PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ESTRUCTURA DE PLAN

En cumplimiento al Decreto 612 de 2018

1. Presentación

El Plan de Seguridad y Privacidad de la Información – PSPI 2026 del Hospital La Buena Esperanza de Yumbo – E.S.E. establece el conjunto de lineamientos, controles, responsabilidades y mecanismos técnicos, administrativos y organizacionales orientados a garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información institucional, así como la protección de los datos personales tratados por la entidad.

Este plan se estructura conforme al Modelo de Seguridad y Privacidad de la Información – MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, y se articula con el Modelo Integrado de Planeación y Gestión – MIPG, la Política de Gobierno Digital y la Política de Seguridad Digital del Estado Colombiano, asegurando el cumplimiento normativo y el fortalecimiento de la gestión institucional.

2. MARCO NORMATIVO Y DE REFERENCIA

Plan de Seguridad y Privacidad de la Información – 2026

El presente Plan de Seguridad y Privacidad de la Información se estructura y desarrolla en cumplimiento del marco constitucional, legal, reglamentario y técnico aplicable a las entidades públicas del orden territorial, en especial a las Empresas Sociales del Estado del sector salud, garantizando la protección de la información y los datos personales tratados por el Hospital La Buena Esperanza de Yumbo – E.S.E.

Constitución Política de Colombia

Artículo 15.

Establece el derecho fundamental a la intimidad personal y familiar, al buen nombre y al habeas data, obligando a las entidades públicas a proteger los datos personales que administran, adoptar medidas de seguridad y garantizar el uso adecuado de la información.

Artículo 74.

Reconoce el derecho de acceso a documentos públicos, el cual debe garantizarse sin perjuicio de las restricciones legales relacionadas con la reserva de la información, la protección de datos personales y la seguridad de la información.

Ley 594 de 2000 – Ley General de Archivos

Regula la función archivística del Estado y establece la obligación de las entidades públicas de garantizar la organización, conservación, custodia y disponibilidad de los documentos, independientemente de su soporte, lo cual se articula con los principios de integridad, disponibilidad y autenticidad de la información.

Ley 527 de 1999 – Mensajes de Datos y Firmas Digitales

Define y regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales, estableciendo criterios de autenticidad, integridad y no repudio de la información electrónica, fundamentales para la gestión segura de la información digital institucional.

Ley 1273 de 2009 – Protección de la Información y de los Datos

Modifica el Código Penal colombiano creando el bien jurídico de la protección de la información y los datos, tipificando delitos informáticos y reforzando la obligación institucional de implementar controles que

prevengan accesos no autorizados, alteración, pérdida o uso indebido de la información.

Ley 1581 de 2012 – Protección de Datos Personales

Establece el régimen general de protección de datos personales en Colombia, definiendo los principios, derechos de los titulares, deberes de los responsables y encargados del tratamiento, y la obligación de implementar medidas técnicas, humanas y administrativas que garanticen la seguridad de los datos personales.

Decreto 1377 de 2013

Reglamenta parcialmente la Ley 1581 de 2012, desarrollando aspectos relacionados con la autorización para el tratamiento de datos personales, las políticas de tratamiento de la información y las medidas de seguridad aplicables a las bases de datos administradas por las entidades públicas.

Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública

Regula el derecho de acceso a la información pública, estableciendo la obligación de las entidades estatales de garantizar la disponibilidad, divulgación proactiva y acceso a la información, sin perjuicio de las excepciones legales relacionadas con la reserva, la seguridad de la información y la protección de datos personales.

Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC

Compila la normativa del sector TIC y establece lineamientos para la gestión de la información, la seguridad digital y el uso de tecnologías de la información en las entidades públicas, sirviendo de base para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

Decreto 1499 de 2017 – Modelo Integrado de Planeación y Gestión (MIPG)

Adopta el Modelo Integrado de Planeación y Gestión, dentro del cual la Dimensión de Información y Comunicación exige la implementación de prácticas de seguridad de la información, gestión documental, transparencia y control interno, articuladas con el presente plan.

Decreto 612 de 2018 – Planes Institucionales

Establece la obligación de integrar y armonizar los planes institucionales, incluyendo el Plan de Seguridad y Privacidad de la Información, como instrumento de planeación y seguimiento en las entidades públicas.

Decreto 1008 de 2018 – Política de Gobierno Digital

Modifica el Decreto 1078 de 2015 e incorpora la Política de Gobierno Digital, la cual contiene el Modelo de Seguridad y Privacidad de la Información – MSPI, definiendo los lineamientos, componentes y responsabilidades para la gestión de la seguridad y privacidad de la información en las entidades del Estado.

CONPES 3854 de 2016 – Política de Seguridad Digital

Define la Política de Seguridad Digital del Estado Colombiano, orientada a fortalecer la gestión de riesgos digitales, la protección de la información y la resiliencia institucional frente a amenazas cibernéticas.

ISO/IEC 27001

Establece los requisitos para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), adoptada como referencia técnica para estructurar los controles y procesos definidos en el presente plan.

ISO/IEC 27002

Proporciona un conjunto de buenas prácticas y controles de seguridad de la información que sirven de guía para la implementación de medidas técnicas, organizacionales y operativas.

ISO/IEC 27005

Define el marco para la gestión de riesgos de seguridad de la información, utilizado como referencia metodológica para la identificación, análisis, evaluación y tratamiento de riesgos institucionales.

3. OBJETIVOS

3.1 Objetivo General

Establecer, implementar y fortalecer el Plan de Seguridad y Privacidad de la Información del Hospital La Buena Esperanza de Yumbo – E.S.E. para la vigencia 2026, mediante la adopción de lineamientos técnicos, administrativos y organizacionales acordes con el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio TIC, con el fin de garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional y los datos personales tratados por la entidad, asegurando el cumplimiento normativo y la continuidad de los procesos misionales, estratégicos y de apoyo.

3.2 Objetivos Específicos

- Promover la aplicación de buenas prácticas de seguridad de la información y seguridad digital en todos los niveles de la organización, conforme a los lineamientos del MSPI MinTIC y la Política de Seguridad Digital del Estado Colombiano.
- Definir y fortalecer los roles, responsabilidades y mecanismos de coordinación relacionados con la seguridad y privacidad de la información,

asegurando su adecuada articulación con el Modelo Integrado de Planeación y Gestión – MIPG.

- Implementar un esquema institucional de identificación, clasificación y valoración de los activos de información, que permita establecer controles acordes al nivel de riesgo y criticidad de la información.
- Gestionar de manera sistemática los riesgos asociados a la seguridad y privacidad de la información, mediante la identificación de amenazas, análisis de vulnerabilidades y definición de planes de tratamiento del riesgo.
- Garantizar la protección de los datos personales tratados por la entidad, en cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios.
- Fortalecer la infraestructura tecnológica y los mecanismos de respaldo, recuperación y continuidad de la información, minimizando el riesgo de pérdida, alteración o indisponibilidad de la información crítica.
- Fomentar la cultura institucional de seguridad de la información, mediante procesos de sensibilización, capacitación y apropiación de buenas prácticas por parte de funcionarios, contratistas y terceros.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información 2026 del Hospital La Buena Esperanza de Yumbo – E.S.E. aplica de manera transversal a toda la organización y comprende:

- Todos los procesos institucionales, tanto misionales como estratégicos, de apoyo y de evaluación.
- La información generada, recibida, almacenada, procesada, transmitida o eliminada por la entidad, en cualquier formato o soporte.
- Los sistemas de información, aplicativos, plataformas tecnológicas, bases de datos y servicios digitales utilizados por la entidad.

- La infraestructura tecnológica, incluyendo servidores, redes, equipos de cómputo, dispositivos de almacenamiento y servicios en la nube.
- Los funcionarios, contratistas, practicantes, proveedores y terceros que tengan acceso a información institucional o datos personales.
- Los servicios tercerizados que impliquen tratamiento, custodia o acceso a información de la entidad.

5. LINEAMIENTOS CONCEPTUALES Y PRINCIPIOS RECTORES

La gestión de la seguridad y privacidad de la información en el Hospital La Buena Esperanza de Yumbo – E.S.E. se fundamenta en los siguientes principios:

Confidencialidad

Garantizar que la información solo sea accesible a personas, sistemas o procesos debidamente autorizados, evitando accesos no autorizados o divulgaciones indebidas.

Integridad

Proteger la información contra alteraciones no autorizadas, asegurando su exactitud, completitud y validez durante todo su ciclo de vida.

Disponibilidad

Asegurar que la información y los servicios asociados estén disponibles y accesibles cuando sean requeridos por los procesos institucionales.

Legalidad

Garantizar que el tratamiento de la información y los datos personales se realice conforme a la normativa vigente y a las políticas institucionales.

Responsabilidad

Asignar responsabilidades claras a los actores involucrados en la gestión de la información, garantizando el uso adecuado y seguro de la misma.

Prevención y Gestión del Riesgo

Adoptar un enfoque preventivo orientado a la identificación, análisis y mitigación de riesgos asociados a la seguridad y privacidad de la información.

6. GOBIERNO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital La Buena Esperanza de Yumbo – E.S.E. establece un esquema de gobierno de la seguridad y privacidad de la información conforme al MSPI MinTIC, el cual comprende:

6.1 Alta Dirección

Responsable de:

- Aprobar el Plan de Seguridad y Privacidad de la Información.
- Asignar los recursos necesarios para su implementación.
- Liderar el compromiso institucional con la seguridad de la información.

6.2 Líder de Seguridad de la Información

Responsable de:

- Coordinar la implementación y seguimiento del MSPI.
- Asesorar a la Alta Dirección en temas de seguridad digital.
- Liderar la gestión de riesgos de seguridad de la información.
- Coordinar la gestión de incidentes de seguridad.

6.3 Responsables de Proceso

Responsables de:

- Identificar y clasificar los activos de información bajo su custodia.
- Garantizar el cumplimiento de los lineamientos de seguridad.
- Reportar incidentes de seguridad de la información.

6.4 Usuarios de la Información

Responsables de:

- Hacer uso adecuado de la información institucional.
- Cumplir las políticas, procedimientos y controles establecidos.
- Proteger las credenciales y accesos asignados.

7. DIAGNÓSTICO INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Hospital La Buena Esperanza de Yumbo – E.S.E. cuenta actualmente con mecanismos básicos de seguridad de la información orientados a la custodia y protección de los datos de pacientes, funcionarios y demás actores institucionales, así como a la protección de la información administrativa, financiera, clínica y operativa.

No obstante, se identifican brechas relacionadas con:

- Ausencia de una política institucional formal de renovación tecnológica alineada con ciclos de vida de los activos.
- Crecimiento de la infraestructura tecnológica no totalmente alineado con la demanda de los sistemas de información.
- Necesidad de formalizar y documentar procesos de clasificación de activos de información.
-

- Dependencia operativa de controles tecnológicos sin una gestión integral del riesgo documentada.
- Necesidad de fortalecer los mecanismos de monitoreo, registro y respuesta ante incidentes de seguridad de la información.

Este diagnóstico evidencia la necesidad de consolidar un enfoque estructurado conforme al MSPI MinTIC, que permita transitar de controles operativos aislados hacia un sistema de gestión integral de seguridad y privacidad de la información.

8. GESTIÓN DE ACTIVOS DE INFORMACIÓN

El Hospital implementará un proceso formal de gestión de activos de información que permita identificar, clasificar y proteger los activos críticos para la operación institucional.

8.1 Identificación de Activos de Información

Se identificarán, como mínimo, los siguientes tipos de activos:

- Información clínica y asistencial.
- Bases de datos de pacientes y funcionarios.
- Sistemas de información institucionales.
- Infraestructura tecnológica (servidores, redes, estaciones de trabajo).
- Servicios tecnológicos internos y tercerizados.
- Documentación física y digital.

8.2 Clasificación de Activos de Información

Los activos serán clasificados según su nivel de sensibilidad:

- **Información pública**
- **Información de uso interno**
- **Información confidencial**
- **Información restringida o sensible**

La clasificación considerará el impacto sobre la confidencialidad, integridad y disponibilidad.

8.3 Responsables de los Activos

Cada activo contará con un responsable de custodia, quien garantizará la aplicación de los controles definidos y el cumplimiento de los lineamientos de seguridad.

9. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La gestión de riesgos de seguridad de la información se realizará conforme a los lineamientos del MSPI MinTIC y la norma ISO/IEC 27005.

9.1 Identificación de Riesgos

Se identificarán amenazas y vulnerabilidades asociadas a los activos de información, incluyendo:

- Amenazas tecnológicas (malware, fallas de hardware, accesos no autorizados).
- Amenazas humanas (errores, negligencia, uso indebido).
- Amenazas ambientales (fallas eléctricas, desastres naturales).

9.2 Análisis y Evaluación del Riesgo

Los riesgos serán evaluados considerando la probabilidad de ocurrencia y el impacto institucional, priorizando aquellos de mayor criticidad.

9.3 Tratamiento del Riesgo

Se definirán planes de tratamiento que incluyan:

- Implementación de controles preventivos.
- Controles detectivos y correctivos.
- Aceptación, mitigación, transferencia o eliminación del riesgo.

9.4 Seguimiento del Riesgo

Se realizará seguimiento periódico a los riesgos identificados y a la efectividad de los controles implementados.

10. PROTECCIÓN DE DATOS PERSONALES

El Hospital La Buena Esperanza de Yumbo – E.S.E. garantiza la protección de los datos personales tratados en el desarrollo de sus funciones, en cumplimiento de la Ley 1581 de 2012 y su normativa reglamentaria.

10.1 Principios Aplicables

- Legalidad
- Finalidad
- Libertad
- Veracidad o calidad
- Transparencia
- Acceso y circulación restringida
- Seguridad
- Confidencialidad

10.2 Medidas de Seguridad

La entidad implementará medidas técnicas, humanas y administrativas que aseguren la protección de los datos personales frente a accesos no autorizados, pérdida, alteración o uso indebido.

10.3 Derechos de los Titulares

Se garantizará el ejercicio de los derechos de los titulares de datos personales, incluyendo consulta, actualización, rectificación y supresión, conforme a los procedimientos institucionales.

11. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El Hospital La Buena Esperanza de Yumbo – E.S.E. establece un proceso formal para la gestión de incidentes de seguridad de la información, orientado a garantizar una respuesta oportuna, coordinada y efectiva ante eventos que puedan afectar la confidencialidad, integridad, disponibilidad o privacidad de la información.

11.1 Definición de Incidente de Seguridad de la Información

Se considera incidente de seguridad de la información cualquier evento,

real o potencial, que comprometa o pueda comprometer la seguridad de los activos de información, incluyendo accesos no autorizados, pérdida de información, indisponibilidad de servicios, alteración de datos o violación de datos personales.

11.2 Detección y Reporte de Incidentes

Los incidentes podrán ser detectados mediante:

- Monitoreo de sistemas y plataformas tecnológicas.
- Reportes realizados por funcionarios, contratistas o terceros.
- Alertas generadas por herramientas de seguridad.

Todo incidente deberá ser reportado de manera inmediata al Líder de Seguridad de la Información, conforme a los canales institucionales definidos.

11.3 Análisis y Clasificación del Incidente

Los incidentes serán analizados y clasificados según su impacto y criticidad, considerando:

- Tipo de información afectada.
- Alcance del incidente.
- Riesgo para la continuidad del servicio.
- Impacto legal y reputacional.

11.4 Respuesta, Contención y Recuperación

Se implementarán acciones de:

- Contención inmediata para limitar el impacto.
- Erradicación de la causa raíz.
- Recuperación de la información y los servicios afectados.

11.5 Registro y Lecciones Aprendidas

Todos los incidentes serán documentados y analizados para fortalecer los controles y prevenir su recurrencia.

12. CONTINUIDAD, RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN

El Hospital implementará lineamientos técnicos y operativos que garanticen la continuidad de la información y los servicios asociados, minimizando el impacto de incidentes tecnológicos.

12.1 Copias de Seguridad (Backups)

Se realizarán copias de seguridad periódicas de:

- Bases de datos institucionales.
- Sistemas de información críticos.
- Estaciones de trabajo con información relevante.

Las copias se realizarán de forma automática y serán almacenadas en repositorios seguros, locales y externos.

12.2 Almacenamiento y Custodia de Copias

Las copias de seguridad serán protegidas mediante:

- Controles de acceso.
- Cifrado de la información.
- Monitoreo de integridad.

12.3 Pruebas de Restauración

Se realizarán pruebas periódicas de restauración con el fin de verificar la efectividad de los mecanismos de respaldo y recuperación.

12.4 Continuidad Operativa

Se definirán lineamientos que permitan la continuidad de los procesos críticos ante eventos que afecten la infraestructura tecnológica o la disponibilidad de la información.

13. CULTURA Y APROPIACIÓN DE LA SEGURIDAD DIGITAL

El fortalecimiento de la cultura de seguridad de la información constituye un eje fundamental del MSPI y del presente plan.

13.1 Sensibilización y Capacitación

Se desarrollarán actividades de sensibilización y capacitación dirigidas a:

- Funcionarios

- Contratistas
- Terceros con acceso a información institucional

13.2 Buenas Prácticas de Seguridad

Se promoverán buenas prácticas relacionadas con:

- Uso seguro de contraseñas.
- Protección de dispositivos.
- Manejo adecuado de la información.
- Prevención de incidentes de seguridad.

13.3 Responsabilidad Individual

Cada usuario es responsable del uso adecuado de la información y del cumplimiento de los lineamientos de seguridad establecidos por la entidad.

14. INDICADORES DE GESTIÓN Y DESEMPEÑO

Con el fin de medir la efectividad del Plan de Seguridad y Privacidad de la Información 2026, el Hospital La Buena Esperanza de Yumbo – E.S.E. definirá indicadores de gestión que permitan realizar seguimiento, evaluación y mejora continua del MSPI.

14.1 Indicadores Institucionales

- **Porcentaje de activos de información identificados y clasificados**

  Permite medir el nivel de avance en la gestión de activos de información.
- **Porcentaje de copias de seguridad ejecutadas exitosamente**

  Mide la efectividad de los procesos de respaldo de la información institucional.
- **Número de incidentes de seguridad de la información gestionados**

  Permite evaluar la capacidad de detección, respuesta y recuperación ante incidentes.
- **Porcentaje de funcionarios y contratistas capacitados en seguridad de la información**

  Evalúa el nivel de apropiación de la cultura de seguridad digital.

- **Nivel de madurez del MSPI**

  Permite evaluar el grado de implementación del Modelo de Seguridad y Privacidad de la Información.

15. SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA

El Plan de Seguridad y Privacidad de la Información será objeto de seguimiento y evaluación permanente, con el fin de garantizar su eficacia y pertinencia.

15.1 Seguimiento

Se realizará seguimiento periódico mediante:

- Informes trimestrales de avance.
- Revisión de indicadores de gestión.
- Verificación del cumplimiento de los controles definidos.

15.2 Evaluación

La evaluación del plan incluirá:

- Análisis de resultados obtenidos.
- Identificación de brechas y oportunidades de mejora.
- Revisión del cumplimiento normativo.

15.3 Mejora Continua

Con base en los resultados del seguimiento y la evaluación, se formularán e implementarán planes de mejora orientados a fortalecer la seguridad y privacidad de la información, en concordancia con el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

16. CRONOGRAMA GENERAL DE CUMPLIMIENTO

El Plan de Seguridad y Privacidad de la Información se ejecutará de manera transversal durante la vigencia 2026, conforme a los siguientes lineamientos generales:

Actividad	Periodicidad
Copias de seguridad de bases de datos	Diaria (incremental)
Copias de seguridad completas	Semanal
Verificación de respaldos	Mensual
Pruebas de restauración	Semestral
Evaluación de riesgos de seguridad	Anual
Capacitación en seguridad de la información	Semestral
Seguimiento e informes del plan	Trimestral

17. ARTICULACIÓN CON MIPG Y OTROS INSTRUMENTOS DE PLANEACIÓN

El presente plan se articula con:

- Plan Estratégico Institucional
- Plan de Acción Institucional
- Plan Anticorrupción y de Atención al Ciudadano
- Plan Institucional de Archivos – PINAR
- PETI
- Sistema de Control Interno
- Modelo Integrado de Planeación y Gestión – MIPG

Claudia Jimena Sánchez Alcalde

Gerente

E.S.E Hospital La Buena Esperanza