



**DEPARTAMENTO ADMINISTRATIVO
NACIONAL DE ESTADÍSTICA – DANE Y FONDO ROTATORIO DEL
DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA
– FONDANE**

**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN**

**OFICINA ASESORA DE PLANEACIÓN
OFICINA DE SISTEMAS - SECRETARIA GENERAL**

Enero de 2026

CONTENIDO

1. JUSTIFICACIÓN	3
2. OBJETIVOS	3
3. ALCANCE	4
4. DOCUMENTOS DE REFERENCIA.....	4
5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	7
6. ESTRATEGIA DE GESTION DE RIESGOS.....	9
6.1 Portafolio de proyectos / Actividades:.....	10
6.2 Cronograma de actividades / Proyectos:.....	11
6.3 Análisis presupuestal:.....	12

1. JUSTIFICACIÓN

Mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el DANE busca establecer medidas para mitigar los riesgos asociados a los activos de información, como la pérdida de confidencialidad, integridad y disponibilidad, procurando así evitar situaciones que generen incertidumbre en el cumplimiento de la misionalidad de la Entidad. El presente plan se elabora con el fin de evaluar las acciones que permitan mitigar los riesgos identificados en los procesos de la entidad estas acciones se encuentran compuestas por actividades que se definen teniendo en cuenta la información obtenida del seguimiento a los riesgos de seguridad y privacidad de la información, las necesidades y el contexto de la entidad; dichas actividades establecen tareas, responsables y fechas de ejecución durante la vigencia. El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se elabora con el fin de dar cumplimiento a lo establecido en el Decreto 612 de 2018 y tiene como base los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la guía de administración de Riesgos y Diseño de Controles, el modelo de Seguridad y Privacidad de la Información-MSPI y el plan de Seguridad y Privacidad de la información, donde se establecen recomendaciones para la identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos y los lineamientos de los estándares ISO 27001 e ISO 31000.

2. OBJETIVOS

- Cumplir con los requisitos legales, reglamentarios y regulatorios en cuanto a riesgos de Seguridad y Privacidad de la Información.
- Realizar una adecuada gestión de riesgos de Seguridad y Privacidad de la información, teniendo en cuenta los lineamientos establecidos en el DANE.
- Proteger y preservar la integridad, confidencialidad, disponibilidad, privacidad y autenticidad de la información, mediante la aplicación de los lineamientos establecidos en la Entidad para la gestión de riesgos de Seguridad y Privacidad de la Información, contribuyendo al logro de los objetivos, la misión y la visión institucionales.
- Definir y establecer la estrategia de seguridad digital de la entidad.

3. ALCANCE

El Plan de Tratamiento incluye los riesgos de Seguridad de la Información que se encuentren en los niveles moderado, alto y extremo, acorde con los lineamientos definidos en la política de riesgos del DANE. Todos, aquellos clasificados en niveles inferiores tendrán tratamiento de aceptación por parte de la Entidad. Lo contenido en este plan será aplicable a todos los procesos del DANE.

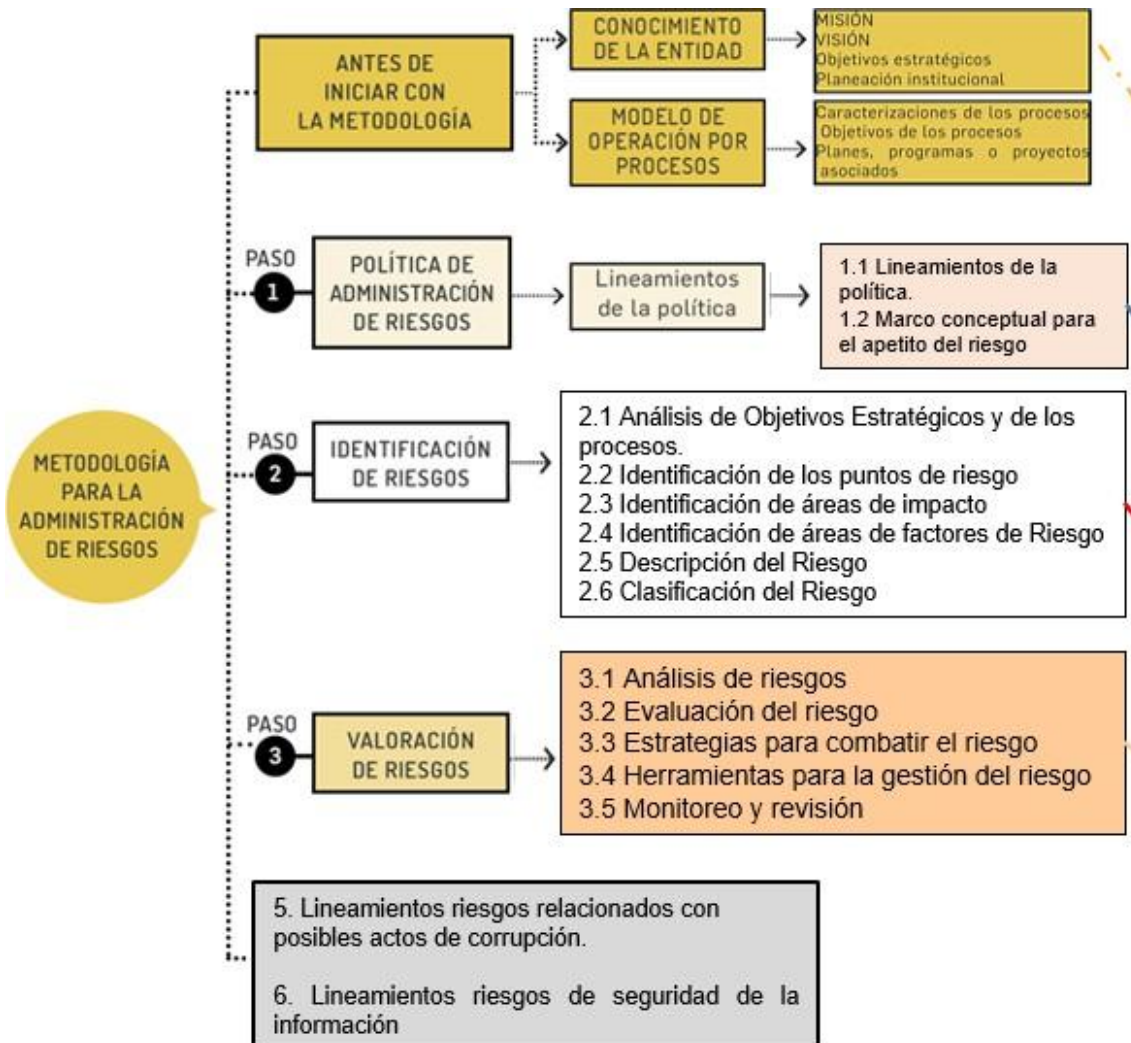
4. DOCUMENTOS DE REFERENCIA

Política de Administración de riesgos: La Alta Dirección e integrantes del nivel directivo de la Entidad se comprometen a administrar los riesgos de gestión, corrupción y fraude, fiscales, de seguridad y privacidad de la información de los procesos de contratación, estableciendo lineamientos que orienten el direccionamiento estratégico y la gestión institucional a evitar su materialización, de forma que se asegure el rigor y la calidad en la producción estadística; así mismo, a asignar los recursos pertinentes que se requieran para la prevención y el tratamiento adecuado de los riesgos.

Metodología para la administración de riesgos: El marco metodológico de la administración de riesgos en el DANE y FONDANE se desarrolla en tres grandes etapas: el establecimiento de la política de administración de riesgos, la identificación de riesgos y la valoración de riesgos, como se muestra en la imagen 1.

Así mismo, las actividades que conforman estas etapas se operativizan a través de documentos y herramientas (procedimientos, guías, formatos) que permiten identificar, valorar y monitorear los riesgos de gestión, de corrupción y fraude, fiscales y de seguridad de la información, que se encuentran dispuestas para consulta en la plataforma tecnológica ISOLUCIÓN <https://dane.isolucion.co/frmHome.apx>.

Imagen 1: metodología para la administración del riesgo



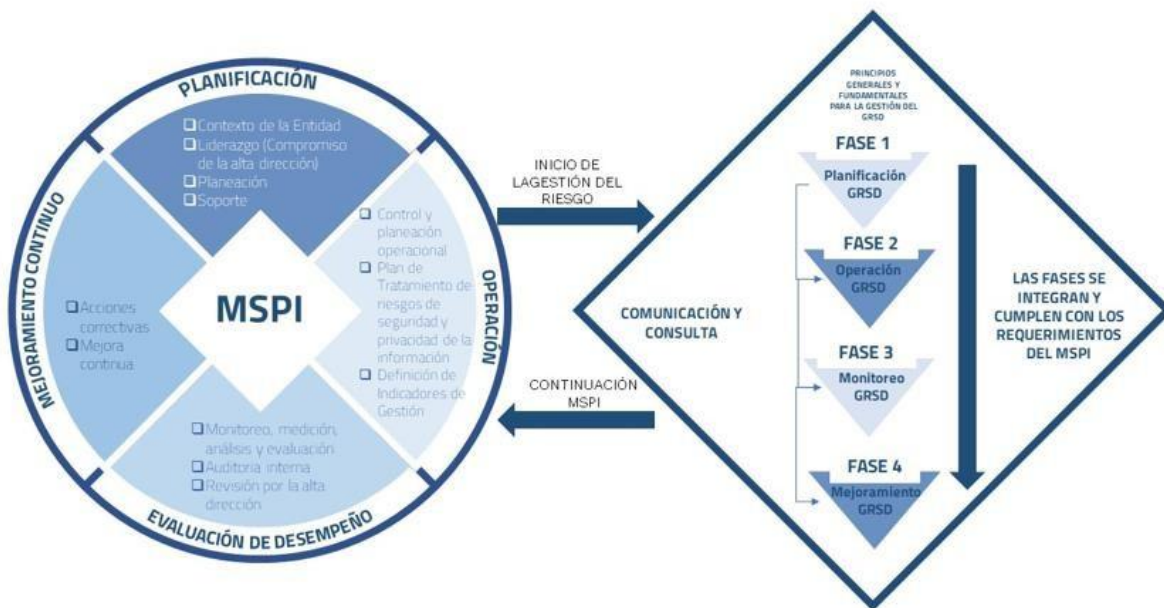
Fuente: presentación Gestión de riesgos Función Pública

Metodología para la identificación de Riesgos de Seguridad de la Información:

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

1. Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.
2. Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.
3. Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de EVALUACIÓN DEL DESEMPEÑO del MSPI.
4. Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

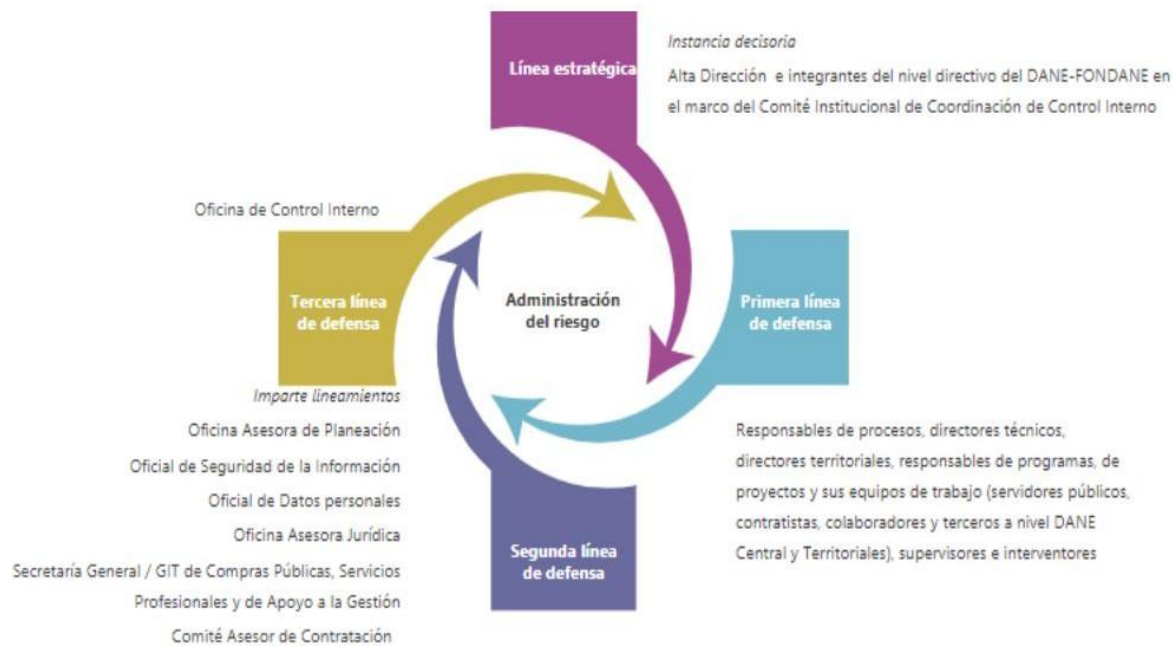
Imagen 2: Integración del modelo de seguridad y privacidad de la Información (MSPI) en el Modelo Nacional de Gestión del Riesgo de Seguridad de la Información (GRSD)



FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Gobernanza de la Administración del Riesgo:

Imagen 3: Gobernanza de la administración del Riesgo DANE



Fuente: Adaptado del Departamento Administrativo de la Función Pública. (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 6.

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la proyección del plan, se toma como insumo de entrada el trabajo de identificación y valoración de riesgos adelantado en versión 6 en la matriz denominada "Identificación y valoración de riesgos de seguridad de la información SIO-040-PDT-002-f-003" por cada proceso, obteniendo los siguientes resultados:

Se identifican un total de cuarenta y seis (46) riesgos de seguridad de la información de acuerdo con su nivel de valoración así:

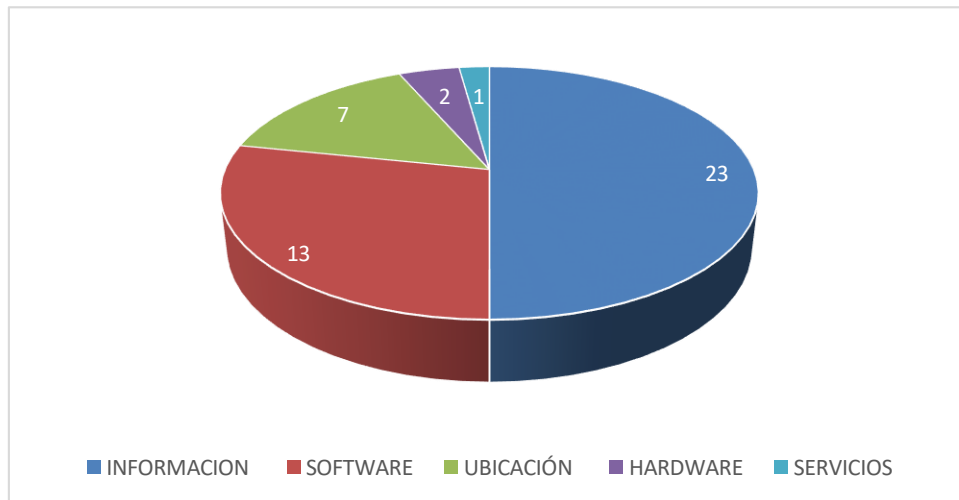
Extrema	Alta	Moderada	Baja	Total
4	2	32	8	46

A continuación, se relacionan los riesgos identificados por proceso y tipo de activo:

PROCESO	INFORMACIÓN	SOFTWARE	UBICACIÓN	HARDWARE	SERVICIOS
REGULACION	1	1			
COMUNICACIONES	4				
CALIDAD ESTADISTICA	1	1			
CONTROL INTERNO	1	1			
DIRECCIONAMIENTO ESTRATEGICO	1	1			
BIENES Y SERVICIOS	1		2	1	
CAPACIDADES E INNOVACION	1				
CONTRACTUAL	1	1	1		
DOCUMENTAL	2		2		
FINANCIERA	1	1			
JURIDICA	2		1		
PROVEEDORES DE DATOS	1	1			
TRANSFORMACIÓN DIGITAL	3	3		1	1
TALENTO HUMANO	1	1	1		
PRODUCCION ESTADISTICA	1	1			
SINERGIA ORGANIZACIONAL	1	1			
TOTAL	23	13	7	2	2

Fuente: consolidada información de riegos V6"Identificación y valoración de riesgos de seguridad de la información SIO-040-PDT-002-f-003"
DANE 2024

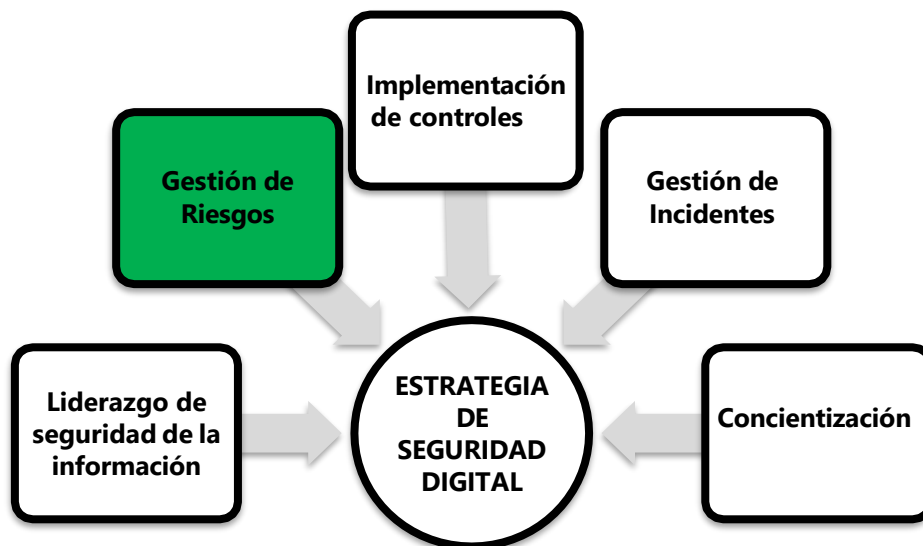
Imagen 4: Riesgos Seguridad de la Información por tipo de Activo DANE 2024



Fuente: consolidada información de riesgos V6"Identificación y valoración de riesgos de seguridad de la información SIO-040-PDT-002-f-003" DANE 2024

6. ESTRATEGIA DE GESTIÓN DE RIESGOS

La estrategia de Gestión de Riesgos se encuentra articulada en el Plan de seguridad y privacidad de la información 2025, en el cual se definen 5 estrategias específicas en torno a la seguridad digital:



Fuente: Ministerio de Tecnologías de La Información y Las Comunicaciones; producto tipo Plan... caja de herramientas.

6.1 Portafolio de proyectos / Actividades:

Para la estrategia de Gestión de Riesgos de seguridad y privacidad de la información, el Departamento Administrativo Nacional de Estadística - DANE y el Fondo Rotatorio del Departamento Administrativo Nacional de Estadística – FONDANE define los siguientes proyectos y productos esperados:

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
Liderazgo de seguridad de la información	1. Revisión del diseño e implementación de indicadores de gestión de seguridad de la información	Indicadores de gestión de seguridad de la información	Oficina Asesora de Planeación (Oficial de seguridad de la información)
Gestión de riesgos	2. Gestión segunda línea de defensa Riesgos: Hacer seguimiento a las actividades de control y los planes de tratamiento implementados por los procesos en su matriz de riesgos de seguridad de la información.	Reporte de seguimiento de riesgos de seguridad de la información	Oficina Asesora de Planeación (Oficial de seguridad de la información)
	3. Actualización del BIA (Análisis de Impacto Empresarial) teniendo en cuenta los cambios organizacionales.	BIA del DANE actualizado	Oficina de Sistemas
	4. Revisión, y de ser necesario, actualización del procedimiento y guía del Inventario de activos.	Procedimiento y guía de inventario de activos	Oficina Asesora de Planeación (Oficial de seguridad de la información)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	5. Revisión y de ser pertinente actualización del Inventario de activos	Inventario de activos de Información actualizado	Oficina Asesora de Planeación (Oficial de seguridad de la información) Dependencias
	6. Revisión, y de ser necesario, actualización del procedimiento y guía de administración de riesgos conforme con la guía para la gestión integral del riesgo en entidades públicas del DAFP- Versión 7	Procedimiento y guía de administración de riesgos	Oficina Asesora de Planeación (Oficial de seguridad de la información)
Concientización	7. Jornadas de sensibilización. Realizar jornadas de sensibilización frente a seguridad de la información a todos los servidores.	Evidencias de las actividades de sensibilización desarrolladas y Listas de asistencia	Oficina de Sistemas - Oficina Asesora de Planeación (Oficial de seguridad de la información)
Implementación de controles	8. Revisión, y de ser necesario, actualización del SOA (declaración de aplicabilidad), en concordancia con la actualización de la matriz de riesgos de seguridad de la información, alineado con la normativa y estándares vigentes de la ISO/EC 27001.	SOA Actualizado	Oficina de Sistemas - Oficina Asesora de Planeación (Oficial de seguridad de la información)- Secretaría General
Gestión de incidentes	9. Monitoreo de los eventos de seguridad de la información para prevenir incidentes que afecten los servicios de la OSIS, incluyendo su impacto, causas y acciones tomadas.	Informe ejecutivo de gestión de eventos de seguridad	Oficina de Sistemas

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	10. Implementación de los procedimientos de continuidad de negocio: Dinamizar la documentación de los BIA por productos crítico.	Procedimientos de Continuidad de Negocio de productos críticos	Oficina Asesora de Planeación (Oficial de seguridad de la información) Dependencias.
	11. Realizar pruebas de recuperación a un sistema de información crítico	Informe de pruebas de recuperación	Oficina de Sistemas

Nota: el presupuesto reflejado en este numeral corresponde a la proyección del costo asociados al talento humano involucrado en el desarrollo de los proyectos y a la atención del sistema de gestión de seguridad de la información desde los recursos de presupuesto de funcionamiento e inversión en PETI.

6.2 Cronograma de actividades / Proyectos:

Evidenciar la ejecución de cada uno de los proyectos previstos:

Proyecto	Ene	Feb	Mar	Abr	May	Jun	Jul	Ag	Sep	Oct	Nov	Dic	Fecha de Terminación
1													Diciembre 31
2													Diciembre 31
3													Junio 30
4													Diciembre 31
5													Diciembre 31
6													Diciembre 31
7													Diciembre 31
8													Diciembre 31
9													Diciembre 31
10													Diciembre 31
11													Diciembre 31

6.3 Análisis presupuestal:

AÑO 2026			
No	Proyecto	Tipo de recurso /Origen de recursos	Presupuesto proyectado
1	Actualización de indicadores de gestión de seguridad de la información	Personal OPLAN/ funcionamiento	\$ 21.490.000
2	Seguimiento a las actividades de control y los planes de tratamiento implementados por los procesos	Personal OPLAN / funcionamiento	\$ 20.892.000
3	Actualización del BIA	Personal OPLAN/ inversión	\$ 31.506.000
4	Actualización procedimiento y guía del Inventario de activos	Personal OPLAN/ funcionamiento	\$ 21.350.608
5	Actualización del Inventario de activos	Personal OPLAN/ funcionamiento	\$ 21.658.231
6	Actualización procedimiento y guía de administración de riesgos	Personal OPLAN/ funcionamiento	\$ 21.593.300
7	Jornadas de sensibilización frente a seguridad de la información	Personal OSIS/ inversión	\$ 21.004.000
8	Actualización del SOA	Personal OSIS/ inversión	\$ 52.510.000

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

9	Monitoreo de los eventos de seguridad de la información	Personal / funcionamiento	\$ 2.330.798.816
10	Documentación de los procedimientos de continuidad de negocio	Personal OPLAN/ funcionamiento	\$ 22.868.957
11	Realizar pruebas de recuperación a un sistema de información crítico	Personal OSIS/ inversión	\$ 47.200.140
TOTAL, PRESUPUESTO AÑO 2026		\$ totalizar el valor \$ 2.612.872.052	

Nota: el presupuesto reflejado en este numeral corresponde a la proyección del costo empleado para la atención del sistema de gestión de seguridad de la información con base al personal disponible y los recursos de presupuesto de funcionamiento e inversión en PETI.