

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 1 de 11



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

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

## 2024

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 2 de 11

## Tabla de contenido

INTRODUCCION.....	3
1. OBJETIVO.....	4
2. ALCANCE.....	4
3. MARCO LEGAL Y NORMATIVO .....	4
4. PROCEDIMIENTO PARA LA GESTION DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION .....	4
a. CICLO DE OPERACION:.....	6
b. FASE DIAGNOSTICO:.....	7
c. FASE PLANEACION:.....	7
d. FASE IMPLEMENTACION:.....	8
e. FASE EVALUACION DE DESEMPEÑO:.....	8
f. FASE DE MEJORA CONTINUA: .....	8
5. SEGUIMIENTO Y CONTROL.....	9
6. CONTROL DE REGISTROS .....	10
7. CONTROL DE CAMBIOS .....	10

## Tabla de ilustraciones

Ilustración 1 – Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información .....	7
---	---

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 3 de 11

## INTRODUCCION

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) es la entidad encargada por parte del gobierno de COLOMBIA de diseñar, adoptar y promover las políticas, planes y proyectos del sector de las tecnologías de la información y comunicación, por tal motivo la Empresa Social del Estado de Popayán ESE como entidad pública en servicios de salud de primer nivel en el municipio de Popayán y el departamento del cauca, en pro del fortalecimiento tecnológico observa de gran importancia el desarrollo e implementación del plan de tratamiento de riesgos de seguridad y privacidad de la información teniendo como base fundamental las directrices emitidas por el MINTIC con base a este tema, además de encaminarse en la búsqueda de minimizar la vulnerabilidades ante la variedad de riesgos que se presentan, implementando estrategias que permitan contrarrestar estos fenómenos Este tipo de planes buscan definir los mecanismos para la identificación y tratamiento de los riesgos de seguridad y privacidad de la información y permitirá garantizar que estos puedan ser conocidos, gestionados y tratados por parte de la E.S.E POPAYAN.

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 4 de 11

## 1. OBJETIVO

Definir e implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información por parte de la Empresa Social del Estado Popayán E.S.E. para la vigencia 2024 estableciendo un modelo de operación, determinando el alcance, para garantizar que los riesgos de seguridad de la información puedan ser conocidos, gestionados y tratados, por parte de la entidad.

## 2. ALCANCE

El presente plan tiene una vigencia por el año 2024 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.

Una vez elaborado el plan de tratamiento de riesgos de seguridad y privacidad de la información este se socializará a las diferentes dependencias y personal tanto asistencial y administrativo que labore en la E.S.E Popayán.

## 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 Título 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

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 5 de 11

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 título 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 artículo 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 transversales, sedes electrónicas, trámites, 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

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 6 de 11

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 Conformar 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.

#### 4. 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.

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 7 de 11

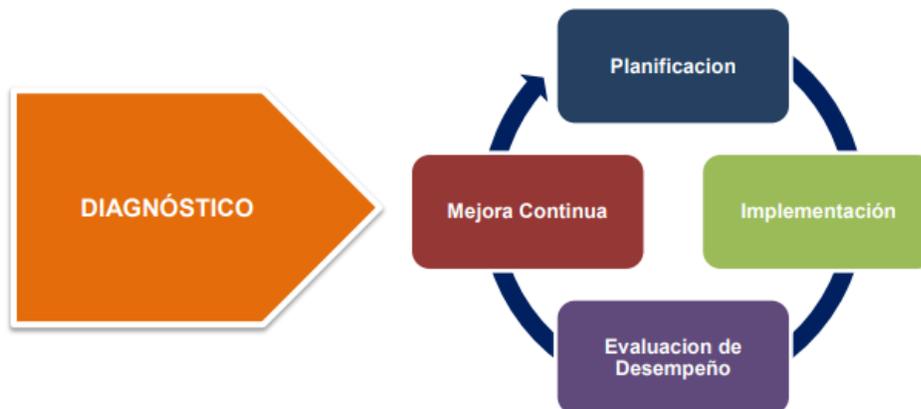


Ilustración 1 – Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

#### 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 para la seguridad y salud de los trabajadores.

#### 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:

$$ICA = \left( \frac{\text{No. de Actividades cumplidas}}{\text{No. de actividades programadas}} \right) * 100$$

Donde ICA es el Índice de Cumplimiento de Actividades

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 8 de 11

#### **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 y operen como se pretende para controlar los riesgos.
- Realizar sugerencias y recomendaciones para mejorar la eficiencia y eficacia de los controles

#### **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 continua 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:

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 9 de 11

- ✓ Revisar y evaluarlos 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 así que su materialización.
- ✓ Registrar documentación de los hallazgos, de las acciones realizadas para disminución del impacto y de 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 2023 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. ANEXOS

### 6.1 Anexo 1: Cronograma Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 10 de 11

## 7. 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. 2024		CALIDAD	CALIDAD	NA	NA

## 8. CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza de los cambios	Responsable
3	Enero de 2024	Actualización cronograma vigencia 2024.	<b>Ing. Jhon Alexander Córdoba Gil</b> Apoyo a Sistemas  <b>Ing. Juan David Lara Rengifo</b> Coordinador Sistemas de Información y Estadística.

	Proceso:	GESTION DE INFORMACION Y COMUNICACIONES	Código:	GIC-SIE-PLAN-06
	Subproceso:	Sistema de Información y Estadística	Versión:	3
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2024
			Página:	Página 11 de 11

ELABORÓ	REVISO	REVISO – PROCESO GESTIÓN DE CALIDAD
<p><b>ORIGINAL FIRMADO</b>  <b>Ing. JHON CÓRDOBA GIL</b>            Cargo: Designado en el proceso de Sistemas de Información y Estadística            Afiliado participe Sintraunpros</p>	<p><b>ORIGINAL FIRMADO</b>  <b>MAYERLY GONZALES VANEGAS</b>            Cargo: Designada como Líder del proceso de Planeación Afiliada participe Sintraunpros</p> <p><b>ORIGINAL FIRMADO</b>  <b>Ing. JUAN DAVID LARA RENGIFO</b>            Cargo: Profesional Designado en el proceso de Sistemas de Información y Estadística.            Afiliado participe Sintraunpros</p> <p><b>ORIGINAL FIRMADO</b>  <b>EDILBERTO PALOMINO</b>            Cargo: Profesional Universitario Asistencia Administrativa</p>	<p><b>ORIGINAL FIRMADO</b>  <b>MARIA CATALINA MANCILLA RAMIREZ</b>            Cargo: Profesional Designada en la Coordinación del proceso Gestión de la Calidad- Afiliada Participe Sintraunpros</p>
<b>Fecha :</b>	<b>Fecha :</b>	<b>Fecha :</b>
<b>APROBO</b>		
<p><b>ORIGINAL FIRMADO</b>  <b>DRA. ZULLY BERNARDA RUIZ MENESES</b>            Cargo: Gerente</p>		