POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL DEL SENADO DE LA REPÚBLICA

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, seguridad digital, 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 y de seguridad digital.
6. Fortalecer la cultura de seguridad y privacidad de la información, así como la seguridad digital.
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.

11. Minimizar el riesgo de vulnerabilidad en la seguridad de la información en la ejecución de los procesos misionales de la entidad.

[1] Política Nacional formulada en el documento CONPES 3995 del 1 de julio de 2020.

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 que en razón del cumplimiento de sus funciones y las del SENADO compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.
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.

Localización.

Esta política aplica para todas las sedes físicas del Senado de la República, la sede electrónica y el catálogo de los servicios de tecnología e información, que se establezcan para el desarrollo de las actividades propias de la misión institucional.

Periodicidad.

La revisión al contenido de la política general de seguridad y privacidad de la información del Senado de la República se realizará como mínimo una vez al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales que afecten la operación de la entidad.

Nivel de cumplimiento.

Todas las personas al igual que los componentes enunciados en el alcance y aplicabilidad, independientemente de su localización, deberán dar cumplimiento a la política general de seguridad y privacidad de la información, Seguridad Digital del Senado de la República..

A continuación, se establecen los principios generales de seguridad que soportan el MSPI y de Seguridad Digital del Senado de la República:

i. El Senado de la República proporciona los recursos que permiten implementar un Gobierno de seguridad de la información alineado a los requisitos de Ley, contractuales, reglamentarios y a las necesidades de las diferentes áreas de la entidad, Así mismo facilita los medios para la educación, formación y concientización en materia de seguridad de la información.
ii. El Senado de la República mantiene el Modelo de Seguridad y Privacidad de la Información, enfocado a las necesidades del negocio con base a los requerimientos regulatorios que le aplican a su naturaleza.
iii. El Senado de la República ha definido instancias, roles y responsabilidades con base a

la normatividad aplicable a la Política General de Seguridad y Privacidad de la Información y Seguridad digital.

iv. El Senado de la República socializará y divulgará las responsabilidades frente a la seguridad de la información y seguridad digital a cada uno de los funcionarios, contratistas, judicantes, practicantes, proveedores, terceros y visitantes, con el fin de generar un cambio organizacional a través de la concienciación y apropiación de la responsabilidad personal en la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.
v. El Senado de la República protegerá la información generada, procesada o resguardada por los procesos del Sistema Integrado de Gestión, y los activos de información que hacen parte de los mismos, aplicando los controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
vi. El Senado de la República identificará y establecerá los controles para salvaguardar sus activos de información de las amenazas y vulnerabilidades que se puedan presentar a partir de la identificación de riesgos y de los controles asociados.
vii. El Senado de la República controlará la operación de sus procesos del Sistema Integrado de Gestión manteniendo la seguridad de los recursos tecnológicos y las redes de datos.
viii. El Senado de la República garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información que son administrados por la División de Planeación y Sistemas.
ix. El Senado de la República aplicará las normas relacionadas con la seguridad y privacidad de la información, seguridad digital y protección de la información personal.
x. El Senado de la República establecerá los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del Senado de la República.
xi. El Senado de la República establecerá los mecanismos pertinentes para proteger y preservar los documentos vitales o esenciales, al igual que el sitio o lugar de almacenamiento (físico o electrónico).

El incumplimiento a la Política General de Seguridad y Privacidad de la información, Seguridad Digital del Senado de la República, traerá consigo las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en la legislación que compete al Gobierno nacional en cuanto a Seguridad y Privacidad de la Información y seguridad digital se refiere.

Las Políticas específicas de manejo de la información se encuentran publicadas en la página web del Senado www.senado.gov.co.
A las anteriores ya existentes a la fecha, se adiciona la nueva Política de Seguridad Digital.
Es deber de todos aquellos a quienes se aplica la Política General de Seguridad y Privacidad de la Información, Seguridad Digital del Senado de la República conocer y acatar sus disposiciones. No podrá alegarse su desconocimiento para justificar la incursión en faltas disciplinarias o delitos.

POLÍTICA DE SEGURIDAD DIGITAL

Aplicación: Todos los empleados públicos o contratistas que hagan uso de los recursos tecnológicos del Senado de la República o que usando recursos tecnológicos de su propiedad compartan, utilicen, recolecten, procesen, intercambien o consulten su información, independientemente de su ubicación tienen la responsabilidad de cumplir cabalmente las

políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por tanto, el cumplimiento de la Misión del Senado de la República.

Para ello, deben acatar las siguientes disposiciones:

a. **Del uso del correo electrónico.** El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas del Senado de la República, cuyo uso se permitirá en los siguientes términos:

1. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional es el asignado por la División de Planeación y Sistemas, que cuenta con el dominio @senado.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
2. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
3. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo autorice.
4. Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la validez de los mensajes de datos.
5. La División de Planeación y Sistemas implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.
6. Se prohíbe el envío de correos masivos (más de 30 destinatarios) internos o externos, salvo los enviados por la Dirección General Administrativa, Presidencia del Senado, Secretaría General del Senado y los jefes de las Divisiones.

Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

7. Todo mensaje de correo electrónico enviado por el Senado de la República mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @senado.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.
8. Para apoyar la gestión de correo electrónico de los Senadores, el titular debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionado con los colaboradores que podrán escribir o responder en nombre del titular, con el fin de prevenir la suplantación.
9. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser reportado inmediatamente a la División de Planeación y Sistemas a través de la Mesa de Ayuda como incidente de Seguridad, según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif o explícitas referencias no relacionadas con la misión de la entidad.
10. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, pornografía, y/o cualquier otra ajena a los fines de la entidad.

Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes,

ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.

11. Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada del Senado de la República a otras entidades o ciudadanos sin la debida autorización previa y escrita del Presidente del Senado, de la Directora General Administrativa, del Secretario General y del Jefe de la División Jurídica.

El Senado de la República se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus empleados públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados por la misma, previa solicitud expresa del nominador, del Presidente del Senado, del Jefe de la Oficina de Control Interno. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que el Senado de la República realiza el referido monitoreo.

b. Del Uso de Internet: La División de Planeación y Sistemas, en conjunto con el Oficial de Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

1. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol, funciones u obligaciones que desempeña en el Senado de la República y para las cuáles esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.
2. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
3. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación del Senado de la República.
4. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
5. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

El Senado de la República se reserva el derecho de monitorear los accesos y el uso del servicio de internet, además de limitar el acceso a determinadas páginas de internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

C. Del uso de los recursos tecnológicos: Los recursos tecnológicos del Senado de la República son herramientas de apoyo a las funciones, responsabilidades y obligaciones de los empleados públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

1. Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del empleado público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Oficina de Planeación y Sistemas, salvo solicitud previa del Presidente del Senado, La Dirección General Administrativa, Los Jefes de División a través de la Mesa de Ayuda
2. Sólo está permitido el uso de software licenciado por el Senado y aquel que, sin requerir

licencia, sea expresamente autorizado por la Oficina de Planeación y Sistemas.

3. En caso de que el empleado público o contratista deba hacer uso de equipos ajenos al Senado, éstos deberán cumplir con la legalidad del software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red del Senado una vez avalado por la Oficina de Planeación y Sistemas.
4. Los empleados públicos y contratistas deben realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación.
5. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional o que violen los derechos de autor.
6. Los empleados públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la División de Planeación y Sistemas para gestionar la información digital del Senado de la República.
7. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren recursos tecnológicos o información física que por este hecho pueda estar expuesta al daño parcial o total y por ende a la pérdida de la integridad de ésta.
8. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los recursos tecnológicos por fallas en el suministro eléctrico o los equipos de cómputo.
9. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus elementos, son las designadas por la División de Planeación y Sistemas.
10. La División de Planeación y Sistemas realizará control y monitoreo sobre los dispositivos de almacenamiento externo como USB, CD-ROM, Discos duros externos, etc, con el fin de detectar fuga de información clasificada y reservada.
11. La única División autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la División de Bienes y Servicios con notificación a la División de Planeación y Sistemas, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
12. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la División de Bienes y Servicios y a la División de Planeación y Sistemas por el empleado público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea suministrado por el Senado, deberá reportarse a la División Jurídica siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias a que haya lugar.
13. La pérdida de información deberá ser informada con detalle a la División de Planeación y Sistemas, a través de Mesa de Ayuda, como incidente de seguridad.
14. La División de Planeación y Sistemas es la única dependencia autorizada para la administración de software del Senado de la República, el cual no debe ser copiado, suministrado a terceros ni utilizado para fines personales.
15. Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado autorizado y controlado por la División de Planeación y Sistemas.
16. La conexión a la red wifi institucional para empleados públicos y contratistas deberá ser administrada desde la División de Planeación y Sistemas mediante un SSID (SERVICE SET IDENTIFIER) único; la autenticación se debe poder realizar con usuario y contraseña de directorio activo.
17. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la División de Planeación y Sistemas, las contraseñas deberán cambiarse con una frecuencia establecida por la División.
18. La red wifi para empleados públicos y contratistas estará disponible para sus equipos

personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por el Senado de la República

19. Los equipos deberán quedar apagados una vez que el empleado público o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la seguridad y distribuir bien los recursos de la entidad, siempre y cuando no vaya a realizar actividades vía remota. Se excluyen de esta obligación, obviamente aquellos recursos tecnológicos de permanente funcionamiento y que son operados 24/7 por personal bajo turnos.
20. Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la División de Planeación y Sistemas con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, garantizando el cumplimiento de la Política de privacidad de la información.

d. Del uso de los sistemas o herramientas de información: Todos los empleados públicos y contratistas del Senado de la República son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

1. Las credenciales de acceso a la red y a los recursos informáticos (usuario y clave) son de carácter personal e intransferible; los empleados públicos y contratistas no deben revelarlos a terceros, ni utilizar claves ajenas.
2. Todo empleado público y contratista es responsable del cambio periódico de su clave de acceso a sistemas de información o recursos informáticos.
3. Todo empleado público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
4. Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución del contrato con el Senado de la República, todos los privilegios sobre los recursos informáticos otorgados deben suspenderse inmediatamente; la información que estos ostenten será almacenada en los repositorios de la entidad.
5. Cuando un empleado público o contratista cesa sus funciones o culmina la ejecución de su contrato con el Senado, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normatividad vigente.
6. Todos los empleados públicos y contratistas de la entidad deben respetar los derechos de autor establecidos en la Ley 23 de 1982, la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que la adicione, modifique o reglamente.

POLÍTICA DE CIBERSEGURIDAD

El Senado de la República protege y asegura los datos, sistemas y aplicaciones, provenientes y los que viajan, en el ciberespacio que son esenciales para la operación de la Entidad, para prevenir, mitigar y disminuir los impactos negativos potenciales de amenazas o ataques cibernéticos mediante los controles tecnológicos, las políticas de seguridad digital, los procedimientos y el trabajo conjunto con Entidades de apoyo en ciberseguridad y ciberdefensa.

La gestión de ciberseguridad contempla las etapas de prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, las cuales están enfocadas a la adecuada administración de riesgos de ciberseguridad y al mejoramiento continuo de la seguridad digital.

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD

El Senado de la República asegura la gestión de incidentes de seguridad digital incluyendo la comunicación interna y autoridades competentes de ser necesario.
Se tienen definidas las responsabilidades a través de procedimientos de gestión de incidentes para asegurar una respuesta eficaz y oportuna.

DIVULGACIÓN.

La Política General de Privacidad y Seguridad de la Información, Seguridad Digital del Senado de la República es un tema que debe ser conocido por todas las personas enunciadas en el alcance y aplicabilidad, para lo cual se utilizarán los medios de comunicación masiva para su divulgación. De igual forma es responsabilidad de la División de Planeación y Sistemas publicarla en los medios electrónicos institucionales existentes y socializarla continuamente, una vez sea aprobada.

ASTRID SALAMANCA RAHIN
Directora General
Senado de la República

Elaboró: Aldair Suarez R.
Actualizó en mayo 2022- Beatriz Suárez teniendo como base la actualización de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del MinTIC en la Resolución 448 de 2 de febrero de 2022 del MINTIC

Revisó: Pablo Eduardo Álzate
Revisó: Novoa Buendía S.A.S