Agencia Nacional de Defensa Jurídica del Estado

PLAN DE SEGURIDAD DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL
AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO
ENERO DE 2023

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, en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos, así como el autodiagnóstico del Modelo Integrado de Planeación y Gestión - MIPG (DAFP, 2018) que es un instrumento que mide el nivel de madurez de los componentes TIC y para el caso en concreto el del nivel de MSPI.

2. OBJETIVO

Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – en el marco del Modelo de Seguridad y Privacidad de la Información MSPI.

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 Sistema de Gestión de Seguridad de la Información – SGSI

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 líder 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. ESTRATEGIA

La estrategia para el desarrollo del siguiente plan estará alienada y enfocada con el modelo de seguridad y privacidad de la información MSPI del MINTIC.

7. DESARROLLO

Este plan presenta las actividades a desarrollar durante la vigencia 2023 por parte de la ANDJE, qué con el apoyo de la Dirección General, permitirá gestionar y mejorar de forma continua, el sistema de Gestión de Seguridad y Privacidad de la Información, para proteger la confidencialidad, integridad y disponibilidad de la información física y digital, que se genera, procesa y resguardada en cada uno de los procesos que la conforman, mediante el establecimiento de controles físicos, lógicos y humanos, dando cumplimiento a los lineamientos establecidos por el Gobierno Nacional en materia de Seguridad de la información.

Este documento presenta el mapa de ruta con el cual se identificaron las actividades para la mejora continua del sistema de gestión de privacidad y seguridad de la información.

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

NÚMERO	ACTIVIDAD	RESPONSABLE	PRODUCTO O RESULTADO ESPERADO
1	Contratación SOC-NOC-Análisis de vulnerabilidades	SGSI	Servicio Contratado
2	Adquisición de infraestructura de T.I - DRP y Ciberseguridad	SGSI	Servicios DRP
3	Elaboración plan de comunicaciones 2023	SGSI	Plan de Comunicaciones
4	Actualización Activos de Información	SGSI	Matriz activos actualizada
5	Actualización declaración de aplicabilidad	SGSI	Matriz declaración de aplicabilidad actualizada
6	Manual de Seguridad de la Información	SGSI	Manual de Seguridad de la Información
7	Documento Uso aceptable activos de información	SGSI	Documento Uso aceptable activos de información
8	Documento contacto con las autoridades	SGSI	Documento contacto con las autoridades
9	Formato base de conocimiento Incidentes de Seguridad	SGSI	Formato base de conocimiento Incidentes de Seguridad

8. DISTRIBUCIÓN PRESUPUESTAL

De acuerdo a 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
Prestación de servicios de monitoreo SOC/NOC	$569.507.295
Orden de Compra para la adquisición de infraestructura de T.I - DRP y Ciberseguridad	$600.000.000

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.

9. 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

10. 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

11. CRONOGRAMA

RESULTADO ESPERADO	PESO (%)	RESULTADOS / ENTREGABLES INTERMEDIOS	PESO (%)	RESPONSABLE	EJECUCIÓN	
					Fecha Inicio	Fecha Final
Contratación SOC-NOC-Análisis de vulnerabilidades	100%	Términos de Referencia	100%	SGSI	15/01/2023	30/03/2023
Adquisición de infraestructura de T.I - DRP y Ciberseguridad	100%	Términos de Referencia	100%	SGSI	15/02/2023	30/04/2023
Plan de Comunicaciones	100%	Elaboración plan de comunicaciones 2023	100%	Fredy Zea-Gestor T1-14	12/01/2023	28/02/2023
Declaración de Aplicabilidad	100%	Actualización declaración de aplicabilidad	100%	Fredy Zea-Gestor T1-14	01/04/2023	30/05/2023
Documento	100%	Documento contacto con las autoridades	100%	Fredy Zea-Gestor T1-14	01/06/2023	30/06/2023
Matriz activos de información	100%	Actualización Activos de Información	100%	Fredy Zea-Gestor T1-14	02/05/2023	30/07/2023
Documento	100%	Documento Uso aceptable activos de información	100%	Fredy Zea-Gestor T1-14	01/08/2023	30/08/2023
Manual	100%	Manual de Seguridad de la Información	100%	Fredy Zea-Gestor T1-14	01/09/2023	30/10/2023
Formato	100%	Formato base de conocimiento Incidentes de Seguridad	100%	Fredy Zea-Gestor T1-14	01/10/2023	30/11/2023

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