

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (PESI) 2024-2027



Tabla de Contenido

1. OBJETIVO	3
1.1. Objetivos específicos	3
2. ALCANCE	4
3. MARCO NORMATIVO	4
4. DEFINICIONES	6
5. ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GOBERNACION DE CALDAS	8
5.1. Instrumento de Evaluación del MSPI	8
5.2. Resultados medición IDI a través del FURAG	10
6. ESTRATEGIA DE SEGURIDAD DIGITAL	11
6.1. Descripción de las Estrategias Específicas (Ejes)	13
7. PORTAFOLIO DE PROYECTOS / ACTIVIDADES	14
8. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:	17
9. RESPONSABLES	18
10. APROBACIÓN	18

1. OBJETIVO

Definir un Plan Estratégico de Seguridad de la Información, fortaleciendo la integridad, confidencialidad y disponibilidad de los activos de información de la Gobernación de Caldas, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de controles, programas de concientización en el buen uso de los datos y la mejora continua del modelo, definidas en este documento para las vigencias 2024 - 2027.

1.1. Objetivos específicos

- Definir y establecer una estrategia de seguridad de la información en la entidad.
- Identificar las necesidades y definir los requerimientos en la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Implementar las políticas y controles de seguridad de la información y privacidad de la información alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI) para alcanzar un nivel de madurez aceptable, objetivo de la Entidad.
- Planificar la evaluación y seguimiento de los controles definidos en la matriz de evaluación del modelo de seguridad y privacidad de la información de la entidad.
- Definir acciones que permitan gestionar los incidentes de seguridad y ciberseguridad de la Entidad.
- Identificar los activos de información de los procesos estratégicos de la Entidad

- Ejecutar el plan de tratamiento de riesgos de seguridad a los activos de información valorados.
- Ejecutar el plan de concientización de seguridad y privacidad de la información y generar una cultura de uso seguro de la misma, en funcionarios, contratistas y practicantes de la Entidad.

2. ALCANCE

El alcance del Plan Estratégico de Seguridad y Privacidad de la Información 2024-2027, busca la implementación del Sistema de Gestión de Seguridad de la Información aprobado en la entidad y la Política General de Seguridad, la cual aplica a la protección de los activos de información y deben ser cumplidos por los servidores públicos, practicantes, contratistas y proveedores que gestionan la información que soporta los procesos estratégicos, misionales y de evaluación de la entidad.

3. MARCO NORMATIVO

La Gobernación de Caldas, como entidad de orden territorial, pública y de carácter gubernamental, se encuentra enmarcada en todos los lineamientos correspondientes a entidades de tales características. El marco normativo puede ser consultado en el numeral 3 del documento MinTIC *MAE.G.GEN.01 - Documento Maestro del Modelo de Arquitectura Empresarial*. La Gobernación de Caldas considera adicionalmente para el desarrollo de su Plan Estratégico en Seguridad de la Información la siguiente normatividad:

Título de la norma o documento	Descripción
Ordenanza 974 de mayo de 2024	Plan de Desarrollo Departamental de Caldas 2024 - 2027
Ley 274 de 2023 del Senado. Ley 338 de 2023 de la Cámara.	Plan Nacional de Desarrollo 2022-2026. "Colombia potencia mundial de la vida".
Decreto 695 de 2023 de la Gobernación de Caldas	Por medio del cual se actualiza el Sistema de Gestión de Seguridad de la Información de la Gobernación de Caldas
Decreto 338 de 2022 del MinTIC	Por el cual se adiciona el Título 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital.
Decreto 767 de 2022 del MinTIC	Por el 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 las Comunicaciones.
NTC-ISO 27001:2022	Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información.
Resolución 500 de 2021 del MinTIC	Documento donde se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
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, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
Decreto 1008 de 2018 del MinTIC	Por el 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 las Comunicaciones.

Título de la norma o documento	Descripción
CONPES 3854 de 2016	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015 del MinTIC	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
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.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012 la cual constituye el marco general de la protección de los datos personales en Colombia.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales, reconociendo y protegiendo el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos
CONPES 3650 de 2010	Importancia Estratégica de la Estrategia de Gobierno en Línea.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Tabla 1 - Marco Normativo

4. DEFINICIONES

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
- **PESI:** Plan estratégico de Seguridad y Privacidad de la Información.

- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000:2013).
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].
- **Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos. [Fuente: ISO Guide 73:2009].
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006].
- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006].
- **Política:** Conjunto de orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado.
- **Política de Seguridad de la Información:** Conjunto de Directrices que permiten resguardar los activos de información.
- **Procedimiento:** Define los pasos para realizar una actividad específica. Evita que se aplique el criterio personal.
- **Riesgo:** Un efecto es una desviación de lo esperado: positivo o negativo Seguridad de la Información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua. El SGSI se implementa en la Entidad a través del MSPI establecido por el MinTIC.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información

5. ESTADO ACTUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GOBERNACION DE CALDAS

5.1. Instrumento de Evaluación del MSPI

La Gobernación de Caldas, ha realizado ejercicios de medición y diagnóstico, haciendo uso del "Instrumento de Evaluación MSPI" del MinTIC que permite identificar el nivel de madurez en la implementación del MSPI en la Gobernación de Caldas. Actualmente el estado de gestión y adopción de controles técnicos y administrativos al interior de la Entidad tiene un nivel de madurez "Repetible". A continuación, se presenta los resultados de la evaluación realizada en mayo de 2024, siguiendo los lineamientos del MSPI del Ministerio de Tecnologías de la información y las Comunicaciones.

Evaluación de Controles - ISO 27001:2013 Anexo A

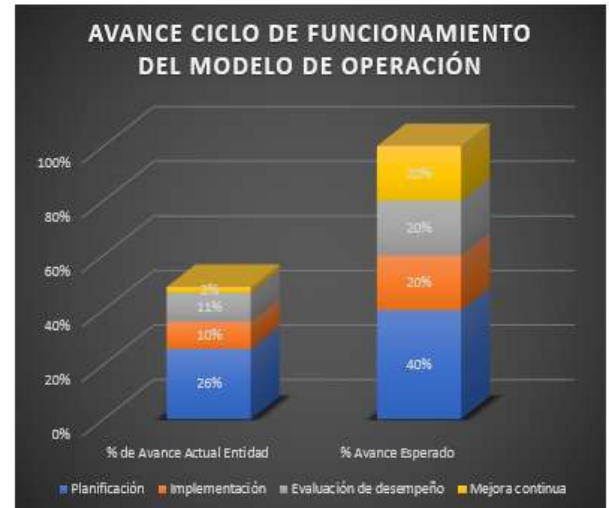
No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL 12/31/2024
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	80	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	43	80	EFFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	43	80	EFFECTIVO
A.8	GESTIÓN DE ACTIVOS	23	80	REPETIBLE
A.9	CONTROL DE ACCESO	60	80	EFFECTIVO
A.10	CRİPTOGRAFÍA	60	60	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	43	80	EFFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	44	80	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	28	60	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	4	60	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	50	80	EFFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	29	80	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	50	REPETIBLE
A.18	CUMPLIMIENTO	17,5	60	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		39	72,142857	REPETIBLE

Nivel	Descripción
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.



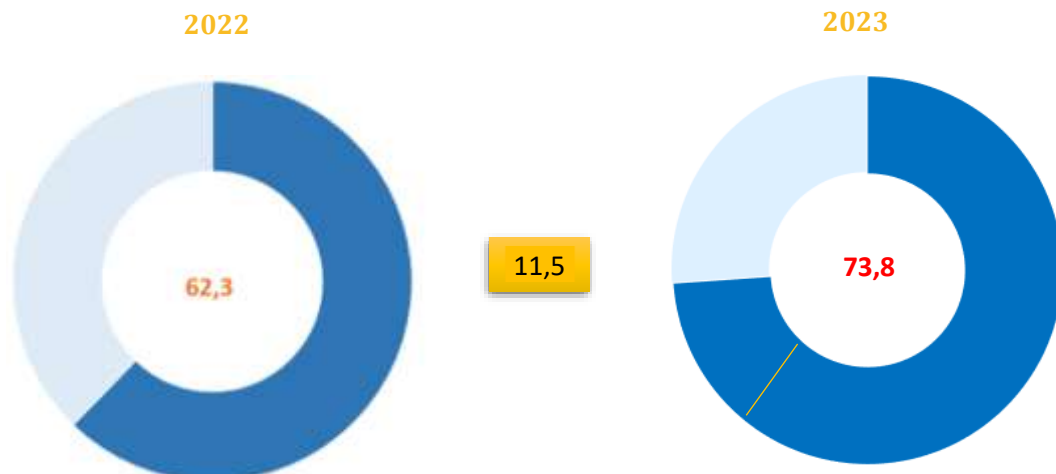
Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	26%	40%
2024	Implementación	10%	20%
2025	Evaluación de desempeño	11%	20%
2026	Mejora continua	2%	20%
TOTAL		48%	100%



5.2. Resultados medición IDI a través del FURAG

La Gobernación de Caldas ha incrementado en 11,5 puntos en la implementación de la Política de Seguridad Digital, tomando como línea base la calificación del IDI a través del FURAG de la vigencia 2022:



Detalle	2022	2023	Diferencia
Asignación de recursos	46,88	39,6	-7,28
Implementación de lineamientos de políticas	64,67	84,4	19,73
Despliegue de controles	75	96,4	19,4

El incremento corresponde a:

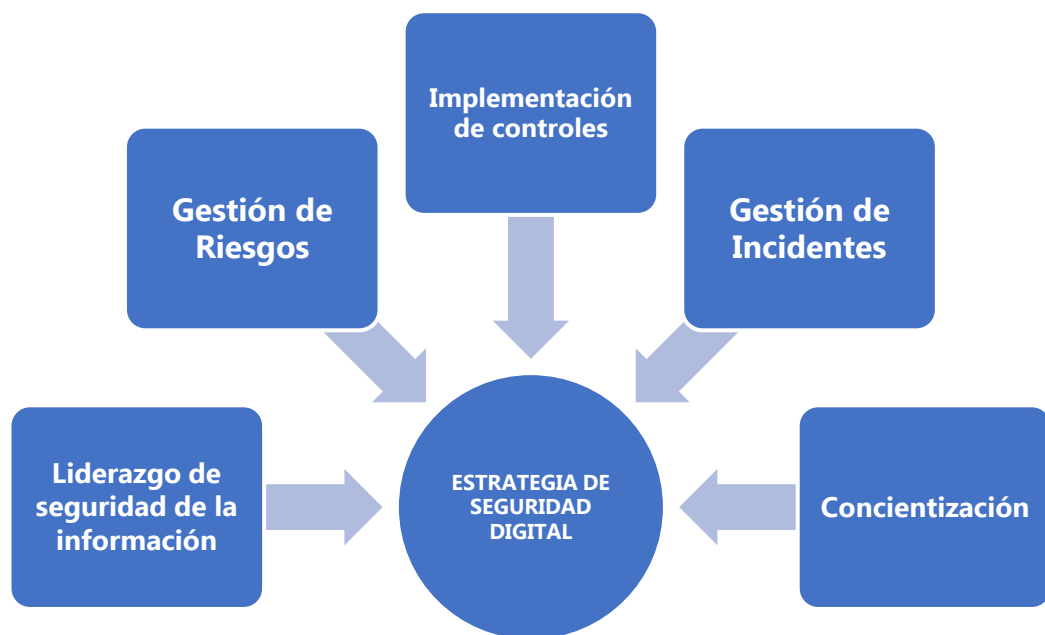
- El esfuerzo administrativo en la creación del procedimiento de Seguridad y Privacidad de la información y los 8 manuales que lo componen.
- La mitigación de ataques cibernéticos a través de la administración del sistema FORTINET.
- La actualización del Sistema de Gestión de Seguridad y Privacidad de la Información.
- La actualización e implementación del Manual de Políticas de Seguridad y Privacidad de la Información.
- Licenciamiento de sistemas operativos, antivirus, sistemas de información y aplicaciones.
- Gestión de vulnerabilidades, actualización de equipos y parches de seguridad a equipos de escritorio, portátiles, servidores, firewall y AccesPoint.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

La Gobernación de Caldas establecerá una estrategia de seguridad digital para el periodo 2024-2027, en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la

Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse, esto acorde a la resolución 500 de 2021 expedida por el MinTIC.

Por tal motivo, **La Gobernación de Caldas** define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



6.1. Descripción de las Estrategias Específicas (Ejes)

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Verificar y Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) en la Gobernación de Caldas abordando temáticas específicas, como complemento a lo definido en la “Política General de Seguridad de la Información de la Entidad” y el “Manual de políticas de seguridad y privacidad de la información” y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Gobernación de Caldas, a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Gestionar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad en el plan de tratamiento de riesgos.
Concientización	Fomentar una cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la entidad.

7. PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para cada estrategia específica, **La Gobernación de Caldas** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	PROYECTO 1: Promover la aplicación de las políticas de seguridad y privacidad de la información.	Políticas de seguridad y privacidad de la información establecidas en los procesos de la entidad.
	PROYECTO 2: Construcción, aprobación y ejecución del PESI 2024 - 2027	Documentos PESI aprobado y en ejecución
	PROYECTO 3: Construcción, aprobación y ejecución PETI 2024-2027	Documento PETI aprobado
	PROYECTO 4: Identificación y gestión de indicadores de seguridad de la información	Informe de Evaluación de Indicadores
	PROYECTO 5: Elaboración e implementación del plan de mantenimiento de servicios tecnológicos.	Plan de mantenimiento de servicios tecnológicos
Gestión de riesgos	PROYECTO 1: Actualizar los riesgos asociados a los activos de información identificados, valorarlos y clasificarlos.	Matriz de riesgos de seguridad de la información actualizada
	PROYECTO 2: Actualizar en cada vigencia el plan de tratamiento de riesgos de seguridad y realizar seguimiento.	Plan de tratamiento de riesgos actualizado en cada vigencia.

Concientización	<p>PROYECTO 1: Elaborar un plan de sensibilización en seguridad de la información para cada vigencia.</p> <p>PROYECTO 2: Realizar jornadas de sensibilización a todo el personal por medio de los diferentes canales de comunicación.</p> <p>PROYECTO 3: Involucrar a funcionarios o contratistas en convocatorias, talleres o capacitaciones en seguridad de la información.</p>	<p>Plan de Sensibilización para cada vigencia.</p> <p>Evidencias de las actividades desarrolladas</p> <p>Certificados o constancias de las capacitaciones</p>
Implementación de controles	<p>CONTROL 1 Identificar las necesidades para realizar los respaldos o copias de información.</p> <p>CONTROL 2 Definir controles de seguridad acceso lógico y físico, monitoreo gestión de incidentes por medio de la plataforma de ciberseguridad Fortinet en la Gobernación de Caldas.</p> <p>CONTROL 3 Seguimiento al buzón de correo electrónico en la entidad.</p> <p>CONTROL 4 Asistencia técnica, mantenimiento y soporte de equipos e instalación de aplicaciones básicas.</p>	<p>Asignación recurso compartido para los respaldos de información.</p> <p>Lineamientos de servicios de seguridad informática para reducir los riesgos en la infraestructura tecnológica de la Gobernación de Caldas</p> <p>Plataforma de administración de correo electrónico 365 y Gmail.</p> <p>Verificación de condiciones óptimas y rendimiento de los equipos de la entidad.</p> <p>Políticas de Desarrollo Seguro WAF desplegado y funcional Fortinac.</p>

Gestión de incidentes	PROYECTO 1: Solución especializada – Mesa de ayuda Soportes Nivel I, Nivel II, Nivel III, para solución de inconvenientes en la infraestructura tecnológica de la Gobernación de Caldas.	Solución de incidentes reportados en la mesa de ayuda menor a 3 días.
	PROYECTO 2: Capacitar al personal de la Unidad de sistemas de la Gobernación de Caldas, en la solución de incidentes de seguridad de la información.	Manual operativo gestión de incidentes con su respectivo procedimiento formalizado en la Gobernación de Caldas.
	PROYECTO 3: Implementación de plan de gestión de incidentes en la entidad.	Plan de gestión de incidentes aprobado e implementado

8. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Actividad	Año 2024	Año 2025				Año 2026				Año 2027			
	Cuatre 3	Trim 1	Trim 2	Trim 3	Trim 4	Trim 1	Trim 2	Trim 3	Trim 4	Trim 1	Trim 2	Trim 3	Trim 4
Promover la aplicación de las políticas de seguridad y privacidad de la información	X		X			X			X		X		
Construcción y aprobación PESI 2024 - 2027	X												
Ejecución del PESI 2024 - 2027	X	X	X	X	X	X	X	X	X	X	X	X	X
Construcción y aprobación del PETI 2024-2027	X												
Ejecución PETI 2024-2027	X	X	X	X	X	X	X	X	X	X	X	X	X
Identificación y gestión de indicadores de seguridad de la información	X		X				X				X		
Construcción y aprobación del plan de mantenimiento de servicios tecnológicos		X				X				X			
Actualizar los riesgos asociados a los activos de información identificados, valorarlos y clasificarlos.	X			X				X				X	
Actualizar en cada vigencia el plan de tratamiento de riesgos de seguridad y realizar seguimiento		X				X				X			
Elaborar un plan de sensibilización en seguridad de la información para cada vigencia.		X				X				X			
Involucrar a funcionarios o contratistas en convocatorias, talleres o capacitaciones en seguridad de la información.	X		X				X				X		
Identificar las necesidades para realizar los respaldos o copias de información.	X		X				X			X			
Definir controles de seguridad acceso lógico y físico, monitoreo gestión de incidentes por medio de la plataforma de ciberseguridad Fortinet en la Gobernación de Caldas.	X	X	X	X	X	X	X	X	X	X	X	X	X
Seguimiento al buzón de correo electrónico en la entidad.	X	X	X	X	X	X	X	X	X	X	X	X	X
Asistencia técnica, mantenimiento y soporte de equipos e instalación de aplicaciones básicas	X	X	X	X	X	X	X	X	X	X	X	X	X
Solución especializada – Mesa de ayuda Soportes Nivel I, Nivel II, Nivel III, para solución de inconvenientes en la infraestructura tecnológica de la Gobernación de Caldas.	X	X	X	X	X	X	X	X	X	X	X	X	X
Capacitar al personal de la Unidad de sistemas de la Gobernación de Caldas, en la solución de incidentes de seguridad de la información.	X			X			X				X		
Implementación de plan de gestión de incidentes en la entidad.			X										

9. RESPONSABLES

- Gobernador, en calidad de representante legal y responsable de la implementación del Modelo Integrado de Planeación y Gestión (MIPG).
- Jefe oficina tecnología de información, en calidad de responsable de la implementación de la política de Gobierno digital y coordinador de las actividades de implementación del MSPI.
- Comité de Seguridad de la Información de la Gobernación de Caldas.
- Funcionarios, contratistas y colaboradores en la implementación de políticas, procedimientos, lineamientos y controles del MSPI en la Gobernación de Caldas.
- Equipo de trabajo como apoyo en las actividades y acciones de implementación del MSPI.

10.APROBACIÓN

El presente plan estratégico PESI 2024-2027 se someterá a consideración y conocimiento del comité institucional, con el objetivo de ser aprobado y aplicado en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI) conforme a lo que aquí se define.

Control de cambios de documentos

Versión	Fecha de aprobación			Descripción del cambio	Elaborado por	Aprobado por
	aaaa	mm	dd			
1	2021	01	28	Creación documento	Jefatura Gestión de la Información	Comité Institucional de Gestión y Desempeño
2	2023	01	23	Actualización mapa de ruta.	Unidad de Sistemas	Jefatura Gestión de la Información
3	2024	08	15	Actualización documento periodo 2024-2027	Unidad de Sistemas Ing. Andrés Felipe Martínez García Jefatura Gestión de la Información Ing. Olga Lucía Ordoñez Clavijo	Comité Institucional de Gestión y Desempeño