



**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 2025

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, 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 institucional 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.

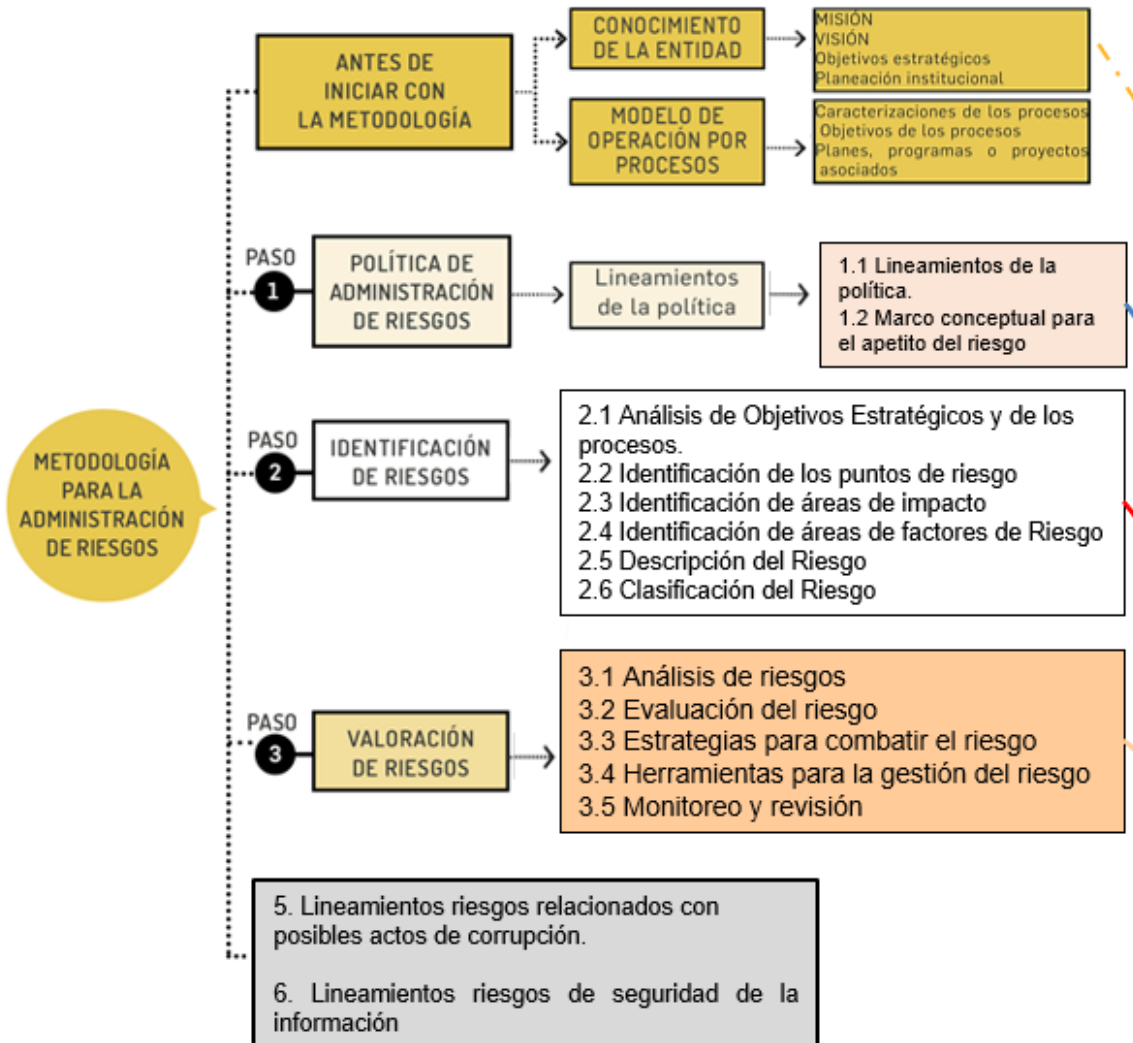
4. DOCUMENTOS DE REFERENCIA

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 encuentran dispuestas para consulta en la plataforma tecnológica ISOLUCIÓN <https://dane.isolucion.co/frmHome.apx>.

Imagen 1: metodología para la administración del riesgo



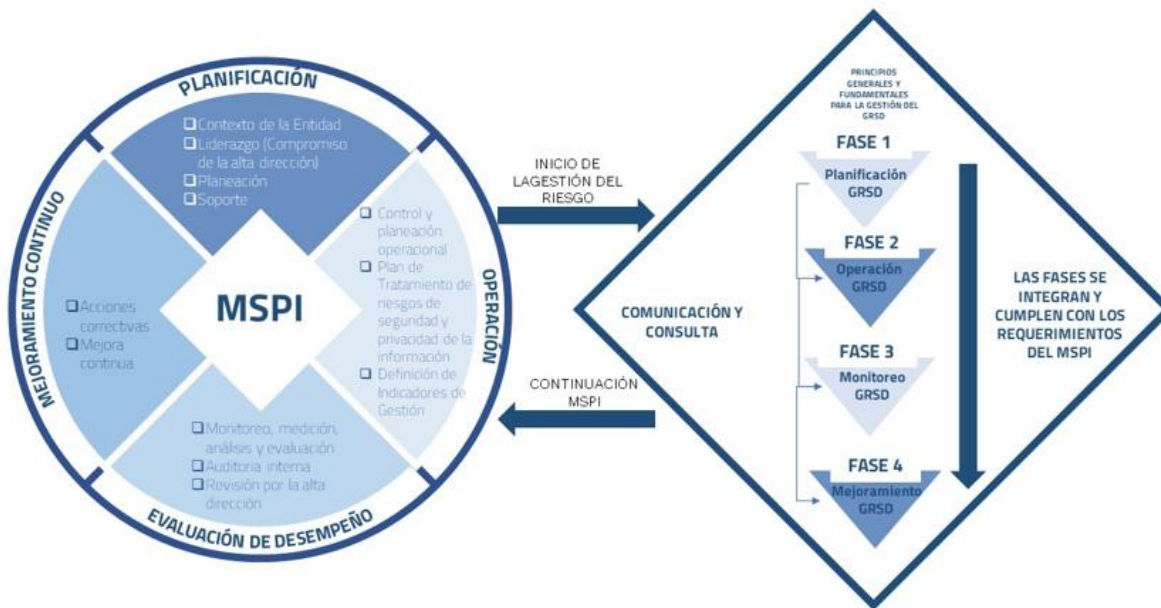
Fuente: presentación Gestión de riesgos Función Pública

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.

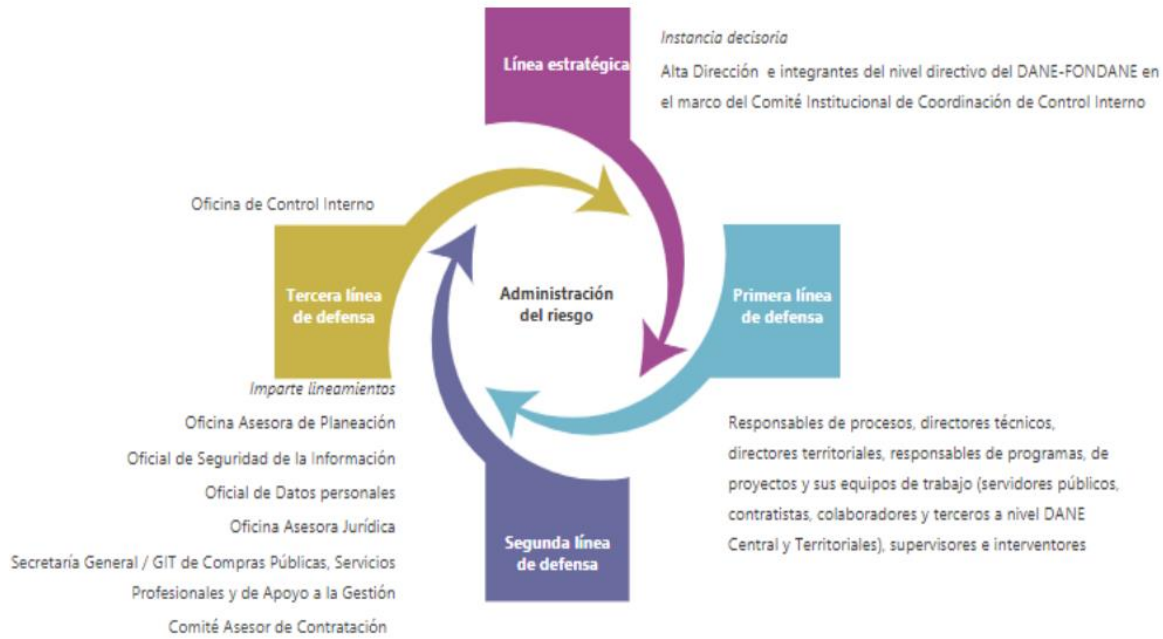
Imagen 2: Integración del modelo de seguridad y privacidad de la Información (MSPI) en el Modelo Nacional de Gestión del Riesgo de Seguridad de la Información (GRSD)



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 la siguiente información al respecto:

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

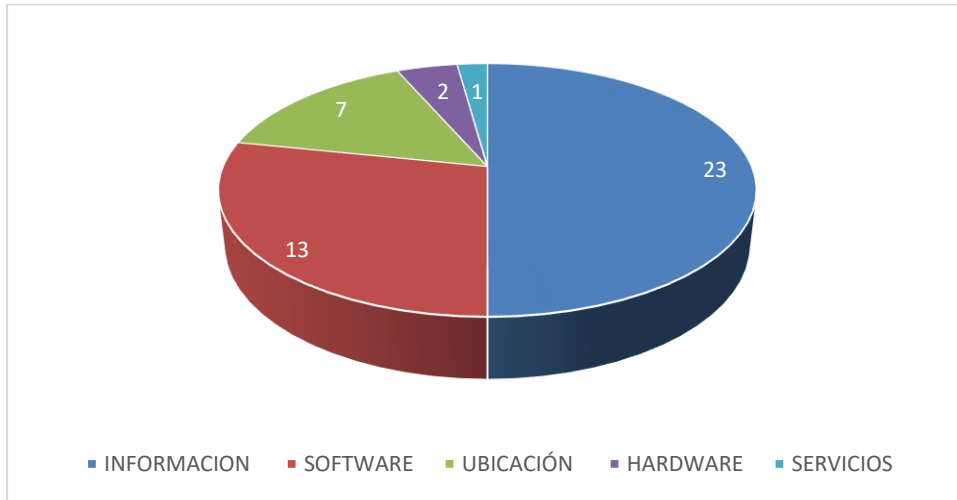
Extrema	Alta	Moderada	Baja	Total
4	2	32	8	46

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

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

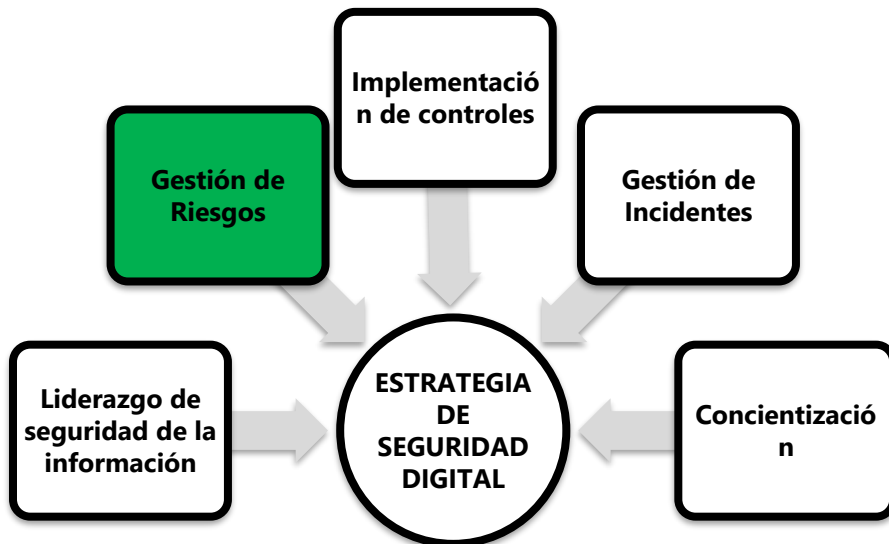
Imagen 4: Riesgos Seguridad de la Información por tipo de Activo DANE 2024



Fuente: consolidado 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 GESTION DE RIESGOS

La estrategia de Gestión de Riesgos, se encuentra articulada en el Plan de seguridad y privacidad de la información 2025; 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 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 la seguridad de la información	1 CSIRT: Adelantar la planificación y diseño del CSIRT Sectorial DANE- IGAC (equipo de respuesta a incidentes de seguridad informática)	Conformación del CSIRT Sectorial	Oficina de Sistemas -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.	Matriz de riesgos con seguimientos	Oficina Asesora de Planeación (Oficial de seguridad de la información)
	3 Actualización SOA: Actualización de la declaración de aplicabilidad, en concordancia con la actualización de la matriz de riesgos alineado con la normativa y estándares vigentes de la ISO/EC 27001.	SOA (declaración de aplicabilidad) Actualizado	Oficina de Sistemas -Oficina Asesora de Planeación (Oficial de seguridad de la información)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
Gestión de incidentes	4. Registrar en caso de que se presenten, de manera detallada y oportuna todos los incidentes que afecten los servicios de la OSIS, incluyendo su impacto, causas y acciones tomadas.	Registro de incidentes de servicios de TI, en caso de que se presenten	Oficina de Sistemas
	5. Sensibilización incidentes: Sensibilizar al personal en la gestión de incidentes de seguridad de la información.	Registro de sesiones de sensibilización desarrolladas.	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 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:

de 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													dic-31
2													dic-31
3													sep-30
4													dic-31
5													oct-31

6.3 Análisis presupuestal:

AÑO 2025			
No	Proyecto	Tipo de recurso /Origen de recursos	Presupuesto proyectado
1	Diseño y planificación CSIRT	Colaboradores OPLAN / funcionamiento	\$ 17.879.887,93
2	Acompañamiento Riesgos	Colaboradores OPLAN/ funcionamiento	\$ 9.752.666,14
3	Actualización (declaración aplicabilidad) SOA de	Colaboradores OSIS- OPLAN	\$ 3.250.888,71
4	Incidentes	Colaboradores OSIS/servicios TI (programas articulados al PETI)	\$ 1.408.853.670,00
5	Sensibilizaciones incidentes	Servidores OSIS/	\$ 1.625.444,36
TOTAL PRESUPUESTO AÑO 2025			\$ 1,441,362,557