Defensa Jurídica del Estado

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Alineados con el CONPES 3971/2019 y el Decreto 1008 de 2018 de Política de Gobierno Digital que tiene definido tres habilitadores transversales, dentro de los cuales está el de Seguridad y Privacidad de la Información, que incluye la adopción del Marco de Seguridad y Privacidad de la Información – MSPI del Estado Colombiano, como instrumento para la implementación de los lineamientos de seguridad de la información establecidos para sus procesos, tramites, servicios, sistemas de información, infraestructura y alineados con los requisitos del establecimiento para la estrategia de seguridad digital, de acuerdo con lo establecido en el artículo 5 de la resolución 500 de 2021, se estructura este documento que permite visualizar las actividades para preservar la confidencialidad, integridad y disponibilidad y privacidad de la información en la Agencia Nacional de Defensa Jurídica del Estado.

2. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, 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.

3. ALCANCE

Este plan va dirigido a todos los procesos de la Agencia Nacional de Defensa Jurídica del Estado, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información.

4. DEFINICIONES Y ABREVIATURAS

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: Es la propiedad que garantiza que la información solo sea accesible para aquellas personas, entidades o procesos que están autorizados a acceder a ella. La confidencialidad protege la información sensible de accesos no autorizados, evitando su divulgación indebida.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Disponibilidad: Es la propiedad que garantiza que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo necesitan. Esto implica que los sistemas deben estar operativos y accesibles de manera confiable, minimizando tiempos de inactividad o fallos.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Integridad: Es la propiedad que asegura que la información y sus métodos de procesamiento son completos y precisos, es decir, que no han sido alterados de manera no autorizada, ya sea accidental o intencionalmente. La integridad protege contra la modificación o destrucción de la información sin autorización.

PETI: Plan Estratégico de Tecnologías de la Información.

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

SIGI: Es el Sistema Integrado de Gestión Institucional, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y trasparente, con el fin de aumentar la satisfacción de los clientes.[1]

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. RESPONSABILIDADES

El Oficial de Seguridad de la Información o en su ausencia el líder del proceso de Gestión de Tecnologías de la Información es el encargado de dar continuidad a las actividades descritas en este plan.

6. DESARROLLO

6.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTRO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

[1] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

La Entidad ha venido fortaleciendo el Modelo de Seguridad y Privacidad de la Información desde el año 2016, desde un enfoque técnico y un enfoque estratégico, desde el nivel técnico se han adquirido herramientas para el monitoreo y correlación de eventos, contratación de servicios para análisis de vulnerabilidades, servicios de monitoreo de seguridad y revisión de marca. Desde el punto de vista estratégico se encamina a fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI) y para ello se busca actualizar las políticas de seguridad, la documentación procedimental, verificar los activos y riesgos de seguridad y documentar el plan de continuidad del negocio y plan de recuperación de desastres, resaltando para la vigencia 2024 la implementación fase I de la estrategia para DRP basado en nube pública. De este trabajo realizado, se muestra el estado de los indicadores de implementación del MSPI tomando como base el instrumento de evaluación de MINTIC:

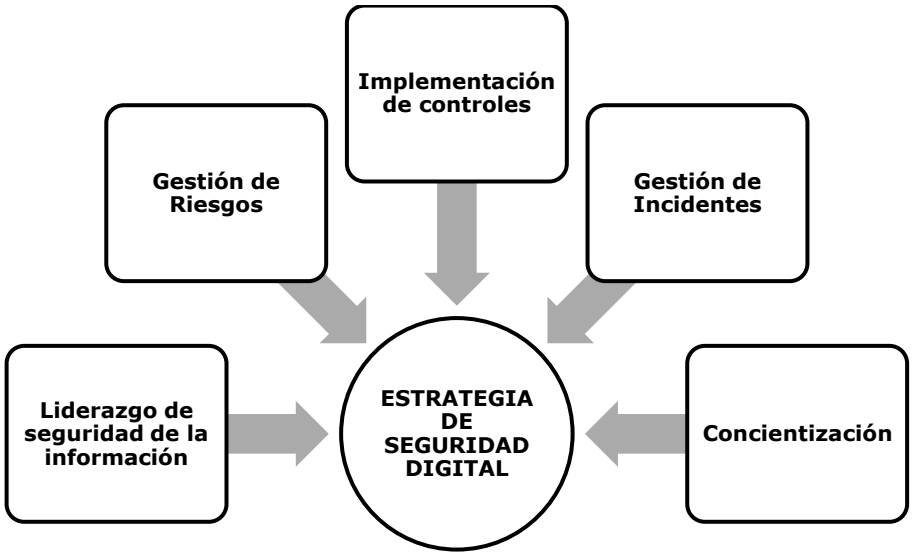
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	96	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	99	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	99	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	97	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	95	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	97	100	OPTIMIZADO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**97**	100	100

6.2 ESTRATEGIA DE SEGURIDAD DIGITAL[2]

La Agencia establece una estrategia de seguridad digital en la que se integren 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 en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes.

Por tal motivo, la Agencia define las siguientes 5 estrategias específicas, que permiten establecer en su conjunto una estrategia general de la seguridad digital:

[2] PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)-MINTIC



6.3DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECIFICAS (EJES)[3]

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

[3] PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)-MINTIC

	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.

6.4PORTAFOLIO DE PROYECTOS / ACTIVIDADES

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**ACTIVIDAD 1** Actualizar Políticas de seguridad. **ACTIVIDAD 2:** Revisar el MSPI por la Dirección. **ACTIVIDAD 3:** Formalizar estrategias de continuidad del negocio. **ACTIVIDAD 4:** Aprobar el Autodiagnóstico de Seguridad por parte del CIGD.	**ACTIVIDAD 1** Políticas de Seguridad de la información actualizadas. **ACTIVIDAD 2** Informe de resultados de la vigencia 2024 del MSPI relacionada con activos, incidentes y riesgos. **ACTIVIDAD 3** Formalizar en el sistema de calidad las estrategias de Gestión del Talento Humano, Gestión Contractual, Gestión de Bienes y Servicios y Gestión de Tecnologías de la Información. **ACTIVIDAD 4:** Autodiagnóstico de Seguridad aprobado.
Gestión de riesgos	**ACTIVIDAD 1** Incorporar los riesgos asociados a continuidad del negocio a la Matriz de Riesgos de la Agencia. **ACTIVIDAD 2** Realizar el seguimiento al Plan de Tratamiento de Riesgos de Seguridad	**ACTIVIDAD 1** Publicar en Daruma la Matriz de Riesgos de Continuidad del Negocio. **ACTIVIDAD 2** Informe de riesgos de seguridad.

Concientización	**ACTIVIDAD 1** Publicar campañas de sensibilización (Lunes Seguro). **ACTIVIDAD 2** Participar en inducciones y reinducciones de Talento Humano. **ACTIVIDAD 3** Desarrollar Día de la Seguridad. **ACTIVIDAD 4** Realizar la encuesta de apropiación de actividades relacionados con el Plan de Seguridad y Privacidad de la Información.	**ACTIVIDAD 1** 36 campañas publicadas. **ACTIVIDAD 2** 2 inducciones y 2 reinducciones. **ACTIVIDAD 3** Informe Día de la Seguridad. **ACTIVIDAD 5** Resultado de las encuestas de medición del nivel de apropiación.
Implementación de controles	**ACTIVIDAD 1** Realizar rediseño e implementación DRP. **ACTIVIDAD 2** Mantener el servicio de Monitoreo de Seguridad. **ACTIVIDAD 3** Realizar Análisis de Vulnerabilidades. **ACTIVIDAD 4** Realizar Análisis de Marca.	**ACTIVIDAD 1** Infraestructura desplegada de acuerdo con el alcance definido. **ACTIVIDAD 2** Informes del Servicio SOC. **ACTIVIDAD 3** Informe de resultados de los análisis realizados. **ACTIVIDAD 4** Informe de resultados del análisis de marca.
Gestión de incidentes	**ACTIVIDAD 1** Gestión de incidentes de seguridad de la información.	**ACTIVIDAD 1** Registro del indicador de incidentes en el sistema Daruma.

6.5DISTRIBUCIÓN PRESUPUESTAL

De acuerdo con la proyección del PAA las siguientes adquisiciones hacen parte de los controles para fortalecer el Modelo de Seguridad y Privacidad de la Información.

OBJETO	VALOR ESTIMADO EN LA VIGENCIA ACTUAL
Profesional especializado responsable del Rol de Oficial de Seguridad de la Agencia para asegurar y mantener el Modelo de Seguridad y Privacidad de la Información.	$100.000.000
Servicio de ciberseguridad para monitoreo de seguridad, monitoreo de red, análisis de vulnerabilidades, marca y afinamiento e implementación de estrategia de recuperación ante desastres en nube hibrida.	$819.249.762

Nota: El seguimiento de los proyectos que implican presupuesto es reportado en el seguimiento del plan de implementación y seguimiento del mapa de ruta de los proyectos e iniciativas de tecnología de información -PETI el cual esta soportado en PAA.

7. RIESGOS

CLASIFICACIÓN DEL RIESGO	DESCRIPCIÓN DEL RIESGO	CAUSAS	CONSECUENCIAS	CONTROLES
Estratégico	Incumplimiento de metas propuestas para los planes de acción institucional de TI.	Insuficiente de asignación de tiempos y recursos Disminución de presupuesto	Incumplimientos legales y llamados de atención	Planificación y entrega del PAA a Financiera

8. INDICADORES

(A) (Actividades ejecutadas / Actividades programadas) *100

9. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Actualizar Políticas de Seguridad	6,66%	Políticas de Seguridad de la información actualizadas.	100%	Oficial seguridad de la Información	1-feb-25	30-abr-25
Revisión del MSPI por parte de la Dirección	8,00%	Informe resultados vigencia 2023 del MSPI relacionada con activos, incidentes, activos y riesgos.	100%	Oficial seguridad de la Información	15-ene-25	30-abr-25
Formalizar estrategias de continuidad del negocio	8,00%	Estrategia Talento Humano Gestión Contractual Servicios Gestión Bienes y Servicios Gestión tecnologías	100%	Oficial seguridad de la Información	1-abr-25	30-may-25

Autodiagnóstico de Seguridad con base en el instrumento del MSPI de MINTIC	8,00%	Autodiagnóstico Aprobado por el CIGD	100%	Oficial seguridad de la Información	1-jun-25	30-jul-25
Identificar Riesgos de Continuidad del Negocio	7,00%	Incorporar riesgos asociados a continuidad del negocio a la Matriz de Riesgos de la Agencia.	100%	Oficial seguridad de la Información	1-jun-25	30-ago-25
Gestionar de Riesgos de Seguridad de la Información	6,66%	Seguimiento planes de tratamiento de riesgos de seguridad	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Sensibilzación sobre seguridad de la Información	9,00%	36 campañas de Lunes Seguros	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Sensibilzación sobre seguridad de la Información	6,62%	2 inducciones y 2 reinducciones	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Sensibilzación sobre seguridad de la Información	6,66%	Realización Día de la Seguridad	100%	Oficial seguridad de la Información	1-ago-25	30-sep-24
Encuesta apropiación.	6,66%	Resultado de las encuestas de medición	100%	Oficial seguridad de la Información	1-sep-25	30-oct-25
Realizar rediseño e implementación DRP	6,76%	Infraestructura implementada de acuerdo con el alcance definido	100%	Oficial seguridad de la Información	15-feb-25	30-jul-25
Mantener el servicio de Monitoreo de Seguridad	6,66%	Informes Servicio SOC	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Análisis de vulnerabilidades y marca	6,66%	Informe de resultados	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25
Gestión de incidentes de seguridad de la información	6,66%	Registro indicador Sistema Daruma.	100%	Oficial seguridad de la Información	15-feb-25	30-nov-25

Elaboró	Revisó	Aprobó
Fredy Zea Rodriguez Contratista	**Oswaldo Useche** Jefe T.I **Carlos Adolfo Rangel** Gestor T1-14	Comité Institucional de Gestión y Desempeño - CIGD