Departamento Nacional de Planeación - **DNP**

PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍA Y SISTEMAS DE LA INFORMACIÓN

DEPARTAMENTO NACIONAL DE PLANEACIÓN
2024

Control de Versiones

Versión	Fecha	Modificación
1.0	12/01/2024	Versión inicial del documento

Tabla de contenido

1. OBJETIVO

Realizar el mejoramiento continuo del componente de gestión de seguridad de la información en el DNP, con fin de mitigar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información digital institucional, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2024

1.1. OBJETIVOS ESPECÍFICOS

- Fortalecer la cultura de seguridad de la información en el DNP a través de la ejecución integral del Plan de capacitación, sensibilización y comunicación durante el año.
- Mejorar la protección y gestión de los activos de información del DNP mediante la actualización periódica de los activos de información y la declaración de aplicabilidad ISO 27001.
- Evaluar y mitigar riesgos de seguridad de la información mediante la realización de ejercicios de ingeniería social en ambos semestres y la actualización del diagnóstico del Anexo de Seguridad Digital conforme a la resolución 1519 de 2020 y la elaboración del documento autodiagnóstico MSPI 2024.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la mejora continua el componente de Gestión de Seguridad de la Información y la estrategia de seguridad digital del DNP, comparte el alcance definido dentro M-PG-07 Manual Operativo de Seguridad de la información y el MC Manual del SIG, donde se indica que el componente de seguridad aplica a todos los procesos de la Entidad incluidos en el Modelo de Operación por procesos.

3.DOCUMENTOS DE REFERENCIA

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

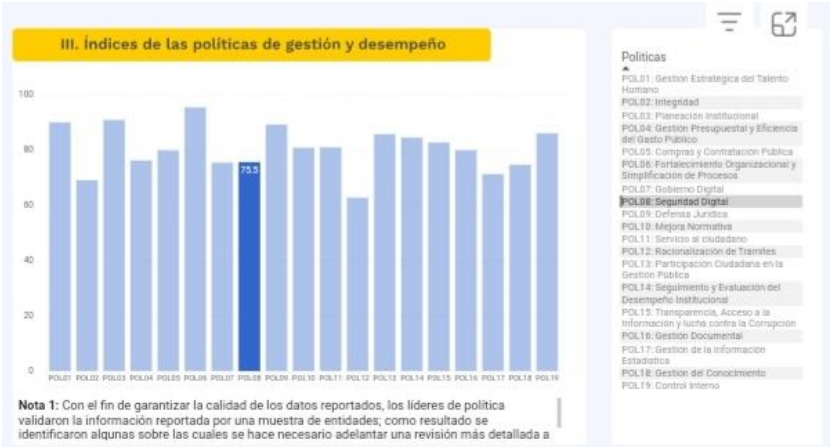
- Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar 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.
- Normativa relacionada con seguridad de la información incluida en el Normograma institucional

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

Como entidad del Gobierno Nacional, el DNP evalúa el cumplimiento de las políticas de Gobierno Digital y Seguridad Digital a través del Formulario Único Reporte de Avances de la Gestión (FURAG) del Modelo Integrado de Planeación y Gestión de la Función Pública, el Índice de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el autodiagnóstico del MSPI.

En el FURAG de 2022, la entidad obtuvo una calificación de 90.4 (gráfica 1) para la política de seguridad digital, superando el promedio nacional de 75.5. (gráfica 2).

Grafica 1. Puntaje de la Politica de Seguridad Digital en DNP año 2022



Grafica 2. Puntaje de la Politica de Seguridad Digital promedio nacional año 2022

En el Índice de Gobierno Digital de 2022, el puntaje para el habilitador de seguridad digital fue de 94.4 (gráfica 3), mientras que el promedio del sector fue de 83.3(gráfica 3) y el promedio nacional de 74.9(gráfica 4).

Grafica 3. Puntaje habilitador de seguridad digital del DNP

Grafica 4. Puntaje habilitador de seguridad digital de las entidades del Sector Gobierno

El puntaje en el autodiagnóstico del Modelo de Seguridad y privacidad del 2022 es de 95.10 y para 2023 es de 95.5.

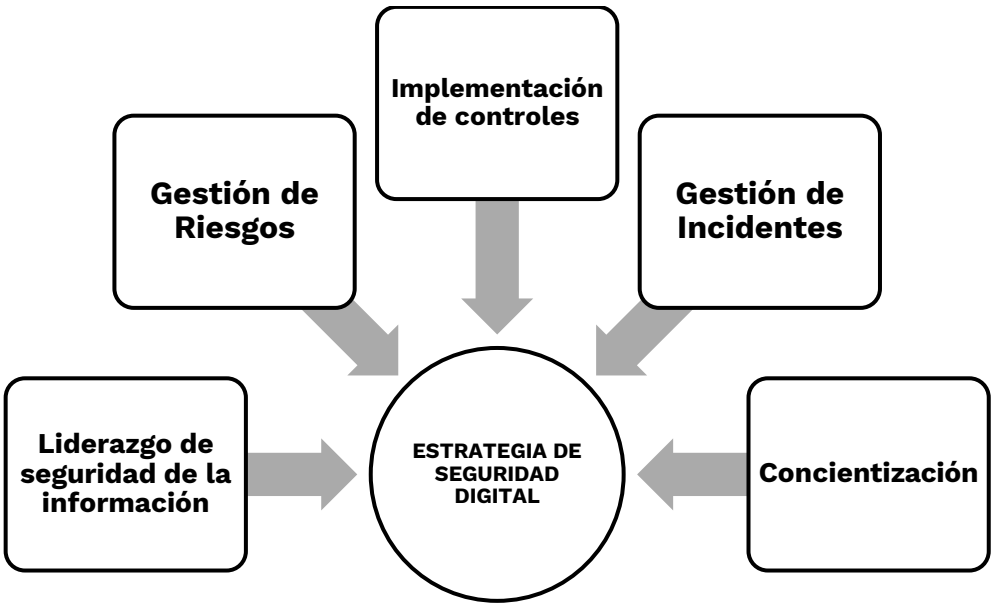
Grafica 5. Puntaje MSPI año 2022

Gráfica 6. Puntaje MSPI año 2023

Estos puntajes demuestran la mejora continua y el compromiso de la Entidad por la implementación de controles y lineamientos en seguridad de la información, seguridad informática y seguridad digital acorde a los lineamientos del Gobierno Nacional.

5. ESTRATEGIA DE SEGURIDAD DIGITAL

En cumplimiento de la Resolución 500 de 2021 la entidad establece una estrategia de seguridad digital que integra los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información MSPI de MINTIC, el procedimiento PT-PG-01 Gestión integral de riesgos y el procedimiento PT-TI-01 Atención a Requerimientos de Servicios TIC que incluye la de gestión de incidentes. Por lo anterior la Entidad adopta las 5 estrategias específicas propuestas por MINTIC, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



Fuente: MINTIC https://gobiernodigital.mintic.gov.co/portal/Biblioteca/#data=%7B%22filter%22:%2247254%22,%22page%22:6%7D

5.1. 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:

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.

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
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: MINTIC https://gobiernodigital.mintic.gov.co/portal/Biblioteca/#data=%7B%22filter%22:%2247254%22,%22page%22:6%7D

5.2. Actividades

Las estrategias se incluyeron en el producto denominado "4. Plan especial de gestión de seguridad y privacidad de la información." que hace parte del plan de acción institucional disponible en https://www.dnp.gov.co/LaEntidad_/Direccion-general/oficina-asesora-planeacion/Paginas/planeacion-institucional.aspx

Nombre_Dependencia	OTSI - OFICINA DE TECNOLOGIAS Y SISTEMAS DE INFORMACIÓN
Nombre_ObjetivoInstitucional	Gestión integral institucional - Posicionar al DNP como referente en gestión institucional articulada, innovadora y efectiva.
Eje Estrategico / Proyecto	5. Fortalecer las capacidades de articulación interna y de gestión integral, hacia la toma de decisiones, para la generación de resultados efectivos y con vocación de servicio hacia los grupos de valor.
NombreCatalogo	PLANEACIÓN Y GESTIÓN ORIENTADA A RESULTADOS
NombreLineaAccion	Administración y mantenimiento del MOP
NombreProcedimiento	Planeación y mantenimiento del MOP
Codigo_Producto	6232
Nombre_Producto	4.Plan especial de gestión de seguridad y privacidad de la información.
Tipo de servicio	Servicio por oferta
Codigo Entregable	17069
Nombre_Entregable	4.Plan especial de gestión de seguridad y privacidad de la información.
DenominacionEntregable	4.Plan especial de gestión de seguridad y privacidad de la información.
Fecha_Inicio	2/01/2024
Fecha_Fin	31/12/2024
ProgramacionMeta	Trimestral
Denominacion	4.Plan especial de gestión de seguridad y privacidad de la información.
Tipo de clasificador	Planes MIPG
ClasificadorProducto	11. MIPG - Seguridad digital

Fuente: Plan de acción Institucional vigencia 2024

5.3. Alineación con los objetivos del componente de seguridad de la información

Las actividades definidas están alineadas a los 4 objetivos específicos del componente de seguridad de la información

Objetivo: Crear una cultura de seguridad de la información, como medida preventiva para mitigar los riesgos que afecten la información digital y ofrecer un lenguaje común sobre de seguridad de la información dentro de la Entidad.

ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	ACTIVIDAD	ENTREGABLE
Concientización	Plan de capacitación, sensibilización y comunicación de seguridad de la información en el DNP	Plan de capacitación, sensibilización y comunicación de seguridad de la información en el DNP

Objetivo: Fortalecer la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC que permita establecer, implementar, monitorear, revisar, mantener y mejorar el Componente de Seguridad de la Información.

ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	ACTIVIDAD	ENTREGABLE
Gestión de riesgos	Declaración de aplicabilidad ISO 27001 actualizada	Declaración de aplicabilidad
Liderazgo de seguridad de la información Implementación de controles	Documento autodiagnóstico MSPI 2024	Instrumento MSPI 2024 e Informe detallado de controles
Liderazgo de seguridad de la información	Actualización del diagnóstico del Anexo de Seguridad Digital en la resolución 1519 de 2020	Fortalecer los controles y las capacidades de ciberdefensa con un enfoque de gestión de riesgos y poder definir en la metodología de riesgos las nuevas amenazas y vulnerabilidades cibernéticas

Objetivo: Fortalecer la gestión de riesgos asociados a la seguridad de la información digital para que sean identificados, valorados, controlados y administrados, de una forma estructurada, repetible, eficiente, documentada y adaptada a los cambios que se produzcan en el entorno y las tecnologías

ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	ACTIVIDAD	ENTREGABLE
Liderazgo de seguridad de la información	Realizar ejercicios de ingeniera social en el primer semestre	Presentación resultada de los ejercicios del primer semestre
Gestión de riesgos	Realizar ejercicios de ingeniera social en el segundo semestre	Presentación resultada de los ejercicios del segundo semestre
Gestión de riesgos Implementación de controles	Revisión de la Matriz Integral de Riesgos para identificar mejoras en los controles de seguridad de la Información	Documento las actividades relacionadas con el monitoreo de segunda línea de defensa

Objetivo: Gestionar la seguridad informática en su componente tecnológico para resguardar su confidencialidad, integridad y disponibilidad, realizando actualizaciones anuales de las políticas y las responsabilidades de los usuarios de acuerdo con las disposiciones legales vigentes aplicables a la utilización de la información digital

ALCANCE ESTRATEGIA DE SEGURIDAD DIGITAL	ACTIVIDAD	ENTREGABLE
Liderazgo de seguridad de la información	Actualización de los activos de información	Actualización Matriz de inventario y clasificación de activos de Información

La estrategia de gestión de incidentes se gestiona con la atención de los incidentes que se reportan mensualmente en el indicador Tratamientos de eventos relacionados con la seguridad y privacidad de la información y en el reporte de los incidentes al Colcert y CSIRT Gobierno según corresponda.

5.4. Cronograma de actividades

La Oficial de seguridad de la información, establece el cronograma de actividades que hace parte del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información que se publican en https://www.dnp.gov.co/LaEntidad_/Direccion-general/oficina-asesora-planeacion/Paginas/planeacion-institucional.aspx. Los donde planes evidencian como se llevarán a cabo cada una de las actividades previstas.

5.4.1. Plan de Seguridad y Privacidad de la Información

No.	Actividad	Fecha Inicio (DD/MM/AAAA)	Fecha Fin (DD/MM/AAAA)	Registro / Soporte	Responsable	Observaciones
1	Ejecutar el Plan de capacitación, sensibilización y comunicación de seguridad de la información en el DNP	1/02/2024	31/12/2024	Campañas y charlas de sensibilización	Oficial de Seguridad de la Información	Ver seguimiento plan de acción
2	Actualizar los activos de información	1/02/2024	31/12/2024	La actualización depende de la actualización de la Tablas de retención documental Catálogo de Infraestructura Crítica Cibernética F-TI-26. Matriz de inventario y clasificación de activos de Información F-PG-26. Registro de Activos de Información Transparencia F-PG-28. Índice de Información Clasificada y Reservada Transparencia F-PG-29 Matriz interna de seguimiento. Soportes Correos electrónicos	Oficial de Seguridad de la Información	Ver seguimiento plan de acción
3	Realizar ejercicios de ingeniera social en el primer semestre	1/04/2024	31/10/2024	Presentación de los resultados de los ejercicios del primer semestre	Oficial de Seguridad de la Información/SOC	Ver seguimiento plan de acción
4	Realizar ejercicios de ingeniera social en el segundo semestre	22/10/2024	31/12/2024	Presentación de los resultados de los ejercicios del Segundo semestre	Oficial de Seguridad de la Información/SOC	Ver seguimiento plan de acción
5	Actualizar la declaración de aplicabilidad ISO 27001	1/09/2024	30/11/2024	Declaración de aplicabilidad	Oficial de Seguridad de la Información	Ver seguimiento plan de acción
6	Realizar documento autodiagnóstico MSPI 2024	1/09/2024	31/12/2024	Instrumento MSPI 2024 e Informe detallado de controles	Oficial de Seguridad de la Información	Ver seguimiento plan de acción
7	Actualizar el diagnóstico del Anexo de Seguridad Digital en la resolución 1519 de 2020	1/04/2024	31/10/2024	Instrumento de Diagnostico Actualizado	Oficial de Seguridad de la Información y Arquitecto SharePoint	Ver seguimiento plan de acción

5.4.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

No.	Actividad	Fecha Inicio (DD/MM/AAAA)	Fecha Fin (DD/MM/AAAA)	Registro / Soporte	Responsable	Observaciones
1	Revisar la Matriz Integral de Riesgos para identificar mejoras en los controles de seguridad de la Información	5/02/2024	30/11/2024	Reuniones con OAP Controles de seguridad actualizados de acuerdo con el Monitoreo cuatrimestral de riesgos los avances se presentan en los informes trimestrales del producto 6232 del plan de acción	Oficial de Seguridad de la Información	Ver seguimiento plan de acción

5.5. Análisis Presupuestal

Las adquisiciones de seguridad de la información que se requieran se gestionan a través del plan anual de adquisiciones disponible en https://www.dnp.gov.co/LaEntidad_/secretaria-general/Subdireccion-contratacion/contratacion/Paginas/plan-anual-de-adquisiciones.aspx y el proyecto de inversión "Fortalecimiento de las tic para el cumplimiento de los objetivos del DNP a nivel Nacional"

6. RESPONSABLES

1. Jefe de la Oficina de Tecnología y Sistemas de la información líder del operacional del componente de seguridad de la información.
2. Oficial de Seguridad de la Información
3. Oficina Asesora de Planeación líder del Sistema Integrado de Gestión
4. Dependencias responsables de la actualización de los activos de información.
5. Líderes técnicos y funcionales responsables del monitoreo de primera línea de defensa de los riesgos de seguridad de la información.

7. APROBACIÓN

Los planes de tratamiento de riesgos de seguridad y privacidad de la información, así como el plan de seguridad y privacidad de la información en los que se basa este documento, fueron presentados para la consideración y revisión de la alta dirección y el comité de gestión y desempeño institucional, con el objetivo de ser aprobados y aplicados de acuerdo con lo aquí establecido.

ELABORÓ	REVISÓ	APROBÓ
Sandra Fernanda Poveda Oficial de Seguridad de la información. 10 de enero de 2024	Oficina de Tecnología y sistemas de la información 12 de enero de 2024 Soporte: Correo Formulación planes especiales 2024 - Decreto 612 del 2018 enviado a Sistema Gestion de Calidad <gpcalidad@dnp.gov.co>	Comité institucional de Gestión y Desempeño 29 y 30 de enero de 2024 Soporte: Acta No. 01 de 2024. Expediente Orfeo 20246900040630001E