PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SENADO DE LA REPUBLICA

2023

CONTENIDO

INTRODUCCION 3

1. OBJETIVO 3

2. ALCANCE 4

3. DOCUMENTO DE REFERENCIA 4

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

5. ALINEACION CON EL PLAN ESTRATEGICO 6

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

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

8. RESPONSABLES 9

9. APROBACION 10

INTRODUCCION

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 2023 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 2023

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. DOCUMENTO 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.

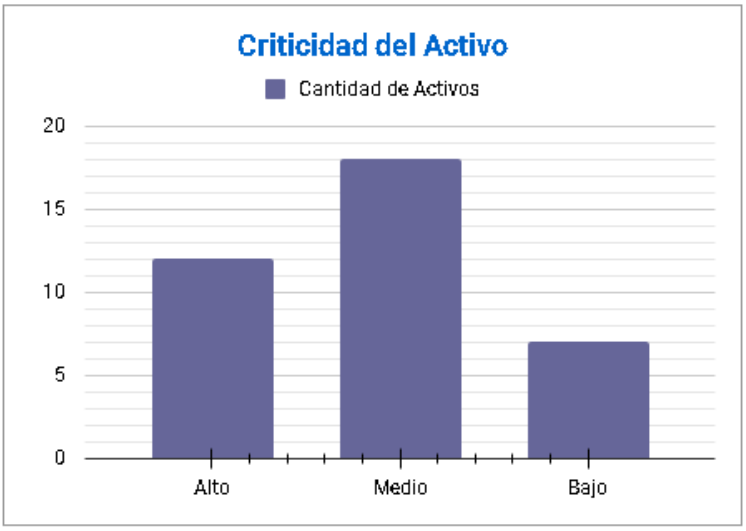
A partir de allí, se ha avanzado con la adopción de la política general de seguridad y privacidad de la información, procedimientos asociados a la seguridad y la elaboración del inventario de activos de información, que han permitido realizar la identificación de riesgos de seguridad con los controles 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	12
Medio	18
Bajo	7
TOTAL	37



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

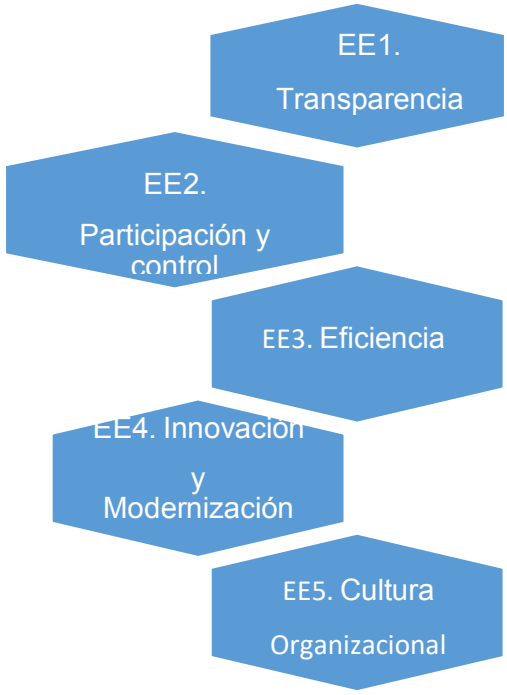
Se han adelantado actividades de divulgación y socialización de las políticas con el objetivo de fomentar la cultura de seguridad digital y se ha incorporado la protección de datos personales dentro de los documentos del modelo de seguridad y privacidad de la información.

En el año 2022 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 adelantaran acciones en el plan de 2023.

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. ALINEACION CON EL PLAN ESTRATEGICO

Dentro del plan estratégico 2021 -2024 del Senado de la Republica se encuentran los siguientes 5 ejes estratégicos: Transparencia, participación y control ciudadano, eficiencia, Innovación y Modernización Tecnológica y Cultura organizacional.



Dentro del eje estratégico 4 Innovación y modernización tecnológica, se encuentran considerada 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:

- Minimizar el riesgo en los procesos físicos y digitales del tratamiento de información.
- Cumplir con los principios de confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información institucional.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas específicas en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información.
- Garantizar la continuidad del negocio y la prestación de los servicios.
- Apoyar la innovación tecnológica.
- Fomentar la transformación digital.
- 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:

- Todos los niveles jerárquicos y dependencias del Senado de la República.
- 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.
- 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.
- Todos los activos de información del Senado de la República.
- 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 2023, incluyen la continuación con la implementación del modelo, y actividades resultado de la auditoria llevada a cabo en la vigencia 2022, 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

SEGURIDAD Y PRIVACIDAD DE LA INFORMACION		
VIGENCIA PLAN: 2023		
# Acción	**Acción**	**Fuente de verificación**
1	Realizar solicitud de los mantenimientos preventivos de la plataforma tecnológica (servidores, computadores, impresoras, Aires acondicionado, escáneres, UPS)	Comunicación a DGA con la solicitud realizada y la documentación requerida
2	Realizar solicitud de una bolsa de repuestos	Comunicación a DGA con la solicitud realizada y la documentación requerida
3	Revisar la política de seguridad y privacidad de la información.	Acta de reunión.
4	Actualizar inventario de activos de información.	Formato con Inventario de activos actualizado.
5	Realizar la gestión para adquirir herramienta de análisis de vulnerabilidades	Comunicación a DGA con la solicitud realizada y la documentación requerida
6	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.
7	Actualizar Matriz de riesgos de seguridad y privacidad de la información	Documento con la matriz de riesgos Actualizada
8	Realizar la actualización del plan de recuperación ante desastres	Plan de recuperación ante desastres actualizado
9	Realizar la actualización del plan de continuidad de negocio	Plan de Continuidad (BCP) actualizado
10	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 diagnóstico del Modelo de seguridad y privacidad de la información.

11	Actualizar la Declaración de aplicabilidad si es requerido luego de revisar efectividad de los controles.	Documento con la declaración de aplicabilidad.
12	Solicitar la renovación de los servicios asociados a la seguridad de la información como son: firewall, IPS, WAF, certificados digitales y Antivirus	Solicitudes realizadas a DGA con soportes
13	Actualizar el Plan de estrategia de seguridad digital	Plan actualizado
14	Realizar revisión de reportes del programa de gestión de monitoreo de la plataforma tecnológica -Orion-	Documento con reportes
15	Actualizar el Plan de sensibilización de seguridad de la información	Plan actualizado
16	Identificar los proyectos de seguridad digital y de tecnología que se pueden implementar en las áreas de la entidad	Proyectos identificados

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 lasactividades del Sistema de gestión de seguridad de la información SGSI.
- Jefe de la división de planeación y sistemas gestionar la implementación del MSPI.

9. APROBACION

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 de apoyo al área de sistemas	PABLO EDUARDO ALZATE PEREZ	ASTRID SALAMANCA RAHIN
División Planeación y Sistemas.	jefe División Planeación y Sistemas(E)	Directora General Administrativa