E.S.E. Hospital San Lorenzo

Al servicio de la vida

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

Contenido

1. INTRODUCCION

En el marco del **Modelo Integrado de Planeación y Gestión (MIPG)**, la información se reconoce como un **activo estratégico fundamental** para el cumplimiento de los objetivos institucionales y la adecuada prestación de los servicios de salud. En este contexto, la gestión responsable de la información y la implementación de controles efectivos de **seguridad y privacidad** se constituyen en elementos esenciales para garantizar la eficiencia, transparencia y continuidad de los procesos misionales de la **E.S.E. Hospital San Lorenzo de Liborina**.

El uso creciente de los sistemas de información y de las infraestructuras tecnológicas para soportar procesos de misión crítica exige la adopción de **estrategias de alto nivel** que permitan el control, protección y administración adecuada de los activos de información. La entidad enfrenta diversas **amenazas de seguridad digital**, tales como fraude informático, espionaje, sabotaje, vandalismo, incendios, robos, inundaciones, así como riesgos derivados del uso indebido de los sistemas, la presencia de código malicioso y los ataques de denegación de servicio, los cuales pueden afectar la confidencialidad, integridad, disponibilidad y privacidad de la información.

En cumplimiento de lo dispuesto en el **Decreto 612 de 2018**, y en concordancia con la **Política de Seguridad Digital** y la **Política de Gobierno Digital**, la E.S.E. Hospital San Lorenzo de Liborina adopta el presente **Plan de Seguridad y Privacidad de la Información**, como un instrumento de planeación que se integra al MIPG y contribuye al fortalecimiento del control interno, la gestión del riesgo y la protección de los datos personales y demás activos de información institucionales.

Este plan tiene como propósito **garantizar la confidencialidad, integridad y disponibilidad de la información**, así como la protección de la privacidad de los datos personales, mediante la definición de lineamientos, responsabilidades, controles y acciones orientadas a la prevención, mitigación y tratamiento de los riesgos de seguridad digital, asegurando la continuidad de los servicios de salud y el cumplimiento de la normatividad vigente, en coherencia con los objetivos misionales y estratégicos de la entidad.

2. MARCO NORMATIVO

El **Plan de Seguridad y Privacidad de la Información** de la **E.S.E. Hospital San Lorenzo de Liborina** se fundamenta en la normatividad vigente que regula la gestión de la información, la seguridad digital, la protección de datos personales y la planeación institucional en las entidades públicas del Estado colombiano, en especial en el sector salud. Entre las principales disposiciones normativas se encuentran:

2.1 Normativa Constitucional

- **Constitución Política de Colombia**
  Artículos 15 y 20, que consagran el derecho fundamental a la intimidad, al buen nombre, al habeas data y al acceso a la información, así como la obligación de proteger los datos personales y garantizar su adecuado tratamiento.

2.2 Normativa sobre Planeación y Gestión Institucional

- **Decreto 1499 de 2017**
  Por el cual se adopta el **Modelo Integrado de Planeación y Gestión (MIPG)**, que establece la gestión de la información y la seguridad digital como componentes esenciales para el desempeño institucional y el control interno.
- **Decreto 612 de 2018**
  Por el cual se fijan las directrices para la integración de los planes institucionales y estratégicos al MIPG, incluyendo el **Plan de Seguridad y Privacidad de la Información**, como instrumento obligatorio de planeación en las entidades públicas.

2.3 Normativa sobre Gobierno Digital y Seguridad Digital

- **Decreto 1078 de 2015** – Decreto Único Reglamentario del Sector TIC
  Establece los lineamientos de la **Política de Gobierno Digital**, incluyendo los componentes de seguridad y privacidad de la información en las entidades del Estado.
- **CONPES 3854 de 2016**
  Define la **Política Nacional de Seguridad Digital**, orientada a la gestión de riesgos digitales, la protección de los activos de información y el fortalecimiento de la confianza en el entorno digital.
- **Resolución 500 de 2021 – MinTIC**
  Establece los lineamientos para la implementación de la **Política de Gobierno Digital**, incluyendo el componente de seguridad y privacidad de la información y la gestión de riesgos de seguridad digital.

2.4 Normativa sobre Protección de Datos Personales

- **Ley 1581 de 2012**
  Por la cual se dictan disposiciones generales para la protección de datos personales y se regula el derecho constitucional del habeas data.
- **Decreto 1377 de 2013**
  Reglamenta parcialmente la Ley 1581 de 2012, en relación con la autorización para el tratamiento de datos personales y las políticas de privacidad.
- **Decreto 1074 de 2015**
  Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que compila las normas relacionadas con la protección de datos personales.

2.5 Normativa del Sector Salud

- **Ley 23 de 1981** – Normas en materia de ética médica
  Establece el deber de confidencialidad sobre la información clínica y los datos de los pacientes.
- **Resolución 1995 de 1999**
  Regula el manejo, confidencialidad, custodia y archivo de las historias clínicas.
- **Ley 1438 de 2011**
  Fortalece el Sistema General de Seguridad Social en Salud e incorpora principios de calidad, confidencialidad y protección de la información del paciente.

2.6 Normas y Estándares de Referencia

- **ISO/IEC 27001**
  Estándar internacional para la implementación de Sistemas de Gestión de Seguridad de la Información (SGSI).
- **ISO/IEC 27002**
  Código de buenas prácticas para los controles de seguridad de la información.

3. ALCANCE

El **Plan de Seguridad y Privacidad de la Información** de la **E.S.E. Hospital San Lorenzo de Liborina** aplica a **todos los procesos, dependencias, funcionarios, contratistas, terceros y partes interesadas** que, en el desarrollo de sus funciones, tengan acceso, usen, administren, custodien o traten información institucional, independientemente del medio o formato en el que esta se encuentre.

El alcance del plan comprende la protección de **todos los activos de información** de la entidad, incluidos, pero no limitados a:

- Información clínica y asistencial de los pacientes.
- Datos personales y sensibles de usuarios, funcionarios, contratistas y proveedores.
- Información administrativa, financiera, contractual y jurídica.
- Sistemas de información, aplicaciones, bases de datos y plataformas tecnológicas.
- Infraestructura tecnológica, redes de comunicación y servicios digitales.
- Información contenida en medios físicos, electrónicos, magnéticos, ópticos y en la nube.

Asimismo, el presente plan cubre los **procesos estratégicos, misionales, de apoyo y de evaluación**, así como los servicios prestados a través de medios digitales, garantizando la aplicación de controles de seguridad y privacidad durante todo el ciclo de vida de la información, desde su creación, almacenamiento, uso y transmisión, hasta su conservación o disposición final.

El plan se articula con el **Modelo Integrado de Planeación y Gestión (MIPG)**, el **Sistema de Control Interno**, la **gestión del riesgo institucional** y la **Política de Seguridad Digital**, y establece lineamientos para la prevención, detección, respuesta y recuperación frente a incidentes de seguridad de la información, con el fin de asegurar la **confidencialidad, integridad, disponibilidad y privacidad** de la información, así como la continuidad de los servicios de salud y el cumplimiento de la normatividad vigente.

4. OBJETIVOS

4.1 Objetivo General

Establecer los lineamientos, controles y acciones necesarias para **proteger los activos de información** de la **E.S.E. Hospital San Lorenzo de Liborina**, garantizando la **seguridad y privacidad de la información**, mediante la gestión adecuada de los riesgos de seguridad digital, con el fin de asegurar la **confidencialidad, integridad y disponibilidad de la información**, la protección de los datos personales y la continuidad

de los servicios de salud, en cumplimiento de la normatividad vigente y de los objetivos misionales de la entidad.

4.2 Objetivos Específicos

1. Identificar, clasificar y proteger los activos de información de la entidad, de acuerdo con su nivel de criticidad y sensibilidad.
2. Implementar controles técnicos, administrativos y físicos orientados a prevenir, mitigar y tratar los riesgos de seguridad y privacidad de la información.
3. Garantizar la protección de los datos personales y sensibles, especialmente la información clínica de los pacientes, en cumplimiento de la Ley 1581 de 2012 y demás normas aplicables.
4. Fortalecer la gestión del riesgo de seguridad digital, articulándola con el MIPG, el Sistema de Control Interno y el mapa de riesgos institucional.
5. Establecer lineamientos para la prevención, detección, atención y recuperación frente a incidentes de seguridad de la información.
6. Promover la cultura de seguridad y privacidad de la información mediante programas de sensibilización y capacitación dirigidos a funcionarios, contratistas y terceros.
7. Asegurar la continuidad y disponibilidad de los sistemas de información y servicios digitales que soportan los procesos misionales y administrativos de la entidad.
8. Realizar seguimiento y evaluación periódica al cumplimiento del Plan de Seguridad y Privacidad de la Información, con el fin de garantizar su mejora continua y actualización conforme a los cambios normativos, tecnológicos y organizacionales.

5. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El **Plan de Seguridad y Privacidad de la Información** de la **E.S.E. Hospital San Lorenzo de Liborina** se fundamenta en los siguientes principios, los cuales orientan la gestión, el uso y la protección de la información institucional, en concordancia con la normatividad vigente y las buenas prácticas en seguridad digital:

5.1 Confidencialidad

La información debe ser accesible únicamente a las personas, procesos o sistemas debidamente autorizados. La E.S.E. adoptará los controles necesarios para evitar el acceso, uso, divulgación o modificación no autorizada de la información, especialmente aquella que contiene datos personales, sensibles y clínicos.

5.2 Integridad

La información debe ser exacta, completa y confiable, garantizando que no sea alterada de manera indebida o no autorizada durante su almacenamiento, procesamiento o transmisión.

5.3 Disponibilidad

La información y los sistemas que la soportan deben estar disponibles y accesibles cuando sean requeridos por los usuarios autorizados, asegurando la continuidad de los procesos misionales, administrativos y asistenciales.

5.4 Privacidad

El tratamiento de los datos personales se realizará respetando los derechos de los titulares, garantizando el habeas data, la legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, conforme a la Ley 1581 de 2012 y demás normas aplicables.

5.5 Legalidad

La gestión de la seguridad y privacidad de la información se realizará en cumplimiento de la Constitución, la ley y la normatividad vigente, así como de las políticas y lineamientos institucionales.

5.6 Responsabilidad

Todos los funcionarios, contratistas y terceros son responsables del adecuado uso y protección de la información a la que tengan acceso, de acuerdo con su rol y funciones, y deberán cumplir los lineamientos establecidos en este plan.

5.7 Gestión del Riesgo

La seguridad y privacidad de la información se gestionarán mediante un enfoque basado en riesgos, permitiendo identificar, analizar, evaluar y tratar oportunamente las amenazas y vulnerabilidades que puedan afectar los activos de información.

5.8 Mejora Continua

El Plan de Seguridad y Privacidad de la Información será objeto de seguimiento, evaluación y actualización permanente, con el fin de adaptarse a los cambios tecnológicos, normativos y organizacionales, y fortalecer continuamente los controles de seguridad digital.

6. ROLES Y RESPONSABILIDADES

Para la adecuada implementación del **Plan de Seguridad y Privacidad de la Información**, la E.S.E. Hospital San Lorenzo de Liborina define los siguientes roles y responsabilidades:

6.1 Gerencia

- Aprobar y respaldar el Plan de Seguridad y Privacidad de la Información.
- Garantizar la asignación de recursos necesarios para su implementación.
- Promover la cultura de seguridad y privacidad de la información en la entidad.

6.2 Responsable de Seguridad Digital / TIC

- Coordinar la implementación, seguimiento y actualización del plan.
- Identificar y gestionar los riesgos de seguridad digital.
- Proponer e implementar controles de seguridad de la información.
- Atender y coordinar la gestión de incidentes de seguridad de la información.

6.3 Líderes de Proceso

- Identificar los activos de información de sus procesos.
- Velar por el cumplimiento de los lineamientos de seguridad y privacidad.
- Reportar incidentes o eventos que afecten la información.

6.4 Funcionarios, Contratistas y Terceros

- Cumplir las políticas, procedimientos y controles de seguridad de la información.
- Proteger la información a la que tengan acceso.
- Reportar oportunamente cualquier incidente de seguridad.

6.5 Control Interno

- Verificar el cumplimiento del plan.
- Evaluar la efectividad de los controles implementados.
- Formular recomendaciones de mejora.

7. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La E.S.E. Hospital San Lorenzo de Liborina gestionará los riesgos de seguridad digital mediante un enfoque sistemático y preventivo, articulado con el **Mapa de Riesgos Institucional** y el **MIPG**.

La gestión del riesgo comprende:

- Identificación de activos de información.
- Identificación de amenazas y vulnerabilidades.
- Análisis y evaluación de riesgos.
- Definición e implementación de tratamientos de riesgo.
- Monitoreo y revisión periódica.

Esta gestión permitirá reducir la probabilidad e impacto de eventos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información.

8. CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

La entidad implementará controles de seguridad de tipo **administrativo, técnico y físico**, de acuerdo con la criticidad de los activos de información, entre ellos:

8.1 Controles Administrativos

- Políticas y procedimientos de seguridad de la información.
- Acuerdos de confidencialidad.
- Clasificación de la información.
- Gestión de accesos y perfiles de usuario.

8.2 Controles Técnicos

- Uso de contraseñas seguras.
- Control de accesos a sistemas de información.
- Copias de seguridad (backups).
- Protección contra malware y software no autorizado.

8.3 Controles Físicos

- Control de acceso a áreas críticas.
- Protección de equipos y servidores.
- Medidas de seguridad para archivos físicos.

9. PROTECCIÓN DE DATOS PERSONALES

La E.S.E. garantizará el tratamiento adecuado de los datos personales conforme a la **Ley 1581 de 2012**, sus decretos reglamentarios y la normatividad del sector salud.

Se asegurará:

- El respeto por los derechos de los titulares.
- El uso de datos únicamente para fines autorizados.
- La confidencialidad de la información clínica y sensible.
- La adopción de medidas de seguridad para prevenir accesos no autorizados.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La entidad establecerá un procedimiento para la **detección, reporte, análisis, atención y recuperación** de incidentes de seguridad de la información, tales como:

- Pérdida o filtración de información.
- Accesos no autorizados.
- Ataques informáticos.
- Fallas en sistemas de información.

Todos los funcionarios y contratistas deberán reportar de manera inmediata cualquier incidente identificado.

11. SENSIBILIZACIÓN Y CAPACITACIÓN

La E.S.E. promoverá una **cultura de seguridad y privacidad de la información** mediante:

- Jornadas de capacitación periódicas.
- Sensibilización sobre el manejo adecuado de la información.
- Divulgación de políticas y buenas prácticas de seguridad digital.

12. SEGUIMIENTO, MEDICIÓN Y MEJORA CONTINUA

El cumplimiento y efectividad del Plan de Seguridad y Privacidad de la Información será objeto de:

- Seguimiento periódico.
- Evaluaciones internas.
- Auditorías de control interno.
- Ajustes y mejoras continuas.

Los resultados permitirán fortalecer los controles y garantizar la actualización permanente del plan.

13. VIGENCIA Y ACTUALIZACIÓN DEL PLAN

El presente **Plan de Seguridad y Privacidad de la Información** tendrá vigencia anual y será actualizado cuando se presenten cambios normativos, tecnológicos, organizacionales o cuando los resultados del seguimiento así lo requieran, garantizando su alineación con el **MIPG** y la **Política de Seguridad Digital**.

14. CONTROL DE CAMBIOS

DESCRIPCIÓN			*FECHA*	
Elabora: Laura Jaramillo Estrada- Asesora administrativa			*Enero 2026*	
Revisa: José Darío Martínez – Subgerente administrativo			*Enero 2026*	
Aprueba: Robertson Orozco Escudero - Gerente			*Enero 2026*	
CONTROL DE ACTUALIZACIONES				
Versión	*Fecha*	*Cambios*	*Responsable*	*Aprueba*
01	*Enero 30 de 2026*	*NA*	*Asesora administrativa*	*Gerente*