PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GOBERNACIÓN DE PUTUMAYO

OBJETIVO:

Proporcionar a las entidades del orden nacional y territorial una guía estructurada para la creación de su Plan Estratégico de Seguridad y Privacidad de la Información (PESI). Este plan busca fortalecer la estrategia de seguridad digital mediante el cumplimiento de los requisitos establecidos en el artículo 5 de la Resolución 500 de 2021, promoviendo la integridad, confidencialidad y disponibilidad de la información institucional.

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

GOBERNACIÓN DE PUTUMAYO

2025

Control de Versiones

Versión	Fecha	Modificación
1.0		Versión inicial del documento

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, reduciendo los riesgos a niveles aceptables. Esto se logrará mediante la implementación de estrategias de seguridad digital definidas en este documento, alineadas con las vigencias 2024-2025 y orientadas a garantizar la protección y gestión eficiente de la información institucional.

1.1 OBJETIVOS ESPECÍFICOS

- Diseñar y establecer una estrategia integral de seguridad digital para la entidad.
- Identificar y atender las necesidades relacionadas con la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).
- Priorizar los proyectos clave para garantizar una implementación efectiva del SGSI.
- Planificar la evaluación y el seguimiento continuo de los controles y lineamientos establecidos en el marco del SGSI.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información busca implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y una estrategia integral de seguridad digital que aborde las amenazas actuales, considerando la evolución de las tecnologías emergentes. Este alcance incluye todos los procesos de la entidad, asegurando la protección de los datos, la infraestructura tecnológica y la continuidad operativa frente a los retos del entorno digital moderno.

El plan se alinea con la Política General de Seguridad de la Información y abarca áreas clave como la gestión de riesgos cibernéticos, la adopción de tecnologías basadas en inteligencia artificial, el uso de infraestructura en la nube y la implementación de estándares avanzados de ciberseguridad. Su objetivo es garantizar la seguridad de la información en todos los niveles operativos de la entidad.

DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se fundamenta en los siguientes documentos, normas y lineamientos actualizados para garantizar su relevancia y eficacia:

- **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", destacando el PESI como un requisito esencial para el cumplimiento normativo.
- **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.
- **ISO/IEC 27001:2022**: Estándar internacional para sistemas de gestión de seguridad de la información.
- **NIST Cybersecurity Framework**: Marco de referencia para gestionar y reducir riesgos cibernéticos.
- **Lineamientos para el uso de tecnologías emergentes**: Políticas de adopción de IA, computación en la nube y protección de datos en el contexto digital.

3. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE LA INFORMACIÓN

La Gobernación de Putumayo enfrenta desafíos significativos debido a la insuficiencia de activos de información esenciales, como hardware, software, bases de datos, procesos y recursos humanos especializados. Estas limitaciones afectan la capacidad de la entidad para gestionar datos de manera eficiente y proteger la información crítica en sus áreas misionales, operativas y administrativas.

En un entorno digital dinámico y tecnológicamente avanzado, los activos de información son fundamentales para el funcionamiento óptimo de cualquier organización. La ausencia de estos activos compromete la seguridad, la eficiencia operativa y la toma de decisiones basadas en datos confiables.

Principales activos de información requeridos:

- **Hardware:** Computadoras, servidores, dispositivos de almacenamiento y redes modernas que respalden una infraestructura robusta.

- **Software:** Aplicaciones avanzadas y sistemas de gestión que integren herramientas de análisis, automatización y seguridad.
- **Bases de datos:** Soluciones escalables y estructuradas que permitan almacenar, procesar y recuperar datos críticos en tiempo real.
- **Procesos y procedimientos:** Flujos de trabajo digitalizados y adaptativos que fortalezcan la gestión de la información.
- **Recursos humanos:** Profesionales capacitados en ciberseguridad, gestión de datos y tecnologías emergentes, con acceso a formación continua.

La falta de estos recursos representa un riesgo elevado, dificultando la continuidad operativa, la protección de la información sensible y el cumplimiento normativo.

Recomendaciones prioritarias:

1. **Adquisición de activos tecnológicos:** Implementar hardware moderno, soluciones de software integradas y servicios en la nube para optimizar la gestión de datos.
2. **Fortalecimiento del talento humano:** Diseñar programas de capacitación en ciberseguridad, gestión de riesgos y uso de tecnologías emergentes.
3. **Implementación de políticas y estándares internacionales:** Adoptar frameworks como ISO/IEC 27001 y NIST Cybersecurity Framework para robustecer la seguridad de la información.
4. **Desarrollo de estrategias de continuidad del negocio:** Diseñar y mantener planes que garanticen la recuperación y resiliencia frente a incidentes de seguridad.

Con estas acciones, la Gobernación podrá establecer una base sólida para la gestión eficiente de sus activos de información, asegurando la protección, disponibilidad y confiabilidad de los datos en beneficio de la organización y sus stakeholders.

4. ESTRATEGIA DE SEGURIDAD DIGITAL

La entidad implementará una estrategia integral de seguridad digital basada en principios, políticas, procedimientos y lineamientos modernos, que permitan gestionar de manera eficaz los riesgos asociados al entorno digital actual. Esta estrategia estará alineada con las mejores prácticas internacionales, la adopción de tecnologías emergentes y el cumplimiento normativo, promoviendo una gestión proactiva y resiliente de la seguridad de la información.

El enfoque principal de esta estrategia incluye:

- **Transformación tecnológica:** Integrar soluciones avanzadas como inteligencia artificial, aprendizaje automático y blockchain para mejorar la detección y respuesta a amenazas.
- **Infraestructura en la nube:** Adoptar plataformas en la nube seguras y escalables para optimizar el almacenamiento, procesamiento y protección de datos.
- **Ciberseguridad avanzada:** Implementar sistemas de defensa como firewalls de próxima generación (NGFW), soluciones de Endpoint Detection and Response (EDR) y sistemas de autenticación multifactor (MFA).
- **Gestión de riesgos en tiempo real:** Utilizar herramientas de análisis predictivo y simulaciones para identificar y mitigar riesgos de forma dinámica.
- **Protección de datos:** Cumplir con estándares internacionales como ISO/IEC 27001 y normativas de protección de datos personales, garantizando la privacidad y seguridad de la información.
- **Gestión de incidentes:** Diseñar procedimientos robustos y automatizados para responder rápidamente a cualquier incidente de seguridad, minimizando el impacto en la operación de la entidad.

Por tal motivo, **la Gobernación de Putumayo** define las siguientes cinco estrategias específicas, diseñadas para establecer una estrategia general de seguridad digital:

1. **Liderazgo en seguridad de la información:** Fortalecer el compromiso de los líderes institucionales en la promoción y cumplimiento de las políticas de seguridad digital.
2. **Gestión de riesgos:** Desarrollar planes de mitigación y respuesta basados en el análisis continuo de amenazas y vulnerabilidades.
3. **Concientización y cultura de seguridad:** Promover la formación y sensibilización del personal sobre la importancia de la seguridad de la información y el uso responsable de las tecnologías.
4. **Implementación de controles avanzados:** Incorporar tecnologías de última generación para proteger los activos de información críticos.
5. **Monitoreo continuo:** Establecer sistemas automatizados para supervisar el cumplimiento de las políticas y la evolución de los riesgos en tiempo real.

Esta estrategia permitirá a la Gobernación de Putumayo estar preparada para los retos del entorno digital moderno, asegurando la integridad, confidencialidad y disponibilidad de la información en todos los niveles.

4.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

1. Liderazgo en seguridad de la información

Asegurar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la aprobación de políticas, normas y lineamientos que fortalezcan la protección de la información. Esto incluye fomentar el liderazgo activo de la alta dirección y la participación de los responsables de cada área, asegurando que la seguridad digital sea una prioridad estratégica en la toma de decisiones.

2. Gestión de riesgos

Identificar, analizar y gestionar los riesgos asociados a los activos de información mediante herramientas avanzadas de análisis de datos y simulaciones predictivas. Esto incluye el desarrollo de planes de mitigación y controles adaptativos para prevenir incidentes, reduciendo los riesgos en tiempo real.

3. Concientización

Fomentar una cultura organizacional orientada a la seguridad de la información mediante programas continuos de capacitación, campañas de sensibilización y transferencias de conocimiento. Estas iniciativas deben incluir temas como ciberseguridad, uso responsable de tecnologías emergentes, y prevención de ataques como phishing y ransomware.

4. Implementación de controles avanzados

Planificar e implementar soluciones tecnológicas de última generación, como inteligencia artificial para la detección de amenazas, sistemas de autenticación multifactor (MFA) y soluciones basadas en la nube. Estos controles deben garantizar la integridad, disponibilidad y confidencialidad de la información en todos los niveles operativos.

5. Gestión de incidentes

Establecer un procedimiento robusto y automatizado para la gestión de incidentes de seguridad, integrando herramientas de monitoreo en tiempo real y capacidades de respuesta inmediata. Este enfoque debe garantizar una

resolución eficiente de incidentes, minimizando impactos operativos y fortaleciendo la resiliencia organizacional frente a amenazas emergentes.

4.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

Para cada estrategia específica, la Gobernación de Putumayo define los siguientes proyectos y actividades, diseñados para fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar la seguridad digital en todos los niveles de la entidad:

Estrategia/Eje	Proyecto	Productos Esperados
Liderazgo en seguridad de la información	Desarrollo e implementación de la política general de seguridad de la información.	Política formalizada y aprobada por la alta dirección.
	Diseño de un plan de gobernanza de la seguridad digital.	Roles y responsabilidades claramente definidos en toda la organización.
Gestión de riesgos	Identificación y clasificación de riesgos cibernéticos.	Matriz de riesgos actualizada en tiempo real con tecnologías predictivas.
	Implementación de un sistema automatizado de gestión de riesgos basado en inteligencia artificial.	Solución tecnológica integrada que permite la gestión dinámica de riesgos.
Concientización	Creación de un programa continuo de capacitación en ciberseguridad y buenas prácticas digitales.	- Plan anual de capacitación documentado. - Evidencias de jornadas de sensibilización. - Certificaciones obtenidas por el personal.
	Realización de simulaciones periódicas de incidentes (ej.	Reportes de resultados y aprendizaje obtenido de simulaciones.

	phishing, ataques de ransomware).	
Implementación de controles avanzados	Adopción de tecnologías avanzadas como firewalls de próxima generación (NGFW) y soluciones WAF.	- Controles tecnológicos implementados y operativos. - Procedimientos de monitoreo y respuesta establecidos.
	Desarrollo de políticas de desarrollo seguro y clasificación de la información.	Políticas de desarrollo seguro formalizadas y operativas.
Gestión de incidentes	Implementación de un sistema de detección y respuesta ante amenazas (EDR).	- Procedimientos de gestión de incidentes documentados y automatizados. - Informes de incidentes tratados.
	- Capacitación especializada en gestión de incidentes para el personal clave de la entidad.	- Reportes de sesiones de capacitación y mejora en los tiempos de respuesta ante incidentes.

Nota: Cada uno de estos proyectos debe estar alineado con los estándares internacionales (como ISO/IEC 27001 y NIST Cybersecurity Framework), integrando herramientas tecnológicas modernas que optimicen la gestión y respuesta en el ámbito de la seguridad digital.

4.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS

El responsable de seguridad de la información establecerá un cronograma detallado para ejecutar cada proyecto definido, asegurando una implementación eficiente y el cumplimiento de los objetivos establecidos. Las actividades pueden desarrollarse de forma secuencial o paralela, según las necesidades y recursos de la entidad.

Año	Trimestre	Actividad / Proyecto	Responsable	Resultado Esperado
2025	**Trimestre 1**	- Diagnóstico inicial de seguridad	Responsable de Seguridad Digital	Informe diagnóstico con línea base de

		digital y evaluación de riesgos.		seguridad de la información.
		- Diseño y formalización de la política de seguridad de la información.	Alta Dirección	Política de seguridad aprobada y comunicada.
		- Adquisición e implementación de solución EDR y WAF.	Equipo de TI	Sistemas de defensa avanzados operativos.
		- Capacitación inicial al personal en ciberseguridad.	Área de Recursos Humanos	Evidencias de formación documentadas.
2025	**Trimestre 2**	- Clasificación de activos de información críticos.	Responsable de Seguridad Digital	Matriz de clasificación de activos completada.
		- Inicio de la implementación del sistema automatizado de gestión de riesgos.	Equipo de TI	Sistema de gestión de riesgos funcional.
		- Realización de simulacros de incidentes de seguridad (phishing y ransomware).	Responsable de Seguridad Digital	Informe de resultados y mejoras en la respuesta a incidentes.
2025	**Trimestre 3**	- Ejecución de auditorías internas para evaluar el cumplimiento de la política de seguridad.	Auditor Interno	Informe de auditoría con recomendaciones.
		- Implementación de controles avanzados como autenticación multifactor (MFA) y cifrado de datos.	Equipo de TI	Controles avanzados implementados y probados.
		- Desarrollo de jornadas de sensibilización para todos los niveles de la organización.	Área de Recursos Humanos	Evidencias de actividades de sensibilización realizadas.

2025	**Trimestre 4**	- Actualización y ajuste del cronograma de seguridad basado en los avances y resultados del año.	Alta Dirección	Cronograma ajustado y aprobado para el próximo año.
		- Evaluación del desempeño del sistema de gestión de incidentes.	Responsable de Seguridad Digital	Informe de efectividad del sistema de incidentes.
2026	**Trimestre 1**	- Optimización de la infraestructura tecnológica para garantizar la escalabilidad de las soluciones.	Equipo de TI	Infraestructura optimizada y lista para futuras expansiones.
		- Continuación de las capacitaciones especializadas en gestión de riesgos y uso de herramientas.	Área de Recursos Humanos	Personal capacitado en el uso de tecnologías avanzadas.
	Trimestres 2-4	- Monitoreo continuo y mejora de las estrategias implementadas.	Responsable de Seguridad Digital	Informes trimestrales de desempeño y ajuste de estrategias.

4.4 ANÁLISIS PRESUPUESTAL

Dada la falta de recursos suficientes en la entidad, la estrategia de seguridad digital será implementada de manera gradual, priorizando proyectos críticos y ajustando el presupuesto para vigencias futuras. Este enfoque permitirá a la entidad gestionar los recursos de manera eficiente, formulando proyectos específicos para garantizar su sostenibilidad a largo plazo.

Año	Proyecto / Actividad	Descripción	Presupuesto Aproximado (COP)
2025	Diagnóstico inicial y formulación de proyectos	Realizar un diagnóstico detallado del estado actual de la seguridad de la información y estructurar proyectos estratégicos para su implementación.	$ 30,000,000

	Adquisición de infraestructura básica para seguridad digital	Compra inicial de hardware esencial como servidores y equipos de red para garantizar una base segura.	$ 100,000,000
	Diseño e implementación de políticas de seguridad de la información	Creación de políticas basadas en estándares internacionales (ISO 27001) y normativas locales.	$ 20,000,000
	Capacitación inicial en ciberseguridad	Sensibilización del personal en buenas prácticas digitales y gestión de riesgos básicos.	$ 10,000,000
2026	Implementación de soluciones tecnológicas esenciales	Adopción de tecnologías críticas como firewalls de próxima generación (NGFW) y soluciones de Endpoint Detection and Response (EDR).	$ 200,000,000
	Gestión de riesgos automatizada	Implementación de herramientas básicas para la identificación y clasificación de riesgos cibernéticos.	$ 50,000,000
	Sensibilización continua	Desarrollo de campañas y jornadas de capacitación enfocadas en ciberseguridad avanzada.	$ 20,000,000
2027	Implementación de tecnologías emergentes	Inicio de proyectos piloto para el uso de inteligencia artificial y blockchain en la gestión de seguridad.	$ 150,000,000
	Mantenimiento de sistemas y actualizaciones	Renovación de licencias, soporte técnico y actualizaciones de soluciones tecnológicas implementadas.	$ 50,000,000
	Auditorías internas y evaluación de desempeño	Realización de auditorías para medir el impacto de las estrategias implementadas.	$ 30,000,000

2028	Escalamiento de la infraestructura tecnológica	Ampliación de capacidades tecnológicas para soportar un entorno digital más avanzado y seguro.	$ 200,000,000
	Formación especializada en nuevas tecnologías	Cursos avanzados para el personal en áreas como inteligencia artificial, machine learning y blockchain.	$ 40,000,000
	Optimización y ajustes del Sistema de Gestión de Seguridad de la Información (SGSI)	Mejoras basadas en resultados de auditorías y monitoreo continuo.	$ 50,000,000

TOTAL, PRESUPUESTO (2025-2028): $950,000,000 COP

Estrategia de implementación gradual:

Prioridad en diagnósticos y políticas: El primer año (2025) se centrará en establecer una base sólida, con diagnósticos claros y políticas bien definidas.

Adopción escalonada de tecnología: En 2026 se iniciará la implementación de soluciones críticas, priorizando aquellas con mayor impacto en la seguridad.

Proyectos piloto para tecnologías emergentes: En 2027 se pondrán en marcha pilotos para blockchain, evaluando su impacto antes de una adopción masiva.

Ajustes y escalamiento: A partir de 2028 se consolidará el sistema, con actualizaciones regulares y un enfoque en la sostenibilidad a largo plazo.