PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ, ENERO 2023

CONTENIDO

Proceso: Seguridad y Privacidad de la Información
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 1

1. INTRODUCCIÓN

Actualmente la entidad cuenta con una Política general que integra a los subsistemas de gestión, la cual se encuentra debidamente formalizada, donde se establecieron los objetivos y el compromiso de la alta dirección, adicionalmente se cuentan con las políticas complementarias de Seguridad y Privacidad de la Información donde se detallan los lineamientos y las actuaciones que deben seguir los colaboradores para mantener una adecuada seguridad de la información en la entidad.

Para dar alcance a lo estipulado en la Política de seguridad digital frente al Plan de Tratamiento de Riesgos, se definió adoptar la metodología definida por el Departamento Administrativo de la Función Pública siguiendo lo descrito en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, basándose en una integración adecuada entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y el enfoque por procesos, permitiendo identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos de información identificados. Actualmente se cuenta con el Plan de Tratamiento de Riesgos basado en esta metodología. Por otra parte, el Plan de Seguridad y Privacidad de la Información (PSPI), determina los objetivos y actividades tendientes a la protección de la información de la Agencia Nacional Digital (AND), específicamente en sus tres (3) pilares fundamentales de confidencialidad, integridad y disponibilidad, tomando como base los activos críticos de la entidad y los riesgos asociados a estos.

El PSPI de la Agencia Nacional Digital, se encuentra alineado con los siguientes documentos:

i) Política de Gobierno Digital, específicamente con la implementación del Modelo de Seguridad y Privacidad de la Información.

ii) Política de Seguridad Digital en lo referente a la gestión de riesgos de seguridad digital; y

iii) Norma ISO NTC/IEC ISO 27001:2013 de Seguridad de la Información.

De acuerdo con lo anterior, el Sistema de Gestión de Seguridad de la Información el cual hace parte del Sistema Integrado de Gestión, tiene como finalidad el fortalecimiento de las capacidades institucionales para gestionar, tratar y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información, a través de la aplicación de mecanismos y controles técnicos y administrativos que velan por el cumplimiento y mejora de la confidencialidad, integridad y disponibilidad de los mismos.

2. OBJETIVO GENERAL

Implementar, y evaluar acciones efectivas a través de la elaboración del Plan de Seguridad y Privacidad de la Información para fortalecer el Subsistema de Gestión de Seguridad de la Información en la AND, en procura de la mejora continua y de la salvaguarda de la información para la vigencia 2023.

2.1. OBJETIVOS ESPECÍFICOS

- Establecer las principales líneas de actuación a seguir en el corto y mediano plazo para la implementación y mantenimiento del SGSI.
- Definir las actividades para implementar los controles, procedimientos, políticas necesarias para realizar un adecuado tratamiento de los riesgos de seguridad y privacidad de la información en todos los procesos de la AND de acuerdo con la criticidad de los activos de información relacionados.
- Definir los indicadores, metas y recursos necesarios para la consecución del plan.
- Definir acciones para la evaluación y el monitoreo del plan.
- Continuar la implementación del Sistema de Gestión de Seguridad de la Información.
- Realizar seguimiento al plan de tratamiento de Riesgos, conforme a los planes de acción establecidos en el mismo.
- Adoptar las mejores prácticas de Desarrollo de Software Seguro a través del enfoque DevSecOps.
- Mantener Actualizado el inventario de activos y riesgos de seguridad digital conforme al Modelo de Gestión de Riesgos.
- Fortalecer la seguridad de la información en la Agencia Nacional Digital.
- Realizar sensibilización y capacitación en Seguridad de la Información.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Agencia Nacional Digital, comprende la implementación del Modelo de Seguridad y Privacidad de la Información en sus fases del modelo de operación (Planear, Hacer, Verificar y Actuar) aplicable a los quince (15) procesos institucionales.

Así mismo aplica para todos los usuarios internos, externos, proveedores y a la ciudadanía en general, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, prácticas y aborde toda la cadena de valor, en torno a los objetivos estratégicos de la Entidad, con el fin de que esta cuente con un escenario donde se apliquen buenas prácticas en materia de seguridad de la información y fortalezca los niveles de protección de la Seguridad de la Información, reduciendo las vulnerabilidades a las que se encuentran expuestos los activos de información institucionales.

4. METODOLOGÍA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información hace parte del Sistema Integrado de Gestión de la Agencia Nacional Digital, por lo tanto, los documentos procesos y procedimientos resultantes de la implementación de controles de la Norma ISO 27001 son adoptados y formalizados en este último.

La gestión de Sistema de Gestión de Seguridad de la Información se realizará en la plataforma tecnológica que la Agencia disponga para tal fin, en la cual se consolidará los resultados de la ejecución de las fases del ciclo PHVA.

La AND ha adoptado el MSPI como guía para la construcción del Subsistema de Gestión de Seguridad de la Información (SGSI), este modelo está basado en el Marco de Referencia de Arquitectura TI el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en soporte de la Política de Gobierno Digital.

El MSPI permite que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Este modelo contempla un ciclo de operación que consta de cinco (5) fases:

Ilustración 1. Fases del Ciclo PHVA

Modelo PHVA, fuente MINTIC

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

2. **Planificación**: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo

3. **Operación**: Implementar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. **Evaluación de desempeño**: Determinar el sistema y forma de evaluación de la adopción del modelo.

5. **Mejoramiento Continuo**: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

4.1. Compromiso de la Dirección

El Plan de Seguridad y Privacidad de la Información, en el cual se define la hoja de ruta de la implementación del Modelo de Seguridad y Privacidad de la Información a través del SGSI, es socializado, revisado y aprobado por el Comité Institucional de Gestión y Desempeño.

4.2. Política General de Seguridad de la Información

La Política de Seguridad de la Información de la Agencia, se encuentra enmarcada en el Control 5.1. de la Norma ISO 27001:2013 y establece el que se va a proteger en términos generales, y se encuentra alineada con la política de calidad institucional, que a su vez debe apoya el cumplimiento de la misión. Está enfocada a la protección de los activos de información en términos de confidencialidad, integridad y disponibilidad y contempla la aplicación de diferentes contramedidas que permitan la gestión de los riesgos de seguridad de la información. La política de seguridad y privacidad de la información se encuentra definida en el documento: “POLÍTICA INSTITUCIONAL DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN”.

4.3. Meta

Cumplir el 100% de las actividades establecidas en Cronograma Anexo.

4.4. Sensibilización y Concientización

Desarrollo de estrategias de sensibilización y formación en Seguridad de la Información que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de estos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento al control 7.2.2 de la Norma ISO 27002 “Concientización, educación y capacitación de la seguridad de la información”.

El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que giran alrededor de la formación de competencias en los colaboradores de la Agencia, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

4.5. Riesgos Institucionales

Los riesgos instituciones comprenden los riesgos generales de seguridad de la información, en los cuales se definen a grandes rasgos los controles a implementar para reducir la probabilidad de ocurrencia, el tratamiento de estos se desarrolla en la herramienta dispuesta para ello dentro de la Agencia.

4.6. Indicadores

De acuerdo con el Manual de Gobierno Digital, se realiza el seguimiento de la eficacia de la implementación del Modelo de Seguridad y Privacidad de la Información, adicionalmente se adoptarán mecanismos de medición de eficacia en la implementación de controles contenidos en la declaratoria de aplicabilidad y de la efectividad de estos.

4.6.1. Indicador 1:

Tipo de indicador: Cumplimiento
Nombre: Avance plan de seguridad
Formula: (No. de actividades ejecutadas / No. Actividades programadas) * 100
Meta: 90%
Fuente de información: Plan de seguridad y privacidad de la información

4.6.2. Indicador 2:

Tipo de indicador: Cumplimiento
Nombre: Sensibilización en seguridad de la información
Formula: (No. de personas capacitadas en seguridad / Total de personas invitadas) * 100
Meta: 90%
Fuente de información: Plan de sensibilización y capacitación

4.6.3. Indicador 3:

Tipo de indicador: Gestión

Nombre: Eficacia de la capacitación

Formula: (No. de personas que aprobaron la capacitación de seguridad / Total de personas evaluadas) * 100

Meta: 80%

Fuente de información: Plan de sensibilización y capacitación

5. FASES PROPUESTAS DEL PLAN

Se adjunta cronograma de implementación.