



# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

**VALENTINA SOSA CARVAJAL**

Gerente ESE Metrosalud

**Dirección sistemas de información**

**31/01/2023**

**Versión [03]**



**Alcaldía de Medellín**  
Distrito de  
**Ciencia, Tecnología e Innovación**

## Contenido

|                              |                                                                           |         |
|------------------------------|---------------------------------------------------------------------------|---------|
| 1.....                       | LINEAMIENTOS DE POLÍTICA                                                  | 3       |
| 2.....                       | INTRODUCCIÓN                                                              | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 3.....                       | OBJETIVOS                                                                 | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 3.1. ....                    | OBJETIVO GENERAL                                                          | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 3.2. ....                    | OBJETIVOS ESPECÍFICOS                                                     | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 4.....                       | ALCANCE                                                                   | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.....                       | MARCO TEÓRICO O CONCEPTUAL                                                | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 4.1. ....                    | MARCO NORMATIVO                                                           | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.....                       | DESARROLLO DEL PLAN:                                                      | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1. ....                    | FORMULACIÓN                                                               | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.1. ....                  | ÁMBITO DE APLICACIÓN                                                      | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.2. ....                  | ROLES Y RESPONSABILIDADES EN LA GESTIÓN DEL RIESGO                        | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.3. ....                  | POLÍTICA DE GESTION DEL RIESGO                                            | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.4. ....                  | ANÁLISIS DE RIESGOS PARA EL SISTEMA DE INFORMACION EN LA E.S.E METROSALUD | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.5. ....                  | CALIFICACIÓN DEL RIESGO                                                   | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.6. ....                  | DESCRIPCION DEL METODO                                                    | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |
| 5.1.7. ....                  | IDENTIFICACION DE LOS CONTROLES                                           | ¡Error! |
| <b>Marcador no definido.</b> |                                                                           |         |

5.1.8. .... ANALISIS DE RIESGOS E.S.E METROSALUD **¡Error!**

**Marcador no definido.**

□ ACTIVIDADES INHERENTES A LA GESTION INFORMATICA (ESCENARIOS SUJETOS A CONTROL)

..... **¡Error! Marcador no definido.**

5.2. .... IMPLEMENTACIÓN Y DESPLIEGUE **¡Error!**

**Marcador no definido.**

5.3. .... SEGUIMIENTO – MONITOREO **¡Error!**

**Marcador no definido.**

5.4. .... EVALUACIÓN **¡Error!**

**Marcador no definido.**

6. .... DEFINICIONES Y CONCEPTOS **¡Error!**

**Marcador no definido.**

7. .... BIBLIOGRAFÍA 11

8. .... DOCUMENTOS RELACIONADOS: 12

Los documentos institucionales están sujetos a actualización permanente de sus versiones. Serán puestos a disposición de los servidores de Microsalud en el aplicativo del Sistema Integrado de Gestión

## PLATAFORMA ESTRATÉGICA Y CONTENIDO INSTITUCIONAL

Misión, Visión Ventaja competitiva, Promesa de valor, Objetivos corporativos, Competencias corporativas. Ver enlace <http://www.metrosalud.gov.co/metrosalud/institucional>

Principios y valores corporativos. Ver enlace: <http://www.metrosalud.gov.co/metrosalud/principios-y-valores>

Organigrama institucional. Ver enlace:

<http://www.metrosalud.gov.co/metrosalud/organigrama>

Mapa de procesos. Ver enlace:

<http://www.metrosalud.gov.co/metrosalud/estructura-de-procesos>

Deberes y Derechos de los usuarios. Ver enlace

<http://www.metrosalud.gov.co/usuarios/derechos-y-deberes>

### 1. LINEAMIENTOS DE POLÍTICA

PE01 PO 46 POLÍTICA GESTIÓN DE RIESGOS

PE01 PO 57 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Articulación del plan con otros planes y proyectos estratégicos a nivel interno y externo a la institución.

A nivel interno el Plan De Seguridad y Privacidad de la Información, se articula con los siguientes planes:

- ☐ Plan Estratégico de ESE METROSALUD.
- ☐ Plan del Sistema Integrado de Gestión de ESE METROSALUD.
- ☐ Plan Estratégico de Sistemas de Información de ESE METROSALUD.
- ☐ Plan de Comunicaciones de ESE METROSALUD.
- ☐ Plan de Capacitaciones de ESE METROSALUD.
- ☐ Planes de Acción y de Mejora Continua de ESE METROSALUD.
- ☐ Planes de Atención Usuarios de ESE METROSALUD.

## **1. INTRODUCCIÓN**

METROSALUD, Empresa Social del Estado (ESE), dando cumplimiento al artículo 2.2.9.1.2.2 del Decreto 1078 de 2015, el cual permite adoptar los instrumentos para implementar la estrategia de Gobierno en Línea, dentro de los cuales exige la elaboración de un Plan Estratégico de Tecnologías de la información y las comunicaciones – PETI y de un plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información y el Plan de Seguridad y Privacidad de la Información.

Por lo anterior, se resalta su importancia como soporte a la planeación estratégica en los aspectos de Tratamiento de los Riesgos en la Seguridad y Privacidad de la Información, en el orden normativo, administrativo, económico, técnico y tecnológico; teniendo presente que el tratamiento de la información y el control de los riesgos, contribuyen a la eficacia y eficiencia administrativa, el servicio al ciudadano y el acceso a la información.

## **2. OBJETIVO**

Servir como marco de referencia para la planeación y desarrollo del que hacer en el tratamiento de la información y la gestión del riesgo.

### **2.1. Objetivos institucionales**

- Referenciar sobre la importancia de la contar con procedimientos validados como instrumentos para garantizar la Seguridad y Privacidad de la Información
- Garantizar la preservación y conservación de la información que conforma el acervo documental de la Empresa Social del Estado ESE METROSALUD, como un derecho a la información clara, oportuna y actual, y el deber de suministrar información completa y veraz al personal de salud.
- Formalizar y ponderar los recursos humanos, financieros, tecnológicos y, de infraestructura, como soporte para la ejecución de los proyectos previstos a corto, mediano y largo plazo en la gestión de asignación oportuna.
- Afirmar que la entidad cuente con procedimientos claros para la gestión y accesibilidad a los sistemas de información
- Apoyar el apalancamiento institucional, la transparencia, la eficacia y el acceso a la información.

### **2.2. Objetivos específicos (plan de seguridad y privacidad de la información)**

- Garantizar el buen uso de las herramientas que permitan de forma segura y controlada el acceso a la información.

- Mejorar la eficiencia administrativa e incrementar la productividad organizacional.
- Articular y coordinar los planes, programas, proyectos y modelos relacionados en función de La Seguridad y Privacidad de la información.
- Facilitar el seguimiento, medición y mejora de los planes y proyectos formulados.

### 3. ALCANCE

**RESPONSABILIDAD:** La responsabilidad de la seguridad y privacidad de la información y la administración del riesgo de la seguridad y privacidad de la información, está a cargo en primera instancia de la Dirección de ESE METROSALUD, a través de la Gerencia General y la Dirección de Sistemas de Información con la participación directa del área de gestión documental; más sin embargo la información es transversal a la entidad, esta debe asociarse a los procesos de todos los responsables de oficinas productoras de información administración, custodia, conservación total, selección, eliminación y aplicación de tecnologías de seguridad.

### 4. MARCO TEÓRICO O CONCEPTUAL

#### 4.1. MARCO NORMATIVO

- ☐ Ley 1712 de 2014. Congreso de la República. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- ☐ Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- ☐ Ley 594 de 2000. Congreso de Colombia. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Artículo 21. Programas de Gestión Documental.
- ☐ Decreto 1078 de 2015. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- ☐ Decreto 612 de 2018. Presidente de la República de Colombia. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- ☐ Ley 1474 de 2011 (Estatuto Anticorrupción).

## **4.2. MARCO TEÓRICO**

Esquema de medición del plan:

### **4.2.1. Identificación de la situación actual**

La ESE METROSALUD, es una organización de carácter pública, comprometida con generar cultura de vida sana, en Medellín y en la región.

Los servicios de la ESE METROSALUD, están basados en el acompañamiento al usuario en cada una de las etapas de su ciclo de vital a través de acciones integrales de promoción de la salud, prevención de la enfermedad, protección específica y atención de enfermedades de interés en salud pública. Nuestro objetivo es favorecer los factores protectores y detectar y controlar los factores de riesgo.

La fuente de la información, que se almacena en los sistemas de información de METROSALUD, se originan desde atención del usuario, y corresponde a información sensible y delicada, la cual se encuentra protegida por la normatividad vigente, relacionada a la confidencialidad y tratamiento de la información.

Frente a los procesos de tecnología de la información ESE METROSALUD, cuenta con sistema de respaldo que le permite mantener buenas políticas de seguridad y de acceso, igualmente cuenta con un sistema de información donde se almacena los datos transaccionales de los afiliados de la ESE METROSALUD, garantizando su trazabilidad e integridad de la información.

El sistema de información transaccional SAFIX, se mantiene en constante actualización por parte del proveedor XENCO, lo cual garantiza que constantemente cumple con el marco normativo.

A nivel de infraestructura el sistema de información está soportado por los respectivos servidores que cuentan con las normas técnicas que garantizan una alta disponibilidad de la información.

Los accesos a los cuartos del cableado estructurado, se están adecuando con el fin de garantizar la seguridad perimetral y controlar los respectivos accesos.

La entidad cuenta con el aplicativo SAFIX, el cual controla por usuario, su respectivo acceso, lo cual garantiza la seguridad en el acceso a la información.

Los proveedores de tecnología con los que cuenta actualmente la ESE METROSALUD, al momento de establecer cualquier vínculo laboral, firman Acuerdos de Confidencialidad.

Los usuarios del sistema de información, pueden en cualquier momento realizar el cambio de la contraseña, así se garantiza controla cualquier ingreso fraudulento.

La continuidad y disponibilidad del sistema de información y el cual soporta la gestión y transaccionalidad, está garantizada por diferentes esquemas de atención que se tienen y que se activan al momento de llegar a ocurrir una falla que coloque en riesgo el acceso al sistema de información

#### **4.2.2. Metodología para el desarrollo del plan de seguridad y privacidad de la información**

Para la realización del Plan de Seguridad y Privacidad de la Información, en ESE METROSALUD, se toma como base la guía de Procedimientos de Seguridad de la Información – MINTIC, la cual contempla el desarrollo de los siguientes Dominios:

- ☐ Seguridad del Recurso Humano
- ☐ Gestión de Activos
- ☐ Control de accesos
- ☐ Criptografía
- ☐ Seguridad Física y del Entorno
- ☐ Seguridad de las Operaciones
- ☐ Seguridad de las comunicaciones
- ☐ Relaciones con los proveedores
- ☐ Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- ☐ Gestión de Incidentes de Seguridad de la Información
- ☐ Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio

Para realizar la identificación de la situación actual en ESE METROSALUD, se toma como alcance para su implementación todas las instalaciones de la ESE METROSALUD, donde se evaluarán los ítems anteriores con el fin de identificar cuales están documentados y cuales están pendientes para su documentación.

Se identificarán cada una de las actividades relacionadas a cada procedimiento, se destinará el respectivo plan de trabajo, con el objetivo de dar cumplimiento a que cada procedimiento este documentado.

Se contemplarán todos los componentes tecnológicos (infraestructura, accesos, sistema de información) y que hacen parte del ciclo de vida del almacenamiento de la información

Se tuvo además en cuenta la orientación del Plan Estratégico Institucional y el Plan de Acción Anual, que la alta Dirección de ESE METROSALUD, desde su rol estratégico, realiza para definir actividades de planeación, revisión y mejora, y lograr la eficiencia, eficacia y cumplimiento con los objetivos y metas trazadas para la entidad.

#### 4.2.3. Identificación de los procedimientos

Para la identificación de cada una de las actividades correspondiente a los distintos procedimientos de las que habla la Guía MinTIC para la Gestión y seguridad y privacidad de la información ([https://www.mintic.gov.co/gestioni/615/articles-5482\\_G3\\_Procedimiento\\_de\\_Seguridad.pdf](https://www.mintic.gov.co/gestioni/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf)), se realizó una verificación sobre los procedimientos existentes y sobre los cuales se debe de realizar una estrategia, con el fin de poder desarrollar cada uno de los procedimiento y poder disponer de ellos de una manera documental.

Dichas actividades a desarrollar son:

- ☐ Diagnostico general de los procedimientos a documentar
- ☐ Plan de actividades con cronograma para el seguimiento y ejecución de cada una de ellas.

Como resultado del análisis, se identifican para ESE METROSALUD, las siguientes actividades que se deben de desarrollar.

| PLANES /PROYECTOS                                              | Plan de Desarrollo 2021 - 2025 Ruta estratégica Metrosalud transparente, clara, inteligente e innovadora /Sistema de información que soporta la toma de decisiones – Transformación digital |              |            |                                                |
|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|------------|------------------------------------------------|
| OBJETIVOS                                                      | Garantizar y velar la conservación de la información de la ESE METROSALUD, en cumplimiento de la normatividad, en el tratamiento y privacidad de la información y la gestión del riesgo.    |              |            |                                                |
| ACTIVIDADES                                                    | RESPONSABLE                                                                                                                                                                                 | FECHA INICIO | FECHA FIN  | ENTREGABLE                                     |
| Actividad: Verificación de la Seguridad de los accesos físicos | Dirección de Sistemas de Información / Activos Fijos                                                                                                                                        | 01/02/2023   | 30/12/2023 | Plan de mantenimiento / Informe de Seguimiento |

|                                                                                                       |                                                    |            |            |                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------|------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                       |                                                    |            |            | / Documento de especificaciones técnicas                                                                                                                                                                            |
| Actividad: Validar la seguridad y continuidad de la Operación                                         | Dirección de Sistemas de Información / Proveedores | 02/05/2023 | 30/12/2023 | Informe técnico de comportamiento y disponibilidad de los ambientes                                                                                                                                                 |
| Actividad: Verificar el tratamiento de la información con los distintos proveedores                   | Dirección de Sistemas de Información / Proveedores | 02/01/2023 | 30/11/2023 | Constancia del registro de BD                                                                                                                                                                                       |
| Actividad: Verificar como es el seguimiento y el control de los incidentes                            | Dirección de Sistemas de Información / Proveedores | 02/01/2023 | 30/12/2023 | Documento Detallado de Incidentes / Informe de actividades de mitigación por cada evento                                                                                                                            |
| Actividad: Validar políticas de seguridad y su vigencia descritas en el documento de especificaciones | Dirección de Sistemas de Información / Proveedores | 2/01/2023  | 30/06/2023 | Informe con cumplimiento de cada una de las políticas, Documento ajustado, Ejecución del plan de remediación. Documento de acuerdo aprobado y socializado con las áreas de contratación, talento humano y mercadeo. |

#### 4.2.4. Formulación

Para la formulación del plan se tomó en cuenta las oportunidades de mejora generadas a partir de los análisis de seguridad realizados y las mejores prácticas del mercado. En su formulación contó con la participación de la Dirección de sistemas de información y los criterios y conceptos de los ingenieros analistas en este campo.

#### **4.2.5. Implementación y despliegue**

Se divulgará a través del software Almera se publicará en la página web (ítem transparencia) y se socializará al personal de la Dirección de sistemas de información.

#### **4.2.6. Seguimiento – Monitoreo**

Para dar cumplimiento al Decreto 612 de 2018, se realizará el respectivo seguimiento a cada una de las actividades mencionadas anteriormente.

ESE METROSALUD, generará los mecanismos e instrumentos necesarios que brinden las garantías para el desarrollo del Plan de Seguridad y Privacidad de la Información.

ESE METROSALUD, implementará con los diferentes equipos de trabajo, los distintos procedimientos que permitan tener la documentación actualizada y disponible como guía para las buenas prácticas.

Se realizará a través del software Almera y se apoyará en la matriz de seguimiento de actividades plan adjunta.

#### **4.2.7. Evaluación**

El seguimiento se realizará en el aplicativo Almera trimestralmente con reportes de avance del mismo. Se obtendrá el nivel de cumplimiento del plan a través del software Almera.

La evaluación estará a cargo de la Dirección de sistemas de información y se articulará en el reporte del seguimiento y evaluación al plan de acción de la vigencia.

### **5. DEFINICIONES Y CONCEPTOS**

Sistemas de información: Conjunto de elementos orientados al tratamiento y administración de los datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Privacidad de la información: Es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros.

|                         |            |                                                                 |                                                                                     |
|-------------------------|------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Código:                 | PE01 PL 19 | <b>PLAN DE SEGURIDAD Y<br/>PRIVACIDAD DE LA<br/>INFORMACIÓN</b> |  |
| Versión:                | 03         |                                                                 |                                                                                     |
| Vigente a<br>partir de: | 31/01/2023 |                                                                 |                                                                                     |
| Página:                 | 12 de 13   |                                                                 |                                                                                     |

**Riesgo:** Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos Institucionales o del proceso. Se expresa en términos de probabilidad y consecuencia.

**Plan:** Diseño o esquema detallado de lo que habrá de hacerse en el futuro.

**Confidencialidad:** La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona.

**Seguridad Informática:** La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

**Aspecto crítico:** Percepción de problemáticas referentes a la función de la información que presenta la entidad, como resultado de la evaluación de la situación actual.

**Plan Estratégico Institucional:** Instrumento que organiza y orienta estratégicamente las acciones de la entidad en un plazo de 4 años para alcanzar objetivos acordes con su misión y con el Plan Nacional de Desarrollo.

**Plan de Acción Anual:** Es la programación anual de las actividades, proyectos y recursos que va a desarrollar en la vigencia cada dependencia en la entidad, articulado con el Plan Estratégico Sectorial Institucional.

## 6. BIBLIOGRAFÍA

Guía Procedimientos y Seguridad de la información MinTic.

Decreto 612 de 2018. Presidente de la República de Colombia. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

Decreto 1080 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura, artículo 2.8.2.5.8." Instrumentos Archivísticos para la Gestión Documental página 123  
Decreto 1499 de 2017 "Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"

## 4. BIBLIOGRAFÍA

No aplica

|                      |            |                                                                 |                                                                                     |
|----------------------|------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Código:              | PE01 PL 19 | <b>PLAN DE SEGURIDAD Y<br/>PRIVACIDAD DE LA<br/>INFORMACIÓN</b> |  |
| Versión:             | 03         |                                                                 |                                                                                     |
| Vigente a partir de: | 31/01/2023 |                                                                 |                                                                                     |
| Página:              | 13 de 13   |                                                                 |                                                                                     |

## 5. DOCUMENTOS RELACIONADOS:

No aplica.

| ELABORADO POR:                      |                                                  |
|-------------------------------------|--------------------------------------------------|
| Nombre: Jaime Alberto Henao Acevedo | Cargo: Director Sistemas de Información          |
| Nombre: Santiago Zapata García      | Cargo: Profesional Universitario infraestructura |

| CONTROL DE ACTUALIZACIÓN |            |                                                                  |                                                             |                                  |
|--------------------------|------------|------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------|
| VERSIÓN                  | FECHA      | DESCRIPCIÓN DEL CAMBIO O AJUSTE                                  | RAZÓN DEL CAMBIO O AJUSTE                                   | RESPONSABLE DEL CAMBIO O AJUSTE  |
| 01 Almera                | 22/01/2019 | Se crea el plan en el software Almera.                           | Actualización de la documentación en el nuevo software.     | Director Sistemas de Información |
| 02 Almera                | 30/01/2019 | Se crea el plan en correspondencia con la estructura documental. | Se crea el plan para responder a requerimientos normativos. | Director Sistemas de Información |
| 03 Almera                | 23/01/2023 | Se crea el plan en correspondencia con la estructura documental. | Se crea el plan para responder a requerimientos normativos. | Director Sistemas de Información |