PRESIDENCIA DE LA REPÚBLICA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá D.C. Julio de 2018

TABLA DE CONTENIDO

1. OBJETIVO

Definir las actividades del plan de Seguridad y Privacidad de la Información para la implementación, gestión, verificación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI del Departamento Administrativo de la Presidencia de la República.

2. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos del Departamento Administrativo de la Presidencia de la República, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información - SGSI[1].

3. TERMINOS Y DEFINICIONES

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.[2]

SIGEPRE: Es el sistema integrado de Gestión de la Presidencia de la República, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y trasparente, con el fin de aumentar la satisfacción de los clientes.

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL DAPRE

[1] Ver Manual del Sistema Integrado de Gestión de la Presidencia de la República SIGEPRE M-DE-02, sección: Alcance del Sistema de Gestión de Seguridad de la Información - SGSI.
[2] Decreto 1008 de 14 de Junio de 2018, por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.

El Departamento Administrativo de la Presidencia de la Republica, se compromete a administrar los riesgos de seguridad de la información para generar, implementar y monitorear los controles que permitan mantener la confidencialidad, integridad y disponibilidad de sus activos de información en cumplimiento de los requisitos aplicables. De igual manera, promueve una cultura en seguridad para evitar y administrar incidentes que contribuyan a la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. Administrar los eventos de seguridad de la información de la Presidencia de la República.
2. Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
3. Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
4. Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes, judicantes y personal en comisión de la Presidencia de la Republica).
5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN - SGSI

EL SGSI es aplicable a los activos de información de todos los procesos del DAPRE, verificándolo y aplicándolo a las sedes, comprende las políticas, procedimientos y controles para la preservación de confidencialidad, integridad y disponibilidad de la información, en concordancia con la declaración de aplicabilidad avalada por el Comité de Seguridad de la Información y el Comité Institucional de Gestión y Desempeño.

7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información, es creado en el DAPRE mediante acto administrativo y el cual tiene dentro de sus funciones la de impulsar, hacer seguimiento y/o verificación de la implementación del Sistema de Gestión de Seguridad de la Información SGSI, del Departamento Administrativo de la Presidencia de la República.

Está conformado por:

- ✓ El Director de Operaciones del Departamento Administrativo de la Presidencia de la República o su delegado quien lo presidirá.
- ✓ El Director de Gestión General del Departamento Administrativo de la presidencia de la República.
- ✓ El Jefe de Casa Militar o su delegado.
- ✓ El Jefe del Área de Tecnología y Sistemas de Información del Departamento Administrativo de la Presidencia de la República.
- ✓ El Jefe del Área Administrativa del Departamento Administrativo de la Presidencia de la República.

Invitados:

- ✓ El Jefe de la Oficina de Control Interno de Gestión del Departamento Administrativo de la Presidencia de la República
- ✓ Designado del Equipo de Respuesta a Incidentes de Seguridad Informática de Casa Militar.
- ✓ El Coordinador del Grupo de Gestión Documental.

Estos funcionarios asistirán como invitados, con voz pero sin voto.

Las funciones del Comité de Seguridad de la Información son:

- ✓ Impulsar la implementación del Sistema de Gestión de Seguridad de la Información SGSI de la Presidencia de la República.
- ✓ Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información SGSI del Departamento Administrativo de la Presidencia de la República.
- ✓ Supervisar la integración del Sistema de Gestión de Seguridad de la Información - SGSI con el Sistema Integrado de Gestión- SIGEPRE del Departamento Administrativo de la Presidencia de la República.
- ✓ Aprobar las medidas y Políticas de Seguridad de la Información y sus modificaciones, en relación con los activos de la información para la Presidencia de la República.
- ✓ Adoptar las medidas y acciones a que haya lugar, de conformidad con los resultados de los diagnósticos de la seguridad de la información para el DAPRE, con el fin de tomar y establecer las medidas necesarias.
- ✓ Establecer mecanismos necesarios para prevenir situaciones de riesgo o incidentes de seguridad física o virtual que puedan generar pérdidas patrimoniales o afectar los recursos de Información de la entidad.
- ✓ Aprobar el uso de metodologías específicas para garantizar confiabilidad, disponibilidad e integridad de la seguridad de la información.
- ✓ Revisar y aprobar los proyectos de seguridad de la información y servir de facilitadores para su implementación.

- ✓ Recomendar la investigación de los incidentes de seguridad de la información ante las instancias necesarias cuando haya lugar a ello.
- ✓ Evaluar los planes de acción para mitigar y/o eliminar riesgos en seguridad de la información.
- ✓ Alinear sus acciones y decisiones a la normatividad vigente en materia de tecnologías y seguridad de la información.
- ✓ Las demás funciones inherentes a la naturaleza del Comité.

8. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A partir del desarrollo e implementación del Sistema de Gestión de Seguridad de la Información – SGSI del Departamento Administrativo de la Presidencia de la República, el cual hace parte del Sistema Integrado de la Presidencia de la República – SIGEPRE, se definieron las siguientes actividades para la vigencia 2018 con las cuales se establece el plan de seguridad y privacidad de la información, permitiendo así la mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI:

8.1 Planeación

A continuación se dan a conocer las actividades definidas para en la etapa de planeación para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013), el cual se encuentra en SIGEPRE:

Actividad	Fecha Inicial	Fecha Final	Responsable
1.1 Revisión de documentación del SGSI.	17/ene/2018 08:00:00	27/abr/2018 23:59:00	Ana Rocio Castro Paez
1.2 Revisión de la Lineamiento de Administración del Riesgo.	17/ene/2018 08:00:00	27/abr/2018 23:59:00	Ana Rocio Castro Paez
1.3 Informar sobre el SGSI a los funcionarios y colaboradores del DAPRE.	17/ene/2018 08:00:00	27/abr/2018 23:59:00	Ana Rocio Castro Paez
1.4 Identificación de Amenazas y vulnerabilidades (factores internos y externos).	17/ene/2018 08:00:00	31/may/2018 23:59:00	Ana Rocio Castro Paez
1.5 Análisis y Evaluación de los riesgos.	17/ene/2018 08:00:00	31/may/2018 23:59:00	Ana Rocio Castro Paez
1.6 Selección de Controles.	17/ene/2018 08:00:00	31/may/2018 23:59:00	Ana Rocio Castro Paez
1.7 Verificación de Declaración de Aplicabilidad (SOA) listado con todos los controles seleccionados.	15/feb/2018 08:00:00	31/may/2018 23:59:00	Ana Rocio Castro Paez

8.2 Implementación

A continuación se dan a conocer las actividades definidas para en la etapa de implementación para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013), el cual se encuentra en SIGEPRE:

Actividad	Fecha Inicial	Fecha Final	Responsable
2.1 Plan de tratamiento de los riesgos.	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez
2.2 Implementar los controles (Definidos en la Declaración de aplicabilidad).	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez
2.3 Concienciación sobre Seguridad de la Información.	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez

8.3 Seguimiento

A continuación se dan a conocer las actividades definidas para en la etapa de Seguimiento para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013), el cual se encuentra en SIGEPRE:

Actividad	Fecha Inicial	Fecha Final	Responsable
2.1 Plan de tratamiento de los riesgos.	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez
2.2 Implementar los controles (Definidos en la Declaración de aplicabilidad).	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez
2.3 Concienciación sobre Seguridad de la Información.	01/feb/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez

8.4 Mejora Continua

A continuación se dan a conocer las actividades definidas para en la etapa de Mejora continua para el Sistema de Gestión de Seguridad de la Información en la vigencia 2018, las cuales se desarrollaron en el Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013), el cual se encuentra en SIGEPRE:

Actividad	Fecha Inicial	Fecha Final	Responsable
4.1 Definir y desarrollar Oportunidades de mejora.	02/abr/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez
4.2 Acciones correctivas.	02/abr/2018 08:00:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez

4.3 Actualización de documentos del Sistema de Gestión de Seguridad de la Información.	07/ene/2018 08:01:00	19/jul/2018 23:59:00	Ana Rocio Castro Paez

9. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

10. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.

11. DOCUMENTOS ASOCIADOS

- M-TI-01 Manual de Políticas de Seguridad de la Información.

12. RESPONSABLE DEL DOCUMENTO

Jefe Área de Tecnologías y Sistemas de Información.