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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN V.1

OFICINA ASESORA DE PLANEACIÓN
OFICINA DE SISTEMAS

Enero de 2026

CONTENIDO

1. JUSTIFICACIÓN

En cumplimiento de los lineamientos establecidos en los Decretos 1078 de 2015 artículo 2.2.9.1.2.2 y 612 de 2018, en la Resolución 500 de 2021 (MSPI), Normas ISO/IEC 27001:2022, y Manual de Gobierno Digital, el Departamento Administrativo Nacional de Estadística - DANE y el Fondo Rotatorio del Departamento Administrativo Nacional de Estadística – FONDANE elaboran el Plan de Seguridad y Privacidad de la Información, que permite mitigar los riesgos de seguridad de la información a los que se encuentra expuesta la entidad, a través de la implementación de estrategias de seguridad digital para proteger los sistemas y servicios y garantizar que las operaciones estadísticas y administrativas se lleven a cabo de una manera segura y confiable.

2. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Departamento Administrativo Nacional de Estadística – DANE y el Fondo Rotatorio del Departamento Administrativo Nacional de Estadística – FONDANE, para reducir los riesgos de seguridad de la información a los que está expuesta la entidad hasta niveles aceptables.

2.1. Objetivos específicos

- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información-SGSI. Identificar, analizar y evaluar los puntos críticos o problemas relacionados con la seguridad de la información de la entidad).
- Priorizar los proyectos a desarrollar para la correcta implementación del SGSI. (Definir estrategias de seguridad digital y acciones concretas y priorizadas que aseguren la protección de los sistemas internos de información).
- Planificar la evaluación y seguimiento de los controles y lineamientos a implementar en el marco del SGSI (Elaborar un plan de trabajo o cronograma para aplicar las estrategias y acciones definidas) –
- Definir y establecer la estrategia de seguridad digital de la entidad. (Evaluar los resultados de las estrategias de seguridad digital y acciones aplicadas y determinar su efectividad)

3. ALCANCE

El Plan de Seguridad de la Información al buscar la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSI 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 entidad.

4. DOCUMENTOS DE REFERENCIA

El Plan de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Artículo 2.2.9.1.2.2: lineamientos, guías y estándares para facilitar la comprensión, sistematización e implementación integral de la Política de Gobierno Digital.

- 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 que se constituye el 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".

- Normas ISO/IEC 27001:2022: es la norma para sistemas de gestión de la seguridad de la información (SGSI) y define los requisitos que debe cumplir un SGSI.

- Manual de Gobierno Digital – MINTIC.Modelo de Seguridad y Privacidad de la Información – MINTIC.

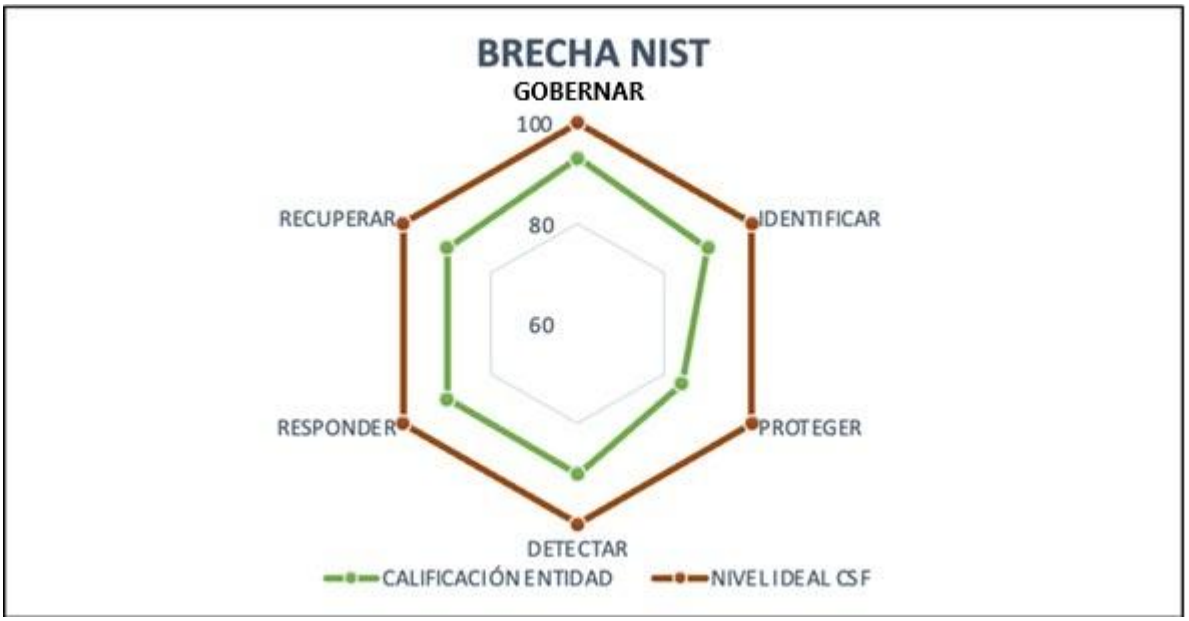
5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Para la proyección del plan se toma como insumo de entrada para identificar las necesidades institucionales, el informe de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información; los siguientes son los resultados entregados de la evaluación a la efectividad de los controles de seguridad de la información, identificados mediante el Instrumento de Evaluación MSPI 2025 del MinTIC, con su respectiva calificación, con el fin de determinar el nivel de madurez alcanzado en la gestión de la seguridad de la información.

TABLA 1: EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	90	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	93	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	84	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	78	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

Fuente: informe definitivo de seguimiento a la evaluación del modelo de seguridad y privacidad de la información



Fuente: Instrumento de identificación de la línea base de seguridad hoja portada- DANE.

La entidad obtuvo una calificación de 96,6 sobre 100 en la política de seguridad digital, según la evaluación del Formulario Único de Reporte de Avance a la Gestión (FURAG) 2024, establecida por el Departamento Administrativo de la Función Pública (DAFP). Además, en el componente de seguridad y privacidad de la información de la política de Gobierno Digital alcanzó una calificación de 88,1 sobre 100. A continuación, se describen recomendaciones publicadas por el DAFP para mejorar los resultados:

TABLA 2: Recomendaciones FURAG 2024 DANE

Función Pública

mipg modelo integrado de planeación y gestión

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA

RECOMENDACIONES FURAG VIGENCIA 2024

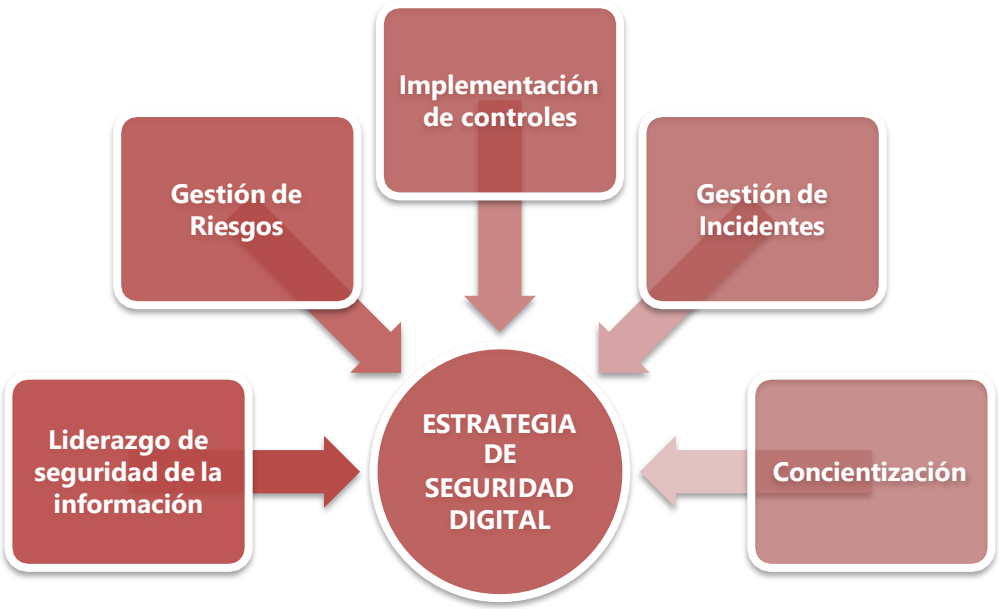
Entidad		
20	DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADISTICA	NACION

Política	Recomendación	Índice
Seguridad Digital	Realizar pruebas de recuperación de cada uno de los sistemas de información críticos de la entidad.	POL09
Seguridad Digital	Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.	POL09
Gobierno Digital	Realizar auditorías internas, externas y de certificación o recertificación respecto al estándar ISO 27001 en la entidad.	POL10

Fuente FURAG 2024-DAFP-Recuperado de:
https://www1.funcionpublica.gov.co/web/mipg/resultados-medicion

6. ESTRATEGIA DE SEGURIDAD DIGITAL

La Entidad define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



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

6.1. 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:

TABLA 3: Descripción Estrategias

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.
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.

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

6.2. Portafolio de proyectos / Actividades

Para cada estrategia específica, 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, 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	RESPONSABLE
Liderazgo de seguridad de la información	1. Revisión, y de ser necesario, actualización del manual de Políticas de Seguridad de la Información DANE – FONDANE	Manual de Políticas de Seguridad de la Información DANE - FONDANE	Oficina Asesora de Planeación (Oficial de seguridad de la información)
	2. 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	3. 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)
	4. Actualización del BIA (Análisis de Impacto Empresarial) teniendo en cuenta los cambios organizacionales.	BIA del DANE actualizado	Oficina de Sistemas
	5. 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)
	6. 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

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	7. 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)
	8. Realizar auditoría interna a la implementación del MSPI*	Informe de auditoría al MSPI	Oficina de Control Interno
Concientización	9. 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	10. 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	11. 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

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

* La auditoría en referencia da cumplimiento al nuevo modelo de seguridad y privacidad de información emitido por MINTIC y es la misma auditoría plasmada el Plan Anual de Auditorías formulado por la Oficina de Control Interno - OCI.

6.3 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													Diciembre 31
4													Junio 30
5													Diciembre 31
6													Diciembre 31
7													Diciembre 31
8													Diciembre 31
9													Diciembre 31
10													Diciembre 31
11													Diciembre 31
12													Diciembre 31
13													Diciembre 31

6.4. Análisis presupuestal:

AÑO 2026			
No	**Proyecto**	**Tipo de recurso /Origen de recursos**	**Presupuesto proyectado**
1	Actualización del manual de Políticas de Seguridad de la Información DANE - FONDANE	Personal OPLAN/ funcionamiento	$ 21.593.300
2	Actualización de indicadores de gestión de seguridad de la información	Personal OPLAN/ funcionamiento	$ 21.490.000
3	Seguimiento a las actividades de control y los planes de tratamiento implementados por los procesos	Personal OPLAN / funcionamiento	$ 20.892.000
4	Actualización del BIA	Personal OPLAN/ inversión	$ 31.506.000
5	Actualización procedimiento y guía del Inventario de activos	Personal OPLAN/ funcionamiento	$ 21.350.608
6	Actualización del Inventario de activos	Personal OPLAN/ funcionamiento	$ 21.658.231
7	Actualización procedimiento y guía de administración de riesgos	Personal OPLAN/ funcionamiento	$ 21.593.300
8	Auditoría interna a la implementación del MSPI	Personal OCI/ funcionamiento	$21.300.000
9	Jornadas de sensibilización frente a seguridad de la información	Personal OSIS/ inversión	$ 21.004.000
10	Actualización del SOA	Personal OSIS/ inversión	$ 52.510.000

AÑO 2026			
11	Monitoreo de los eventos de seguridad de la información	Personal / funcionamiento	$ 2.330.798.816
12	Documentación de los procedimientos de continuidad de negocio	Personal OPLAN/ funcionamiento	$ 22.868.957
13	Realizar pruebas de recuperación a un sistema de información crítico	Personal OSIS/ inversión	$ 47.200.140
TOTAL PRESUPUESTO AÑO 2026		**$ totalizar el valor** $ 2.655.765.352	

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.

7. RESPONSABLES

1. Representante legal de la entidad: aprobar los documentos de alto nivel.
2. Secretario (a) general: velar por la implementación del MSPI y garantizar los recursos requeridos.
3. Responsable de segurida digital / jefe de OPLAN: Coordinar las actividades de implementación del MSPI
4. Áreas de la entidad: participar en la implementación del MSPI, asegurando la integración de las estrategias de seguridad digital en los procesos institucionales.