Dirección TIC

GOBERNACIÓN de BOLÍVAR

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GOBERNACIÓN DEL DEPARTAMENTO DE BOLÍVAR

2024 - 2027

Vía Cartagena - Turbaco, Km 3 Sector Bajo Miranda, El Cortijo
Teléfono: 60 - 5 - 6517444 Ext: 1010 - 1007 - 1006 - 2103
E-mail: contactenos@bolivar.gov.co
www.bolivar.gov.co

Control de Versiones

Versión	Fecha	Modificación
1.0	28/12/2018	• Versión inicial del documento
2.0	26/12/2019	• Cambio en la definición de la aplicabilidad y finalidad. • Se agregaron términos y definiciones. • Se incluyen tablas de referencias. • Se agregaron términos y definiciones. • Se agregó un objetivo general. • Se modificó el alcance, antes nombrado aplicabilidad. • Se sustituyó nivel de cumplimiento por los principios de seguridad y privacidad de la información. • Se definieron roles y responsabilidades.
3.0	30/11/2020	• Se cambió nombre del documento por “Plan de seguridad y privacidad de la Información”. • Se ajustaron los roles y responsabilidades de seguridad y privacidad de la información. • Se incluyeron las actividades a realizar.
4.0	06/12/2022	• Se agregaron responsables y fechas de ejecución a las actividades del plan.
5.0	26/01/2024	• Se actualiza utilizando lineamientos de la plantilla propuesto por el Ministerio de las TICs

Tabla de contenido

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para mitigar los riesgos digitales a los que está expuesta la Gobernación del Departamento de Bolívar hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en la Resolución 261 de 2023 por medio de la cual "*se conforma el Comité de Seguridad de la Información, define sus Funciones y adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar*" para las vigencias 2024-2027.

1.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer las acciones de la estrategia de seguridad digital de la Gobernación del Departamento de Bolívar.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información según lineamientos de la Resolución 500 de 2021 "*Por la cual 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*".
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.
- Generar una cultura de seguridad y privacidad de la información en los funcionarios, contratistas y ciudadanos.

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que "*Esta política aplica a todos los funcionarios, contratistas y grupos de interés que para el cumplimiento de sus funciones y obligaciones contractuales recolecta, utilizan y almacenan información para la ejecución de los procesos enmarcados en el mapa de procesos de la entidad.*"

3. DOCUMENTOS DE REFERENCIA

El Plan de Seguridad y Privacidad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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.
- Resolución 500 de 2021. "*Por la cual 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*".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- CONPES No. 3701 del 2011 "Lineamientos de Políticas para la Ciberseguridad y Ciberdefensa"
- CONPES No. 3854 de 2016 "Política Nacional de Seguridad Digital"
- CONPES No. 3995 de 2020 "Política Nacional de Confianza y Seguridad Digital"
- Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital..." del Ministerio de las Tecnologías de la información y las Comunicaciones.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas v5
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"
- Decreto No. 222 de 2022 "Por medio del cual se actualiza el Modelo Integral de Planeación y Gestión -MIPG en la Gobernación de Bolívar, establecido en el Decreto No. 169 de 2018 y Decreto 489 de 2018"
- Decreto No. 531 de 2018 "Por el cual se adopta el Manual de Políticas y Procedimientos de Protección de Datos de la Gobernación de Bolívar y se dictan otras disposiciones"
- Resolución 261 de 2023 por medio de la cual "*se conforma el Comité de Seguridad de la Información, define sus Funciones y adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar*"

4.TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información:

Activo: 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) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2015b)

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema u organización. (International Organization for Standardization, 2016)

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y para determinar su nivel. El análisis de riesgos proporciona la base para la evaluación del riesgo y las decisiones sobre el tratamiento del riesgo. El análisis de riesgo incluye estimación de riesgo. (International Organization for Standardization, 2016)

Ataque: Intento de destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información. (International Organization for Standardization, 2016)

Confidencialidad: Propiedad que la información no esté disponible o sea revelada a personas, entidades o procesos no autorizados. (International Organization for Standardization, 2016)

Control: Mecanismo que modifica el valor de un riesgo. Los controles incluyen cualquier proceso, política, dispositivo, práctica u otras acciones que modifiquen el riesgo. Los controles no siempre ejercen el efecto modificador previsto o asumido. (International Organization for Standardization, 2016)

Detectar: Descubrir la existencia de algo que no era patente. (Real Academia Española, 2019a)

Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada. (International Organization for Standardization, 2016)

Evaluación del riesgo: Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si es aceptable o tolerable la magnitud del riesgo. La evaluación del riesgo ayuda a la decisión sobre el tratamiento del riesgo. (International Organization for Standardization, 2016) 2016)

Evento de seguridad de la información: Acontecimiento identificado en el estado de un sistema, servicio o red que indica una posible violación a la política de seguridad de la información o fallo de los controles o una situación previamente desconocida que puede ser relevante para la seguridad. (International Organization for Standardization, 2016)

Gestión de incidentes de seguridad de la información: Proceso para detectar, informar, evaluar, responder ante los incidentes de seguridad, mitigarlos y aprender de ellos. (International Organization for Standardization, 2016)

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos. (International Organization for Standardization, 2016)

Identificar: Reconocer si una persona o cosa es la misma que se supone o se busca. (Real Academia Española, 2019b)

Identificación del riesgo: Proceso de encontrar, reconocer y describir los riesgos. La identificación del riesgo implica la identificación de fuentes de riesgo, eventos, sus causas y sus potenciales consecuencias. La identificación de riesgos puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos y necesidades de los interesados. (International Organization for Standardization,

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información no deseados o inesperados que tienen una significativa probabilidad de comprometer de manera negativa las operaciones de la empresa y amenazar la seguridad de la información. (International Organization for Standardization, 2016)

Integridad: Propiedad de la exactitud y completitud de la información. (International Organization for Standardization, 2016)

MSPI: Modelo Seguridad y Privacidad de la Información.

Monitoreo: Determinación del estado de un sistema, proceso o una actividad. (International Organization for Standardization, 2016)

Política: Intenciones y directrices de una organización expresada formalmente por su alta dirección. (International Organization for Standardization, 2016)

Proceso de gestión del riesgo: Aplicación sistemática de políticas de gestión, procedimientos y prácticas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de los riesgos. (International Organization for Standardization, 2016)

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado positiva o negativamente. La incertidumbre es el estado total o parcial de la insuficiencia de la información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad. (...). En el contexto de la seguridad de la información, los sistemas de gestión, los riesgos de la seguridad de la información pueden expresarse como efecto de la incertidumbre en los objetivos de la seguridad de la información. El riesgo de seguridad de la información se asocia 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 daño a una organización. (International Organization for Standardization, 2016)

Riesgo residual: Riesgo restante después de realizado tratamiento. (International Organization for Standardization, 2016)

Seguridad de la información: Preservación de la confidencialidad, disponibilidad e integridad de la información. (International Organization for Standardization, 2016)

Tratamiento de riesgo: Proceso para modificar el valor del riesgo. El tratamiento del riesgo puede incluir lo siguiente:

- Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo.
- Tomar o aumentar el riesgo para poder aprovechar una oportunidad.
- Eliminación de la fuente de riesgo.
- Cambiar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo con otra parte o partes.
- Asumir el riesgo mediante una elección informada.

Los tratamientos de riesgo que se ocupan de las consecuencias negativas se denominan a veces "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo". El tratamiento de riesgos puede crear nuevos riesgos o modificar los riesgos existentes. (International Organization for Standardization, 2016)

Valoración de riesgo: Es el proceso global de la identificación del riesgo, el análisis de riesgo y la evaluación del riesgo. (International Organization for Standardization, 2016)

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (International Organization for Standardization, 2016)

5.ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Documento Conpes 3995 o Política Nacional de Confianza y Seguridad Digital tiene como objetivo general "*Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías*"

Con base en los lineamientos impartidos por el Ministerio de las tecnologías de la Información y las Comunicaciones en el año 2020 la Gobernación de Bolívar publicó el Plan de Seguridad y Privacidad de la Información 2020-2023, enmarcado en el ciclo Deming consta de 5 fases Diagnóstico, Planificación, Implementación, Evaluación de Desempeño y Mejora Continua.

En el año 2020 se establece:

- La versión inicial de la Política de Seguridad de la Información.

En el año 2021, el Comité Institucional de Gestión y Desempeño aprobó:

- La Política de Tratamiento de Datos personales.
- El Procedimiento para la Gestión de Incidentes de Seguridad Informática.
- El Procedimiento para la Gestión de Incidentes de Datos Personales.
- El Diagnóstico para determinar el estado actual y nivel de madurez de seguridad y privacidad de la información.

Lo que resultó en un nivel de madurez **Repetible**.

Diagnóstico

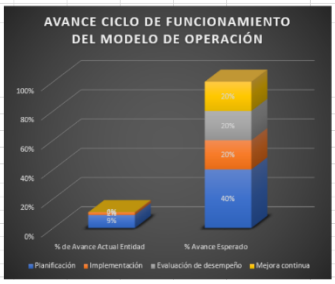
El futuro digital es de todos — Gobierno de Colombia MinTIC	**INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD HOJA PORTADA**
ENTIDAD EVALUADA	Gobernación de Bolívar
FECHAS DE EVALUACIÓN	12/05/2021
CONTACTO	Tairo Mendoza, Profesional Especializado, Tel: 3145337785, E-Mail: tmendoza@bolivar.gov.co
ELABORADO POR	Tairo Mendoza

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

No.	Evaluación de Efectividad de controles — DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	46	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	37	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	47	100	EFECTIVO
A.9	CONTROL DE ACCESO	43	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	38	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	43	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	30	100	REPETIBLE
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	24	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	34	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	42,5	100	EFECTIVO
	PROMEDIO EVALUACIÓN DE CONTROLES	37	100	REPETIBLE

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA — COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	9%	40%
	Implementación	2%	20%
	Evaluación de desempeño	0%	20%
	Mejora continua	0%	20%
TOTAL		**11%**	**100%**



NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	CRITICO
Repetible	CRÍTICO
Definido	CRÍTICO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la 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.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Luego en el año 2022 se aprobaron por parte del Comité Institucional de Gestión y Desempeño:

- Las Políticas (Controles) de Seguridad de la Información

Y se realizó:

- La implementación del protocolo IPv6.

Con base en esta información se desarrolló una estrategia que intenta alcanzar el nivel de madurez **Definido**.

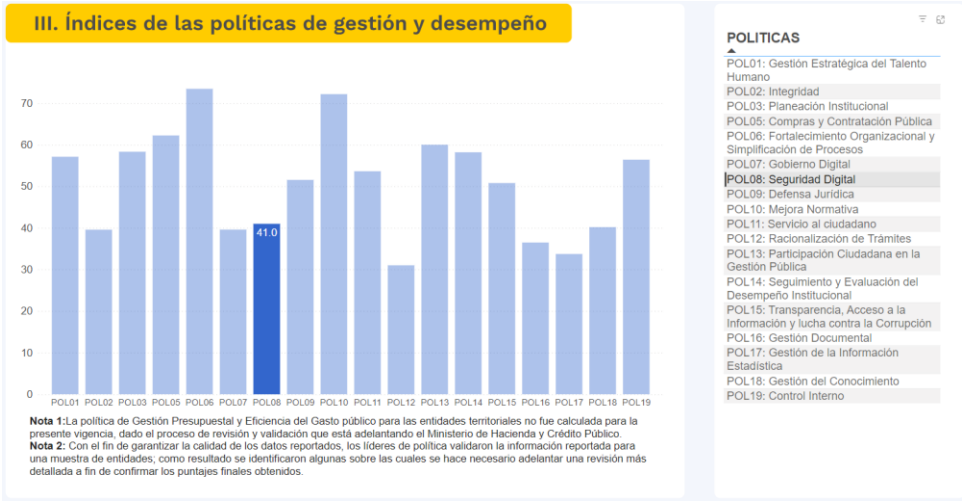
En el año 2023 se impulsó y aprobó:

- La Actualización del Plan de Seguridad y Privacidad de la Información
- La Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- La Actualización de la Política de Tratamiento de Datos Personales
- El Programa integral de Gestión de Datos Personales
- Acuerdo de Confidencialidad
- Aviso de Privacidad
- Instructivo Inventario de Activos de TI Gobernación de Bolívar
- Instructivo Metodología de Riesgos de Seguridad Digital
- La resolución 261 de 2023 por medio de la cual "*se conforma el Comité de Seguridad de la Información, define sus Funciones y adopta la Estrategia de Seguridad Digital de la Gobernación de Bolívar*", en dicha resolución se conforma el Comité de Seguridad de la Información, se establecen sus objetivos, funciones, se adopta la Estrategia de Seguridad Digital, se establece el Sistema de Gestión de Seguridad de la Información basado en el Modelo de Seguridad y Privacidad de la Información y se establecen responsabilidades.

En el Plan de Seguridad y Privacidad de la Información se encuentra explicita la Actividad del Plan de Tratamiento de Riesgos de Seguridad de la Información, sin embargo, este es un proceso en sí mismo, por lo cual es necesario establecerlo como un proceso paralelo.

También en el 2023, se implementó por primera vez el 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información donde intervinieron todas las dependencias, las conclusiones se encuentran en el documento final del proceso.

Calificación de FURAG del año 2022



Como un capítulo especial, el Programa integral de protección de datos personales junto con el Procedimiento de Gestión de Incidentes de Datos Personales permitió que la Superintendencia de Industria y Comercio expidiera un acta de conformidad para la gestión de incidentes de seguridad donde se comprometieron datos personales.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

La Gobernación del Departamento de Bolívar establece una estrategia de seguridad digital 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.

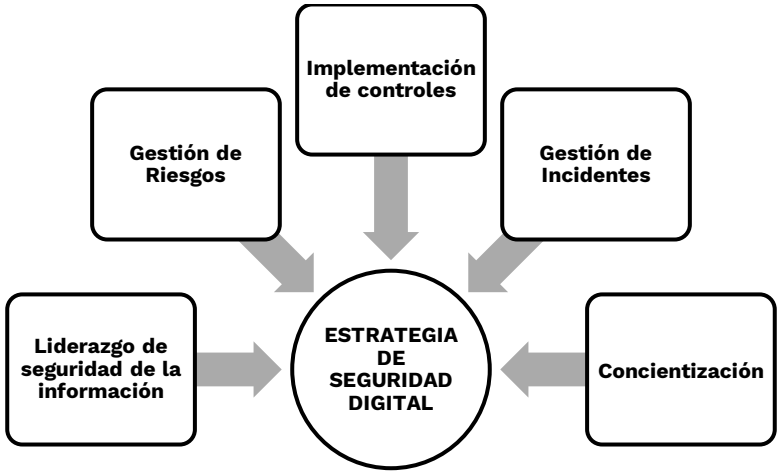
Fases de la Implementación del Modelo de Seguridad y Privacidad de la Información

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

Teniendo en cuenta que las condiciones para llegar al nivel de madurez **Definido** del MSPI son:

- *La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.*
- *La Entidad ha determinado los objetivos, alcance y límites de seguridad de la información.*
- *La Entidad ha establecido formalmente políticas de seguridad de la información y estas han sido divulgadas.*
- *La Entidad tiene procedimientos formales de seguridad de la información.*
- *La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.*
- *La Entidad ha realizado un inventario de activos de información aplicando una metodología.*
- *La Entidad trata riesgos de seguridad de la información a través de una metodología.*
- *Se implementa el plan de tratamiento de riesgos.*
- *La Entidad cuenta con un plan de transición de IPv4 a IPv6.*

Por tal motivo, ***la Gobernación del Departamento de Bolívar*** 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)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general 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 Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar 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 para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la 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.

6.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, la Gobernación del Departamento de Bolívar 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: **Diagnóstico** Determinar el estado actual de la gestión de seguridad de la información y el nivel de madurez del Sistema de Gestión de Seguridad PROYECTO 2: **Planificación** Revisar: • Alcance • Objetivos • Roles y Responsabilidades • Política de Seguridad y Privacidad de la Información • Documento con la Declaración de Aplicabilidad • Políticas de Seguridad y Privacidad de la Información • Procedimientos, Instructivos y Formatos • Metodología para Identificación, Clasificación y Valoración de Activos de Información • Metodología de Identificación, Valoración y Tratamiento de Riesgo. • Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información • Programa Integral de Gestión de Datos Personales • Procedimiento de Gestión de Incidentes	1. • Documento del Diagnóstico 2. • Documento Plan de Seguridad y Privacidad de la Información • Documento Política de Seguridad de la Información • Documento Políticas de Seguridad y Privacidad de la Información • Documentos Procedimientos, Instructivos y Formatos • Documento Metodología para Identificación, Clasificación y Valoración de Activos de Información • Documento Metodología de Identificación, Valoración y Tratamiento de Riesgo. • Documento con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información • Documento Programa Integral de Gestión de Datos Personales • Documento Procedimiento de Gestión de Incidentes de Seguridad y Datos Personales • Documentos de Implementación de la transición IPv6 • Resolución 261 revisada • Documento con el Plan de Comunicación, Sensibilización y Capacitación 3. • Acta del Comité de Seguridad de la Información • Acta del Comité Institucional de Gestión y Desempeño 4. • Evaluación de los indicadores de gestión de seguridad y privacidad de la información definidos en la Resolución 261 de 2023 5. • Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	de Seguridad y Datos Personales • Documentos de Implementación del transición IPv6 • Resolución 261 del 2023 • Plan de Comunicaciones PROYECTO 3: **Aprobación** • Aprobación de documentos por parte del Comité de Seguridad de la Información • Aprobación de documentos por parte del Comité Institucional de Gestión y Desempeño PROYECTO 4: **Evaluación de Desempeño** • Indicadores de gestión PROYECTO 5: **Mejora Continua** • Plan de mejora continua	• Documento con el plan de mejoramiento • Documento de comunicación de resultados del proceso
Gestión de riesgos	PROYECTO 1: **Implementación** • Ejecución del Plan de Tratamiento de Riesgos	• Matriz de Identificación, Valoración y Clasificación de Activos de Información • Matriz de Riesgos de Seguridad Digital • Formato de Registro Nacional de Bases de Datos
Concientización	PROYECTO 1: **Ejecución de capacitaciones**	• Evidencias de Capacitaciones de Seguridad de la Información • Evidencias de ejecución de las capacitaciones del Plan de Tratamiento de Riesgos
Implementación de controles	PROYECTO 1: **Identificación e Implementación de Controles**	• Matriz de Riesgos de Seguridad Digital • Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso
Gestión de incidentes	PROYECTO 1: **Gestión de Incidentes** Capacitar al personal en la gestión de incidentes de seguridad de la información.	• Registro de asistencia a capacitaciones

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

La Dirección TIC como Responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, establece el cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos.

ESTRATEGIA / EJE	PROYECTO	RESPONSABLE	FECHA DE ENTREGA
Liderazgo de seguridad de la información	PROYECTO 1: **Diagnóstico**	Dirección TIC	31/03/24
	PROYECTO 2: **Planificación**	Dirección TIC	31/03/24
	PROYECTO 3: **Aprobación**	Dirección TIC	31/03/24
	PROYECTO 4: **Evaluación de Desempeño**	Dirección TIC	31/11/24
	PROYECTO 5: **Mejora Continua**	Dirección TIC	31/12/24
Gestión de riesgos	PROYECTO 1: **Implementación**	• Dirección TIC • Dependencias	30/11/24
Concientización	PROYECTO 1: **Ejecución de capacitaciones**	• Dirección TIC	30/11/24
Implementación de controles	PROYECTO 1: **Identificación e Implementación de Controles**	• Dirección TIC • Dependencias	30/11/24
Gestión de incidentes	PROYECTO 1: **Gestión de Incidentes**	Dirección TIC	30/11/24

5.4 ANÁLISIS PRESUPUESTAL:

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

AÑO 2024	
PROYECTO	**Inversión**
Liderazgo de seguridad de la información	$70.000.000
Gestión de riesgos	$ 40.000.000
Concientización	$ 30.000.000
Implementación de controles	$ 200.000.000
Gestión de incidentes	$ 60.000.000
TOTAL PRESUPUESTO AÑO 2024	**$400,000,000**

Nota: El presupuesto proyectado fue desglosado en el Plan Anual de Adquisiciones y está limitado a los recursos asignados.

7. RESPONSABLES

1. Gobernador del Departamento de Bolívar - Representante Legal
2. Comité Institucional de Gestión y Desempeño - Aprobación
3. Comité de Seguridad de la Información - Seguimiento y Aprobación de documentos
4. Director(a) TIC - Diseño, Implementación y Acompañamiento
5. Dependencias - Implementación

8. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la alta dirección, el comité de gestión y desempeño institucional y el comité de seguridad de la información de la Gobernación del Departamento de Bolívar con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Tairo Mendoza **Cargo: Profesional Especializado**	Nombre: Nohora Mercado **Cargo: Directora TICs**	Nombre: Comité Institucional de Gestión y Desempeño Fecha: 26/01/2024