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

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

2025

Tabla de contenido

Tabla de ilustraciones

INTRODUCCION

La Empresa Social del Estado Popayán E.S.E. en cumplimiento de las directrices adoptadas por el MINTIC y la normatividad vigente en referencia a la seguridad de la información, y con el pleno objetivo de garantizar la seguridad y privacidad de la información de sus usuarios y pacientes, definirá e implementar un plan de tratamiento de riesgos de seguridad de la información basado en las mejores prácticas y estándares internacionales, que permitirá identificar, evaluar y mitigar los riesgos, amenazas y vulnerabilidades de los datos e información de la entidad, asegurando la continuidad de los servicios de salud y fortaleciendo la confianza, propendiendo que la E.S.E. Popayán se posicione como una entidad comprometida con la protección de los datos y la prestación de servicios de salud de calidad.

1. OBJETIVO

Establecer e implementar un plan de tratamiento de riesgos de seguridad y privacidad de la información vigencia 2025 para la E.S.E. Popayán; a partir, del establecimiento de un modelo de operación que permita gestionar de manera proactiva los riesgos de seguridad de la información identificando, evaluando y mitigando las vulnerabilidades de los activos de información asegurando su confidencialidad, integridad y disponibilidad cumpliendo con los requisitos legales y normativos.

2. ALCANCE

El presente plan tiene una vigencia por el año 2025 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.

3. 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.

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

a. CICLO DE OPERACION:

ConbasealasdirectricesemitidasporelMINTICseadoptaelciclodeoperacióndelmodelo de seguridad y privacidad de la información el cual cuenta con 5 diferentes fases como lo es:diagnóstico,planeación,implementación,gestiónymejoracontinua.

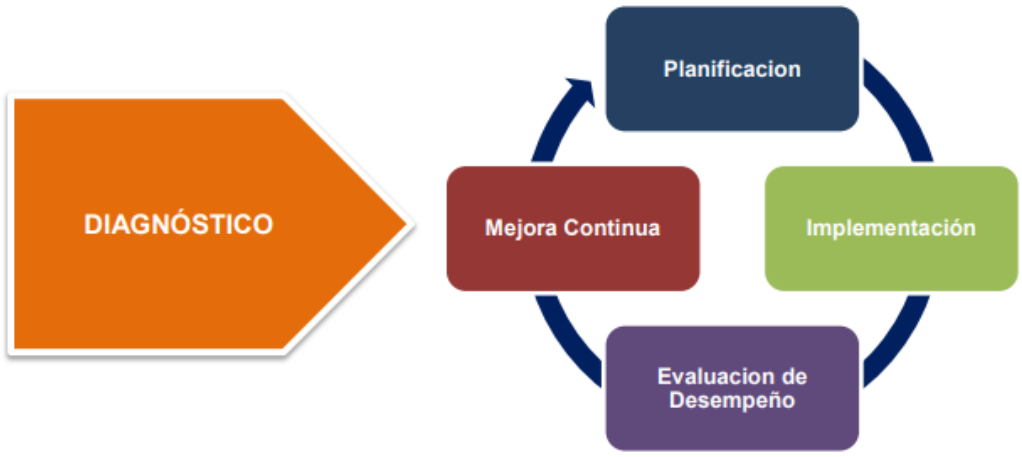

Ilustración 1–Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

b. FASE DIAGNOSTICO:

LaEmpresaSocialdelEstadoPopayánE.S.E.requierediligenciarunautodiagnóstico para identificar el tipo de riesgos y determinarel nivel en que se encuentra en la actualidad,frentealaseguridadyalaprivacidaddeinformaciónencadaunadesusdependencias 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 comoproductodesuaplicación,elaborarla**matrizderiesgosinstitucional**, la cual, esunaherramientadegestiónquepermitedeterminarlosriesgosrelevantesde seguridad y privacidad de la información.

c. FASE PLANEACION:

Una vez realizadoel diagnóstico, laentidaddebe formular una seriedeestrategiaslascuales permitan desarrollar un adecuado plan de tratamiento de riesgos de seguridad yprivacidaddelainformaciónconbasealoslineamientosemanadosporelMINTIC.

Conlamatrizderiesgosinstitucionalyaelaborada,seprocedeafijar**indicadoresindividuales**porcadariesgoyporcadacontrolpropuesto,peroanivelgeneralespertinenteestableceruninidicadorglobal,queabarquetodaslasactividades,elcualquedaríadelasiguientemaneraysirveparamedir laeficaciaenlaejecucióndelplan:

ICA=
(No.deActividadescumplidas/No.deactividadesprogramadas)*100

DondeICAeselÍndicedeCumplimientodeActividades

d. FASE IMPLEMENTACION:

En esta fase se ejecutarán las estrategias trazadas en la fase de planeaciónpara así poder implementar el plan de tratamiento y poder registrar los resultados obtenidosporcadaobjetivo planteado paraeldesarrollo delplan.

Laejecuciónconsisteentoncesenllevaracabolaimplementacióndeloscontrolespropuestos en la fase anterior, procurando realizarlos dentro de los tiempos establecidosy desarrolladosporlos responsables asignados.

e. FASE EVALUACION DE DESEMPEÑO:

Una vez implementada las estrategias y registrados los resultados obtenidos se procede arealizarunamedicióndelaefectividaddecadaunadelasestrategiasplanteadasyejecutadasporla entidadfrentealosriesgosdeseguridadyprivacidaddelainformación.

La entidad debe realizar unseguimiento al presente plan para determinar su efectividad,paralo cualdebe realizar las siguientes actividades:

- Realizarseguimientoymonitoreoalplandeacciónenlaetapadeimplementaciónyfinalización.
- Revisarperiódicamentedelasactividadesdecontrolparadeterminarsurelevanciayactualizacionespertinentes.
- Monitorearlosriesgosycontrolestecnológicos.
- Evaluarelplande acción.
- Realizarvaloracióndelosriesgosdeseguridaddigitalparaverificarsuefectividad.
- Verificarqueloscontrolesestándiseñadoseimplementadosdemaneraefectivayoperencomo sepretende para controlar los riesgos.
- Realizarsugerenciasyrecomendacionesparamejorarlaeficienciayeficaciadeloscontroles

f. FASE DE MEJORA CONTINUA:

Conseguido los resultados de la evaluación de desempeño frente a las estrategias planteadasdel plan de tratamiento de riesgos de seguridad y privacidad de información se procede arealizar un análisis de los resultados con el fin de determinar las medidas correctivas necesarias, los cualespermitan garantizaruna mejoracontinua alo establecido por la entidad en elrespectivoplan.En caso de que existan hallazgos, falencias o incidentes de seguridad y privacidad de lainformación se debe disminuir el impacto de su existencia y tomar acciones para prevenciónycontrol.Estas accionesdemejoracontinua,debendefinirsedelasiguientemanera:

- ✓ Revisaryevaluarloshallazgosencontrados,encasodequeexistan.
- ✓ Analizaryestablecerlasposiblescausasyconsecuenciasdelhallazgo.

- ✓ Determinarsiexistenhallazgossimilaresparaestableceraccionescorrectivasyevitarasíque sumaterialización.
- ✓ Registrardocumentacióndeloshallazgos, delasaccionesrealizadasparadisminucióndelimpacto yde resultados.

5. 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 2025 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:

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

6. CONTROL DE REGISTROS

CONTROL DE REGISTROS DEL SISTEMA DE GESTIÓN DE CALIDAD					
Nombre del registro	**Código**	**Recuperación**	**Almacenamiento**	**Conservación**	**Disposición**
Cronograma Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. 2025		CALIDAD	CALIDAD	NA	NA

7 CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza de los cambios	Responsable

01	22/01/2024	Actualización Cronograma de Actividades vigencia 2025.	Subproceso Sistemas de Información y Estadística

ELABORÓ	REVISO	REVISO
ORIGINAL FIRMADO **Ing. Jhon Córdoba Gil** Cargo: Profesional Apoyo al Subproceso Sistemas de Información y Estadística Afiliado participe Sintraunpros	ORIGINAL FIRMADO **Ing. Juan David Lara Rengifo** Cargo: Profesional designado como Coordinador del Subproceso de Sistemas de Información y Estadística. Afiliado participe Sintraunpros ORIGINAL FIRMADO **Marcela Alejandra Ramírez Otero** Afiliado participe Sintraunpros designada en la Coordinación del Proceso de Gestión de Calidad ORIGINAL FIRMADO **María Catalina Mancilla Ramírez** Afiliado participe Sintraunpros designada en la Coordinación del proceso de Planeación	ORIGINAL FIRMADO **Edilberto Palomino Martínez** PU -Área Administrativa y Financiera
Fecha :23/01/2025	**Fecha : 23/01/2025**	**Fecha : 23/01/2025**

ORIGINAL FIRMADO

Juan Carlos Cotazo Urrea
Cargo: Gerente Empresa Social del Estado Popayán E.S.E

Fecha : 23/01/2025