# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## SENADO DE LA REPUBLICA

2022

CONTENIDO

## Contenido

## INTRODUCCIÓN

En los últimos años el acceso a internet ha desempeñado un papel significativo en las entidades a nivel mundial y lo convierte en una herramienta importante para la intercomunicación continua entre las diversas instancias tales como la ciudadanía, sociedad civil, entidades del orden nacional y congresos del mundo, entre otros.

Así mismo, los cambios provocados por la transformación y mejoramiento de las herramientas tecnológicas, y en general de las redes informáticas, se han convertido en instrumentos claves para las entidades y los ciudadanos a utilizarlas como medios con el fin de incrementar su productividad, ser más competitivos, satisfacer necesidades propias y generar valor.

El incremento en el uso de la tecnología para el cumplimiento de la misión de las organizaciones ha generado también incremento en el uso de la tecnología con para generar amenazas informáticas; y con el propósito de afectar otras infraestructuras tecnológicas, sistemas de información financieros, sistemas personales de información, con fines delictivos.

Lo anterior ha conducido a incorporar mejoras en la organización para la administración de los riesgos de seguridad de la información, y generar conciencia en seguridad de la información para todo el personal que la integra, con el objetivo de tener controles que disminuyan la probabilidad de ocurrencia de incidentes informáticos que expongan la infraestructura tecnológica de la entidad y la información.

El Senado de la República en el avance de la implementación del Modelo de Seguridad y privacidad de la información, ha elaborado el presente plan para la vigencia 2022 que permita continuar creciendo en la madurez del modelo y mantener los activos de información protegidos, con un adecuado conjunto de controles y procedimientos para alcanzar un correcto nivel de seguridad y de igual forma administrar y hacer seguimiento a estos controles para mantenerlos y mejorarlos a lo largo del tiempo. Donde se unen esfuerzos para cumplimiento de los habilitadores transversales considerados en la política de Gobierno Digital

## 1. OBJETIVO.

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, para fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, con el propósito de ayudar a reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2021

## 2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica entre otros que se tendrán en cuenta todos los activos de información de la entidad.

## 3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 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”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

## 4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El senado de la República comenzó la implementación del sistema de seguridad y privacidad de la información en el año 2019 de acuerdo con el resultado obtenido en el diagnostico de seguridad y privacidad realizado con la herramienta de MINTIC, donde se encontraba en un nivel inicial.

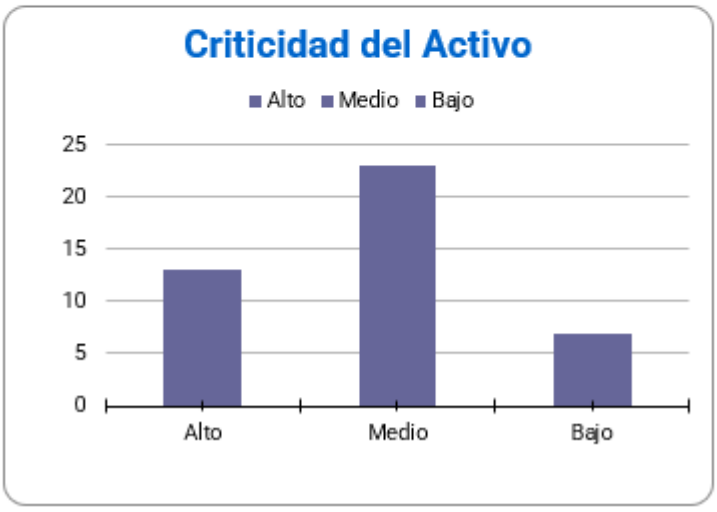
A partir de allí, se ha avanzado con la adopción de la política general de seguridad y privacidad de la información, procedimientos asociados a la seguridad y la elaboración del inventario de activos de información, que han permitido realizar la identificación de riesgos de seguridad con los controles asociados y a partir de allí generar acciones de mejora para continuar fortaleciendo los controles.

En la identificación de activos de información se ha encontrado

***ACTIVOS DE INFORMACION PROCESOS SGSI***

Resumen de Activos

| Criticidad del Activo | Cantidad de Activos |
|---|---|
| Alto | 13 |
| Medio | 23 |
| Bajo | 7 |
| TOTAL | 43 |




Y los activos valorados en alto fueron llevados a identificación de riesgos que se encuentran en el plan de tratamiento de riesgos de seguridad de la información.

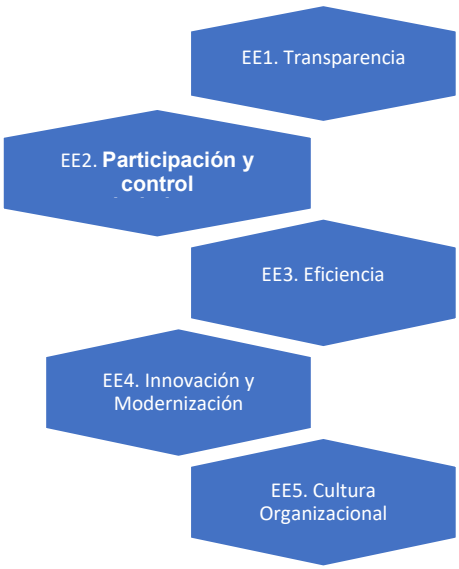
Se han adelantado actividades de divulgación y socialización de las políticas con el objetivo de fomentar la cultura de seguridad digital y se ha incorporado la protección de datos personales dentro de los documentos del modelo de seguridad y privacidad de la información.

En el año 2020 se llevó a cabo una auditoría interna al modelo, con el objetivo de identificar fortalezas y aspectos por mejorar para seguir avanzando en la implementación, con los resultados obtenidos se adelantaron acciones en el plan de 2021 y otras que se han considerado para el plan de 2022.

En el presente plan se busca dar cumplimiento a la resolución 500 de 2021 del MINTIC, con lo que se busca generar la estrategia de seguridad digital como una de las actividades a desarrollar.

## 5. ALINEACIÓN CON EL PLAN ESTRATEGICO.

Dentro del plan estratégico 2021 -2024 se encuentran 5 ejes estratégicos.




Dentro del eje estratégico 4 Innovación y modernización tecnológica, se encuentran considerado el objetivo estratégico OE9 Continuar con la modernización de la infraestructura tecnológica, que incorporan la estrategia 14 Cumplir con el Plan de

Seguridad y privacidad de la Información y evidencian la alineación del plan con el plan estratégico de acuerdo con lo definido en el Decreto 612 de 2018.

## 6. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se presenta una parte de la política de seguridad y privacidad de la información, para complementar el alcance manifestado en este documento.

El Senado de la República, encargado de ejercer las funciones constitucionales y legales del país, determina que el uso adecuado de la información es trascendental para la realización de las actividades propias de la Entidad, promoviendo el bien común y el desarrollo de la sociedad; razón por la cual, la corporación está comprometida a proteger sus activos de información (componente humano, tecnológico, software y documental), a través del Sistema de Gestión de Seguridad de la Información, con el firme propósito de preservar la confidencialidad, integridad y disponibilidad de la información, por medio de la generación de lineamientos, controles y asignación de responsabilidades, fundamentados en la Política 1 Nacional de Confianza y Seguridad Digital y en el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Para preservar la dirección estratégica institucional, el Senado de la República adopta la política general de seguridad y privacidad de la información, estableciendo su reciprocidad con los siguientes derroteros:

1. Minimizar el riesgo en los procesos físicos y digitales del tratamiento de información.
2. Cumplir con los principios de confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información institucional.
3. Implementar el sistema de gestión de seguridad de la información.
4. Proteger los activos de información.
5. Establecer las políticas específicas en materia de seguridad de la información.
6. Fortalecer la cultura de seguridad de la información.
7. Garantizar la continuidad del negocio y la prestación de los servicios.
8. Apoyar la innovación tecnológica.
9. Fomentar la transformación digital.
10. Generar confianza con las partes interesadas en el intercambio de información

**Alcance y aplicabilidad**.

La Política General de Seguridad y Privacidad de la Información aplica a:

a. Todos los niveles jerárquicos y dependencias del Senado de la República.
b. Todos los funcionarios, contratistas, judicantes, practicantes y visitantes que usen, tengan acceso o sean responsables de la información en el marco de la misión del Senado de la República, al igual que los proveedores que diseñen, administren, operen o sean responsables por la gestión de la información propiedad de la Entidad, y terceros con los cuales se tenga vínculo.
c. Toda la información creada, procesada o utilizada por el Senado de la República, sin distinción alguna del medio, formato, presentación o lugar en el que se encuentre.
d. Todos los activos de información del Senado de la República.
e. Todos los dispositivos que se conecten a las redes informáticas de la Entidad

## 7. PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Las actividades consideradas a cumplir para la vigencia 2022, incluyen la continuación con la implementación del modelo, y actividades resultado de la auditoria llevada a cabo en la vigencia 2020, así como el autodiagnóstico de MIPG en la opción de gobierno digital.

El seguimiento se realizará trimestralmente y se controlará el avance en el desarrollo de estas con reuniones mensuales.

**SENADO DE LA REPÚBLICA**

**PLAN INSTITUCIONAL**

| **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.** | | |
|---|---|---|
| **VIGENCIA PLAN: 2022** | | |
| **No.** | **Acción** | **Fuente de verificación** |
| **1** | Revisar la política de seguridad y privacidad de la información. | Acta de reunión. |

| | | |
|---|---|---|
| **2** | Definir y documentar la estrategia de seguridad digital, de acuerdo con lo establecido en la resolución 500 de 2021. | Plan actualizado con la estrategia de seguridad digital |
| **3** | Apoyar técnicamente la implementación de soluciones de protección perimetral de los sistemas de información ante ataques cibernéticos (WAF) | Informe de la Implementación del sistema firewall para aplicaciones Web |
| **4** | Identificar vulnerabilidades sobre elementos de la plataforma tecnológica institucional y formular planes de mejoramiento para realizar su tratamiento | Informe y recomendaciones de un análisis de vulnerabilidad. |
| **5** | Diseñar y apoyar la adopción de controles y lineamientos de seguridad de la información para la estrategia institucional de teletrabajo | Lineamientos de seguridad para la estrategia de teletrabajo institucional |
| **6** | Diseñar lineamientos y controles de seguridad que mitiguen los riesgos que puedan impactar la infraestructura de servicios de nube privada institucional | Lineamientos de seguridad para el uso de plataformas de nube contratada por la entidad. |
| **7** | Realizar revisión de procedimientos de seguridad de la información y generar actualización a los que corresponda. | Acta de reunión de la revisión de los procedimientos. |
| **8** | Elaboración del plan de recuperación ante desastres | plan de recuperación ante desastres |
| **9** | Elaboración del plan de continuidad de negocio | Plan de Continuidad (BCP) |
| **10** | Realizar la evaluación de la efectividad de los controles de seguridad de la información adoptados por la Entidad para el tratamiento de los riesgos de seguridad Digital | Informe de desempeño de los controles de seguridad de la información |
| **11** | Diseñar e implementar lineamientos y controles que mejoren los niveles de seguridad de los repositorios de información configurados en la plataforma Google Drive y FTP (***carpetas compartidas***) | Acta de reunión: Implementación de controles de seguridad de la información de la plataforma Google Drive y FTP (carpetas compartidas) |

| | | |
|---|---|---|
| **12** | Mejoramiento de roles y privilegios sobre las aplicaciones y servicios informáticos de la entidad | Acta de reunión para definir e implementar controles para el esquema de roles y privilegios de los sistemas de información y bases de datos gestionadas por la Entidad |
| **13** | Diseñar una estrategia para el desarrollo de pruebas de ingeniería social para evaluar el nivel de conciencia en seguridad de la información de los funcionarios y contratistas de la entidad | Documento con la estrategia. |
| **14** | Actualizar la Declaración de aplicabilidad si es requerido luego de revisar efectividad de los controles. | Documento con la declaración de aplicabilidad. |
| **15** | Actualizar inventario de activos de información. | Documento con Inventario de activos actualizado. |
| **16** | Actualizar Matriz de riesgos de seguridad y privacidad de la información. | Documento con la matriz de riesgos Actualizada |
| **17** | Elaborar y ejecutar plan de comunicación y sensibilización sobre seguridad de la información. | registros de ejecución del plan de comunicación y sensibilización. |
| **18.** | Realizar la identificación de riesgos asociados a la implementación de tecnologías emergentes. | Documento con los riesgos identificados. |
| **19** | Actualizar el diagnóstico de seguridad y privacidad de la información para la vigencia, construido a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) | Informe resumen del diagnostico del Modelo de seguridad y privacidad de la información. |
| **20** | Realizar la medición del sistema de gestión de seguridad y privacidad mediante la alimentación de los indicadores. | Informe con el resultado de los indicadores. |
| **21** | Elaborar el plan de apertura, mejora y uso de datos abiertos (MIPG) | Plan elaborado. |
| **22** | Determinar mejores prácticas que garanticen la privacidad de todos los conjuntos de datos personales. (MIPG) | Documento con la identificación de las mejores prácticas. |

| | | |
|---|---|---|
| **23** | Realizar la gestión para adquirir herramienta de análisis de vulnerabilidades. | Comunicación a DGA con la solicitud realizada con estudio de mercado. |
| **24** | Capacitar al personal en la gestión de incidentes de seguridad de la información | Evidencia de sesiones de capacitación desarrolladas. |
| **25** | Realizar cursos relacionados con la seguridad de la información, de acuerdo con las solicitudes realizadas en el Plan Institucional de Capacitación - PIC | Evidencia de los cursos realizados. |
| **26** | Identificar los proyectos en seguridad digital, que se pueden implementar para mejorar en áreas como CIC, data center y networking. | Informe de proyectos identificados. |
| **27** | Solicitar la renovación de los servicios asociados a la seguridad de la información como son firewall, IPS, antivirus, WAF y servidores en la nube. | Solicitudes realizadas a DGA. |

## 8. RESPONSABLES

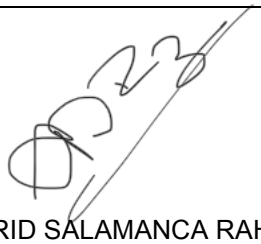
Dirección General Administrativa, responsable de aprobar los documentos de alto nivel del modelo de seguridad y privacidad de la información y de aprobar los recursos requeridos.

Las personas responsables en la elaboración del plan son los profesionales de la división de planeación y sistemas que apoyan las actividades relacionadas con el área de tecnología y son también responsables en la implementación de las actividades del Sistema de gestión de seguridad de la información SGSI.

Jefe de la división de planeación y sistemas gestionar la implementación del MSPI.

## 9. APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento de la Dirección General Administrativa, con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| Profesionales División Planeación y Sistemas. | DIANA ROCIO PLATA ARANGO<br>jefe División Planeación y Sistemas. |  <br>ASTRID SALAMANCA RAHIN<br>Directora General Administrativa<br>Fecha: Enero de 2022 |