CONTROL DE CAMBIOS

Act.	Fecha	Páginas	Descripción
01	2006.may.16	-	Lanzamiento
02	2008.feb.10	-	Actualización año 2008
03	2009.mar.19	-	Cambio de Formato. Se reorganiza el documento agregándole el aparte “Gestión de la Seguridad Informática”. Se revisan, ajustan y actualizan las políticas para el año 2009.
04	2010.abr.11	Todas	Asignación de código al manual. Se realiza revisión, ajuste y actualización de las políticas para el año 2010.
05	2011.mar.21	Todas	Se agregan políticas de acuerdo con la Norma Internacional ISO 27001. Se realiza revisión, ajuste y actualización de las políticas para el año 2011.
06	2012.abr.22	Todas	Se armoniza el manual con el panorama general de seguridad informática, incluyendo los Planes de Contingencia y el Plan de Continuidad del Negocio. Se actualizan los nombres de los cargos de quien elabora y revisa el Manual. Se realiza revisión, ajuste y actualización de las políticas para el año 2011.
07	2012.ago.13	22-28	Se incluye el ítem políticas de uso de la red de COOSALUD
08	2013.abr.02	6	Se incluye dentro del punto 2 “Manejo de Información” el siguiente ítem, teniendo presente que el tiempo de implementación es de 1 año “Todos los equipos pertenecientes a COOSALUD deberán estar sujetos al control de Aranda, cualquier equipo que no cumpla con lo indicado solo podrá acceder a internet a través de la red de invitados y no podrá tener acceso a los programas de trabajo.”
09	2013.abr.02	-	Se actualiza el documento
10	2013.dic.20	6	Se incluyeron dentro del punto 2 “Manejo de Información” las siguientes políticas: • Queda prohibido el uso de dispositivos de almacenamiento masivo para escritura de archivos. Se restringe el uso de unidades de CD/DVD regrabable
11	2016.feb.08	-	Se actualiza de acuerdo a la operación actual
12	2017.may.19	Todo	Se actualiza el documento
13	2021.abr.29	7,10,11,14 y 15	• Se agregó políticas de trabajo en casa (8.16) • Se actualizo el numeral dispositivo móviles y de proveedores • Se actualizo el numeral nombre de usuarios y contraseñas respecto a parámetros de SAP. • Se actualizo el numeral de responsabilidades del usuario. Se actualizo el numeral de confidencialidad de la información.
14	2021.jun.17	-	Se revisa y ajusta el documento
15	2021.jun.24	-	Se revisa y ajusta el documento
16	2023.mar.01	-	Se revisa y ajusta de acuerdo a la operación actual
17	2024.ago.02	-	Se actualiza la estructura del documento y se incluyen los capítulos y contenidos requeridos frente a los referentes del Sistema de Gestión de Seguridad de Información actualizado.
18	2026.ene.28	Todo	Se actualiza el documento y se incluye 8.12. Política Cumplimiento Normativo y Legal.

APROBACIÓN Y MANTENIMIENTO DEL DOCUMENTO	
Dirección responsable del mantenimiento	Vicepresidente de Innovación Tecnología y Data
Fecha última revisión	2026.ene.28
Periodicidad mínima de revisión	Anual
Órganos responsables de la aprobación	Comité de políticas institucionales
Fecha aprobación	2026.ene.28
Fecha de divulgación en la Compañía	2026.feb.16

CONTENIDO

1. CLASIFICACION Y CONFIDENCIALIDAD

Se considera un documento que debe usarse para fines exclusivos de los colaboradores internos de Coosalud EPS y los demás actores definidos como parte del Sistema de Gestión de Seguridad de la Información (SGSI).

Este documento es clasificado como "**público**".

No se autoriza la reproducción total ni parcial de este documento sin previa autorización de los entes definidos al interior de la organización como responsables.

2. LISTA DE DISTRIBUCIÓN

La distribución de este documento solo puede realizarse por los colaboradores de Coosalud EPS, bajo los lineamientos del Sistema de Calidad según lo establecido para la distribución de copias no controladas.

Su consulta está disponible en el Portal de Calidad para los colaboradores y en la Página Web Oficial de Coosalud EPS para los públicos de interés en general.

3. OBJETIVO

Establecer una política de seguridad de la información y ciberseguridad alineada con la estrategia organizacional.

4. ALCANCE

La política de seguridad de la información y ciberseguridad aplica a las sedes administrativas y puntos de atención, colaboradores, proveedores y partes interesadas que tengan bajo su custodia y manejo, almacenamiento y consulta de información de Coosalud EPS y/o de terceros, enmarcado en el alcance del Sistema de Seguridad de la Información como se determina en el documento TIC-M-47 MANUAL DE GESTION DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD.

5. RESPONSABILIDADES Y ROLES

Se define como Líder del SGSI de Coosalud EPS al colaborador que se encuentre desempeñando el cargo de “subdirector de Seguridad Informática”, los demás roles que de manera directa soportan el alcance del SGSI, se relacionan en el documento TIC-M-47 MANUAL DE GESTION DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD.

6. DECLARACIÓN GENERAL

En Coosalud EPS, como administradores de servicios de salud, entendemos nuestra responsabilidad con los clientes, colaboradores y partes interesadas para salvaguardar sus datos y mantener la confianza que depositan en nosotros, por lo cual se establece esta “**Política de Seguridad de Información y Ciberseguridad”**, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información que manejamos. Nuestra política se alinea con el cumplimiento de los objetivos estratégicos y las definiciones normativas y regulatorias aplicables a los procesos organizacionales, bajo el liderazgo y compromiso de la alta dirección al dar los recursos necesarios para definir, implementar, supervisar y mejorar el sistema de gestión de seguridad de información (SGSI).

7. OBJETIVOS DE SEGURIDAD DE INFORMACION

Los objetivos de seguridad de la información se encuentran descritos a continuación:

1. Implementar controles de seguridad de la información y ciberseguridad de acuerdo con el tipo de activo a disponer y proteger.
2. Mantener la precisión y completitud de la información y los métodos de procesamiento.
3. Implementar mecanismos que controlen el acceso a la información solo a usuarios o sistemas autorizados, basándose en las políticas definidas.
4. Realizar seguimiento y revisión de las actividades en los sistemas de información para detectar posibles violaciones de seguridad o anomalías en el uso de la información.
5. Desarrollar y mantener un plan efectivo para responder a incidentes de seguridad, minimizando el impacto en la operación.
6. Establecer planes y procedimientos para mantener y restaurar las operaciones de negocio en caso de interrupciones o desastres.
7. Educar a los colaboradores sobre sus responsabilidades en cuanto a la seguridad de la información y asegurarse que comprenden las políticas y procedimientos de seguridad.
8. Asegurar que el SGSI cumple con todas las leyes, regulaciones y obligaciones contractuales pertinentes, así como con las políticas internas de la organización.

8. POLITICAS ESPECIFICAS DE SEGURIDAD DE INFORMACIÓN

8.1. Política de Gestión de Activos de Información

Coosalud EPS establece su compromiso con asegurar que los activos de información de la organización sean adecuadamente identificados, protegidos y gestionados a lo largo de su ciclo de vida, para garantizar la confidencialidad, integridad y disponibilidad de la información.

8.2. Política de Gestión y Control de Acceso

Coosalud EPS establece su compromiso con garantizar que solo los usuarios autorizados puedan acceder a los recursos y datos de la organización, mientras se protege la seguridad de la información y se cumplen los requisitos legales y regulatorios.

8.3. Política de Gestión de la Seguridad Física

Coosalud EPS establece su compromiso con garantizar un entorno seguro y protegido para los activos de información de la organización, minimizando los riesgos de seguridad y asegurando la continuidad y la integridad de las operaciones tecnológicas.

8.4. Política de Seguridad de Datos e Información

Coosalud EPS establece su compromiso con proteger la información sensible y crítica de la organización, garantizando su confidencialidad, integridad y disponibilidad.

8.5. Política de Operaciones de Tecnología

Coosalud EPS establece su compromiso con identificar, implementar, monitorear y mejorar de manera continua, los controles relacionados con la gestión de seguridad de redes y la transferencia de información al igual que garantizar la disponibilidad y la integridad de los datos críticos de la organización en caso de pérdida, corrupción o daño a través de la gestión de copias de respaldo.

8.6. Política de Gestión de Proveedores de TI

Coosalud EPS establece su compromiso con asegurar que la organización tenga acceso a productos y servicios tecnológicos de calidad, seguros y confiables, que cumplan con los requisitos de negocio y regulatorios, y que contribuyan como aliado a la administración de las operaciones en el marco de la seguridad de la información.

8.7. Política de Gestión de Desarrollo de Software

Coosalud EPS establece su compromiso con garantizar que las aplicaciones y sistemas desarrollados o de terceros empleados en las operaciones de la organización sean robustos, seguros y resistentes a las amenazas y vulnerabilidades.

8.8. Política de Administración Infraestructura Tecnológica

Coosalud EPS se compromete a garantizar que todos los componentes de la infraestructura tecnológica de la organización estén configurados, gestionados y protegidos eficazmente para minimizar los riesgos de seguridad y mantener la integridad, confidencialidad y disponibilidad de datos y sistemas.

8.9. Política de Gestión de Incidentes

Coosalud EPS establece su compromiso con identificar, gestionar y resolver de manera eficiente y efectiva cualquier incidente de seguridad que pueda ocurrir mediante la implementación de acciones que permitan reducir el impacto de los eventos de seguridad adversos, proteger los activos de la organización y mantener la integridad y disponibilidad de los sistemas y datos críticos.

8.10. Política de Gestión de Ciberseguridad

Coosalud EPS establece su compromiso con establecer un marco de referencia y directrices claras para proteger los activos digitales y la información sensible de la organización contra amenazas cibernéticas con estrategias que promuevan una cultura de seguridad proactiva y resiliente en toda la organización.

8.11. Política de Recuperación y Restauración de la Operación Tecnológica

Coosalud EPS establece su compromiso con restaurar sus sistemas tecnológicos y recuperar la operación normal después de un incidente o desastre que interrumpa su funcionamiento bajo un plan estructurado que permita proteger la integridad y disponibilidad de los datos y sistemas críticos.

8.12. Política Cumplimiento Normativo y Legal

Coosalud EPS establece su compromiso con el cumplimiento de todos los requisitos legales, reglamentarios, estatutarios y contractuales aplicables en materia de seguridad de la información y ciberseguridad, incluyendo: Ley 1581 de 2012 Protección de Datos, Ley 1266 de 2008 Habeas Data, Resolución 497 de 2021 del Ministerio de Salud – Estándar XII-Tecnologías de Información, Modelo de Seguridad y Privacidad de la Información de MINTIC, entre otros.

9. COMUNICACIÓN, ACTUALIZACIÓN Y ACEPTACIÓN

a. La política de seguridad de información y ciberseguridad debe estar disponible para consulta de las partes interesadas y será divulgada y comunicada como se establece en el documento TIC-M-47 MANUAL DE GESTION DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD.
b. La política de seguridad de información y ciberseguridad debe ser actualizada al menos una vez al año y/o cuando se presenten cambios normativos y regulatorios o de negocio que impacten las definiciones establecidas en este documento.
c. Los colaboradores, proveedores, terceros y demás partes interesadas según aplique, deberán conocer y aceptar las políticas de seguridad de información una vez ingresen a desarrollar actividades en la compañía, incluyendo las actualizaciones que se realicen a dichas directrices.

10. MEDICIÓN

Para medir el desempeño del Sistema de Seguridad de la Información de Coosalud EPS, se han definido indicadores relacionados en el Consolidado de Indicadores del SGSI.

11. REFERENTES

Para la elaboración del marco de políticas, procesos, manuales, guías e instructivos se han utilizado las siguientes normas y mejores prácticas de seguridad de la información y ciberseguridad:

- Marco de Ciberseguridad NIST versión 1.1
- ISO 27001: 2022
- Ley 1581 de 2012 Protección de Datos
- Ley 1266 de 2008 Habeas Data
- Resolución 497 de 2021 del Ministerio de Salud – Estándar XII-Tecnologías de Información
- Modelo de Seguridad y Privacidad de la Información de MINTIC

La metodología empleada para la homologación de estos referentes/estándares se describe en el documento TIC-M-47 MANUAL DE GESTION DE SEGURIDAD DE INFORMACIÓN Y CIBERSEGURIDAD.