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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA ASESORA DE PLANEACIÓN
OFICINA DE SISTEMAS - SECRETARIA GENERAL

Enero de 2025

CONTENIDO

1. JUSTIFICACIÓN

El presente plan se elabora en cumplimiento de los lineamientos establecidos en los Decretos 1078 de 2015 artículo 2.2.9.1.2.2 y 612 de 2018, dentro de los cuales se exige la elaboración por parte del Departamento Administrativo Nacional de Estadística y el Fondo Rotatorio del Departamento Administrativo Nacional de Estadística – FONDANE de un Plan de Seguridad y Privacidad de la Información, que permita mitigar los riesgos a los que se encuentra expuesta la organización: a través de la implementación de estrategias de seguridad digital.

2. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Departamento Administrativo Nacional de Estadística y el Fondo Rotatorio del Departamento Administrativo Nacional de Estadística – FONDANE, 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 la vigencia 2025.

2.1 Objetivos específicos

- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a desarrollar 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.
- Definir y establecer la estrategia de seguridad digital de la entidad.

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 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.

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 definitivo de Seguimiento a la Evaluación del Modelo de Seguridad y Privacidad de la Información remitido por la Oficina de control interno el día 31 de diciembre de 2024; 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 2023 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**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	93	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	88	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	92	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	80	100	**GESTIONADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	96	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	91	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	82	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	89	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	**GESTIONADO**
A.18	CUMPLIMIENTO	100	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**92**	**100**	**OPTIMIZADO**

Fuente: informe definitivo de seguimiento a la evaluación del modelo de seguridad y privacidad de la información Oficina de Control Interno DANE

Fuente: Instrumento de identificación de la línea base de seguridad hoja portada; basada en información informe OCI DANE.

Para ampliar el panorama de la situación de la entidad a continuación se relaciona la evaluación del autodiagnóstico FURAG 2023, en el componente de Seguridad y privacidad de la información

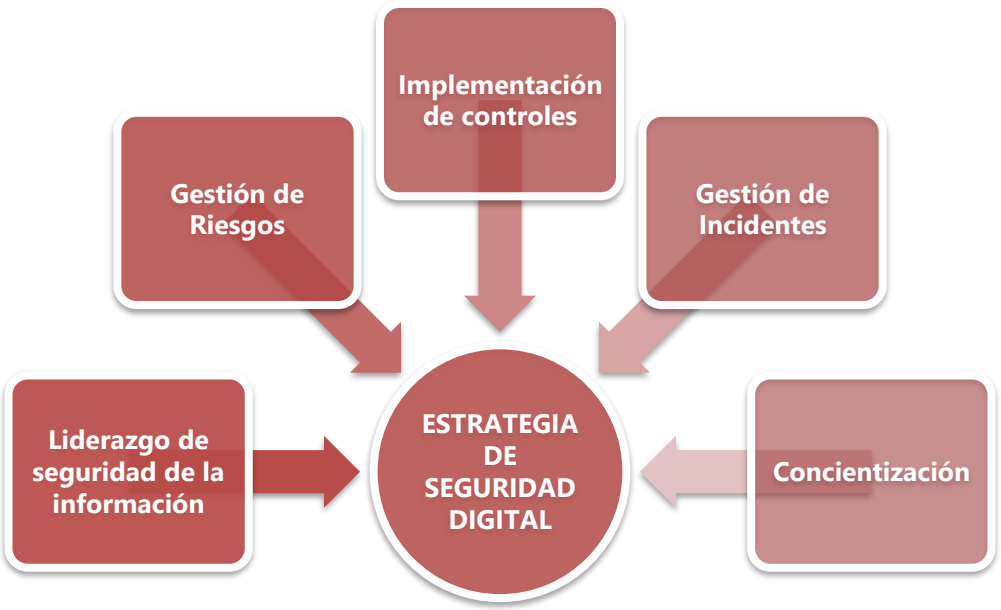
TABLA 2: Autodiagnóstico FURAG 2023 DANE

NO. INDICE	COMPONENTE	POLITICA GOBIERNO DIGITAL	% DE CUMPLIMIENTO		#	GUÍAS, NORMAS Y TÉCNICAS	ACCIONES DE MEJORA
I13	HABILITADOR	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		81,82	1	https://gobiernodigital.mintic.gov.co/portal/Transformate-con-Gobierno-Digital-/Caja-de-herramientas/#data=%7B%22filter%22:%2247254%22,%22page%22:1%7D	Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI).
					2	https://gobiernodigital.mintic.gov.co/692/articles-176924_recurso_1.xlsx	Elaborar un diagnóstico de seguridad y privacidad de la información para la entidad a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). Posteriormente, presentar y lograr la aprobación del diagnóstico en el Comité de Gestión y Desempeño Institucional.
					3	https://gobiernodigital.mintic.gov.co/692/articles-272944_recurso_1.zip	Implementar en la entidad el plan de tratamiento de riesgos de seguridad de la información.
					4	https://www.colcert.gov.co/800/w3-article-198656.html	Reportar los incidentes de seguridad digital de la entidad, acorde con lo establecido en la Resolución 500 de 2022.
					5	https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf	Realizar pruebas de recuperación de la información y continuidad a todos los sistemas críticos de la entidad.
					6	https://colcert.gov.co/800/w3-channel.html	Realizar el análisis de vulnerabilidades de seguridad de los activos de información de la entidad (hardware, software, aplicaciones, redes) de la mano del CSIRT Gobierno, ColCert o un CSIRT sectorial.

Fuente Autodiagnóstico 2023 FURAG, Oficina asesora de planeación DANE.

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 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 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)
	2 Actualización Plan de continuidad de negocio: Gestionar la actualización del plan de continuidad de negocio del DANE atendiendo al trabajo de las matrices de riesgos en versión 6.	Plan de Continuidad de Negocio del DANE actualizado	Oficina de Sistemas - Oficina Asesora de Planeación (Oficial de seguridad de la información)
	3 Procedimientos continuidad de negocio: Dinamizar la documentación de los procedimientos de continuidad de negocio por proceso.	Procedimientos de Continuidad de Negocio por proceso	Oficina de Sistemas - Oficina Asesora de Planeación (Oficial de seguridad de la información)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	4 Actualización instrumentos de Gestión: Adelantar la revisión y actualización de instrumentos de gestión de información pública: -Registro de activos de información y su publicación, teniendo en cuenta el nuevo inventario y la actualización de las TRD -Índice de información clasificada y reservada - Esquema de Publicación de Información	Registro de activos de información actualizados Índice de información clasificada y reservada actualizado Esquema de Publicación de Información	Oficina Asesora de Planeación (Oficial de seguridad de la información)
Gestión de riesgos	5 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)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	6 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 Actualizado	Oficina de Sistemas - Oficina Asesora de Planeación (Oficial de seguridad de la información)
Concientización	7 Socializar lo documentos: · Manual de Políticas de Seguridad de la Información DANE-FONDANE V.1 (SIO-030-MAN-001-Versión · Procedimiento Gestión de Activos de Información V.1 (SIO-040-PDT-008-Versión 1)	Evidencias de actividades de despliegue	Oficina Asesora de Planeación (Oficial de seguridad de la información)
	8 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)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
	9 Transferencia de conocimiento. Realizar gestiones para la trasferencia de conocimiento a colaboradores de la Entidad en diferentes temas de ciberseguridad.	Evidencias de las actividades para transferencia de conocimiento desarrolladas	Oficina de Sistemas
	10 Medición: Medir el grado de sensibilización a toda la Entidad.	Resultado de la encuesta de medición	Oficina Asesora de Planeación (Oficial de seguridad de la información)
Implementación de controles	11 Etiqueta Inventario de activos Territoriales: Adelantar el trabajo para identificación, valoración y etiquetado al inventario DANE de los activos de información de las Direcciones Territoriales y sus sedes.	Inventario de activos de Información actualizado y etiquetado.	Oficina Asesora de Planeación (Oficial de seguridad de la información)

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS	RESPONSABLE
Gestión de incidentes	12 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
	13 Sensibilización incidentes: Sensibilizar al personal en la gestión de incidentes de seguridad de la información.	Registro de sesiones de sensibilización desarrolladas.	Oficina de Sistemas

6.3 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													Diciembre 31
2													Mayo 31
3													Diciembre 31
4													Diciembre 31
5													Diciembre 31
6													Septiembre 30
7													Junio 30
8													Noviembre 30
9													Noviembre 30
10													Diciembre 31
11													Septiembre 30
12													Diciembre 31
13													Octubre 31

6.4 Análisis presupuestal:

AÑO 2025			
No	**Proyecto**	**Tipo de recurso /Origen de recursos**	**Presupuesto proyectado**
1	CSIRT	Colaboradores OPLAN / funcionamiento	$ 17.879.887
2	Modificación Plan de continuidad de negocio	Colaboradores/ funcionamiento	$ 4.876.333
3	Procedimientos continuidad de negocio	Colaboradores OPLAN/ funcionamiento	$ 14.628.999
4	Actualización instrumentos de Gestión	Colaboradores OPLAN / funcionamiento	$ 16.254.443
5	Acompañamiento Riesgos	Colaboradores OPLAN/ funcionamiento	$ 9.752.666
6	Actualización SOA	Colaboradores OPLAN - OSIS	$ 3.250.888
7	Socializar Documentos	Colaboradores OPLAN y recursos digitales DANE / funcionamiento	$ 3.250.888
8	Jornadas de sensibilización	Colaboradores OPLAN y recursos digitales DANE(Sharepoint-Danenet / funcionamiento	$ 8.127.221

AÑO 2025			
9	Transferencia de conocimiento	Colaboradores OSIS/ OPLAN	$ 3.250.888
10	Medición	Colaboradores y recursos digitales DANE(Sharepoint-Danenet / funcionamiento	$ 1.625.444
11	Inventario Territoriales	Colaboradores OPLAN/ funcionamiento	$ 14.628.999
12	Osis incidentes	Colaboradores OSIS/servicios TI (proyectos articulados al PETI)	$ 1.408.853.670
13	Sensibilización incidentes	Colaboradores OSIS/	$ 1.625.444
TOTAL PRESUPUESTO AÑO 2025		**$ 1.508.005.775,79**	

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.

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 Seguridad 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