



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ, ENERO 2022



CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	3
3. ALCANCE	4
4. METODOLOGÍA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	4
5. FASES PROPUESTAS DEL PLAN	7

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información, consiste en determinar los objetivos y actividades tendientes a la protección de la información de la Agencia Nacional Digital, 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 Plan de Seguridad de la Información 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. OBJETIVOS DEL PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Plan de Seguridad de la Información de la Agencia Nacional Digital, tiene como objetivos.

- Continuar La implementación del Sistema de Gestión de Seguridad de la Información.
- Establecer e implementar las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital.
- Actualizar la gestión 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 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.

Ilustración 1. Fases del Ciclo PHVA



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 apoyar 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. Objetivos Generales de Seguridad de la Información

Los objetivos de seguridad de la información de la Agencia Nacional Digital definen cómo se aplica la Política General de Seguridad de la Información y contienen el compromiso de la dirección en la implementación y operación del SGSI, así como se puede observar a continuación:

- ✓ Velar por la protección de información, fortaleciendo la confidencialidad, integridad y disponibilidad de esta.
- ✓ Contribuir al incremento de la transparencia en la gestión pública.
- ✓ Promover el uso de las mejores prácticas en seguridad de la información.
- ✓ Fortalecer los controles de seguridad para los procesos de intercambio de información pública.
- ✓ Apropiar al interior de la Agencia la gestión de la seguridad de la información.
- ✓ Contribuir en el desarrollo de los planes estratégicos de la Agencia como: el Plan institucional y el plan de tecnologías de la información.
- ✓ Tener en cuenta las mejores prácticas para la construcción de una política de tratamiento de datos personales alineada con la Ley 1581 de 2012.

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. Sistema de Métricas

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.

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

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

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.