	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA (Tecnologías de la Información)	CÓDIGO PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN 29 01 2024 VERSIÓN 02		

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**GOBERNACIÓN DEL DEPARTAMENTO DE
ARAUCA**



	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO		
		PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN		
		29	01	2024
VERSIÓN 02				

Tabla de contenido

1. OBJETIVOS	
1.1 OBJETIVOS ESPECÍFICOS	3
2. ALCANCE	4
3. DOCUMENTOS DE REFERENCIA	5
4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	6
5. ESTRATEGIA DE SEGURIDAD DIGITAL	7
5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)	8
5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:	9
5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:	13
5.4 ANÁLISIS PRESUPUESTAL:	14
6. RESPONSABLES	15
7. APROBACIÓN	16


	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO		
		PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN		
		29	01	2024
VERSIÓN 02				

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2023-2024.


1.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de 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.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO		
		PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN		
		29	01	2024
VERSIÓN 02				

2. ALCANCE


El Plan Estratégico de Seguridad 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 se tendrán en cuenta todos los procesos de la Gobernación de Arauca.

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO		
		PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN		
		29	01	2024
VERSIÓN 02				

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad 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.

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO		
		PL-SI - 03		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	FECHA DE EMISIÓN		
		29	01	2024
VERSIÓN 02				

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

De acuerdo al Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información y la lista de chequeo del marco referencia de arquitectura empresarial, se evidencia que son muy bajos los porcentajes de avance en la implementación de las políticas, procesos procedimientos, controles, manuales e instructivos MSPI.

La entidad está comprometida con la implementación de la estrategia de la política de Gobierno digital, con la proyección de lograr la transformación digital y protección de la información mediante la aplicación de los habilitadores de arquitectura, seguridad y privacidad de la información, servicios y ciudadanos digitales y cultura y apropiación, fortaleciendo a la entidad en cuanto a competitividad y prestación de servicios seguros y eficientes.

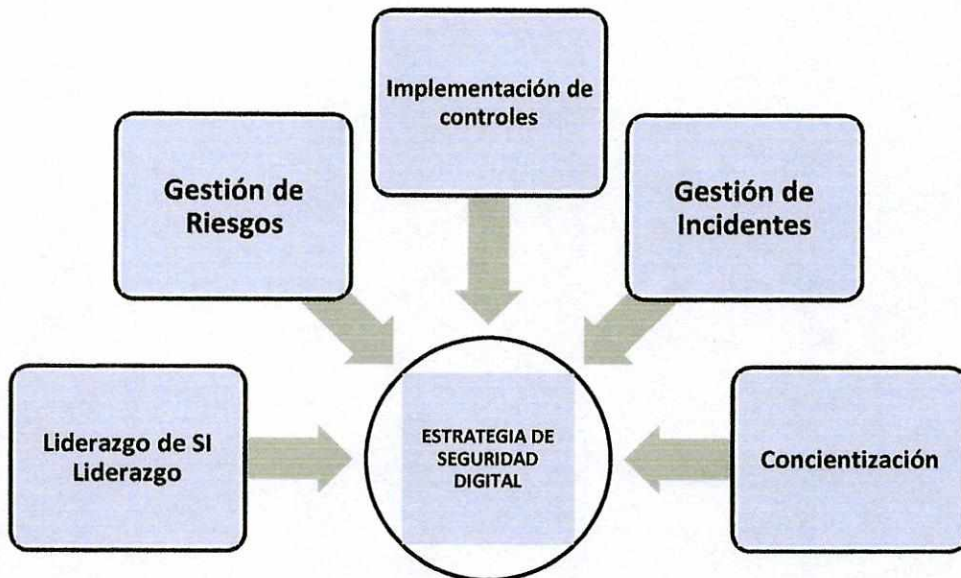
	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03				
		PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION				
	FECHA DE EMISIÓN			29	01	2024
	VERSIÓN 02					


5. ESTRATEGIA DE SEGURIDAD DIGITAL

LA ENTIDAD establecerá 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 que debe establecerse (Ver Resolución 500 de 2021).

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

Nota: Es fundamental que las entidades hagan la lectura de la resolución 500 de 2021 y del Anexo 1, que contiene la actualización del Modelo de Seguridad y Privacidad de la Información.




	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03		
		FECHA DE EMISIÓN 29 01 2024		
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	VERSIÓN 02		

5.1 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.


	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03		
		PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
	FECHA DE EMISIÓN			
	29	01	2024	VERSIÓN 02

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.


5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, GOBERNACIÓN DE ARAUCA 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: Desarrollar e implementar una política de seguridad y manual de Políticas de Seguridad y Privacidad de la Información	Política de Seguridad Formalizada e Implementada y realizar el manual de las políticas.
	PROYECTO 2: Definición de Roles y Responsabilidades de Seguridad de la Información.	Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
	PROYECTO 3: Inventario de los activos de Información.	Inventario de los Activos
	PROYECTO 4: Integrar MSPI y Modelo de Gestión Documental	Caracterización del proceso TI y la integración en el mapa de procesos.

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03		
		PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
	FECHA DE EMISIÓN			
	29	01	2024	VERSIÓN 02

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de riesgos	<p>PROYECTO 1: Identificar, valorar y clasificar los riesgos asociados a los activos de información</p> <p>PROYECTO 2: Definir planes de tratamiento de riesgos de seguridad</p> <p>PROYECTO 3: Diagnóstico al cableado estructurado de la red LAN</p> <p>PROYECTO 4: Implementación de las oportunidades de mejora a la red de cableado estructurado</p>	<p>Matriz de riesgos de seguridad digital</p> <p>Definir planes de tratamiento de riesgos</p> <p>Documento con el plan de mejoramiento</p> <p>las mejoras recomendadas en el diagnóstico</p>
Concientización	<p>PROYECTO 1: Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.</p> <p>PROYECTO 2: Realizar jornadas de sensibilización a todo el personal.</p> <p>PROYECTO 3: Realizar transferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.</p> <p>PROYECTO 4: Medir el grado de sensibilización a toda la Entidad.</p>	<p>1. Plan de Sensibilización</p> <p>2. Evidencias de las actividades desarrolladas</p> <p>3. Certificaciones de cursos</p> <p>4. Resultado de las encuestas de medición</p>
Implementación de controles	<p>CONTROL 1 Política de respaldos de información.</p> <p>CONTROL 2 Procedimiento de Gestión de Cambios.</p> <p>CONTROL 3 Clasificación de la información.</p> <p>CONTROL 4 Políticas de Desarrollo de software Seguro</p> <p>CONTROL 5 Implementación de solución Seguridad Perimetral HA.</p> <p>Web Application Firewall (WAF)</p> <p>CONTROL 6</p>	<p>Política de respaldos de información.</p> <p>Procedimiento de Gestión de Cambios.</p> <p>Clasificación de la información.</p> <p>Políticas de Desarrollo Seguro WAF desplegado y funcional.</p> <p>Adquisición de Hardware y configuración de equipos de protección perimetral.</p>

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03		
		PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
	FECHA DE EMISIÓN			
	29	01	2024	VERSIÓN 02

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	Implementación de respaldos de copias de Seguridad en la nube CONTROL 7 Control de acceso biométrico y CCTV CONTROL 8 Control de Incendios CONTROL 9 Control de Temperatura CONTROL 10 Política y procedimiento para la adquisición de hardware y Software CONTROL 11 Control de acceso externo a sistemas de información CONTROL 12 Control de autenticar y autorización de usuario CONTROL 13 Control de instalación y configuración de Software en estaciones de trabajo CONTROL 14 Control de Contraseñas de las aplicaciones de Gestión CONTROL 15 Control de solicitud de servicio mesa de ayuda	Adquisición de servicio de almacenamiento en la nube Adquisición de hardware y software para el control de acceso. Sistema de Control de Incendios Sistema de control de Temperatura para el Centro de Datos Política y procedimiento para la adquisición de hardware y software formatos de autorizaciones de acceso de Software para el control de acceso externo Solicitud para creación de usuario, acta de entrega de servicio Configuración de política de Grupo GPO Formato de Solicitud de servicio de mesa de ayuda

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA	CÓDIGO PL-SI - 03		
		PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
	FECHA DE EMISIÓN			29 01 2024
	VERSIÓN 02			

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de incidentes	PROYECTO 1: Definir y formalizar un procedimiento de Gestión de Incidentes de seguridad de la información. PROYECTO 2: Capacitar al personal en la gestión de incidentes de seguridad de la información.	1. Procedimiento de gestión de incidentes de seguridad formalizado. 2. Sesiones de capacitación desarrolladas.




PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA (Tecnologías de la Información)		Código	
		PL-SI - 03	
PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA DE EMISIÓN	
		29	01 2024
		VERSIÓN 02	

5.3 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie cómo se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

AÑO 2023				AÑO 2024	
TRIMESTRE 1	TRIMESTRE 2	TRIMESTRE 3	TRIMESTRE 4	TRIMESTRE 1	TRIMESTRE 2
Realizar diagnóstico seguridad y privacidad		Definir y formalizar un procedimiento de gestión de incidentes de seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.	Actualización Diagnóstico de Seguridad	
Identificación de activos procesos misionales		Implementación de solución Seguridad Perimetral HA. Web Application Firewall (WAF)	Gestión de Riesgos de Seguridad	Adquisición e Implementación IPS	
Desarrollo Plan de Sensibilización 2023		Adquisición e implementación Sistema de Análisis de Vulnerabilidades		Desarrollo Sensibilización 2024	Implementación Estrategias de Capacitación en Seguridad

(Esta tabla solo muestra proyectos de ejemplo, cada entidad debe realizar la identificación de los posibles proyectos a plantear según lo establecido en la sección 5.2 o también con base a los controles o planes de tratamiento de riesgos para mitigar los riesgos de seguridad de la información, con base a la dimensión y necesidades específicas de cada entidad).

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA		Código	
			PL-SI - 03	
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA DE EMISIÓN	
29			01	2024
			VERSIÓN 02	

Nota: Al finalizar cada vigencia, LA ENTIDAD, realizará una actualización del cronograma, incorporando el estado del avance de los proyectos formulados y si en efecto se cumplieron o se plantean aplazamientos para las vigencias posteriores. Así mismo, el cronograma podrá ser modificado o ajustado de acuerdo con las necesidades o situaciones que surjan en la entidad.

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 2023		AÑO 2024		AÑO 2025	
PROYECTO	Inversión	PROYECTO	Inversión	PROYECTO	Inversión
Construir los lineamientos técnicos e implementación de controles que se definan en el plan operacional de seguridad y privacidad de la información.	\$ 470.000.000	Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento.	\$ 527.280.000	Mantener el funcionamiento del Modelo de seguridad y privacidad de la Información	\$ 200.000.000
Implementación de solución WAF	\$ 150.000.000	Diagnóstico de la Red LAN Implementación de la Red LAN	\$ 20.000.000 \$ 800.000.000	Adquisición Servicio Ethical Hacking	\$ 50.000.000



PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA		CÓDIGO	
		PL-SI - 03	
PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA DE EMISIÓN	
		29	01
		2024	
VERSIÓN 02			

Adquisición Sistema de Análisis de Vulnerabilidades	\$ 100.000.000	Adquisición y despliegue de soluciones de IPS	\$ 200.000.000	Renovación WAF, IPS y Análisis de Vulnerabilidades	\$ 225.000.000
Adquisición Servicio Ethical Hacking	\$ 50.000.000	Renovación WAF y Sistema de Análisis de Vulnerabilidades	\$ 125.000.000		
TOTAL PRESUPUESTO AÑO 2023	\$770,000,000	TOTAL PRESUPUESTO AÑO 2024	\$1672,000,000	TOTAL PRESUPUESTO AÑO 2025	\$274,500,000

6. RESPONSABLES

1. Gobernador: Aprobar los documentos de Alto Nivel
2. Secretario (a) General y de Gobierno: Velar por la implementación del MSP1 y garantizar los recursos requeridos.
3. Responsable de Seguridad Digital / CIO / Enlace TIC: Coordinar las actividades de implementación del MSP1


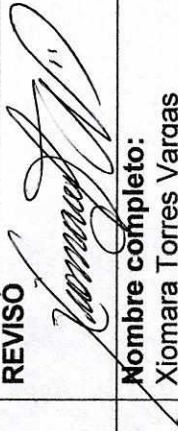

	PROCESO: PROVISION DE RECURSOS PARA LA MEJORA CONTINUA		CÓDIGO
			PL-SI - 03
	PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		FECHA DE EMISIÓN
		29	01 2024
VERSIÓN 02			

7. APROBACIÓN

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

CONTROL DE CAMBIOS

VERSIÓN Y FECHA	DESCRIPCION Y JUSTIFICACIÓN DEL CAMBIO
Versión 1 31-01-2023	Se realiza la creación del PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION VIGENCIA 2023.
Versión 2 29-01-2024	Se modifica encabezado se cambia nombre a PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION (sin vigencia)

REVISOR	REVISOR	APROBADO
 Nombre completo: Mauricio Alberto Reyes Castilla	 Nombre completo: Xiomara Torres Vargas Cargo: Profesional Universitario Dirección de sistemas e informática	 Nombre completo: Neida Rocío Parada Cáceres Cargo: Representante de la Alta Dirección. (Resolución 2573 del 06 Octubre 2021)
Fecha: 29 de enero de 2024	Fecha 29 de enero de 2024	Fecha 29 de enero de 2024