PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2024

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 permitirá visualizar las actividades que permitan preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos 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 2024.

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).

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).

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).

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).

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

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.

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]

5. RESPONSABILIDADES

El Oficial de seguridad de la información o en su ausencia el líder del proceso de Gestión de Tecnologías de la Información será 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

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 encaminó a fortalecer el Modelo de Seguridad y Privacidad de la Información (MSPI) y para ello se buscó 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 2023 la implementación del DRP. De este trabajo realizado a continuación, se copian 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	84	100	**OPTIMIZADO**

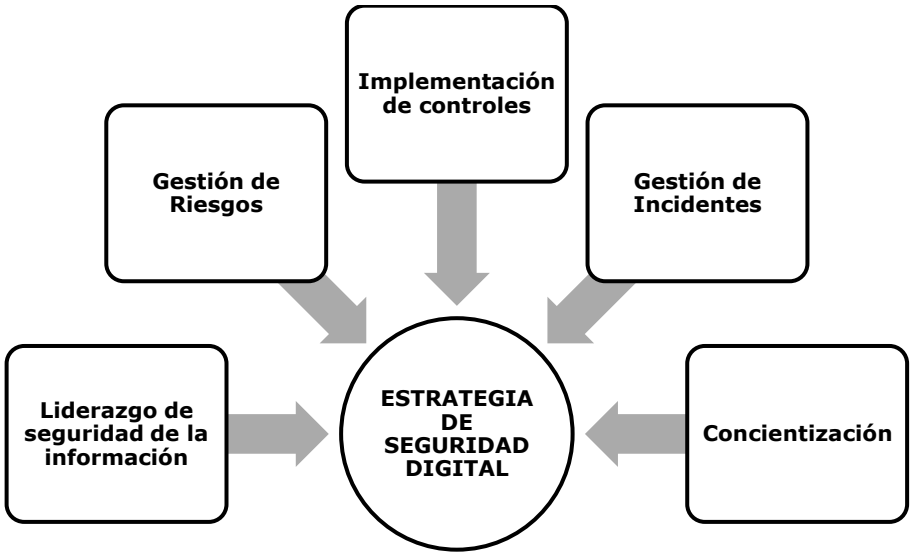
[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	98	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	87	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	98	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	90	100	**OPTIMIZADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	90	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	90	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	90	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	78	100	**GESTIONADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	83	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	90	100	**OPTIMIZADO**
A.18	CUMPLIMIENTO	86	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**90**	**100**	**OPTIMIZADO**

6.2 Estrategia de seguridad digital[2]

La Agencia establecerá 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 entorno 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 que debe establecerse.

Por tal motivo, LA ENTIDAD define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



6.3 DESCRIPCIÓN 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

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

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

	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.

6.4PORTAFOLIO DE PROYECTOS / ACTIVIDADES

ESTRATEGIA / EJE	ACTIVIDADES	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**ACTIVIDAD 1** Actualizar Políticas de seguridad **ACTIVIDAD 2:** Definición de Roles y Responsabilidades de Seguridad de la Información. **ACTIVIDAD 3:** Revisión por la Dirección. **ACTIVIDAD 4:** Implementación estrategias de continuidad del negocio. **ACTIVIDAD 5:** Declaración de Aplicabilidad	**ACTIVIDAD 1** Políticas de Seguridad de la información actualizadas. **ACTIVIDAD 2** Matriz Roles y Responsabilidades en Seguridad de la Información. **ACTIVIDAD 3** Informe resultados vigencia 2022 del MSPI relacionada con activos, incidentes, activos y riesgos. **ACTIVIDAD 4** Estrategia talento Humano Estrategia Gestión Documental Estrategia T.I **ACTIVIDAD 5:** Actualización declaración de aplicabilidad

Gestión de riesgos	**ACTIVIDAD 1** Identificar, valorar y clasificar riesgos asociados a continuidad del negocio. **ACTIVIDAD 2** Seguimiento planes de tratamiento de riesgos de seguridad	**ACTIVIDAD 1** Matriz de riesgos de continuidad del negocio. **ACTIVIDAD 2** Informe riesgos
Concientización	**ACTIVIDAD 1** plan de comunicaciones **ACTIVIDAD 2** campañas de sensibilización (lunes seguro) **ACTIVIDAD 3** Participación inducciones y reinducciones. **ACTIVIDAD 4** Día de la seguridad **ACTIVIDAD 5** Encuesta apropiación.	**ACTIVIDAD 1** Documento plan de comunicaciones **ACTIVIDAD 2** 30 campañas **ACTIVIDAD 3** 2 inducciones y 2 reinducciones **ACTIVIDAD 4** 1 charla de seguridad experto externo. **ACTIVIDAD 5** Resultado de las encuestas de medición
Implementación de controles	**ACTIVIDAD 1** Implementación DRP **ACTIVIDAD 2** Monitoreo seguridad **ACTIVIDAD 3** Análisis de vulnerabilidades **ACTIVIDAD 4** Análisis de Marca	**ACTIVIDAD 1** Infraestructura implementada **ACTIVIDAD 2** Servicio SOC **ACTIVIDAD 3** Informe resultados **ACTIVIDAD 4** Informe resultados
Gestión de incidentes	**ACTIVIDAD 1** Capacitar al personal en la gestión de incidentes de seguridad de la información.	**ACTIVIDAD 1** Sesiones de capacitación desarrolladas.

6.5DISTRIBUCIÓN PRESUPUESTAL

De acuerdo con la proyección PAA las siguientes adquisiciones hacen parte de los controles para fortalecer el sistema 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.	$154.000.000

Nota: El seguimiento de los proyectos que implican presupuesto será 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) Porcentaje de implementación de los hitos del Modelo de Seguridad y Privacidad de la Información definidos.

(B) Calificación del Modelo de Seguridad y Privacidad de la Información.

9. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Actualizar Políticas de seguridad	7,7%	Políticas de Seguridad de la información actualizadas.	7,7%	Oficial seguridad de la Información	15-ene-24	30-mar-24
Definición de Roles y Responsabilidades de Seguridad de la Información.	7,7%	Matriz Roles y Responsabilidades en Seguridad de la Información.	7,7%	Oficial seguridad de la Información	15-mar-24	30-jun-24
Revisión por la Dirección.	7,7%	Informe resultados vigencia 2022 del MSPI relacionada con activos, incidentes, activos y riesgos.	7,7%	Oficial seguridad de la Información	15-ene-24	30-abr-24
Implementación estrategias de continuidad del negocio	7,7%	Estrategia talento Humano Estrategia Gestión Documental Estrategia T.I.	7,7%	Oficial seguridad de la Información	15-feb-24	30-sep-24

Gestión de riesgos	7,7%	Identificar, valorar y clasificar riesgos asociados a continuidad del negocio.	7,7%	Oficial seguridad de la Información	15-jun-24	30-nov-24
Gestión de riesgos	7,7%	Seguimiento planes de tratamiento de riesgos de seguridad	7,7%	Oficial seguridad de la Información	15-feb-24	30-nov-24
Plan de Comunicaciones	7,7%	Elaboración plan de comunicaciones 2023	7,7%	Oficial seguridad de la Información	15-ene-24	28-feb-24
Lunes seguro	7,7%	30 campañas de sensibilización	7,7%	Oficial seguridad de la Información	15-feb-24	30-nov-24
Participación inducciones y reinducciones.	7,7%	2 inducciones y 2 reinducciones	7,7%	Oficial seguridad de la Información	15-feb-24	30-nov-24
Día de la seguridad	7,7%	1 charla de seguridad experto externo.	7,7%	Oficial seguridad de la Información	2-may-24	28-jul-24
Encuesta apropiación.	7,7%	Resultado de las encuestas de medición	7,7%	Oficial seguridad de la Información	1-sep-24	30-nov-24
Implementación DRP	7,7%	Infraestructura implementada	7,7%	Oficial seguridad de la Información	15-feb-24	30-jun-24
Declaración de Aplicabilidad	7,6%	Actualización declaración de aplicabilidad	7,6%	Oficial seguridad de la Información	1-abr-24	30-may-24

Elaboró	Revisó	Aprobó
Fredy Zea Rodriguez Gestor T1-14	**Oswaldo Useche Acevedo** Jefe Oficina	Comité Institucional de Gestión y Desempeño - CIGD