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

TABLA DE CONTENIDO

LISTA FIGURAS

1. INTRODUCCION

La protección de la información de una entidad pública, ante cualquier posibilidad de alteración, pérdida, mal manejo, entre otros, genera un respaldo para el normal desarrollo de la entidad, La información es el lazo de conexión con el ciudadano, por lo tanto, es de gran importancia.

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 permitirá garantizar que los riesgos de seguridad de la información puedan ser conocidos, gestionados y tratados por parte de la E.S.E POPAYAN.

2. OBJETIVOS

Desarrollar el plan de tratamiento de riesgos de seguridad y privacidad de la información por parte de la EMPRESA SOCIAL DEL ESTADO POPAYAN E.S.E. estableciendo un modelo de operación, determinando el alcance, los principales activos a proteger, y su respectivo seguimiento, para garantizar que los riesgos de seguridad de la información puedan ser conocidos, gestionados y tratados, por parte de la entidad.

3. MARCO LEGAL Y NORMATIVO

- Ley 1581 de 2012: Tratamiento de datos personales. Ley 1712 de 2014: Información pública
- Decreto 1074 de 2015: (antiguo Decreto 1377 de 2013) Capítulo 25 – Reglamenta
- parcialmente la Ley 1581 de 2012
- Decreto 1081 de 2015 (antiguo Decreto 103 de 2015): Título 1. Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.

4. ALCANCE

El alcance del plan de tratamiento de riesgos de seguridad y privacidad de la información por parte de la E.S.E POPAYAN es por los años 2020 y 2021 tenerlo diseñado, e implementado en su totalidad, cumpliendo con los principales lineamientos emitidos por parte del MINTIC para garantizar la correcta seguridad y privacidad de la información aplicada a las diferentes dependencias en la institución.

Una vez desarrollado e implementado 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 POPAYAN.

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

5.1 CICLO OPERACIÓN

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.

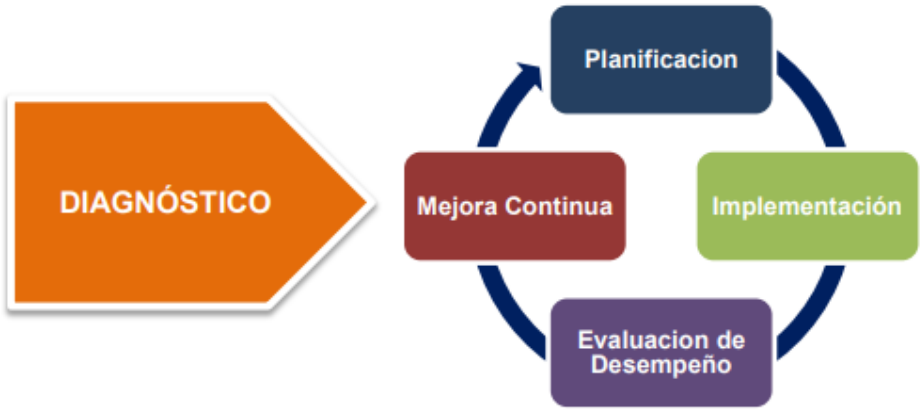

Figura 1. Modelo de seguridad y privacidad de la información

5.1.1 DIAGNOSTICO

La Empresa Social del Estado Popayán E.S.E. se ve en la necesidad de realizar un autodiagnóstico para identificar el tipo de riesgos y determinarel nivel en que se encuentra, 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, tanto para la dependencia como para la E.S.E POPAYAN en general.

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 Matriz de Riesgos es una herramienta de gestión que permite determinar los riesgos relevantes para la seguridad y salud de los trabajadores.

5.1.2 PLANEACIÓN

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

5.1.3 IMPLEMENTACIÓN

En esta fase se realiza la ejecución de las estrategias trazadas en la fase de planeación para así poder implementar el plan de tratamiento y poder registrar los resultados obtenidos por cada meta u 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 ydesarrollados por los responsables asignados.

5.1.4 EVALUACIÓN 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.
- Revisarperiódicamente de las actividades de control para determinar su relevancia y actualizaciones pertinentes.
- Monitorear los riesgos y controles tecnológicos.
- Evaluar el plan de acción.
- Realizar valoraciónde 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

5.1.5 FASE DE MEJORA CONTINÚA

Obtenido 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.

• 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.

5.2 CRONOGRAMA DE ACTIVIDADES

	EMPRESA SOCIAL DEL ESTADO ESE POPAYAN	Código:
	CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION	Versión:
	VIGENCIA 2021	Página:

ACTIVIDADES	META O PRODUCTO	INDICADOR DE GESTIÓN	RESPONSABLES	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
Actualización plan de tratamiento de riesgos	Documento Aprobado	Documento Aprobado	Sistemas de la Información y Estadística - Planeación	x											
Actualizar política y Establecer un procedimiento para la gestión integral del riesgo de seguridad y privacidad de la información	Política y procedimiento de administración de riesgos aprobado	Documentos aprobados /(2) *100%	Sistemas de la Información y Estadística - Planeación - Calidad		x	x									
Identificación de riesgos de seguridad digital según guía para la administración de riesgos y el diseño de controles en entidades	Matriz de riesgos identificatios	Identificador de riesgos de seguridad digital	Sistemas de la Información y Estadística - Planeación			x	x	x							

publicas														
Elaboración matriz de riesgos de seguridad de la información	Documento aprobado	Matriz de riesgos de seguridad digital Elaborada	Sistemas de la Información - Planeación				x	x	x					
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 controla los riesgos.	Valoración individual de riesgos/ total de riesgos de seguridad y privacidad de la información * 100 %	Planeación						x	x				
Mantener copias de seguridad y/o backups en el servidor de las bases de datos de los aplicativos y Software de la E.S.E. Popayán para salvaguardar la información de la entidad	cumplimiento de la seguridad de los archivos en dispositivos externos o servidores	base de datos respaldados / Total de base de datos * 100	Sistemas de Información y Estadística	x	x	x	x	x	x	x	x	x	x	x
Mantener todas las áreas funcionales conectadas a la red	Porcentaje de equipos de cómputo conectados debidamente a la red de datos	Todas las áreas funcionales en la red de la ESE POPAYAN	Sistemas de Información	x	x	x	x	x	x	x	x	x	x	x