



**PRESIDENCIA
DE LA REPÚBLICA**



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ D.C DICIEMBRE DE 2018



Proceso asociado	Tecnología de Información v Comunicaciones
Código	D-TI-25
Versión	02

CONTENIDO

1. OBJETIVO	2
2. ALCANCE	2
3. TERMINOS Y DEFINICIONES	2
4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL DAPRE.....	3
5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	3
6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI.....	3
7. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN	3
8. PLANES DESARROLLADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	5
9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN...6	
10. MARCO LEGAL	7
11. REQUISITOS TÉCNICOS.....	7
12. DOCUMENTOS ASOCIADOS.....	7
13. RESPONSABLE DEL DOCUMENTO	7



1. 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 – 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 – SGSI¹.

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. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

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 transparente, con el fin de aumentar la satisfacción de los clientes.

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.



Proceso asociado	Tecnología de Información v Comunicaciones
Código	D-TI-25
Versión	02

4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL DAPRE

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 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 SEGURIDAD DE LA 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 Tecnologías 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.



Proceso asociado	Tecnología de Información v Comunicaciones
Código	D-TI-25
Versión	02

- ✓ 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. PLANES DESARROLLADOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el desarrollo 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 han desarrollado las actividades hacia el plan de seguridad y privacidad de la información, las cuales se encuentran documentadas en **Plan de Trabajo SGSI - (Norma NTC-ISO-IEC 27001:2013)**, el cual fue creado con Oportunidad de Mejora definida: **OM-0401 TI- Sistema de Gestión de Seguridad de la Información – SGSI**, todo lo anterior puede ser visualizado en el aplicativo SIGEPRE.

Adicional a esto, se definieron y se ejecutaron las oportunidades de mejora para el Sistema de Gestión de Seguridad de la Información – SGSI:

Código	Nombre
OM-0401	TI- Sistema de Gestión de Seguridad de la Información – SGSI.
OM-0421	TI - Creación y documentación de Matriz de riesgos de seguridad de la información versus controles – SGSI.
OM-0422	TI - Creación de nuevos riesgos de seguridad de la información – SGSI.
OM-0423	TI - Fortalecer el conocimiento sobre las políticas del Sistema de Gestión de Seguridad de la Información – SGSI.
OM-0457	TI-SGSI-R+ -Mejorar el aplicativo de gestión de correspondencia SIGOB mediante la implementación del nuevo Sistema de Gestión Documental Escribe Presidencia.
OM-0458	TI-SGSI Mejoramiento del Sistema de Gestión de Seguridad de la Información a partir de la Etapa 1 de auditoría de certificación.



Proceso asociado	Tecnología de Información v Comunicaciones
Código	D-TI-25
Versión	02

Código	Nombre
OM-0459	TI-SGSI-R+ -Fomentar la seguridad de la información y la continuidad de la organización, mediante la adquisición de un dispositivo de tipo Hardware, denominado Firewall.
OM-0461	TI-SGSI Fortalecer el Sistema de Gestión de Seguridad de la Información - SGSI a partir de Auditoría Interna.

9. ACTIVIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la vigencia 2019 se definen las siguientes actividades para Seguridad y Privacidad de Información, las cuales se encuentran enmarcadas en la Estrategia 2 del Plan de Acción del Área de Tecnologías y Sistemas de Información:

Actividad	Descripción	Responsable	Fecha Inicial Planificada	Fecha Final Planificada
Definir el marco de seguridad y privacidad de la información. GD-2019	Se definirán las acciones a implementar a nivel de seguridad y privacidad y de mitigación del riesgo de Seguridad de la Información, en el marco de SGSI de la Entidad.	Ana Rocío Castro Alfonso Rojas Betty Yaneth Daza	02/01/2019	30/12/2019
Ejecutar el plan de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información - SGSI. GD-2019	Se ejecutará el cronograma de aplicación y mejoramiento del Sistema de Gestión de Seguridad de la Información - SGSI el cual consiste en el desarrollo de las tareas correspondientes a la vigencia 2019, como la verificación por parte de la alta dirección del SGSI, cumplimiento de los objetivos e indicadores definidos para el sistema.	Ana Rocio Castro Betty Yaneth Daza William Onofre Alfonso Rojas	02/01/2019	30/12/2019
Aplicar y mejorar la seguridad y privacidad de la información en el marco de SGSI de la Entidad. GD-2019	Se realizarán las actividades para el seguimiento que permitan la medición, análisis y evaluación del desempeño de la seguridad y privacidad de la información, con el fin de generar los ajustes o cambios pertinentes y oportunos.	Ana Rocio Castro Betty Yaneth Daza William Onofre Alfonso Rojas	02/01/2019	30/12/2019



Proceso asociado	Tecnología de Información v Comunicaciones
Código	D-TI-25
Versión	02

10. 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.

11. 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.

12. DOCUMENTOS ASOCIADOS

- L-DE-01 Lineamientos para la Administración del Riesgo.
- G-EM-01 Guía Para La Formulación, Seguimiento y Evaluación de Planes de Mejoramiento.
- M-TI-01 Manual de Políticas de Seguridad de la Información.

13. RESPONSABLE DEL DOCUMENTO

Jefe Área de Tecnologías y Sistemas de Información.