GUÍA DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

2026-2027

Versión 2

REGIÓN ADMINISTRATIVA Y DE PLANEACIÓN ESPECIAL
RAP-E REGION CENTRAL

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA
PROCESO DE GESTIÓN TIC
2026

BOGOTÁ BOYACÁ CUNDINAMARCA META TOLIMA HUILA

REGIÓN CENTRAL
RAP-E | Estamos Construyendo Región

Contenido

1. Introducción 5
2. Objetivo General 6
2.1. Objetivos Específicos 6
3. Alcance 6
4. Marco Normativo 7
5. Ciclo de Operación 9
5.1. Hoja de Ruta del Sistema de Gestión de Seguridad de la Información 9
Fase 1: Diagnóstico: 10
Fase 2: Planificación 14
Fase 3: Implementación 17
Fase 4: Evaluación de Desempeño. 18
Fase 5: Mejora Continua. 20
6. Control de Cambios 21

Contenido de Ilustraciones

Ilustración 1. Ciclo del Modelo de Seguridad y Privacidad de la Información 9
Ilustración 2. Efectividad de controles ISO 27001:2022 vigencia 2026 11
Ilustración 3. Radar controles ISO 27001:2022 12
Ilustración 4. Resultados NIST CSF 13
Ilustración 5. Radar NIST vigencia 2026 13
Ilustración 6. Indicadores SGSI 19

Contenido de tablas

Tabla 1. Hoja de ruta SGSI 10
Tabla 2. Fase de Planificación SGSI 15
Tabla 3. Cronograma SGSI 16
Tabla 4. Fase de implementación SGSI 18
Tabla 5. Fase de evaluación y desempeño 20
Tabla 6. Fase mejora continua SGSI 21

1. Introducción

En un contexto de globalización donde la información se ha constituido como un recurso estratégico, las entidades públicas se enfrentan a la necesidad de gestionar, proteger y, por lo demás, garantizar la privacidad de los datos cumpliendo con las buenas prácticas y los mejores niveles de seguridad. En este sentido, la Región Administrativa y de Planeación Especial – RAP-E Región Central ha entendido la necesidad de implementar un sistema integral de seguridad y de privacidad de la información que le permita cumplir con la normatividad existente y, al mismo tiempo, dotar de garantías en términos de seguridad de la información a sus aliados estratégicos regionales y a los ciudadanos en la gestión de la región central.

En virtud de lo anterior, el Sistema de Gestión de Seguridad de la Información (SGSI) de la RAP-E está basado en los principios de confidencialidad, integridad, disponibilidad, legalidad y transparencia, en estricto cumplimiento de la Ley 1581 de 2012, "Por la cual se dictan disposiciones para la protección de datos personales", de las normas de carácter nacional como el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y estándares internacionales como ISO 27001, sus anexos y normas complementarias, por lo que este modelo busca proteger los activos de información institucionales frente a riesgos tanto internos como externos, a su vez este modelo promueve una cultura de prevención con base en el uso y apropiación de las tecnologías de seguridad y privacidad de la información que impacte de forma positiva y transversal en la RAP-E, con el propósito de proveer la mayor garantía en el cumplimiento los derechos de seguridad y privacidad de la información privada y sensible como lo son los datos de los ciudadanos.

Este Sistema se encuentra desarrollado con base en un enfoque estructurado y dinámico de acuerdo con los lineamientos emitidos por el Ministerio de las Tecnologías de la Información - MinTIC en su modelo MSPI; el sistema también establece políticas, procedimientos y controles que permiten la identificación, evaluación y con el propósito de mitigar riesgos y garantizar que la RAP-E pueda operar y gestionar de manera segura y resiliente en el ciberespacio. Además, define los componentes claves del modelo MSPI con fundamentos normativos y técnicos de seguridad, y establece la estrategia de implementación que garantizará la gestión adecuada de la información institucional, de forma que toda la RAP-E se apoye en su Proceso de Gestión TIC y que esta práctica contribuya al cumplimiento de los objetivos estratégicos institucionales, así como, también al desarrollo sostenible de la región.

2. Objetivo General

Establecer y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) de la RAP-E Región Central, con el fin de garantizar la protección, confidencialidad, integridad, disponibilidad y no repudio de los activos de información institucional. A través de la gestión del riesgo, la implementación de políticas, controles y procesos que mitiguen amenazas y aseguren el cumplimiento normativo. Así mismo, la promoción de una cultura de ciberseguridad, la protección de derechos ciudadanos y la resiliencia operativa, contribuyendo a una gestión transparente y sostenible de la información.

2.1. Objetivos Específicos

a. Evaluar el estado actual de la seguridad y privacidad de la información en la RAP-E Región Central, mediante la aplicación de la herramienta dispuesta por MinTIC, identificando brechas y clasificando los activos, amenazas, vulnerabilidades, nivel de cumplimiento normativo y madurez en la gestión de riesgos.

b. Definir el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), estableciendo políticas, procedimientos, objetivos, controles, responsables y recursos, con base en los resultados del diagnóstico y el enfoque de gestión del riesgo.

c. Implementar y desarrollar los controles, políticas y procedimientos definidos, fortaleciendo las capacidades institucionales, tecnológicas y humanas para la gestión segura de los activos de información.

d. Medir la eficacia de la gestión del riesgo de seguridad y privacidad de la información, mediante el seguimiento a los riesgos identificados que cuentan con planes de tratamiento definidos e implementados, contribuyendo a la reducción de la exposición al riesgo y al fortalecimiento del SGSI.

e. Establecer acciones correctivas y de mejora que permitan optimizar el SGSI, como capacitaciones y sesiones de concientización, fortaleciendo la gestión de riesgos y asegurando su evolución frente a cambios institucionales, tecnológicos y normativos.

3. Alcance

El SGSI de la RAP-E Región Central aplica a todos los procesos, sistemas de información, aplicaciones, plataformas tecnológicas, servicios y activos de información de la entidad. Asimismo, abarca a todos los funcionarios, contratistas y terceros que accedan, gestionen o traten información institucional independientemente del medio, formato o ubicación; comprende la protección de la información en todos sus niveles de clasificación y durante todo su ciclo de vida, incluyendo datos personales y sensibles, mediante la implementación de controles orientados a garantizar la confidencialidad, integridad, disponibilidad, privacidad de la información y no repudio.

El SGSI se implementará de manera gradual a través de las fases de diagnóstico, planificación, implementación, evaluación del desempeño y mejora continua, asegurando su sostenibilidad y alineación con los objetivos estratégicos de la entidad.

4. Marco Normativo

El marco regulatorio del Sistema de Gestión de Seguridad de la Información (SGSI) de la RAP-E define las reglas, lineamientos y principios legales que rigen el diseño, implementación y operación de los sistemas de seguridad, con enfoque en la protección de activos físicos, digitales y de información. En Colombia, este marco se basa en la Constitución, leyes específicas, reglamentos, resoluciones y estándares internacionales, garantizando la protección de los derechos fundamentales, la privacidad ciudadana, la integridad del sistema y la protección contra riesgos de seguridad.

A continuación, se detalla el marco regulatorio que puede considerar los siguientes factores al momento de desarrollar o implementar un modelo de seguridad en Colombia:

TIPO DE NORMA	NÚMERO	AÑO	EMISOR	APLICACIÓN
Ley	Constitución Política de Colombia, Artículo 15	1991	Asamblea constituyente de Colombia	Establece el derecho a la intimidad personal y familiar, el habeas data y la protección de la información, garantizando que los datos recolectados, almacenados o procesados deben ser tratados conforme a los principios de seguridad y confidencialidad.
Ley	Artículo 74 de la Constitución Política de Colombia	1991	Asamblea constituyente de Colombia	Reconoce el derecho al acceso a la información pública, promoviendo la transparencia y regulando el acceso controlado a información sensible para preservar la seguridad nacional y la privacidad de las personas.
Ley	1581	2012	Congreso de la República	Conocida como el Régimen General de Protección de Datos Personales, regula el manejo, tratamiento y circulación de datos personales en Colombia, estableciendo principios como la

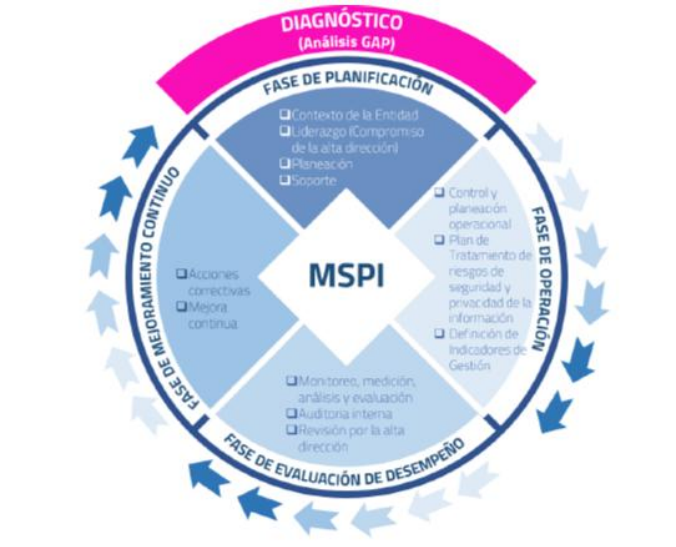
				seguridad de la información, la legalidad y la confidencialidad. La ley exige medidas técnicas, humanas y administrativas para garantizar la seguridad de la información almacenada.
Ley	1273	2009	Congreso de la República	Introdujo el concepto de "bien jurídico protegido" al ámbito de la información, tipificando los delitos informáticos y estableciendo sanciones penales para el acceso no autorizado a sistemas informáticos, alteración de datos y espionaje digital.
Ley	1928	2018	Congreso de la República	Promueve el fortalecimiento de la ciberseguridad y la ciberdefensa en Colombia, vinculando a diferentes entidades públicas y privadas en la protección del ciberespacio.
Ley	1712	2014	Congreso de la República	Establece el derecho de acceso a la información pública, regulando la transparencia activa y pasiva, pero también obliga a implementar medidas de seguridad para proteger información sensible o clasificada que, de divulgarse, pudiera comprometer la seguridad nacional o personal.
Decreto	1078	2015	MinTIC	Reglamento Único del Sector TIC, que incluye disposiciones sobre la protección de la información, la gestión de riesgos y el establecimiento de mecanismos de seguridad en las entidades públicas y privadas del sector.
Decreto	1083	2015	MinTIC	Establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".
Decreto	338	2022	MinTIC	Refuerza la estrategia de ciberseguridad nacional, definiendo responsabilidades para entidades públicas y privadas en la prevención de incidentes de seguridad informática.
Estándar	ISO/IEC 27001	2022	ISO	Estándar internacional para sistemas de gestión de seguridad de la información (SGSI), adoptado en Colombia para garantizar la confidencialidad, integridad y disponibilidad de los datos.

Estándar	ISO/IEC 27002	2022	ISO	Código de buenas prácticas para controles de seguridad de la información, que establece pautas detalladas para mitigar riesgos.
Resolución	02277	2025	MinTIC	Actualiza el MSPI para fortalecer la estrategia de seguridad digital del estado colombiano alineado con el estándar ISO/IEC: 27001:2022 y las nuevas tecnologías como la IA.

5. Ciclo de Operación

De conformidad con la guía del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, este Sistema de Gestión de Seguridad de la Información, está estructurado en cinco (5) fases que permiten a las entidades gestionar y mantener de forma adecuada la seguridad y privacidad de sus activos de información, así:

Ilustración 1. Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: articles-401770_recurso_1.pdf

5.1. Hoja de Ruta del Sistema de Gestión de Seguridad de la Información

Con el fin de proporcionar una visión integral del proceso de implementación y fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), la RAP-E Región Central establece en la tabla la siguiente hoja de ruta, la cual describe de manera secuencial las fases, resultados esperados y principales actividades que orientan la gestión de la seguridad y privacidad de la información institucional. Esta hoja de ruta permite visualizar el ciclo completo del SGSI, desde la identificación del estado actual y las brechas de seguridad, hasta la implementación de controles, la evaluación de

su desempeño y la ejecución de acciones de mejora continua, garantizando su alineación con los objetivos estratégicos institucionales, los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las mejores prácticas internacionales en materia de seguridad de la información.

Tabla 1. Hoja de ruta SGSI

Fase	Resultado esperado
Diagnóstico	Identificación del estado actual, brechas, riesgos y nivel de madurez del SGSI.
Planificación	Definición del PESI, matriz de riesgos, políticas, procedimientos, indicadores y cronograma de implementación.
Implementación	Ejecución de controles, planes de tratamiento de riesgos, socialización y fortalecimiento de capacidades institucionales.
Evaluación del desempeño	Seguimiento de indicadores, evaluación del cumplimiento de controles, auditorías y monitoreo de riesgos.
Mejora continua	Implementación de acciones correctivas y de mejora para fortalecer el SGSI y aumentar su nivel de madurez

Fuente: elaboración propia

Fase 1: Diagnóstico:

Esta fase permite ala RAP-E establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin en esta fase se propone realizar un “Diagnóstico” utilizando el “instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

El resultado de la evaluación del estado actual y sus evidencias correspondientes a la vigencia 2026 representan el estado actual de los controles implantados en la entidad, acorde con lo establecido en la Norma Técnica Colombiana NTC/ISO/IEC 27001:2013, y con base en los lineamientos descritos en el documento maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por MinTIC para todas las entidades públicas. Así mismo, el resultado obtenido después de la aplicación de la fase de evaluación de desempeño del MSPI se incluirá como un insumo, en la fase de mejoramiento continuo.

Así las cosas, en el desarrollo del proceso de evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la RAP-E, se aplicó el instrumento de autodiagnóstico para la medición del

nivel de seguridad y privacidad de la información institucional, el cual busca valorar la efectividad y grado de implementación de los controles de la norma ISO 27001:2022 conforme a los criterios definidos en el anexo A; como resultado de dicha evaluación, se obtuvieron los siguientes resultados:

En la ilustración 2 se muestra la tabla 1 que evidencia el nivel de efectividad cuantitativo de los controles (A.5 – A.8) aplicados de acuerdo con la norma ISO 27001, por lo tanto, muestra que el nivel de madurez es efectivo, pero aún falta avanzar en la implementación y fortalecimiento de controles.

Ilustración 2. Efectividad de controles ISO 27001:2022 vigencia 2026

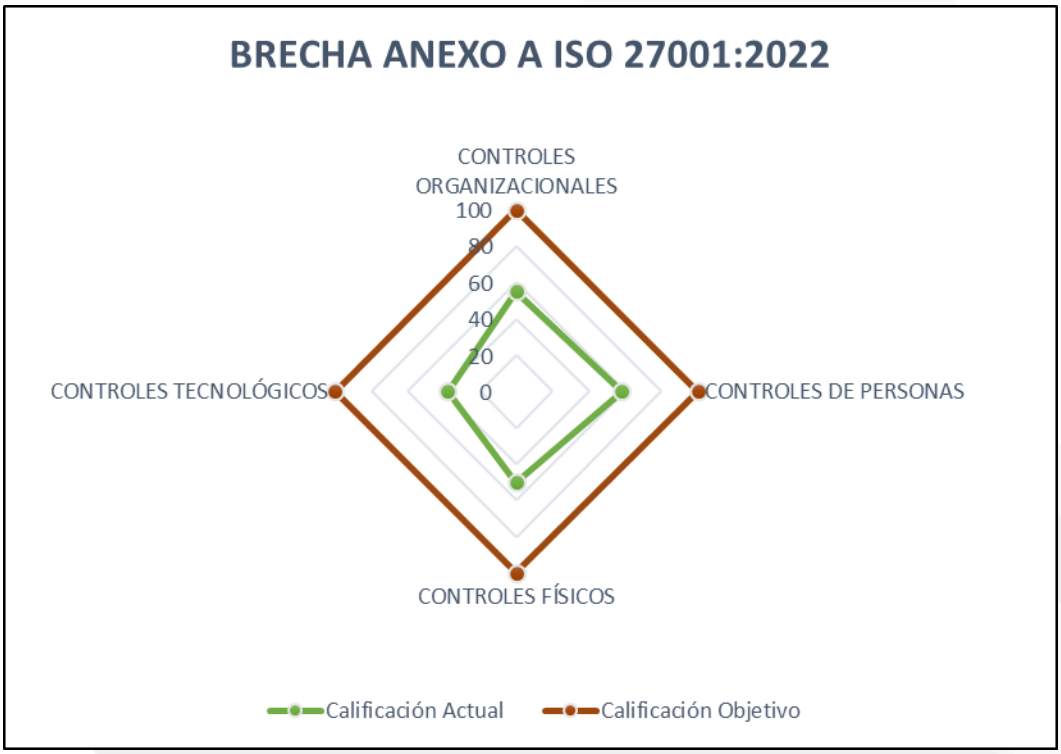
No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	55	100	EFECTIVO
A.6	CONTROLES DE PERSONAS	58	100	EFECTIVO
A.7	CONTROLES FÍSICOS	50	100	EFECTIVO
A.8	CONTROLES TECNOLÓGICOS	38	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		50	100	EFECTIVO

Fuente: herramienta de autodiagnóstico MSPI

la ilustración 2 refleja que la RAP-E presenta un nivel de madurez promedio de 50/100, con resultados relativamente homogéneos en los dominios organizacionales, personas y físicos, pero con una brecha crítica en el dominio tecnológico. Este resultado evidencia que, aunque la entidad tiene una base aceptable en aspectos formales, administrativos y de infraestructura, su principal debilidad se concentra en la operación de la seguridad y el control técnico de los sistemas de información, especialmente en desarrollo de software, gestión de cambios, vulnerabilidades y monitoreo. En términos estratégicos se confirma que la organización se encuentra en un nivel "Repetible–medio", con capacidades parciales, pero no integradas, formalizadas ni gestionadas, lo que la mantiene en una postura reactiva más que preventiva.

Así mismo, la ilustración 3 tipo radar evidencia una brecha significativa entre el estado actual y el esperado (100%), siendo el dominio tecnológico el más rezagado, confirmando el principal punto crítico identificado.
Esto reafirma que, aunque existen bases en lo organizacional, físico y humano, la seguridad no está sostenida por un control técnico sólido ni gobernado estructuralmente.

Ilustración 3. Radar controles ISO 27001:2022



Fuente: herramienta de autodiagnóstico MSPI

De la misma manera los resultados del NIST entregan una respuesta que permite evidenciar que el principal reto es **fortalecer el gobierno TI, en consecuencia, formalizar procesos y cerrar las brechas estructurales en la capa tecnológica**, que hoy representan el mayor riesgo para la seguridad de la información institucional.

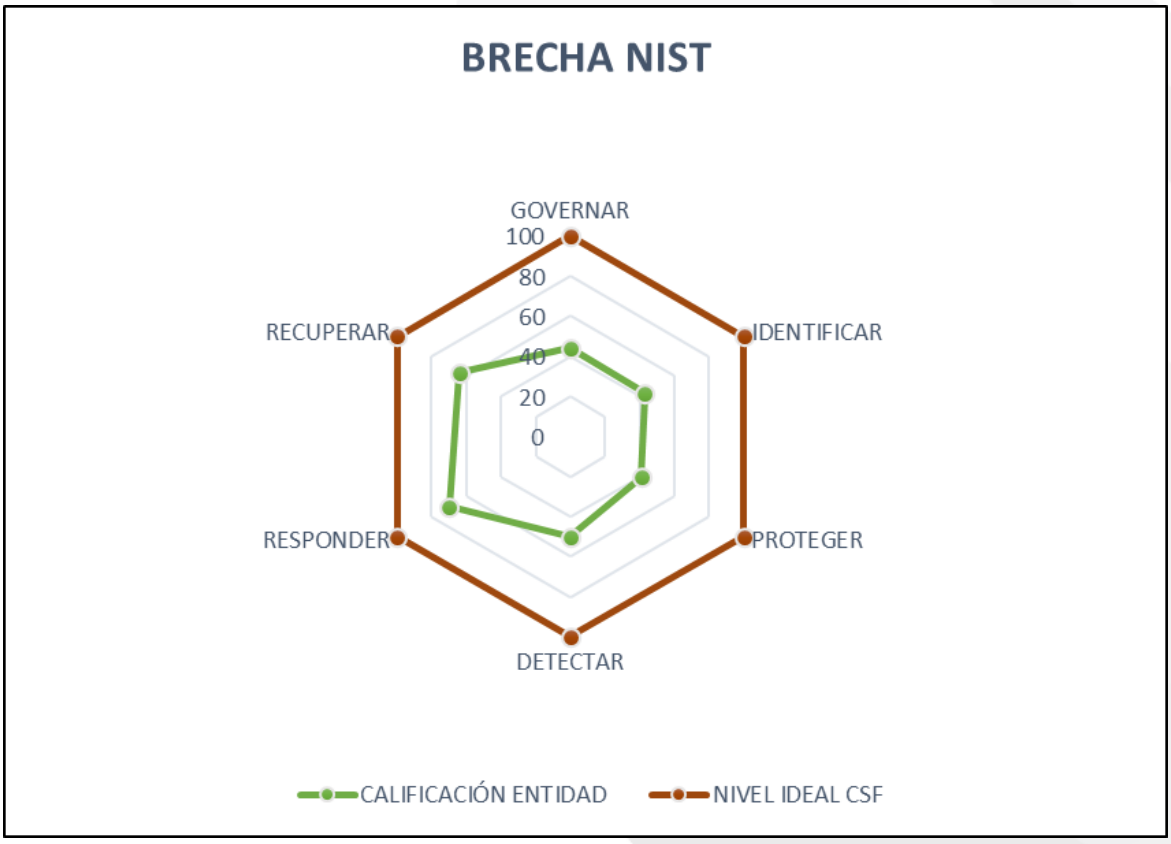
Las ilustraciones 4 y 5 evidencian una **brecha significativa frente al nivel ideal (100)** en todas las funciones del MSPI. destacándose debilidades marcadas en **Gobernar (44), Identificar (43) y Proteger (41)**, lo que confirma la falta de enfoque preventivo y de gobierno TI ya evidenciada en ISO. Sin embargo, los mejores resultados en **Responder (70) y Recuperar (64)** muestran que la entidad ha desarrollado capacidades reactivas, evidenciando una postura de ciberseguridad orientada a responder incidentes más que a prevenirlos.

Ilustración 4. Resultados NIST CSF

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
GOVERNAR	44	100
IDENTIFICAR	43	100
PROTEGER	41	100
DETECTAR	50	100
RESPONDER	70	100
RECUPERAR	64	100

Fuente: herramienta de autodiagnóstico MSPI

Ilustración 5. Radar NIST vigencia 2026



Fuente: herramienta de autodiagnóstico MSPI

El autodiagnóstico del SGSI constituye una oportunidad estratégica clave para avanzar en el proceso de madurez del Gobierno de TI y el fortalecimiento de la seguridad digital en la RAP-E, permitiendo identificar de manera estructurada las brechas existentes en materia de ciberseguridad. Su valor radica en la posibilidad de orientar la toma de decisiones hacia la implementación de controles

robustos, procesos formalizados y capacidades preventivas, que permitan mitigar eficazmente las amenazas cibernéticas. En este sentido, el diagnóstico no solo representa una línea base, sino también un punto de partida para la construcción de un modelo de Gobierno TI sólido, integral y alineado con buenas prácticas internacionales.

Asimismo, al comparar el resultado actual con el obtenido en la vigencia anterior (44), se evidencia un avance significativo en la madurez de la seguridad de la información, lo cual demuestra un progreso en la adopción de controles y lineamientos en el SGSI. No obstante, este nivel aún requiere ser fortalecido mediante la consolidación de procesos, la implementación efectiva de controles técnicos y el establecimiento de mecanismos de seguimiento y mejora continua, garantizando que la evolución del Gobierno TI y la ciberseguridad se realice de forma estructurada, sostenible y alineada con los objetivos estratégicos de la entidad.

Fase 2: Planificación

En la etapa de planificación del Sistema de Gestión de Seguridad de la Información (SGSI) se concreta la identificación pormenorizada de actividades, acciones y resultados para la aprobación de la Política General de Seguridad de la Información y el diseño de un Plan de Seguridad y Privacidad de la Información que sea coherente a los requerimientos de la Entidad. Esta planificación resultante debe estar en consonancia con las metas estratégicas e institucionales asegurando al mismo tiempo que las políticas y medidas propuestas coadyuvan en la gestión de los objetivos de la entidad.

La planificación del SGSI incluye la utilización de un enfoque estructurado de acuerdo con una metodología de gestión de riesgos que permite identificar, valorar y mitigar los riesgos del manejo de la información. Esa metodología significa la realización de una evaluación en detalle de los activos de información, las amenazas y vulnerabilidades, así como la concreción de los controles y mecanismos que permitirán bajar la probabilidad del riesgo a niveles que sean aceptables.

Igualmente se delimitará el alcance del SGSI con la determinación de los ámbitos, procesos, recursos y tipo de información que será objeto de protección mediante la gestión del SGSI. Al implementar límites con el propósito de planear el SGSI permite centrar el mismo en los aspectos relevantes de la seguridad y privacidad de la información.

Así mismo se fijan parámetros y normas de los cuales se regirán la aplicación de las políticas de seguridad donde se determinarán y seleccionarán los controles técnicos, administrativos y físicos mediante los cuales se mitigarán las amenazas determinadas, aunado a que la planificación integral no sólo mejora las condiciones de seguridad de las actividades dentro de los procedimientos y las áreas de la Entidad sino que la cultura organizacional del manejo de la seguridad y privacidad de la información alcanzará niveles de madurez.

Por el lado de la RAP-E Región Central, la fase actual de planeación se encuentra en desarrollo, con un enfoque orientado a la integración de buenas prácticas internacionales en seguridad de la

información, la definición de responsabilidades claras para el personal involucrado y la incorporación de tecnologías y procedimientos modernos que contribuyan a un entorno más seguro y resiliente para la gestión de la información institucional.

Tabla 2. Fase de Planificación SGSI

FASE DE PLANIFICACIÓN		
Metas	**Resultados**	**Instrumento**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por Comité Institucional de Gestión y Desempeño y publicada en la web.	Política General de Seguridad de la Información RAP-E 2026v3.pdf
Plan de Seguridad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por Comité Institucional de Gestión y Desempeño y publicada en la web.	Plan-de-Seguridad-y-Privacidad-de-la-Informacion-.pdf
Plan de Comunicaciones.	Se crea Plan de Cambio y Cultura de Seguridad y Privacidad Información, está pendiente de aprobación del Comité Institucional de Gestión y Desempeño.	Plan de Comunicación de Seguridad de la Información .pdf
Matriz de riesgos de Seguridad de la Información	Riesgos identificados, valorados y con tratamiento definido	

Fuente: elaboración propia

Con el fin de garantizar una implementación gradual, controlada y alineada con los objetivos estratégicos de la RAP-E Región Central, se establece el cronograma de la Tabla 3 de ejecución para las actividades definidas dentro del Sistema de Gestión de Seguridad de la Información SGSI. Este cronograma contempla actividades asociadas a la gestión de activos, gestión de riesgos, implementación de controles, seguimiento, evaluación del desempeño y mejora continua, las cuales

serán ejecutadas y monitoreadas por el proceso de Gestión TIC con el apoyo de las dependencias involucradas.

Tabla 3. Cronograma SGSI 2026-2027

SGSI RAP-E	Cronograma de actividades SGSI 2026-2027						
	Actividad	**Jul**	**Ago**	**Sep**	**Oct**	**Nov**	**Dic**
Segundo semestre 2026	Elaboración del Sistema de Gestión de Seguridad de la Información (SGSI)						
	Presentación del nuevo SGSI que incluye Política General de Seguridad de la Información, Manual de Políticas de Seguridad de la información, Plan de comunicaciones de Seguridad de la Información y la Guía ante la Junta directiva.						
	Evaluación y aprobación de la Política General de Seguridad de la Información por parte del Gerente o quien haga sus veces						
	Elaboración de la resolución de aprobación de la a Política General de Seguridad de la Información						
Primer Semestre 2027	**Actividad**	**Ene**	**Feb**	**Mar**	**Abr**	**May**	**Jun**
	Actualización inventario activos						
	Identificación de riesgos						
	Valoración y clasificación de riesgos (matriz)						
	Definición de tratamiento riesgos						
	Definición de controles						
	Implementación controles						
	Elaboración PESI						
	Ejecución PESI						
	Capacitación seguridad						
	Seguimiento de indicadores						
	Informe Semestral Comité						

	Actividad	Jul	Ago	Sep	Oct	Nov	Dic
Segundo Semestre 2027	Revisión inventario						
	Revisión y actualización de riesgos						
	Actualización tratamiento de riegos						
	Implementación controles						
	Auditoría interna TIC						
	Plan de mejora						
	Capacitación seguridad						
	Medición indicadores						
	Informe Comité						

Fuente: elaboración propia

Fase 3: Implementación

En la fase de Implementación del Sistema de Gestión de Seguridad de la Información (SGSI), la RAP-E asume un enfoque estratégico y operativo para garantizar la adecuada protección de los activos de información, esto quiere decir, que la alta dirección debe revisar, ajustar de ser necesario y aprobar todos los lineamientos para la implementación adecuada del SGSI en la RAP-E. A nivel operativo este proceso abarca la planificación, ejecución y monitoreo constante de todas las actividades necesarias para cumplir con los requisitos establecidos en materia de seguridad y privacidad. Estas acciones no solo están alineadas con las normativas internas de la organización, sino que también cumplen con las disposiciones legales y regulatorias externas aplicables, proporcionando un marco sólido que asegura la integridad, disponibilidad y confidencialidad de la información.

Durante esta fase, es fundamental la documentación rigurosa y sistemática de cada actividad realizada. Esto incluye registrar detalladamente la ejecución de las tareas, los resultados obtenidos, las métricas de desempeño, así como cualquier desviación, ajuste o mejora implementada para optimizar las condiciones de seguridad. La documentación sirve como evidencia de cumplimiento y proporciona insumos para auditorías internas o externas, además de facilitar la gestión continua de riesgos asociados a la información.

La implementación del SGSI también promueve una cultura organizacional basada en la seguridad y la privacidad, involucrando a todos los niveles jerárquicos de la Entidad. La sensibilización y capacitación del personal son componentes críticos para fortalecer las capacidades de prevención, detección y respuesta ante incidentes.

Actualmente, la RAP-E Región Central se encuentra avanzando en la fase de implementación. A continuación, se detallan los logros alcanzados, las actividades en curso y los desafíos identificados, los cuales forman parte del compromiso continuo para garantizar un entorno de información seguro y confiable.

Tabla 4. Fase de implementación SGSI

FASE DE IMPLEMENTACIÓN		
Metas	**Resultados**	**Instrumento**
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por Comité Institucional de Gestión y Desempeño y publicada en la web.	Política General de Seguridad de la Información RAP-E 2027v1.pdf
Plan de Seguridad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por Comité Institucional de Gestión y Desempeño y publicada en la web.	Plan-de-Seguridad-y-Privacidad-de-la-Informacion-2024-2026.pdf

Fuente: elaboración propia

Fase 4: Evaluación de Desempeño.

En el marco de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), liderado por el proceso de Gestión TIC, la RAP-E Región Central establecerá y desarrollará mecanismos estructurados de seguimiento, medición, análisis y evaluación, orientados a garantizar la efectividad del sistema y su alineación con los objetivos estratégicos de la entidad. Estos

mecanismos permitirán evaluar de manera continua el desempeño del MSPI, soportando la toma de decisiones y el fortalecimiento del Gobierno TI y la ciberseguridad institucional.

Para tal fin, se han definido indicadores clave de desempeño que permiten medir el avance y la eficacia de la gestión de riesgos y la implementación de controles de seguridad, como lo muestra la ilustración 6:

Ilustración 6. Indicadores SGSI

ID	Indicador	Objetivo	Fórmula	Meta	Frecuencia	Responsable	Evaluacion	Fuente de información
1	% de evaluación del estado de seguridad de la información	Evaluar el estado actual de la seguridad y privacidad de la información	(Controles evaluados / Controles aplicables) x100	100%	Semestral	Gestión TIC	Jun-Dic	Herramienta de diagnóstico e informe
2	% de implementación de controles	Formular e implementar politicas, procedimientos y controles	(Controles implementados / controles definidos) x100	>80%	Semestral	Gestión TIC	Jun-Dic	Plan de implementación del MSPI
3	% de avance en la formulación y ejecución del PESI	Definir el PESI	(Actividades ejecutadas / actividades programdas) x100	>95%	Semestral	Gestion TIC	Jun-Dic	Plan Estratégico de Seguridad de la información (PESI)
4	% de riesgos identificados y tratados	Evaluar el avance en la gestión y tratamiento de riesgos de seguridad de la inofrmación	(Riesgos con tratamiento / Total riesgos identificados) x100	>80%	Semestral	Gestión TIC	Jun- Dic	Seguimiento Riesgos SGSI
5	% de acciones de mejora implementadas	Actualizar y mejorar el SGSI	(Acciones implementadas / Acciones identificadas) x100	>80%	Semestral	Gestión TIC	Jun-Dic	Informe de mejoramiento

Fuente: elaboración propia

- En primer lugar, se evaluará el porcentaje de riesgos identificados sobre los activos de información, calculado como la relación entre los riesgos identificados y el total de activos de información, con una meta anual igual o superior al 95%, utilizando como fuente el inventario de activos y el mapa de riesgos.

- En segundo lugar, se medirá el porcentaje de riesgos con tratamiento definido, determinado a partir de la relación entre los riesgos que cuentan con planes de tratamiento y el total de riesgos identificados, con una meta semestral igual o superior al 90%, tomando como insumo el Plan de Tratamiento de Riesgos del MSPI.

- Finalmente, se evaluará el nivel de implementación de los controles de seguridad, mediante la relación entre los controles implementados y los controles definidos, con una meta semestral igual o superior al 85%, apoyado en los informes de seguimiento del MSPI.

Estos indicadores serán gestionados por el proceso de Gestión TIC y se integrarán en los informes periódicos dirigidos a la Alta Dirección, incluyendo aquellos asociados al diligenciamiento del instrumento MSPI y el FURAG, con énfasis en el seguimiento a la Política de Gobierno Digital y sus componentes de seguridad digital. De igual manera, la entidad continuará adelantando auditorías internas al proceso de Gestión TIC, cuyos resultados se consolidan en el respectivo Plan de Mejoramiento Institucional, permitiendo la identificación, seguimiento y cierre de brechas.

En cumplimiento de los principios de transparencia y control, tanto los informes de auditoría como el Plan de Mejoramiento serán publicados y actualizados periódicamente en el portal institucional, garantizando la visibilidad de los avances y el compromiso de la RAP-E con la mejora continua, la madurez del MSPI y el fortalecimiento del Gobierno de TI y la ciberseguridad.

Tabla 5. Fase de evaluación y desempeño

FASE DE EVALUACIÓN DE DESEMPEÑO		
Metas	**Resultados**	**Instrumento**
Herramienta - MSPI	Se actualiza anualmente y recopilan las evidencias del instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información (MSPI). Esto incluye la recopilación de datos sobre la efectividad de los controles según ISO 27001:2013, con las evidencias documentales de procedimientos y enlaces de referencia. La evaluación con la herramienta MSPI está disponible en los repositorios SharePoint Gestión TIC.	Herramienta - MSPI
Plan de Ejecución de Auditorias	La Entidad tiene un plan anual de auditoría que evalúa la eficacia y eficiencia del Sistema de Control Interno mediante auditorías y seguimientos independientes, con el objetivo de agregar valor y mejorar los procesos.	Plan Anual de Auditoria
FURAG	Se actualiza anualmente y mide el desempeño de las entidades públicas a través de indicadores asociados al Modelo Integrado de Planeación y Gestión (MIPG), el cual busca fortalecer la eficiencia, transparencia y efectividad en la gestión pública.	FURAG

Fuente: elaboración propia

Fase 5: Mejora Continua.

Es prioritario que la RAP-E defina y desarrolle un plan de mejora continua, orientado principalmente a proponer acciones que permitan corregir, optimizar los procesos y los controles existentes, y elevar el nivel de madurez del Sistema de Gestión de Seguridad de la Información (SGSI). El resultado del trabajo debe exponer de manera explícita, pormenorizada y detallada las acciones necesarias para promover la mejora continua, de forma que el plan prevea de igual forma el seguimiento del

impacto de estas propuestas de mejora continua garantizando la alineación del MSPI con los objetivos estratégicos y los requisitos normativos. En última instancia, el objetivo del plan es garantizar la gestión continua de la seguridad de la información y la privacidad, adaptándola a la inercia de la tecnología, el apercibimiento normativo, y el panorama de las nuevas amenazas que van surgiendo.

Tabla 6. Fase mejora continua SGSI

FASE DE MEJORA CONTINUA		
Metas	**Resultados**	**Instrumento**
Planes de Mejoramiento	Plan de Mejoramiento Interno	Plan anual de auditorías

Fuente: elaboración propia

6. Control de Cambios

VERSIÓN	FECHA	DESCRIPCIÓN	LIDER DEL PROCESO
1	Enero/2025	Versión inicial	Leydi Támara
2	Mayo/2026	Ajuste de forma	Leydi Támara
3	Septiembre/2026	Ajuste del cronograma	Leydi Támara