Empresa Social del Estado
POPAYÁN E.S.E.
Trabajamos de

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

2026

Tabla de contenido

1. INTRODUCCION

En estricto cumplimiento del marco normativo vigente en relación a la seguridad y privacidad de la información, la E.S.E. Popayán establece el compromiso institucional de definir e implementar un Plan de Tratamiento de Riesgos de Seguridad de la Información (PTRSI). Este plan, basado en los estándares internacionales ISO/IEC 27001:2022, se constituye como el eje transversal para la identificación, análisis y mitigación de amenazas y vulnerabilidades que puedan comprometer la confidencialidad de los datos de usuarios y pacientes, y en general de todos los activos de información de la entidad. Más allá del cumplimiento legal, esta iniciativa busca blindar la continuidad operativa de los servicios de salud y consolidar la reputación de la entidad como un referente de confianza, transparencia y calidad en la gestión de la información.

2. OBJETIVO

Definir y ejecutar el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información para la vigencia 2026, mediante la consolidación de un modelo operativo proactivo que garantice la identificación, evaluación y mitigación de vulnerabilidades; consolidando una cultura de protección de datos que certifique la disponibilidad y privacidad de la información bajo parámetros que aseguren el estricto cumplimiento del marco legal vigente.

3. ALCANCE

El presente plan tiene una vigencia por el año 2026 y el alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información por parte de la E.S.E Popayán será diseñado y podrá ser aplicada sobre cualquier proceso de la institución cumpliendo con los principales lineamientos emitidos por parte del MINTIC para garantizar la correcta seguridad y privacidad de la información en la institución, con el propósito de consolidar un marco de protección que cumpla con los estándares de la normatividad actual.

4. MARCO LEGAL Y NORMATIVO

- **Norma Técnica ISO 27001 de 2022.** Norma técnica de Seguridad de la Información.
- **Decreto 767 de 2022.** Por lo cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto único reglamentario del Sector de Tecnologías de la Información y Comunicaciones.
- **Decreto 338 de 2022.** Por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgo y la respuesta a incidentes de Seguridad Digital.

- **Decreto 1951 de 2022.** Por el cual se establecen los requisitos, las condiciones y el trámite de la habilitación de los prestadores de servicios ciudadanos digitales especiales; se dan los lineamientos y estándares para la integración de estos servicios y la coordinación de los prestadores con la Agencia Digital Nacional.

- **Decreto 088 de 2022.** Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto único reglamentario del Sector Tecnologías de la Información y las comunicaciones, Decreto 1078 de 2015, Para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en Línea.

- **Resolución 460 de 2022.** Por el cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la política de gobierno digital, y se dictan los lineamientos generales para su implementación.

- **Decreto 746 de 2022.** Por el cual se fortalece el modelo de seguridad y privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.

- **Resolución 1117 de 2022.** Por el cual se establecen los lineamientos de transformación digital para estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la política de gobierno digital.

- **Decreto 620 de 2020.** Por el cual se subroga el titulo 17 de la parte 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e, j y el literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el articulo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- **Resolución 1519 de 2020.** Por lo cual se definen los estándares y directrices para publicar la información pública, accesibilidad web, seguridad digital y datos abiertos.

- **Resolución 2160 de 2020.** Por la cual se expide la Guía de Lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos.

- **Resolución 2893 de 2020.** Por lo cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas trasversales, sedes electrónicas, tramites, OPA's y consultas de acceso a la información pública, así como en relación con la integración al Portal Único del Estado Colombiano, y se dictan otras disposiciones.

- **Ley 1978 de 2019.** Por el cual se moderniza el sector de las tecnologías de la información y las Comunicaciones TIC, se distribuyen competencias, se crea un regulador Único y se dictan otras disposiciones.

- **CONPES 3975 de 2019.** Política Nacional para la Transformación Digital e inteligencia Artificial.
- **Norma Técnica ISO 22301 de 2019.** Norma internacional para sistemas de gestión de la continuidad de negocio (SGCN) y proporciona un marco de buenas prácticas para ayudar a las organizaciones a gestionar eficazmente el impacto de una interrupción en su funcionamiento.
- **Manual de Gobierno Digital de 2018.** En este documento se desarrolla el proceso de implementación de la Política de Gobierno Digital a través de los siguientes cuatro (4) momentos: 1. Conocer la Política; 2. Planear la política; 3. Ejecutar la política y 4. Medir la Política en las entidades Públicas de nivel nacional y territorial.
- **Resolución 1443 de 2018.** Por el cual se sustituye los artículos 15 y 19 y se modifica el artículo 17 de la resolución 2405 de 2016 (por el cual se adopta el sello de la excelencia Gobierno en Línea y se Conforma su comité).
- **Decreto 612 de 2018.** 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 1499 de 2017.** Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad Digital.
- **Decreto 103 de 2015.** Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Ley 1712 de 2014.** 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 1581 de 2012.** Por lo cual se dictan disposiciones generales para la protección de datos personales.
- **Directiva Presidencial 004 de 2012.** Eficiencia Administrativa y Lineamientos de la Política de Cero Papel.

5. PROCEDIMIENTO PARA LA GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

a. CICLO DE OPERACION:

Con base a las directrices emitidas por el MINTIC se adopta el ciclo de operación del modelo de seguridad y privacidad de la información el cual cuenta con 5 diferentes fases como lo es:

diagnóstico, planeación, implementación, gestión y mejora continua.

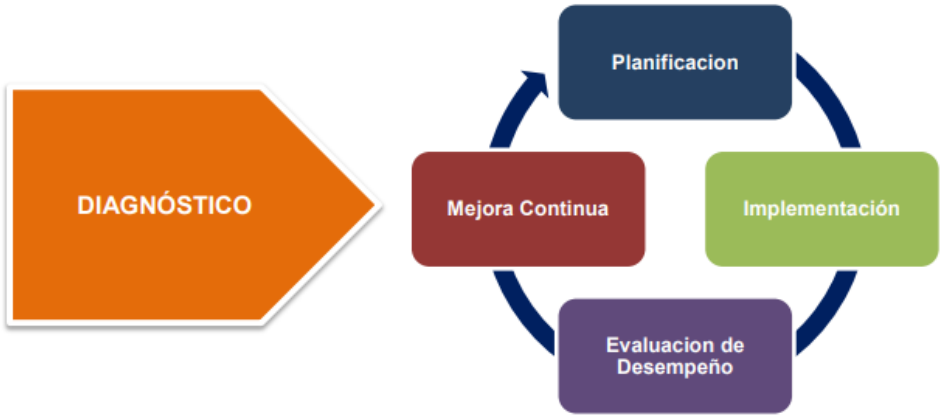

Ilustración 1 – Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

b. FASE DIAGNOSTICO:

La Empresa Social del Estado Popayán E.S.E. requiere diligenciar un autodiagnóstico para identificar el tipo de riesgos y determinar el nivel en que se encuentra en la actualidad, frente a la seguridad y a la privacidad de información en cada una de sus dependencias donde la información es de vital importancia para el desarrollo de sus actividades.

En esta fase se debe establecer un procedimiento para la gestión integral del riesgo y como producto de su aplicación, elaborar la matriz de riesgos institucional, la cual, es una herramienta de gestión que permite determinar los riesgos relevantes de seguridad y privacidad de la información.

c. FASE PLANEACION:

Una vez realizado el diagnóstico, la entidad debe formular una serie de estrategias las cuales permitan desarrollar un adecuado plan de tratamiento de riesgos de seguridad y privacidad de la información con base a los lineamientos emanados por el MINTIC.

Con la matriz de riesgos institucional ya elaborada, se procede a fijar indicadores individuales por cada riesgo y por cada control propuesto, pero a nivel general es pertinente establecer un indicador global, que abarque todas las actividades, el cual quedaría de la siguiente manera y sirve para medir la eficacia en la ejecución del plan:

ICA = (No. de Actividades cumplidas / No. de actividades programadas) *100

Donde ICA es el Índice de Cumplimiento de Actividades

d. FASE IMPLEMENTACION:

En esta fase se ejecutarán las estrategias trazadas en la fase de planeación para así poder implementar el plan de tratamiento y poder registrar los resultados obtenidos por cada objetivo planteado para el desarrollo del plan.

La ejecución consiste entonces en llevar a cabo la implementación de los controles propuestos en la fase anterior, procurando realizarlos dentro de los tiempos establecidos y desarrollados por los responsables asignados.

e. FASE EVALUACION DE DESEMPEÑO:

Una vez implementada las estrategias y registrados los resultados obtenidos se procede a realizar una medición de la efectividad de cada una de las estrategias planteadas y ejecutadas por la entidad frente a los riesgos de seguridad y privacidad de la información.

La entidad debe realizar un seguimiento al presente plan para determinar su efectividad, para lo cual debe realizar las siguientes actividades:

- Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización.
- Revisar periódicamente de las actividades de control para determinar su relevancia y actualizaciones pertinentes.
- Monitorear los riesgos y controles tecnológicos.
- Evaluar el plan de acción.
- Realizar valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva yoperen como se pretende para controlar los riesgos.
- Realizar sugerencias y recomendaciones para mejorar la eficiencia y eficacia de loscontroles

f. FASE DE MEJORA CONTINUA:

Conseguido los resultados de la evaluación de desempeño frente a las estrategias planteadas del plan de tratamiento de riesgos de seguridad y privacidad de información se procede a realizar un análisis de los resultados con el fin de determinar las medidas correctivas necesarias, los cuales permitan garantizar una mejora continúa a lo establecido por la entidad en el respectivo plan. En caso de que existan hallazgos, falencias o incidentes de seguridad y privacidad de la información se debe disminuir el impacto de su existencia y tomar acciones para prevención y control. Estas acciones de mejora continua, deben definirse de la siguiente manera:

- ✓ Revisar y evaluar los hallazgos encontrados, en caso de que existan.

- ✓ Analizar y establecer las posibles causas y consecuencias del hallazgo.
- ✓ Determinar si existen hallazgos similares para establecer acciones correctivas y evitar asíque su materialización.
- ✓ Registrar documentación de los hallazgos, de las acciones realizadas para disminución del impacto y de resultados.

6. SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución del Plan de Tratamiento de Riesgos de Seguridad y privacidad de la Información de la vigencia 2026 se realizará a través del plan de acción del proceso por parte de las oficinas de Planeación y Control Interno con una periodicidad trimestral. Se realiza el siguiente indicador con el fin de evaluar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Porcentaje de cumplimiento del plan:

$$\text{Plan} = \frac{\text{Número de actividades ejecutadas}}{\text{Total, de actividades programadas}} * 100$$

7. ANEXOS

Anexo1: Cronograma de actividades programadas plan de tratamiento de riesgos de seguridad y privacidad de la información Vigencia 2026.

8. CONTROL DE REGISTROS

CONTROL DE REGISTROS DEL SISTEMA DE GESTIÓN DE CALIDAD					
Nombre del registro	**Código**	**Recuperación**	**Almacenamiento**	**Conservación**	**Disposición**
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	APO-GIC-SI-PLA-02	Calidad	Calidad	NA	NA

9. CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza de los cambios	Responsable
01	23-01-2026	Ajustes del documento y actualización cronograma vigencia 2026.	Subproceso Sistemas de Información y Estadística.

ELABORÓ	REVISÓ COORDINACIÓN ADMINISTRATIVA Y FINANCIERA	REVISÓ Y CODIFICÓ
ORIGINAL FIRMADO **JHON ALEXANDER CORDOBA GIL** Cargo: Profesional Apoyo al Subproceso Sistemas de Información y Estadística – E.S.E Popayán - Afiliado participe Sintraunpros ORIGINAL FIRMADO **JUAN DAVID LARA RENGIFO** Cargo: Profesional designado como Líder del Subproceso de Sistemas de Información y Estadística – E.S.E Popayán - Afiliado participe Sintraunpros	ORIGINAL FIRMADO **EDILBERTO PALOMINO MARTÍNEZ** Cargo: PU -Área Administrativa y Financiera	ORIGINAL FIRMADO **MARÍA CATALINA MANCILLA RAMÍREZ** Cargo: Profesional designada como Líder del Proceso de Planeación y Gestión de la Calidad – E.S.E Popayán - Afiliada participe Sintraunpros
Fecha: 23/01/2026	**Fecha: 23/01/2026**	**Fecha: 23/01/2026**
APROBÓ		
ORIGINAL FIRMADO **JUAN CARLOS COTAZO URREA** Cargo: Gerente Empresa Social del Estado E.S.E Popayán		
Fecha: 23/01/2026		