

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 1 de 8



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

2022

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 2 de 8

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:	4
b. FASE DIAGNOSTICO:	5
c. FASE PLANEACION:	5
d. FASE IMPLEMENTACION:	6
e. FASE EVALUACION DE DESEMPEÑO:	6
f. FASE DE MEJORA CONTINUA:	6
5. SEGUIMIENTO Y CONTROL	7
6. CONTROL DE REGISTROS	7
7. CONTROL DE CAMBIOS	8

Tabla de ilustraciones

Ilustración 1 – Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información	5
---	---

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 3 de 8

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 y 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.

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:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 4 de 8

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. 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 2022 y el alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información por parte de la E.S.E POPAYAN 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

- ✓ Modelo de seguridad, Fortalecimiento Tecnologías de la Información
- ✓ Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)

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:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 5 de 8

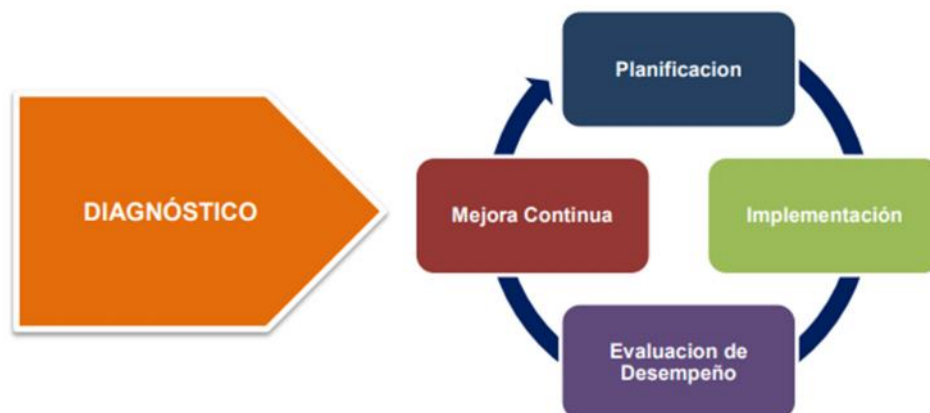


Ilustración 1 – Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

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:

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

Donde ICA es el Índice de Cumplimiento de Actividades

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 6 de 8

d. FASE IMPLEMENTACION:

En esta fase se ejecutaran 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 estudio de los resultados para generar los correctivos necesarios, 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:

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

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 7 de 8

- ✓ Analizar y establecer las posibles causas y consecuencias del hallazgo.
- ✓ Determinar si existen hallazgos similares para establecer acciones correctivas y evitar así 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 2022 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. 2022		CALIDAD	CALIDAD	NA	NA

	Proceso:	Apoyo	Código:	APO-GSI-PLAN-06
	Subproceso:	Gestión Sistemas de Información y Estadística	Versión:	01
	Nombre del documento:	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Fecha:	Enero de 2022
			Página:	Página 8 de 8

7. CONTROL DE CAMBIOS

Versión	Fecha	Naturaleza de los cambios	Responsable
01	31-01-2022	Actualización vigencia 2022.	Jhon Córdoba Gil Apoyo a Sistemas Enrique Betancourt Coordinador Sistemas de Información y Estadística.