PROCESO /SUBPROCESO AL CUAL PERTENECE LA POLÍTICA	SUBPROCESO GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	**RESPONSABLE**	DIRECCIÓN DE TECNOLOGÍA

DEFINICIONES		
No.	**TÉRMINO**	**DEFINICIÓN**
1	Activo de Información	Información o recurso que tiene valor para la entidad y requiere protección.
2	Aplicaciones de Inteligencia Artificial (IA)	Sistemas de software capaces de imitar procesos de inteligencia humana, como aprendizaje, razonamiento y modelos generativos
3	Confidencialidad	Propiedad de que la información no esté disponible ni sea divulgada a individuos o procesos no autorizados
4	Disponibilidad	La propiedad de que los sistemas de información, activos y servicios sean accesibles y utilizables por una entidad autorizada cuando lo requiera.
5	Incidente de Seguridad de la Información	Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de los activos de información.
6	Integridad	La propiedad de que los datos no han sido modificados o alterados de manera no autorizada.
7	Modelo de Seguridad de la Información	Conjunto de principios, estructuras y controles mediante los cuales la entidad gestiona la protección de sus activos de información.
8	Privacidad de la Información	Garantía de tratamiento adecuado de los datos personales conforme a la normatividad vigente.
9	Riesgo de Seguridad	Posibilidad de que una amenaza explote una vulnerabilidad afectando un activo de información.
10	Seguridad de la Información	Conjunto de medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información.
11	Tecnologías emergentes	Tecnologías digitales de reciente adopción o evolución, tales como inteligencia artificial, analítica avanzada o automatización, cuyo uso puede implicar riesgos adicionales para la seguridad de la información.

POLITICA DE SEGURIDAD DE LA INFORMACIÓN - PSI

1. OBJETIVO DE LA POLITICA

Establecer el marco institucional para la protección de los activos de información y datos personales tratados por Capital Salud EPS-S, garantizando su confidencialidad, integridad y disponibilidad conforme a la normatividad vigente y las mejores prácticas reconocidas (nacionales e internacionales).

2. DESCRIPCIÓN DE LA POLÍTICA

Capital Salud EPS-S establece las siguientes directrices institucionales para la protección de la información:

2.1 Protección de la información: La información institucional será protegida de acuerdo con su nivel de sensibilidad y riesgo, garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

2.2 Gestión de accesos a la información: La entidad establecerá mecanismos institucionales para asegurar que el acceso a los sistemas, activos de información y datos institucionales se otorgue únicamente a usuarios autorizados y conforme al principio de necesidad de uso.

2.3 Gestión de riesgos de seguridad de la información: La entidad gestionará los riesgos asociados a la información y a los sistemas tecnológicos en articulación con el modelo institucional de gestión de riesgos.

2.4 Gestión de incidentes de seguridad de la información: La entidad establecerá mecanismos institucionales para la identificación, reporte, análisis y gestión de incidentes de seguridad de la información.

2.5 Protección de datos personales: El tratamiento de datos personales se realizará conforme a la normatividad vigente y a las políticas institucionales de protección de datos.

2.6 Uso responsable de tecnologías emergentes: El uso de aplicaciones de inteligencia artificial (IA) deberá realizarse de manera responsable y segura, conforme a los lineamientos institucionales establecidos.

2.7 Mejora continua de la seguridad de la información: La entidad promoverá el fortalecimiento progresivo de sus capacidades de seguridad mediante la adopción de buenas prácticas y controles apropiados.

2.8 Modelo institucional de seguridad de la información: Capital Salud EPS-S adoptará un modelo institucional de seguridad de la información que articule las capacidades de gobierno, prevención, detección y recuperación, con el fin de proteger los activos de información y fortalecer la resiliencia operativa de la entidad.

2.9 Capital Salud EPS-S promoverá el fortalecimiento de la cultura institucional en materia de seguridad de la información y protección de datos personales, mediante estrategias definidas dentro del Sistema de Gestión de Seguridad de la Información (SGSI) y los lineamientos institucionales que se establezcan para tal fin.

Los mecanismos operativos, controles técnicos y responsabilidades específicas para la implementación de este modelo se desarrollarán mediante los procedimientos, guías e instructivos del sistema de gestión de seguridad de la información.

Fuente: Elaboración Propia

3. ALCANCE

La política aplica a la totalidad de los procesos institucionales; a los funcionarios, contratistas y terceros vinculados a la operación; a los proveedores tecnológicos y responsables del tratamiento de datos; y a todos los activos de información, sistemas, plataformas, servicios digitales, infraestructura y cualquier tipo de soporte físico o electrónico donde la EPS almacene, procese o transmita información.

4. ORIGEN

La presente política se adopta en cumplimiento de:

- Decreto 1377 de 2013.
- Decreto 1499 de 2017.
- Normatividad vigente en materia de protección de datos personales y seguridad digital.
- Buenas prácticas internacionales en gestión de seguridad de la información.
- ISO/IEC 27002 Código de buenas prácticas para controles de seguridad.
- ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.
- Ley 1273 de 2009 Delitos Informáticos Modificó el Código Penal.
- Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública) Regula el acceso a la información pública, procedimientos y excepciones
- Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República
- Artículo 15 de la Constitución Política de Colombia Consagra los derechos a la intimidad personal y familiar, al buen nombre y al hábeas data

5. PLAZO

La política tendrá vigencia indefinida y será revisada anualmente o cuando se presenten cambios normativos, tecnológicos u organizacionales que lo requieran.

6. RECURSOS NECESARIOS PARA EL DESARROLLO DE LA POLÍTICA

Para el desarrollo de la presente política, la entidad dispondrá de:

- Recursos humanos responsables de la gestión de seguridad y privacidad.
- Recursos tecnológicos para el monitoreo y protección de la información.
- Recursos financieros para la implementación progresiva de controles.

7. PERIODICIDAD

La política será revisada anualmente o, cuando ocurra un evento significativo que así lo amerite.

8. REFERENCIAS

DOCUMENTOS DE REFERENCIA	
CÓDIGO (CUANDO APLIQUE)	**NOMBRE DEL DOCUMENTO**
N/A	N/A

9. ELABORACIÓN, REVISIÓN Y APROBACIÓN DE LA POLITICA

NOMBRE RESPONSABLE DE LA ELABORACION	Juan Pablo Pérez	**CARGO**	Técnico de Infraestructura y Seguridad
FECHA DE ELABORACION	10/03/2026		
NOMBRE RESPONSABLE DE LA REVISION	Antonio Jose Romero Vergara Lizeth Mairena Montero Londono	**CARGO**	Director de Tecnología Profesional de Procesos y Calidad
FECHA DE REVISIÓN	04/06/2026		
NOMBRE RESPONSABLE DE LA APROBACION	Comité Institucional de Gestión y Desempeño	**CARGO**	N/A
FECHA DE APROBACION	10/03/2026		

MARCELA BRUN VERGARA
Firmado digitalmente por MARCELA BRUN VERGARA

Marcela Brun Vergara
Gerencia General

Firmado digitalmente por ANTONIO JOSÉ ROMERO VERGARA
Fecha: 2026.07.03 15:02:54 -05'00'

Antonio Jose Romero Vergara
Director de Tecnología