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
NOVIEMBRE DE 2020

TABLA DE CONTENIDO

INTRODUCCIÓN 3

OBJETIVO 3

ALCANCE 3

DEFINICIONES Y ABREVIATURAS 3

RESPONSABILIDADES 5

ESTRATEGIA 5

DESARROLLO 5

DISTRIBUCIÓN PRESUPUESTAL 7

RIESGOS 7

INDICADORES 8

CRONOGRAMA 8

INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo asegurar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

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.

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

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]

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.

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.

DESARROLLO

Este plan presenta las actividades a desarrollar durante la vigencia 2021 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.

NÚMERO	ACTIVIDAD	RESPONSABLE	PRODUCTO O RESULTADO ESPERADO
1	Actualización	SGSI	Declaración de

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

	Declaración de Aplicabilidad		Aplicabilidad aprobada por la Alta Dirección
2	Verificación y actualización documentación MSPI	SGSI	Documentos Actualizados -Uso y Apropiación -Guía Activos de Información -Metodología de Riesgos -Incidentes seguridad de la información -Informes IPv6
3	Actualización Activos de Información	SGSI	Matriz Activos de Información
4	Diagnostico herramientas, lineamientos y políticas de seguridad para aplicar trabajo en casa	SGSI	Documento Diagnóstico
5	**Implementación fase 1** -Concientización (Higiene Digita) -Gestión de Accesos -Estaciones de trabajo -Cifrado de información	SGSI	Tips de seguridad Lunes Seguro
6	**Implementación fase 2** -Concientización (Incidentes de Seguridad) -Seguridad en Infraestructura de TI (conexiones, vpns, configuraciones)	SGSI	Tips de seguridad Lunes Seguro
7	**Implementación fase 3** -Concientización (Almacenamiento en la NUBE) -Implementación uso en la NUBE para el almacenamiento de archivos y datos.	SGSI	Tips de seguridad Lunes Seguro Configuración Almacenamiento en la NUBE
8	Encuesta Apropiación	SGSI	Informe Ejecutivo

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
Contratar "ANÁLISIS DE VULNERABILIDADES Y EXPLOTACIÓN". (ETHICAL HACKING) Contempla: Tiempos de Contratación y Ejecución del Servicio	$ 117.710.412
Contratar "CENTRO OPERACIONES DE SEGURIDAD (SOC)" diagnóstico de Sistemas e Infraestructura a administrar, monitorear, pruebas e implementación.	$ 199.966.815
Contratación "CONTINUIDAD DEL NEGOCIO" Análisis Impacto del Negocio, riesgos, tiempos de recuperación y estrategias de recuperación	$ 549.134.555

Nota: El seguimiento de los proyectos que implican presupuesto será reportado en el seguimiento de del plan Implentación y seguimiento del mapa de ruta de los proyectos e iniciativas de tecnología de información -PETI 2021-2024 el cual esta soportado en PAA

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

INDICADORES

de actividades del Plan de Seguridad y Privacidad de la Información desarrolladas / total de actividades del plan a implementar *100

CRONOGRAMA

Incorporar un cronograma ejecución del plan, el cual debe contener como mínimo;

- Resultado esperado: describir los resultados esperados como consecución del plan.
- Entregables: enumerar los entregables (productos) a entregar asociado al resultado esperado del plan
- Responsables: establecer el responsable del entregable.
- Fechas de ejecución: establece la fecha de inicio y fin de entrega del entregable, estado de cumplimiento y observaciones
- Tipo de recurso; seleccionar que clase de recursos son necesarios para el cumplimiento del entregable; Humanos, Tecnológicos, Infraestructura, Financieros.

CRONOGRAMA EJECUCIÓN PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

AÑO FORMULACIÓN									
FECHA DE CORTE									
RESULTADO ESPERADO	RESULTADOS / ENTREGABLES INTERMEDIOS	RESPONSABLE	EJECUCIÓN		FECHA DE CUMPLIMIENTO	ESTADO	TIPO DE RECURSO	RECURSOS $	OBSERVACIONES
			Fecha Inicio	Fecha Final					
Actualización Declaración de Aplicabilidad	Reunión con los líderes de procesos donde aplique controles de la Declaración de Aplicabilidad. Declaración de Aplicabilidad aprobada por la Alta Dirección	SGSI	12-ene-21	28-feb-21			Humanos	N/A	Funcionarios de TI Líderes y Enlaces de Procesos
Verificación y actualización documentación MSPI	Documentos actualizados y publicados en SIGI. -Uso y Apropiación -Guía Activos de Información -Metodología de Riesgos -Incidentes seguridad de la información -Informes IPv6	SGSI	1-mar-21	30-abr-21			Humanos		Funcionarios de TI
Actualización Activos de Información	Reunión con los líderes de procesos Matriz de Activos de Información actualizada	SGSI	1-feb-21	30-jun-21		#¡REF!	Humanos		Funcionarios de TI Líderes y Enlaces de Procesos misionales y de apoyo Grupo interno de Activos de Información
Encuesta Apropiación	Creación Encuesta en SIGI Informe Ejecutivo	SGSI	1-dic-20	30-dic-21			Humanos		Colaboradores de la ANDJE

Ver formato Cronograma ejecución plan DE-F-31 CRONOGRAMA EJECUCION PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Elaboró	Revisó	Aprobó
Nombre Cargo	Nombre Cargo	Nombre Cargo