Se cuenta con un PD-TI-22 Procedimiento gestión de incidentes de seguridad para la gestión de incidentes de seguridad de la información, incluyendo su detección, registro, análisis, respuesta y aprendizaje posterior.
- **Confidencialidad de los Contratos:** Los acuerdos con terceros, como proveedores o aliados estratégicos, deben incluir cláusulas que garanticen el cumplimiento de los estándares de seguridad y privacidad de la información establecidos por la organización.
- **Copia de Seguridad y Recuperación:** Se deben implementar y mantener políticas de respaldo periódico de la información crítica, asegurando la capacidad de recuperación en caso de pérdida o incidente.
- **Mejora Continua:** La política, los procedimientos y los controles asociados deben ser revisados y actualizados de manera periódica para adaptarse a los cambios en el entorno, las regulaciones y las necesidades de la organización.

6. Excepciones

La política de Seguridad de la Información debe ser aplicada sobre la totalidad de la información gestionada en la entidad, de total cumplimiento.

Todos los activos de información, independientemente de su formato, medio de almacenamiento o canal de comunicación, están sujetos a los lineamientos, controles y disposiciones establecidos en esta política. No se permite la exclusión de ningún tipo de información del alcance de esta política, ya que su correcta aplicación es fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos.

7. Sanciones

El incumplimiento de la política de Seguridad de la Información acarrea diversas sanciones las cuales varían dependiendo de la naturaleza de la infracción, si es un delito o una falta administrativa.

Las **sanciones penales** están tipificadas en el Código Penal (Ley 1273 de 2009). Las sanciones incluyen penas de prisión de 48 a 96 meses y multa de 100 a 1000 Salarios Legales Mensuales Vigentes con circunstancias de agravación punitivas tales como aprovechar la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este, revelar o dar a conocer el contenido de la información en perjuicio de otro, obtener provecho para sí o para un tercero, entre otros (Artículo 269H).

Las **faltas o sanciones administrativas** están reguladas en la Ley 1581 de 2012 y el Decreto 1377 de 2013. Según el *artículo 19* de la Ley mencionada anteriormente, el incumplimiento de las normas sobre la Protección de Datos Personales es sancionado por la Superintendencia de Industria y Comercio (SIC) a través de la Delegatura de Protección de Datos Personales. Se resalta que, las sanciones aplican tanto a personas naturales como a las empresas y entidades.

> "***LEY 1581 DE 2012 - ARTÍCULO 23. SANCIONES.*** *La Superintendencia de Industria y Comercio podrá imponer a los responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*
>
> *a) **Multas de carácter personal e institucional** hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;*
> *b) **Suspensión de las actividades** relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;*
> *c) **Cierre temporal de las operaciones** relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;*
> *d) **Cierre inmediato y definitivo** de la operación que involucre el Tratamiento de datos sensibles;*
>
> ***PARÁGRAFO.** Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva."*

En concordancia a lo anterior, más allá de las sanciones penales o administrativas, el incumplimiento de la Política de Seguridad de la Información puede generar otras consecuencias negativas para SAVIA SALUD EPS tales como, pérdida de reputación y confianza, pérdida de afiliados, y/o altos costos asociados a la remediación de incidentes.

8. Consideraciones

8.1. Medios de difusión

Para garantizar que la Política de Seguridad de la Información sea conocida, comprendida y aplicada, se establecen los siguientes medios de difusión:

- Medios de comunicación corporativos internos y externos.
- Contratos laborales y Acuerdos con proveedores. Carpetas compartidas y la Intranet del Sistema de Gestión de Calidad.
- Sitio web de Transparencia

8.2. Aplicación de la política

La política será publicada en la carpeta del Sistema de Gestión de Calidad de Savia Salud EPS. Su aplicación se realizará mediante la implementación de controles especificados en el MA-TI-01 Manual de Política de Seguridad de la Información, y será actualizado de acuerdo con los cambios normativos, la evolución de la tecnología y las políticas institucionales.

9. Aprobación de la política

La presente Política rige a partir de la fecha de su expedición y debe ser difundida al interior de la organización y con demás entes u organismos según corresponda.

Firmada en Medellín, Antioquia a los 28 días del mes de abril del año 2026.

EDDA LORENA SINTURA GÓMEZ
Agente Especial Interventor - Suplente
Savia Salud EPS

Histórico del documento

<table>
<tr><th>VERSIÓN</th><th>FECHA DE VIGENCIA</th><th>NATURALEZA DEL CAMBIO</th></tr>
<tr><td>01</td><td>02/12/2019</td><td>Creación del documento.
<table><tr><th>ELABORÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr><tr><td>Jefe de TI</td><td>Jefe de TI</td><td>Gerente</td></tr></table></td></tr>
<tr><td>02</td><td>25/01/2022</td><td>Actualización de la política.

Se elimina la condición general “Garantizar la continuidad del negocio frente a incidentes”, el ítem 6 “indicadores” y el ítem 7 “Valores”.
<table><tr><th>ELABORÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr><tr><td>Auxiliar Administrativo TI - Tatiana Ruiz Ocampo</td><td>Jefe de TI - Iván Darío Merizalde Gartner</td><td>Gerente - Luis Gonzalo Morales Sánchez</td></tr></table></td></tr>
<tr><td>03</td><td>28/04/2026</td><td>Actualización de la política.

Se alinea la política de acuerdo con los estándares de la nueva versión de la ISO/IEC 27001:2022.
<table><tr><th>ELABORÓ</th><th>REVISÓ</th><th>APROBÓ</th></tr><tr><td>Juan Camilo Suárez Builes – Coordinador de Infraestructura y Seguridad Informática (E).</td><td>Tatiana Ruiz Ocampo – Directora de Tecnología e Información (E).

Ingrid Tatiana Rojas Avella – Subgerente Administrativo.

Johanna Patricia Castillo Morales – Secretaria General.</td><td>Edda Lorena Sintura Gómez – Agente Especial Interventor Suplente.</td></tr></table></td></tr>
</table>