GOBERNACIÓN DE CALDAS

PLAN ESTRATÉGICO DE SEGURIDAD DE LA DE INFORMACIÓN 2020-2023 v2.0

(PESI)

Manizales

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
1.1 Entidad 3
1.2 Visión 3
1.3 Misión 3
1.4 Definiciones 3
1.5 Normas y modelos aplicables 5
2. OBJETIVO DEL MSPI 5
2.1 Objetivos Específicos del MSPI 5
3. ALCANCE DEL MSPI 5
4. MARCO NORMATIVO 6
5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 6
5.1 Metodología de Implementación 6
5.2 Nivel de Madurez del MSPI 7
5.3 Mapa de Ruta 8

1. INTRODUCCIÓN

1.1 Entidad

La Gobernación de Caldas es una entidad de orden público territorial que desarrolla un papel importante como eje intermedio entre el Gobierno Nacional y el Gobierno Municipal, el departamento posee 27 municipios y 6 subregiones; su sede administrativa está ubicada en la ciudad capital Manizales y el departamento cuenta con 1.018.453 de habitantes, según resultados DANE de 2020.

1.2 Visión

Un Caldas social e incluyente, con mayor innovación social, sociedad civil. un Caldas educado y conectado, que logre con consenso por la productividad y un Caldas sostenible que logre una mejor gestión del medio ambiente.

1.3 Misión

Consolidar un gobierno incluyente, serio y transparente, con un sentido social que brinde oportunidades de desarrollo y crecimiento para los caldenses y que haga del departamento una región foco de prosperidad y confianza.

1.4 Definiciones[1]

- **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).
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000:2013).

[1] Guía para la Implementación de Seguridad de la Información en una MIPYME. 2016. MinTIC.

- **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 especifica. 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.

1.5 Normas y modelos aplicables

- Serie NTC/ISO 27000:2013
- NTC/ISO 31000:2013
- NTC/ISO 22301
- Modelo de Seguridad y Privacidad de la Información MinTIC v.3.0.2
- Guías Seguridad de la Información MinTIC
- Guía para la administración del riesgo y diseño de controles en entidades públicas. 2018.

2. OBJETIVO DEL MSPI

Implementar un el Modelo de Seguridad y Privacidad de la Información (MSPI) en la Gobernación de Caldas para fortalecer la confidencialidad, disponibilidad, integridad y privacidad de la información y los datos de la Entidad a través de la identificación y gestión de riesgos, la implementación de controles, programas de concientización en el buen uso de los datos y la mejora continua del modelo.

2.1 Objetivos Específicos del MSPI

- Identificar los activos de información de los procesos estratégicos de la Entidad.
- Realizar un análisis de riesgos de los activos de información identificado y establecer un plan de tratamiento de los riesgos que generan mayor impacto para la Entidad.
- Generar una cultura de uso seguro de la información en funcionarios y contratistas de la Entidad.
- Implementar las políticas y controles de seguridad de la información y privacidad de la información alineado con el MSPI para alcanzar el nivel de madurez objetivo de la Entidad.
- Implementar el modelo de gestión de incidentes de seguridad y ciberseguridad de la Entidad

3. ALCANCE DEL MSPI

El MSPI tendrá como alcance 2020-2023 los procesos asociados a Administración de Recaudo, Gestión Financiera, Gestión Administrativa y Organizacional y Gestión de la Información.

4. 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
Ley 955 de 2019	Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
Ordenanza 009 de Mayo 1 de 2020	Plan Departamental de Desarrollo 2020-2023 "Unidos es Posible"
Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018	Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad – MSPI de MinTIC
CONPES 3854 de 02014	Política de Seguridad Digital del Estado Colombiano

Tabla 1 - Marco Normativo

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

5.1 Metodología de Implementación

El Modelo de Seguridad y Privacidad de la Información de la Gobernación de Caldas se soporta en la serie ISO 27000:2013 y los lineamientos establecidos por el MinTIC , que incluyen las siguientes fases asociados el ciclo de mejora continua PHVA para su implementación.

Ilustración 1 Metodología de Implementación del PESI

Planeación: En esta fase se establece el patrocinador y equipo del proyecto que implementará el MSPI de la Gobernación, se establece el alcance del MSPI, se documentan las políticas de seguridad y privacidad de la información, se establece el procedimiento de control documental del MSPI, se definen y asigna roles y responsabilidades para la seguridad de la información, se realiza un inventario de los activos de información, se realiza la evaluación de riesgos y se establece un plan para su tratamiento y se establece un plan para la toma de conciencia, educación y formación en seguridad de la información.

Implementación: En esta fase se establece la estrategia de planificación y control operacional con la aprobación de la Alta Dirección, se implementan los controles aprobados, los planes de tratamientos de riesgos y los indicadores de gestión del MSPI.

Evaluación de desempeño: En paralelo con la fase de implementación, se realiza un evaluación del desempeño de los controles, planes de concientización y planes de tratamiento de riesgos con el objetivo de verificar la efectividad y eficacia de los mismos. De forma conjunta se realizan auditorías internas del MSPI con los responsables de Control Interno.

Mejora continua: A partir de la realización de auditorías internas y/o externas sobre el MSPI de la Gobernación de Caldas, se generan planes de seguimiento, evaluación y análisis del MSPI, con la supervisión de Control Interno.

Estado actual de la Gobernación de Caldas

El porcentaje de avance de la Gobernación de Caldas considerando las fases del ciclo PHVA es: Planeación (8%), Implementación (1%), Evaluación de Desempeño (0%) y Mejora Continua (0%).

5.2 Nivel de Madurez del MSPI

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, se estableció que el estado de gestión y adopción de controles técnicos y administrativos al interior de la Entidad tiene un nivel de madurez "Inicial". A continuación se presenta los resultados de la evaluación realizada en julio de 2020 y octubre de 2022:

No.	Evaluación de Efectividad de controles					
	DOMINIO	Calificación 30/07/2020	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 30/07/2020	Calificación Actual 13/10/2022	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 13/10/2022
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	REPETIBLE	30	60	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	38	REPETIBLE	38	60	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	21	REPETIBLE	33	60	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	10	INICIAL	10	60	INICIAL
A.9	CONTROL DE ACCESO	23	REPETIBLE	25	60	REPETIBLE
A.10	CRIPTOGRAFÍA	0	INEXISTENTE	0	60	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	36	REPETIBLE	36	60	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	41	EFECTIVO	41	60	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	28	REPETIBLE	43	60	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	INEXISTENTE	7	30	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	0	INEXISTENTE	40	60	REPETIBLE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	INEXISTENTE	20	60	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	REPETIBLE	27	50	REPETIBLE
A.18	CUMPLIMIENTO	12,5	INICIAL	12,5	60	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		19	INICIAL	26	57,1428571	REPETIBLE

Ilustración 2 Evaluación del Nivel de Madurez del MSPI año 2023

En julio de 2020 se realizó una evaluación del nivel de madurez de la Entidad y se pudo establecer que se encontraba en un **nivel de madurez Inicial**, en este nivel se encuentran las entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información. En octubre de 2022 se realizó una nueva evaluación y se encontró que la Gobernación de Caldas se encuentra en un **nivel de madurez 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 encuentran gestionado dentro del componente planificación del MSPI.

5.3 Mapa de Ruta

A continuación se presenta el alcance del programa de seguridad y privacidad de la información para mejor el nivel de madurez del MSPI de la Gobernación de Caldas y pasar de un nivel "Repetible" a "Definido" en armonía con los lineamientos MinTIC, el Plan Estratégico en TIC y el Plan de Desarrollo de la Gobernación 2020-2023.

Actividad	Avance*	2020	2021				2022				2023			
		Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Definición de indicadores de gestión del MSPI	100%	■												
Documentación de políticas de seguridad y privacidad de la información	30%	■	■	■	■	■					■	■	■	■
Definición de Indicadores de Gestión para la Seguridad de la Información	100%			■										
Definición de Plan Operacional de Seguridad y Privacidad de la Información	100%			■										
Aprobación de Indicadores de Gestión y Plan Operacional de Seguridad de la Información	100%				■									
Definición o actualización de roles y responsabilidades	100%	■									■			
Definición o actualización de inventario de activos de información y datos personales bajo el alcance del MSPI	100%					■				■				■
Adopción, adaptación o actualización de metodología de evaluación de riesgos	100%	■				■				■			■	
Evaluación, análisis y registro de riesgos	100%	■				■				■				
Definición de plan de tratamiento de riesgos de información y privacidad	100%		■				■				■			
Implementación de controles	26%			■	■	■		■	■	■		■	■	■
Evaluación de efectividad y eficacia de controles	50%					■				■				■
Definición de plan de concientización, educación y formación en seguridad y privacidad de la información	50%	■			■				■				■	
Implementación y evaluación de plan de concientización en seguridad y privacidad de la información	50%	■				■	■	■		■	■	■		■
Medición de indicadores de gestión del MSPI	60%			■	■	■	■	■	■	■	■	■	■	■
Evaluación de indicadores de gestión del MSPI	60%				■				■				■	
Presentación de resultados comité institucional de Gestión y Desempeño	100%				■				■				■	

* Porcentaje de avance para el periodo 2020-Q3 a 2022-Q4.