COLOMBIA POTENCIA DE LA VIDA

Agencia Nacional de Minería

Agencia Nacional de Minería

PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2026

Luis Alonso Lugo Charry

Oficial de seguridad de la información CISO

Diciembre 29 de 2025

TABLA DE CONTENIDO

PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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 información en la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 202x-202x.

2. 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 ejecutar 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.

3. ALCANCE

Este informe establece el plan estratégico a desarrollar en el año 2026, con base en el avance realizado en el año 2025. Se encuentra alineado con el plan estratégico de tecnologías de información PETIC, con el plan de arquitectura empresarial en su dominio de seguridad y con la política de gobierno y seguridad digital del estado colombiano.

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.
- *PETIC – Plan estratégico de tecnologías de información y comunicaciones ANM.*

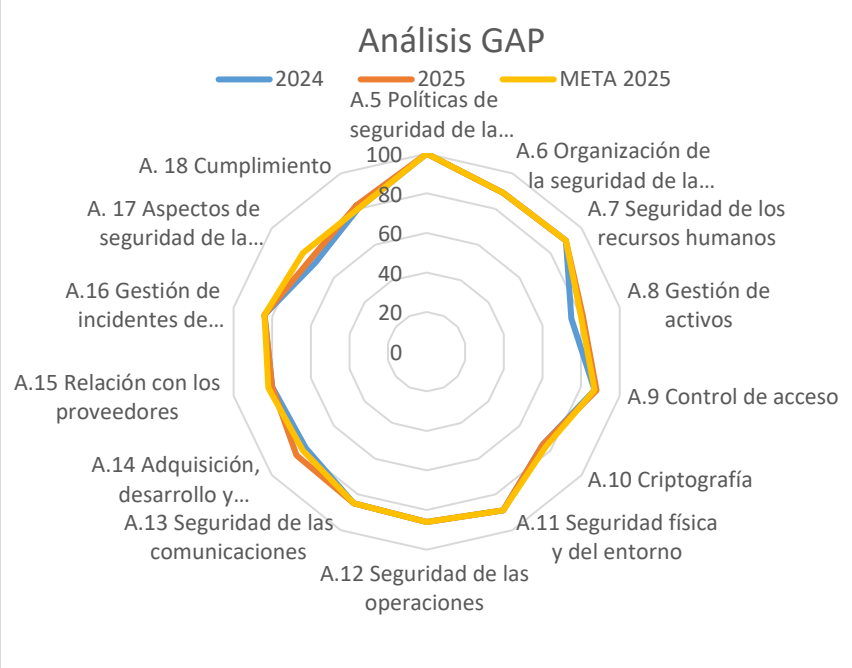
4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Durante el periodo del 2025 se realizó seguimiento mensual y calificación semestral a los controles del SGSI, para lo cual en el segundo semestre se obtuvo un cumplimiento parcial a la estrategia inicial aprobada por el comité de gestión y desempeño de la entidad. Así:

Evaluación de controles				
DOMINIO	*2024*	*2025*	*META 2025*	*EVALUACIÓN CUALITATIVA*
A.5 Políticas de seguridad de la información	*100*	*100*	*100*	*Optimizado*
A.6 Organización de la seguridad de la información	*89*	*89*	*89*	*Optimizado*
A.7 Seguridad de los recursos humanos	*90*	*90*	*90*	*Optimizado*
A.8 Gestión de activos	*75*	*81*	*80*	*Optimizado*
A.9 Control de acceso	*87*	*88*	*87*	*Optimizado*
A.10 Criptografía	*75*	*75*	*77*	*Gestionado*
A.11 Seguridad física y del entorno	*89*	*89*	*89*	*Optimizado*
A.12 Seguridad de las operaciones	*86*	*86*	*86*	*Optimizado*
A.13 Seguridad de las comunicaciones	*85*	*85*	*85*	*Optimizado*
A.14 Adquisición, desarrollo y mantenimientos de sistemas	*78*	*84*	*80*	*Optimizado*
A.15 Relación con los proveedores	*80*	*80*	*82*	*Gestionado*
A.16 Gestión de incidentes de seguridad de la información	*84*	*84*	*84*	*Optimizado*

A. 17 Aspectos de seguridad de la información de la gestión de continuidad de negocio	*72*	*75*	*80*	*Gestionado*
A. 18 Cumplimiento	*80*	*82*	*80*	*Optimizado*
Promedio evaluación de controles	*83,6*	*84,9*	*84,9*	*Optimizado*

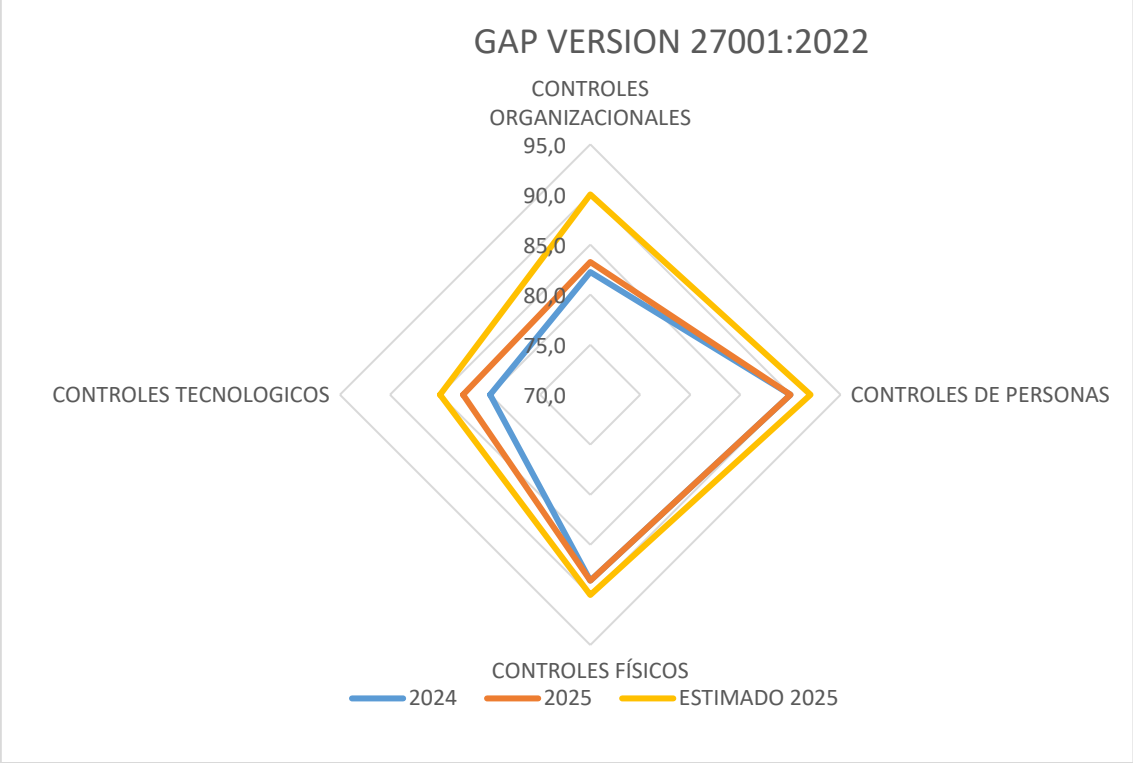
Se observan 3 dominios en los cuales no se alcanzó la meta proyectada y que deben ser priorizadas durante la vigencia 2026. Sin embargo, el esfuerzo en mejorar el nivel de madurez de otros dominios generó un resultado positivo llegando a un resultado general esperado.



De los grandes retos del PESI para la vigencia 2025, correspondió a la actualización del modelo de la versión 2013 a la versión 2022 de la norma ISO27001 en la cual se basa el MSPI. Esto llevó a realizar procesos de reingeniería documental, cambios en algunos objetivos tácticos y estratégicos y la calificación conforme la última versión como se muestra a continuación:

Evaluación de controles			
DOMINIO	**2024**	**2025**	**EVALUACIÓN CUALITATIVA**
CONTROLES ORGANIZACIONALES	*82,3*	*83,3*	***Optimizado***

CONTROLES DE PERSONAS	*90,0*	*90,0*	***Optimizado***
CONTROLES FÍSICOS	*88,6*	*88,6*	***Optimizado***
CONTROLES TECNOLOGICOS	*80,0*	*82,7*	***Optimizado***
Promedio evaluación de controles	*85,2*	*86,1*	***Optimizado***



Análisis gap – Matriz SOA – ANM 2025

Como se observa en la tabla el porcentaje de calificación general cambia, debido a los pesos que les da a algunos controles en la nueva versión 2022.

(En esta sección, se debe indicar y documentar de la forma más estratégica posible el estado actual de la entidad respecto a la implementación de los lineamientos de seguridad de la información requeridos por el MSPI.

Esto permitirá a la entidad establecer la línea base de donde se encuentra la entidad y así proyectar hacía que punto desea llegar con base a las actividades definidas dentro del PESI.

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	10%	14%
		Liderazgo	12%	14%
		Planificación	8%	14%
		Soporte	13%	14%
	Implementación	Operación	15%	16%
	Evaluación de Desempeño	Evaluación del desempeño	12%	14%
	Mejora Continua	Mejora	14%	14%
TOTAL			84%	100%

Imagen extraída del modelo de autodiagnóstico del MPSI

CALIFICACIÓN FRENTE A MEJORES PRÁCTICAS EN CIBERSEGURIDAD (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
GOVERNAR	69	100
IDENTIFICAR	93	100
PROTEGER	80	100
DETECTAR	80	100
RESPONDER	100	100
RECUPERAR	95	100

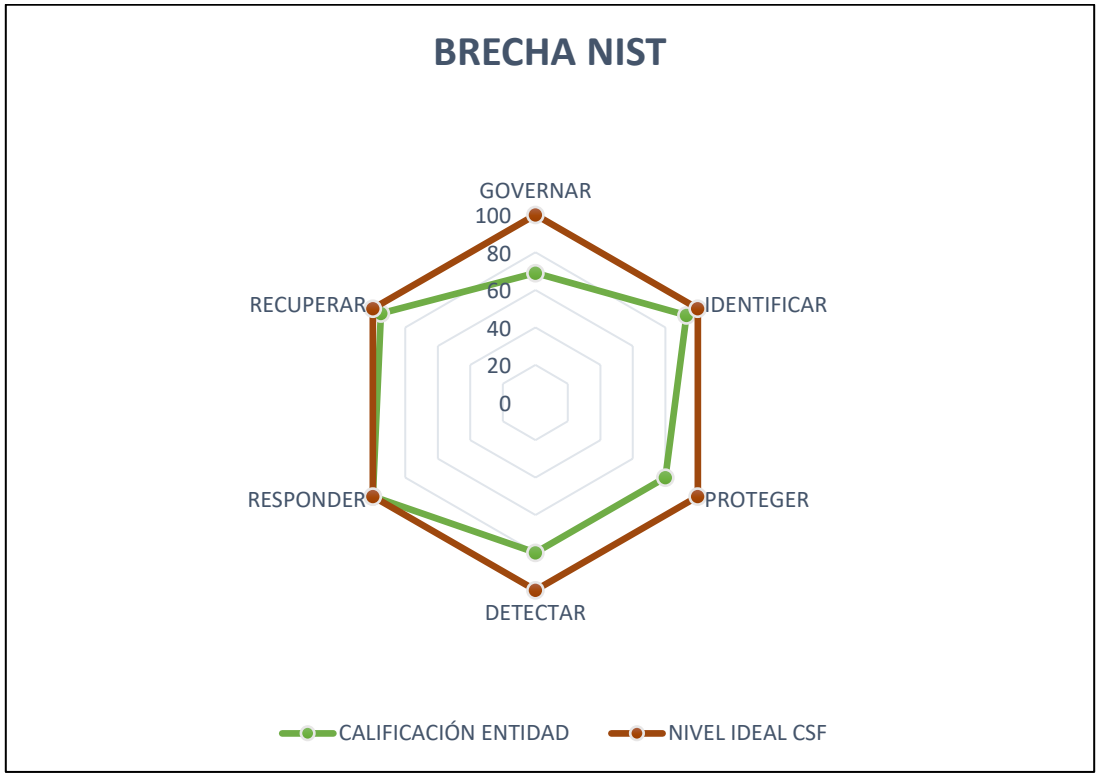
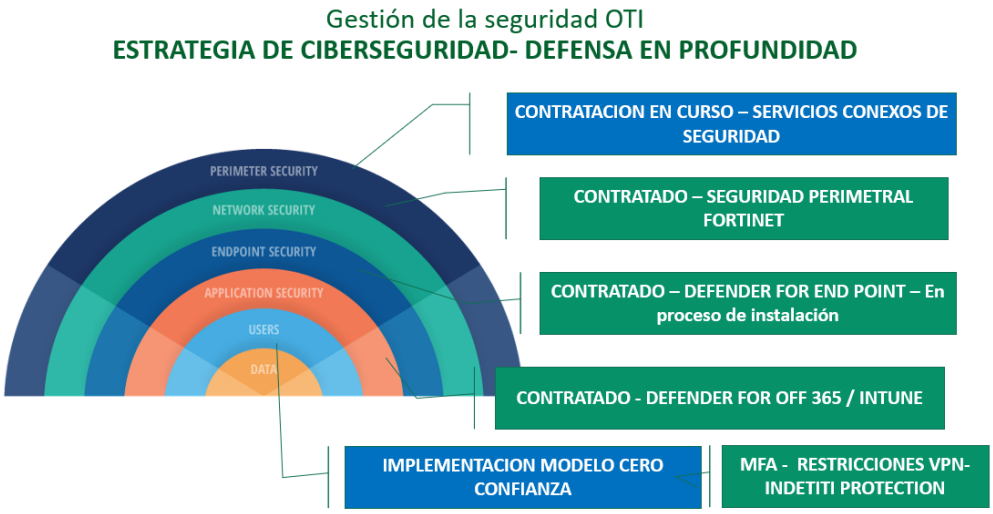


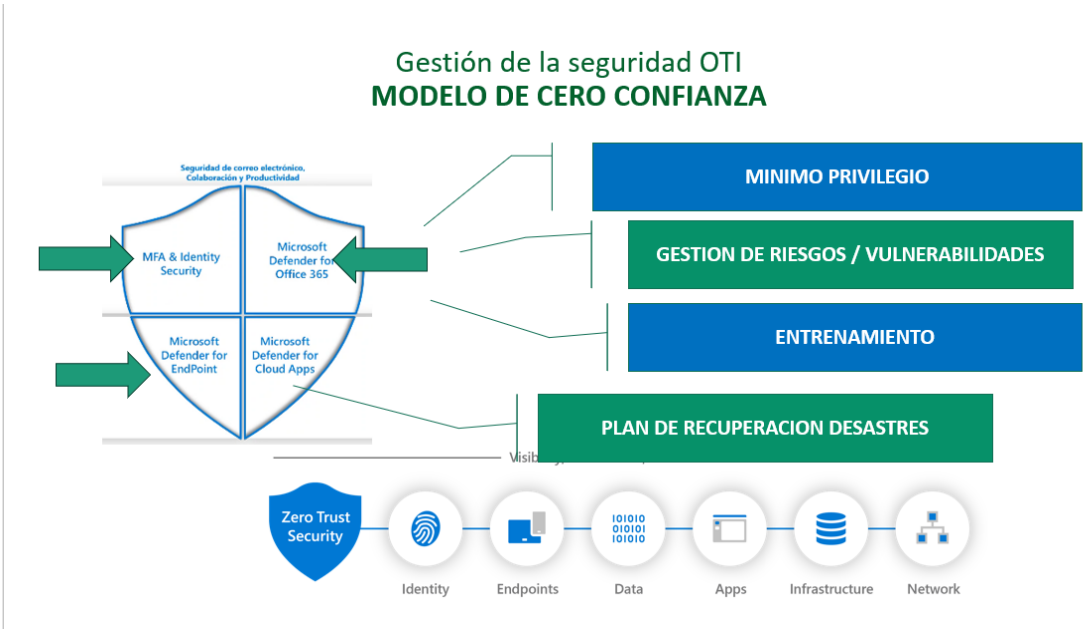
Imagen extraída del modelo de autodiagnóstico del MPSI

5.ESTRATEGIA DE SEGURIDAD DIGITAL

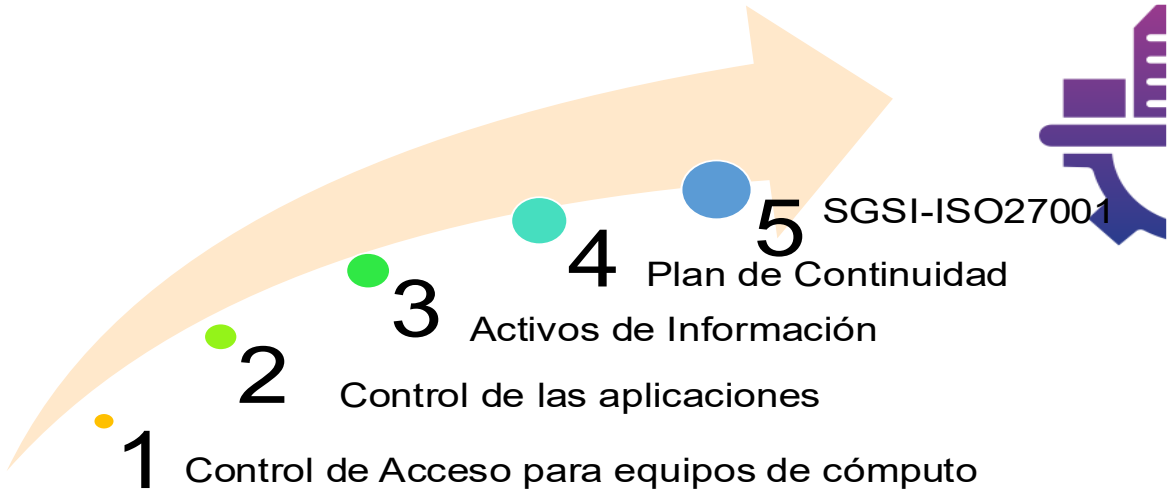
Pilares generales de la estrategia de seguridad digital:



Se debe dar continuidad a las acciones que aporten la estrategia de confianza cero (Zero Trust) en las diferentes etapas.



4.1. DESCRIPCIÓN DE LOS RESTOS Y ESTRATEGIAS ESPECÍFICAS



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
Estrategia de Ciberseguridad –	Se debe dar continuidad al plan de aseguramiento tecnológico basado en el modelo de Cero confianzas (Zero Trust) a nivel de identidad, datos, infraestructura, aplicaciones, conectividad. Se debe dar continuidad al modelo de cero confianzas en servicios tercerizados en Nubes públicas y privada.
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 y apropiando al interior de la entidad 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	Dar continuidad en la implementación de 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 dará continuidad en la implementación de controles técnicos y 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 en la Entidad.
Cumplimiento	Dar continuidad al plan de cumplimiento de entidades públicas relacionado con la gestión de activos de información conforme la ley de transparencia y ley de protección de datos personales.

4.2. ENFOQUE BASADO EN RIESGOS.

Al finalizar el periodo se observa que el tratamiento fue enfocado en los Riesgos Altos y moderados, con una disminución de 14 riesgos moderados a bajo.

También se observa el incremento de un riesgo adicional en el periodo 2025 , que se origina de la prueba de Recuperación de desastres realizada en agosto de 2025, donde se determinó la necesidad de implementar un plan de trabajo ante una posible indisponibilidad masiva de los servicios de la Calle 26 por fallos prolongados de alimentación eléctrica.

Este Riesgo se califica inicialmente en estado ALTO y se coordina con el equipo de Infraestructura para la implementación de un plan orientado a la mitigación y/o moderación.

Al finalizar el periodo 2025 el panorama es el siguiente:

6. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Estrategia de ciberseguridad. **como componente fundamental de la estrategia de seguridad digital.**	**PROYECTO 1:** Gestión de vulnerabilidades Técnicas **PROYECTO 2:** Eliminar Fugas de información **PROYECTO 3:** Implementación de la IA (Inteligencia Artificial) al componente de seguridad.	Reducción de un 50% de a vulnerabilidades técnicas que se detecten en la infraestructura y los sistemas de la entidad Madurar el control tecnológico con restricciones de descargas y accesos a la información clasificada de la entidad Madurar el control tecnológico de conectividad en la entidad.
Gestión de riesgos	**PROYECTO 1:** Definir planes de tratamiento de riesgos de seguridad. **PROYECTO 2:** Plan de Recuperación de Desastres	Definir planes de tratamiento de riesgos para la vigencia actual Actualización del Plan de recuperación

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Concientización	**PROYECTO 1:** Establecer desde el inicio la planeación de sensibilización para todo el año de la vigencia en curso. **PROYECTO 2:** Realizar jornadas de sensibilización a todo el personal.	1. Plan de concienciación anual para el año 2026. 2. Evidencias de las actividades desarrolladas 3. Certificaciones de cursos 4. Resultado de las encuestas de medición
Implementación de controles	CONTROL 1 Fugas de información CONTROL 2 Accesos a recursos clasificados de acuerdo con el Rol y a sus obligaciones. CONTROL 3 Control en cadena de suministro de proveedores críticos CONTROL 4 Políticas de Desarrollo Seguro CONTROL 5 Conexiones Remotas. CONTROL 6 Controles de aseguramiento de la información (cumplimiento en políticas de backup)	Política de respaldos de información. Procedimiento de Gestión de Cambios. Clasificación de la información. Políticas de Desarrollo Seguro WAF desplegado y funcional.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de incidentes	**PROYECTO 1:** Validar el correcto funcionamiento y tratamiento de incidentes de seguridad **PROYECTO 2:** Disminución de Los incidentes adoptando el modelo preventivo.	1. Madurar el procedimiento de gestión de Incidentes. 2. Indicadores de gestión de incidentes
Cumplimiento	**PROYECTO 1:** Actualización del procedimiento de gestión de activos de información conforme Ley de trasparencia y el MSPI. **PROYECTO 2:** Actualización del plan de protección de datos personales.	1. Actualización del procedimiento de gestión de activos de información. 2. plan de revisión y actualización en protección de datos personales.

6.2. 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 2025		AÑO 2026	
PROYECTO	**Inversión**	**PROYECTO**	**Inversión**
Contratar los servicios de Centro de Operaciones de Seguridad, que soportan las actividades misionales y de Fiscalización de la Agencia Nacional de Minería (ANM)	$ 1.059.942.447,41	**Contratar los servicios de Centro de Operaciones de Seguridad, que soportan las actividades misionales y de Fiscalización de la Agencia Nacional de Minería (ANM)**	$ 1.197.734.965,57
Contratación de personal de apoyo	$ 190.000.000	Adquisición Servicio Ethical Hacking	$ $207.000.000
Renovación servicios de seguridad en 365	$ 803.700.480	Renovación WAF, IPS y Análisis de Vulnerabilidades	$ 908.181.542
TOTAL, **PRESUPUESTO AÑO 2025**	**$ 2.053.642.927,41**	**TOTAL, PRESUPUESTO AÑO 2026**	**$ 2.105.916.507,57**

7. RESPONSABLES

1. Representante Legal de la Entidad
2. Comité de gestión y desempeño
3. Jefe de la oficina de tecnología e información
4. Oficial de seguridad de la información
5. ***Responsables de infraestructura y sistemas de información***
6. Terceros asociados – SOC y contratistas especializados.

8. 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.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Luis Alonso Lugo Charry **Cargo/ROL: Oficial de Seguridad de la Información**	Nombre: Nubia Esperanza **Cargo/ROL: Arquitecto empresarial**	Nombre: Andrea Bibiana Peña **Cargo: jefe Oficina de Tecnología e información.**