# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

EMPRESA SOCIAL DEL ESTADO
HOSPITAL LA MARÍA
MEDELLÍN

*Trabajamos con amor por la vida desde 1923*

CERTIFICADO POR SU COMPROMISO FENALCO SOLIDARIO RESPONSABILIDAD SOCIAL

**MEDELLÍN**

**2025**



Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellín, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

## 1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Empresa Social del Estado Hospital La María, en cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la normativa vigente en Colombia, adopta esta política como compromiso institucional para proteger sus activos de información. Esta política tiene como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información, promoviendo una cultura organizacional basada en la gestión responsable y segura de los datos.

## 2. INTRODUCCIÓN

El presente plan establece los lineamientos técnicos, organizacionales y administrativos para la gestión de la seguridad y privacidad de la información del Hospital La María, entidad de salud de tercer nivel. Este documento es el instrumento rector que soporta las acciones para proteger los activos de información y prevenir incidentes de seguridad.

## 3. ALCANCE

Aplica a todos los procesos, servicios, tecnologías y personas que interactúan con la información institucional, incluyendo empleados, contratistas, terceros y proveedores que accedan o administren datos.

## 4. OBJETIVOS

### 4.1. Objetivo General

Establecer el marco de actuación para la protección de los activos de información de la ESE Hospital La María.

### 4.2. Objetivo Específicos

- Definir el rol institucional del Especialista en Seguridad de la Información como líder técnico, articulador entre procesos y garante de la implementación del MSPI.
- Definir roles y responsabilidades claras en materia de seguridad.
- Implementar medidas técnicas y organizacionales para la protección de la información.
- Fomentar la cultura de seguridad digital.
- Garantizar la trazabilidad de los incidentes y su adecuada gestión.

## 5. DEFINICIONES

- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos.

- **Vulnerabilidad**: La vulnerabilidad es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la
- incapacidad para reponerse después de que ha ocurrido un desastre

- **Resguardo**: Es la irrenunciabilidad, es decir, permite probar la participación de las diferentes partes de una comunicación. La diferencia con la autenticación es que la primera se produce entre dos individuos, y la segunda frente un tercero.

  Hay dos tipos de no repudio:

  **En origen**: El emisor no puede negar el envió porque el destinatario tiene pruebas de la emisión.

  **En destino**: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción.

- **Responsabilidad**: Responsabilidad es el cumplimiento de las obligaciones, o el cuidado al tomar decisiones o realizar algo.

## 6. MARCO NORMATIVO

- Ley 1581 de 2012 – Protección de datos personales.
- Ley 1712 de 2014 – Ley de transparencia.
- Ley 527 de 1999 – Comercio electrónico.
- Decreto 620 de 2020 – Modelo de Gobierno Digital.
- ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información.



Calle 92 EE No 67-61 PBX 447192 NIT 890.905.177-9 Medellín, Colombia
gerencia@lamaria.gov.co/www.lamaria.gov.co

- Directrices MSPI del MinTIC.

## 7. DESCRIPCIÓN DEL PLAN

### 7.1. Planear:

- Diagnóstico de seguridad.
- Inventario de activos.
- Matriz de riesgos.
- Plan de tratamiento de riesgos.

### 7.2. Hacer:

- Implementación de controles.
- Capacitación y sensibilización.
- Actualización de procedimientos.

### 7.3. Verificar:

- Auditorías internas.
- Indicadores de desempeño.
- Revisión de incidentes.

### 7.4. Actuar:

- Mejoras continuas.
- Actualización del plan.
- Retroalimentación institucional.

## 8. INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

Cada líder de proceso es responsable por la identificación, clasificación y protección de los activos que gestiona. Se contará con una documentación centralizada y actualizada semestralmente por el área de Gestión Documental.

## 9. ROLES

### 9.1. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Como objetivo principal para la seguridad de la información este comité realiza la aprobación y supervisión a la aplicación de los requisitos definidos en lo relacionado con la seguridad de la información, los lineamientos estratégicos en cuanto a seguridad de la información y garantiza los recursos, para la toma de decisiones orientadas al cumplimiento de la estrategia.

### 9.2. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (CISO)

Tiene la responsabilidad de guiar y realizar el seguimiento de la implementación de los planes de seguridad definidos.

### 9.3. ADMINISTRADOR DE SEGURIDAD DE LA INFORMACIÓN (ISM)

Tienen la responsabilidad de la gestión de los esfuerzos de seguridad de la información, encargado de labores específicas de seguridad.

### 9.4. LÍDERES DE PROCESOS

Tienen la responsabilidad de dar la cobertura de los lineamientos de seguridad a cada uno de sus procesos operacionales

## 10. ELABORACIÓN DE MATRIZ DE RIESGOS

Para realizar una evaluación de riegos efectiva, el Hospital La María utiliza métodos que les permiten garantizar la identificación de peligros potenciales en el lugar de trabajo. Utilizan herramientas basadas en enfoques formales que permitan minimizar el impacto del riesgo.

## 11. DIVULGACIÓN Y COMUNICACIÓN

La oficina de sistemas en con junto con las áreas de comunicaciones realizaran actividades de socialización para el buen manejo de la información haciendo uso de los medios de comunicación actuales, con los cuales podrán impactar masivamente cada uno de colaboradores y clientes internos o externos que hagan uso de los servicios o instalaciones de la ESE Hospital La María.

## 12. PLAN DE IMPLEMENTACION

Se realizarán campañas de sensibilización, envío de boletines informativos digitales. Los boletines se impartirán mínimo dos veces al año para todos los colaboradores.

| Actividad | Responsable | Medio de ejecución | Frecuencia | Indicador |
|---|---|---|---|---|
| **Campañas de sensibilización en seguridad digital** | Oficina TIC + Comunicaciones | Presencial / Digital | Trimestral | % participación por evento |
| **Envío de boletines informativos de seguridad** | Oficina TIC | Correo institucional | Semestral | N° boletines enviados |
| **Evaluaciones de conocimiento básico en seguridad** | Área TIC | Formularios digitales | Anual | % de aciertos por colaborador |

| | NOMBRE – CARGO | FIRMA | FECHA |
|---|---|---|---|
| **PROYECTÓ** | Sebastián Muñoz Mejía – jefe de Sistemas | Electrónicamente | 12-02-25 |
| **APROBÓ** | Elkyn Hernán García Jaramillo - subgerente | Electrónicamente | 12-02-25 |