PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En cumplimiento al Decreto 612 de 2018

1. Presentación

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 del Hospital La Buena Esperanza de Yumbo – E.S.E. tiene como finalidad establecer los lineamientos técnicos, administrativos y operativos para identificar, analizar, evaluar, tratar y monitorear los riesgos asociados a la seguridad y privacidad de la información institucional.

Este plan se enmarca en el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio TIC, la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión – MIPG, con el propósito de proteger los activos de información, garantizar el tratamiento adecuado de los datos personales y fortalecer la resiliencia institucional frente a amenazas digitales.

2. MARCO NORMATIVO Y DE REFERENCIA

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – 2026

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital La Buena Esperanza de Yumbo – E.S.E. se formula y ejecuta en cumplimiento del marco constitucional, legal, reglamentario y técnico vigente, el cual orienta la gestión del riesgo, la protección de la información y el tratamiento de datos personales en las entidades públicas del sector salud.

Constitución Política de Colombia

Artículo 15.

Reconoce el derecho fundamental a la intimidad personal y familiar y al habeas data, imponiendo a las entidades públicas la obligación de proteger los datos personales bajo su custodia y de implementar medidas que prevengan el acceso, uso o divulgación no autorizada de la información.

Artículo 74.

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

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, integridad y disponibilidad de los documentos, lo cual se articula con la gestión del riesgo asociado a la pérdida, alteración o indisponibilidad de la información institucional.

Ley 527 de 1999 – Mensajes de Datos y Firmas Digitales

Define el marco jurídico para el uso de mensajes de datos y firmas digitales, garantizando principios de autenticidad, integridad y no repudio de la información electrónica, elementos esenciales para la gestión de riesgos en entornos digitales.

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

Introduce en el Código Penal el bien jurídico de la protección de la información y los datos, tipificando delitos informáticos y reforzando la necesidad de identificar, evaluar y tratar los riesgos asociados a accesos no autorizados, daño 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 principios, derechos de los titulares y deberes de los responsables del tratamiento, lo que obliga a la entidad a gestionar los riesgos que puedan afectar la seguridad y privacidad de los datos personales.

Decreto 1377 de 2013

Reglamenta parcialmente la Ley 1581 de 2012, desarrollando aspectos relacionados con las autorizaciones, políticas de tratamiento y medidas de seguridad que deben ser consideradas dentro del análisis y tratamiento de riesgos de seguridad y privacidad de la información.

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

Regula el derecho de acceso a la información pública y establece la obligación de las entidades de identificar y gestionar los riesgos relacionados con la divulgación indebida de información sujeta a reserva legal o 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 y la seguridad digital, sirviendo como base para la implementación del Modelo de Seguridad y Privacidad de la Información y la gestión de riesgos digitales.

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

Adopta el MIPG, dentro del cual la Dimensión de Información y Comunicación exige la identificación, evaluación y tratamiento de los riesgos asociados a la información, la seguridad digital y la protección de datos personales.

Decreto 612 de 2018 – Planes Institucionales

Establece la obligación de formular y actualizar los planes institucionales, incluyendo el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información como instrumento de planeación, control y seguimiento.

Decreto 1008 de 2018 – Política de Gobierno Digital

Incorpora el Modelo de Seguridad y Privacidad de la Información – MSPI, el cual define la gestión del riesgo como un componente fundamental para proteger los activos de información del Estado.

CONPES 3854 de 2016 – Política de Seguridad Digital

Define los lineamientos de la Política de Seguridad Digital del Estado Colombiano, orientada a fortalecer la gestión del riesgo digital, la resiliencia institucional y la protección de la información.

ISO/IEC 27001

Establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información, sirviendo como referencia para la definición de controles y el tratamiento de riesgos.

ISO/IEC 27002

Proporciona un conjunto de controles de seguridad de la información que apoyan la mitigación de riesgos identificados.

ISO/IEC 27005

Define el marco metodológico para la gestión de riesgos de seguridad de la información, utilizado como referencia técnica para la identificación, análisis, evaluación y tratamiento de riesgos en el presente plan.

3. OBJETIVOS

3.1 Objetivo General

Controlar, mitigar y minimizar los riesgos asociados a la seguridad y privacidad de la información del Hospital La Buena Esperanza de Yumbo – E.S.E., mediante la implementación de un Plan de Tratamiento de Riesgos estructurado, alineado con el MSPI MinTIC, que permita proteger los activos de información y garantizar el adecuado tratamiento de los datos personales.

3.2 Objetivos Específicos

- Identificar de manera sistemática los riesgos que afectan la seguridad y privacidad de la información en todos los procesos institucionales.
- Analizar y evaluar los riesgos identificados considerando su impacto y probabilidad.
- Definir e implementar planes de tratamiento del riesgo acordes con su nivel de criticidad.
- Fortalecer los controles técnicos, administrativos y organizacionales existentes.
- Reducir la probabilidad de ocurrencia y el impacto de incidentes de seguridad de la información.
- Garantizar la mejora continua del proceso de gestión de riesgos de seguridad digital.

4. DIAGNÓSTICO INSTITUCIONAL

Actualmente, el Hospital La Buena Esperanza de Yumbo – E.S.E. cuenta con controles básicos para la protección de la información y los datos personales; sin embargo, el análisis institucional evidencia:

- Falta de una política formal de renovación tecnológica.
- Limitaciones en la capacidad de la infraestructura de red frente al crecimiento de los sistemas de información.
- Necesidad de formalizar la gestión del riesgo de seguridad digital bajo una metodología documentada.
- Dependencia de controles tecnológicos sin una evaluación integral del riesgo.

Este diagnóstico justifica la formulación y ejecución del presente Plan de Tratamiento de Riesgos 2026.

5. LINEAMIENTOS CONCEPTUALES PARA EL TRATAMIENTO DEL RIESGO

El tratamiento de los riesgos de seguridad y privacidad de la información se desarrollará bajo los siguientes lineamientos:

- Enfoque preventivo y basado en riesgos.
- Aplicación del ciclo PHVA.
- Articulación con Arquitectura Empresarial y MIPG.
- Responsabilidad compartida entre procesos y usuarios.
- Mejora continua y adaptación a cambios tecnológicos y normativos.

6. FORMULACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Hospital La Buena Esperanza de Yumbo – E.S.E. se formula como un instrumento institucional de carácter transversal, integrado al Sistema de Gestión de la Calidad, al MIPG y al Modelo de Seguridad y Privacidad de la Información – MSPI.

La formulación del plan se orienta a garantizar que los riesgos identificados sobre los activos de información sean tratados de manera sistemática, documentada y coherente con el nivel

de riesgo aceptable definido por la Alta Dirección, priorizando aquellos riesgos que puedan afectar la continuidad de los servicios de salud, la confidencialidad de la información clínica y el cumplimiento normativo.

7. DISEÑO DE HERRAMIENTAS DE IDENTIFICACIÓN Y CONTROL DEL RIESGO

El Hospital implementa un conjunto de herramientas técnicas, administrativas y organizacionales destinadas a mitigar los riesgos de seguridad y privacidad de la información, las cuales se describen a continuación:

7.1 Gestión de Usuarios, Roles y Perfiles

Se establecen perfiles de acceso basados en el principio de **mínimo privilegio**, garantizando que cada usuario tenga acceso únicamente a la información necesaria para el desempeño de sus funciones.

7.2 Control de Accesos a Equipos y Sistemas

Cada equipo de cómputo cuenta con cuentas diferenciadas de administrador y usuario final, siendo la cuenta administrativa controlada exclusivamente por el área de sistemas, reduciendo el riesgo de instalación de software no autorizado o alteración de configuraciones críticas.

7.3 Entorno de Dominio Institucional

Los equipos de cómputo se encuentran integrados a un entorno de dominio que permite la aplicación centralizada de políticas de seguridad, control de accesos y gestión de usuarios.

7.4 Infraestructura Cliente-Servidor

Los sistemas de información operan bajo arquitectura cliente-servidor, lo que permite centralizar el almacenamiento de la información y reducir el riesgo de pérdida o fuga de datos.

7.5 Controles Perimetrales y Antimalware

La entidad cuenta con un servidor proxy institucional para controlar accesos externos y un sistema corporativo de protección contra malware, orientado a prevenir infecciones y ataques informáticos.

8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

La gestión del riesgo se desarrolla conforme a los lineamientos de la **ISO/IEC 27005**, integrando el ciclo PHVA.

8.1 Identificación del Riesgo

Se realiza con la participación de los líderes de proceso y responsables de activos de información, identificando amenazas, vulnerabilidades y activos críticos en cada proceso institucional.

8.2 Análisis del Riesgo

Se analiza cada riesgo considerando:

- Probabilidad de ocurrencia.
- Impacto sobre la confidencialidad, integridad y disponibilidad.
- Consecuencias operativas, legales y reputacionales.

8.3 Evaluación del Riesgo

Los riesgos se clasifican según su nivel de criticidad, permitiendo priorizar aquellos que requieren tratamiento inmediato.

8.4 Tratamiento del Riesgo

Para cada riesgo se define una de las siguientes opciones:

- Mitigación mediante controles.
- Aceptación del riesgo.
- Transferencia del riesgo.
- Eliminación del riesgo.

8.5 Seguimiento y Revisión

Se realiza seguimiento periódico al estado de los riesgos y a la efectividad de los controles implementados.

9. IMPLEMENTACIÓN Y SEGUIMIENTO DEL PLAN

La implementación del plan contempla:

- Asignación de responsables por riesgo.
- Definición de controles y recursos necesarios.
- Seguimiento periódico del avance de los planes de tratamiento.
- Documentación de evidencias.

El seguimiento se realizará de manera continua y será reportado a la Alta Dirección.

10. EVALUACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

La evaluación del plan se realizará de forma trimestral, permitiendo:

- Identificar riesgos materializados.
- Evaluar la eficacia de los controles.
- Determinar la necesidad de ajustes o mejoras.
- Fortalecer la toma de decisiones basada en riesgo.

11. DESARROLLO DEL PLAN DE TRATAMIENTO DE RIESGOS

El desarrollo del plan comprende las siguientes actividades, ejecutadas de manera articulada:

- Identificación de riesgos con los líderes de proceso.
- Entrevistas y sesiones de análisis.
- Elaboración y aprobación del plan de tratamiento del riesgo.
- Revisión y actualización de la Política de Seguridad de la Información.
- Gestión de la seguridad ligada a recursos humanos.
- Revisión y fortalecimiento del control de accesos.
- Gestión de incidentes de seguridad de la información.
- Integración de la seguridad en la continuidad del negocio.

12. INDICADORES DE GESTIÓN Y SEGUIMIENTO

Con el fin de medir la efectividad del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Hospital La Buena Esperanza de Yumbo – E.S.E. define indicadores de gestión que permiten evaluar el avance, desempeño y eficacia de las acciones implementadas.

Indicadores Definidos

- **Número de riesgos identificados:**

  Permite medir la cobertura del proceso de identificación de riesgos en los diferentes procesos institucionales.

- **Porcentaje de riesgos evaluados y priorizados:**
  Mide el nivel de avance en el análisis y evaluación del riesgo conforme a la metodología definida.
- **Porcentaje de riesgos con plan de tratamiento implementado:**
  Evalúa la efectividad de la fase de tratamiento del riesgo.
- **Número de riesgos materializados:**
  Permite identificar la efectividad de los controles implementados y la exposición residual al riesgo.
- **Número de incidentes de seguridad asociados a riesgos identificados:**
  Evalúa la relación entre los riesgos identificados y los eventos de seguridad ocurridos.

13. SEGUIMIENTO, EVALUACIÓN Y MEJORA CONTINUA

El seguimiento y evaluación del Plan de Tratamiento de Riesgos se realizará de manera periódica, con el fin de garantizar su mejora continua y adaptación a cambios tecnológicos, normativos y organizacionales.

13.1 Seguimiento

Se realizará seguimiento mediante:

- Informes trimestrales de avance.
- Revisión de indicadores de gestión.
- Verificación del cumplimiento de los planes de tratamiento.

13.2 Evaluación

La evaluación permitirá:

- Identificar brechas en la gestión del riesgo.
- Evaluar la eficacia de los controles implementados.
- Ajustar las estrategias de tratamiento del riesgo.

13.3 Mejora Continua

Con base en los resultados del seguimiento y evaluación, se formularán planes de mejora orientados a fortalecer la gestión de riesgos de seguridad y privacidad de la información, conforme al ciclo PHVA.

14. CRONOGRAMA GENERAL DE CUMPLIMIENTO – VIGENCIA 2026

El Plan de Tratamiento de Riesgos se ejecutará de manera permanente durante la vigencia 2026, conforme al siguiente cronograma general:

Actividad	Periodicidad
Identificación de riesgos	Anual
Análisis y evaluación de riesgos	Anual
Definición del plan de tratamiento	Anual
Implementación de controles	Permanente
Seguimiento a riesgos tratados	Trimestral
Evaluación y mejora del plan	Anual

15. ARTICULACIÓN CON OTROS INSTRUMENTOS DE PLANEACIÓN

El presente plan se articula de manera directa con:

- Plan de Seguridad y Privacidad de la Información 2026
- Modelo Integrado de Planeación y Gestión – MIPG
- Plan Estratégico Institucional
- Plan de Acción Institucional
- PETI
- Sistema de Control Interno
- Arquitectura Empresarial

Claudia Jimena Sánchez Alcalde

Gerente

E.S.E Hospital La Buena Esperanza