Manual.

Manual de Políticas de Seguridad de Información

RT-Ma02

SISTEMA GESTIÓN DE CALIDAD

SENADO DE LA REPÚBLICA

TABLA DE CONTENIDO

Contenido

1. OBJETIVO

Establecer y difundir los criterios y comportamientos que deben seguir todos los servidores publicos, funcionarios de planta, contratistas, practicantes, terceros o cualquier persona natural o jurídica que tenga relación contractual con el Senado de la República, o que tenga acceso a los activos de información, con el propósito de preservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

El presente manual define la política, controles y directrices para el modelo de privacidad y seguridad de la información del Senado de la República. La política establecida aplica a todos los recursos y activos de información de la entidad.

3. TÉRMINOS Y DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la entidad y, en consecuencia, debe ser protegido.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que representa “Valor” para la entidad Independiente del tipo de activo, se deben considerar las siguientes características:

- No es fácil de reemplazar, sin incurrir en costos y/o tiempo.
- Forma parte de la identidad de la entidad y sin el cual puede estar en algún nivel de riesgo, como por ejemplo pérdida de imagen institucional.
- Los niveles de clasificación de la información que se ha establecido son: Información pública, información clasificada e información reservada.

Acuerdo de Confidencialidad: documento en el que los funcionarios del Senado o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tenga acceso en virtud de la labor que desarrollan dentro de la misma.
Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.
Amenaza: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso

físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
Contratista: Persona natural o jurídica que tiene vínculo con la entidad a través de un contrato legal.
Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada
Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.
Evaluación del Riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.
Evento de Seguridad de la Información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
Incidente de Seguridad de la Información: un evento o serie de eventos de seguridad de la información no deseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.
ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
Sistema de Información (SI): Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
Sistema de Gestión de la Seguridad de la Información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
Plan de Continuidad del Negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
Tratamiento del Riesgo: proceso de selección e implementación de medidas para modificar el riesgo.
Valoración del Riesgo: proceso global de análisis y evaluación del riesgo.

[1] Norma Técnica Colombiana NTC/ISO 2000:2011 Gestionando la Calidad de sus Servicios TI.

[1] Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información. Pág. 23

4. DESARROLLO DEL CONTENIDO

4.1 POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

El Senado de la República, como entidad del estado encargada de ejercer las funciones constitucionales y legales, establece que la información es vital para el desarrollo de sus actividades, por tal motivo está comprometido a proteger los activos de información de la entidad preservando la confidencialidad, integridad y la disponibilidad de sus operaciones.

La efectividad de esta política depende principalmente del comportamiento de los funcionarios y los controles establecidos en las políticas de seguridad establecidas en el presente documento, fundamentados en el **Modelo de Privacidad y Seguridad de la Información (MSPI).**

Objetivo:

Definir las directrices y reglas para generar una adecuada seguridad y protección de la información de los procesos del Senado de la República, estableciendo dentro del plan estratégico de TI su liderazgo y desarrollo, y adoptar las mejores prácticas del **Modelo de Privacidad y Seguridad de la Información (MSPI).**
Criterios.

- Se debe definir, implementar, revisar y actualizar las políticas de seguridad de la información, minimo una vez cada año.

- Todos los usuarios de sistemas de información de la entidad, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas. de seguridad de la información establecidas en el presente documento.
- Se debe establecer un programa que permita el fomento continuo de cultura y conciencia de seguridad en los funcionarios, contratistas, practicantes, personas naturales o jurídicas, usuarios de los sistemas de información del Senado de la República.
- Los jefes de división o dependencias deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información del Senado de la República.

Acuerdos de Confidencialidad:

Todos los funcionarios del Senado de la República y terceros deben aceptar los acuerdos de confidencialidad definidos por la Entidad antes de tomar posesión o firmar contrato, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a los activos de información de la entidad a personas o entidades externas. Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Cláusula de Confidencialidad

El contratista, en virtud de la suscripción del presente contrato se compromete a: 1) Manejar de manera confidencial la información que como tal le sea presentada y entregada, y toda aquella que se genere en torno a ella como fruto de la prestación de sus servicios. 2) Guardar confidencialidad sobre esa información y no emplearla en beneficio propio o de terceros mientras conserve sus características de confidencialidad o mientras sea manejada como un secreto empresarial o comercial. 3) Solicitar previamente y por escrito autorización para cualquier publicación relacionada con el tema del contrato, autorización que debe solicitarse ante el Supervisor o Interventor del contrato presentando el texto a publicar con un mes de antelación a la fecha en que desea enviar a edición.

.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

5. 1. Política de estructura organizacional de Seguridad de la información

El Senado de la República en cumplimiento al modelo de privacidad y seguridad de la información, cuenta con un esquema de seguridad de la información donde se encuentran definidos los roles y responsabilidades que involucran las actividades de operación, gestión y administración de la seguridad de la información, así como las funciones del Comité de privacidad y seguridad de la información de acuerdo con el **Modelo Integrado de Planeación y Gestión (MIPG)**.

5.2. Política para uso de dispositivos móviles

La entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, Avanteles, tabletas) entre otros, que hagan uso de los servicios de información de la entidad.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar el software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

El uso de los equipos portátiles y móviles fuera de las instalaciones del Senado de la República, será responsabilidad del usuario, al igual que la información que se encuentre resguardada en estos dispositivos.

5.3. Política de Seguridad para los Recursos Humanos

El Senado de la República implementa acciones para asegurar que los funcionarios, contratistas y demás colaboradores de la Entidad, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Se debe informar a los funcionarios sobre las políticas de seguridad de la información en las jornadas de inducción y reinducción, organizada por la División de Recursos Humanos

Los funcionarios, contratistas, pasantes, judicantes y proveedores deben dar aprobación a la entidad para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en base de datos personales, lo que se deberá ver reflejado en las cláusulas de los contratos.

El aspirante previo a la posesión del cargo de planta o unidad de trabajo legislativo (UTL), deberá cumplir con todos los requisitos de acuerdo con el formato verificación de Requisitos TH-Fr36, una vez posesionado el funcionario

deberá firmar el formato TH-Fr36 comunicación de condiciones para el tratamiento de datos personales.
En la inducción específica el funcionario deberá firmar el formato TH-Fr60 Registro de inducción específica, que incluye la comunicación de responsabilidades que asume en caso de ser encargado del tratamiento de bases de datos que contengan datos personales, de conformidad con la ley.

Se debe dar a conocer y notificar a los funcionarios, contratistas, practicante, judicantes y demás colaboradores del Senado de la República, la adopción de sus responsabilidades en relación con las políticas de seguridad de la información de la entidad y forma de actuar frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información.

En situaciones de incumplimiento o violaciones a las políticas de seguridad de la información, conllevará a notificar a la oficina coordinadora de control interno, conforme a lo dispuesto por las normas estatutarias y convencionales que rigen al personal de la Administración Pública.

El funcionario, **practicantes, judicantes** o contratista debe entregar los activos de información de acuerdo **Procedimiento de Nombramiento, Posesión y Retiro de funcionarios** (**Pr10) y el Formato Paz y Salvo (TH-Fr21)** el cual deberá ser verificado por el jefe a cargo o supervisor del contrato.

5.4. Política de gestión de activos de información

El Senado de la República es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios, contratistas, practicantes, judicantes o terceros, derivadas del objeto del cumplimiento de funciones o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

El Senado de la República es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o terceros que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información de TI.

La entidad debe realizar el tratamiento de información documental de acuerdo a lo establecidos en el **Programa de Gestión Documental (GD-Pg01)**.

Los activos de TI se deben mantener en una base de datos CMDB (*Configuration Management Data Base)*, responsabilidad de la División de Planeación y Sistemas.

5.5. Política de uso de los activos

La entidad definirá las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

El Senado de la República establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de estaciones por los usuarios finales.

Las directrices de uso de estaciones cliente, se encuentran definidas en el **Manual de Políticas de Gestión de Recursos Tecnológicos (RT-Ma01).**

5.6. Política de clasificación de la información

El Senado de la República con el fin de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y la Unidad de Archivo Administrativo, define reglas de cómo clasificar la información, liderado por el proceso de gestión documental de la entidad.

La entidad considera información, toda forma de comunicación o representación de conocimiento o datos digitales, contenido en cualquier medio (papel, intelectual, visual, magnético) que genera el Senado de la República como, por ejemplo:

- información en los sistemas, equipos informáticos, medios magnéticos, electrónicos o medios físicos como el papel.
- Formularios propios o de terceros.
- Soportes magnéticos/electrónicos removibles, móviles o fijos
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

Los funcionarios deben ser responsables de la información, identificar los riesgos a los que está expuesta la

información en sus dependencias, tomando como premisa que puede ser copiada, modificada, divulgada o destruida por personal interno y externo.

5.7. Política de manejo de información, medios y equipos

La entidad definirá las actividades necesarias para evitar la divulgación, modificación, retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por el Senado de la República.

Se deben definir las actividades necesarias para los medios y equipos donde se almacenan, procesan y se comunica la información, los cuales deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento.

Se debe realizar la aplicación del procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la entidad, de acuerdo a lo definido por el Senado de la República.

Para la realización de bajas de equipos que estén en desuso, obsoletos o en mal estado, se deberán seguir las actividades que se definen en el Procedimiento para la baja de bienes muebles BI-Pr08.

5.8. Política de uso de estaciones clientes

El Senado de la República establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de estaciones por los usuarios finales.

Las Directrices de uso de estaciones cliente se encuentran definidas en el **Manual de políticas de Recursos tecnológicos (RT-Ma01).**

5.9. Política de uso de internet

El Senado de la República permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, para prevenir errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones web.

El jefe de la División de Planeación y Sistemas autorizará los cambios solicitados de permisos de navegación a los usuarios de la entidad, previa solicitud del jefe de cada una de las dependencias, de acuerdo a lo definido en el **Manual de políticas de Recursos tecnológicos (RT-Ma01).**

La División de planeación y sistemas implementa herramientas para evitar la descarga e instalación de software no autorizado en los equipos de la entidad.
Los usuarios de los activos de información del Senado de la República tienen restringido el acceso a redes sociales (Facebook, Instagram, twitter, etc.), sistemas de mensajería instantánea, en caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a la División de Planeación y Sistemas.

5.10. Política de control de acceso

El Senado de la República definirá las reglas para asegurar un acceso controlado, físico y/o lógico a la información y plataforma informática, considerándose como importantes para el MSPI.

La conexión remota a la red de área local *(LAN Siglas en ingles)* de la entidad debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser definida, por la División de planeación y sistemas.

El acceso a las áreas de procesamiento de información (*Datacenter*), debe ser controlado por sistemas de control de acceso físicos y lógicos. De igual manera está prohibido el uso de cámaras, teléfonos móviles, equipos de grabación, etc...

Las áreas de procesamiento de información *(Datacenter*) deben estar vigiladas por CCTV, las grabaciones serán aseguradas por la División de planeación y sistemas y contar con su correspondiente respaldo.
Todo aplicativo informático o software comprado debe ser aprobado por la División de Planeación y sistemas en concordancia con el **Procedimiento Precontractual (PC-Pr02).**

5.11. Política de creación, uso y aseguramiento de claves de acceso

El Senado de la República suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta, comunicándose a la mesa de servicios, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña

para otra persona, debe ser realizada por su jefe inmediato mediante envió de oficio a la división de planeación y sistemas.

Las claves o contraseñas deben: Tener mínimo ocho (8) caracteres alfanuméricos. Cada vez que se cambien estas deben ser distintas.

La contraseña debe cumplir como mínimo con tres de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 8 dígitos
- Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)
- El sistema solicitará cambio de contraseña al momento de realizar alguna restauración

Manejo de contraseñas para administradores de tecnología

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Los usuarios súper-administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el *Datacenter* ubicado en la oficina 208B, se debe llevar una plantilla para el registro, uso u manejo de las mismas.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas o eliminadas. En caso de no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal de la división de planeación y sistemas no debe dar a conocer su clave de usuario a terceros de los sistemas de información.
Los administradores de los sistemas de información deben seguir las políticas de cambio de clave.

5.12. Política de uso de disco de red o carpetas virtuales

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Las Directrices de uso de uso de discos de red o carpetas virtuales se encuentran definidas en el **Manual de Políticas de Gestión de Recursos Tecnológicos (RT-Ma01)**.

5.13. Política de uso de puntos de red de datos

Asegurar la operación correcta y segura de los puntos de red.

Las Directrices de uso de puntos de red de datos, se encuentran definidas en el **Manual de Políticas de Gestión de Recursos Tecnológicos (RT-Ma01)**.

5.14. Política de uso de impresoras y servicio de impresión

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Las directrices de uso de impresoras y servicio de impresión, se encuentran definidas en el **Manual de Políticas de Gestión de Recursos Tecnológicos (RT-Ma01)**.

5.15. Política de controles criptográficos

Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

Se deben utilizar controles criptográficos para el resguardo de información, cuando surjan de las evaluaciones de riesgos por el propietario de la información y el responsable de la seguridad de la información.

Todas las paginas publicadas en internet, que se encuentren vinculadas al dominio senado.gov.co, deben utilizar certificado SSL para su funcionamiento.

5.16. Política de seguridad física

Se debe garantizar un control en la custodia de información y aplicativos alojados en los servidores y recursos tecnológicos del Senado de la República. La división de planeación y sistemas tiene implementado controles en el área de ingreso de los servidores y recursos tecnológico.
Las áreas donde se encuentren los servidores serán controladas por la División de Planeación y Sistemas, en donde no podrá ingresar personal sin autorización.

Las actividades realizadas por tercero deberán contar con acompañamiento de un funcionario de la entidad previo

autorización de la División de Planeación y sistemas y se registrará el ingreso y salida del área de servidores, el nombre de las personas que ingresaron, descripción de la actividad y fechas y horas
en el Formato ingreso personal no autorizado áreas seguras (RT-Fr 09)
Con el fin de llevar un control sobre las acciones que se realicen sobre los mismos o en su entorno.

5.17. Política de seguridad del Datacenter y centros de cableado

Se define que los sitios destinados al procesamiento o almacenamiento de información sensible, así como aquellos en los que se encuentren equipos, infraestructura de soporte a los sistemas de información y comunicaciones, son considerados de acceso restringido.
El Senado de la República tiene los siguientes formatos aprobados, los cuales deben ser diligenciados siempre que sea necesario:

- RT-Fr 09 Formato ingreso personal no autorizado áreas seguras
- RT-Fr 08 Formato personal autorizado ingreso áreas seguras

de la misma manera, y con el fin de asegurar la protección de la información en las redes y la protección de la infraestructura de soporte en las instalaciones del centro de datos o de los centros de cableado, no se encuentran permitidas las siguientes actividades:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Cada Gabinete o Rack contiene llave de ingreso, así como cada centro de cableado, las cuales deben permanecer en custodia de la División de Planeación y Sistemas.

5.18. Política de seguridad de los equipos

Se deben definir la protección de la información en los equipos de cómputo de la entidad. Lo anterior se definirá a través del documento de **lineamientos de seguridad de los equipos y de las operaciones de TI**

5.19. Política de pantalla y escritorio limpio

Los funcionarios, contratistas, practicantes, judicantes y proveedores que tienen algún vínculo con el Senado de la República deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicación de la entidad deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de la entidad deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Toda vez que se impriman documentos con información pública reservada o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

5.20. Política de seguridad de las operaciones de TI

Se deben definir las directrices de uso de seguridad de las operaciones de TI de la entidad. Lo anterior se definirá a través del documento de **lineamientos de seguridad de los equipos y de las operaciones de TI**

5.21. Política de adquisición, desarrollo y mantenimiento de sistemas de información

Se dictan las directrices de adquisición, desarrollo y mantenimiento de sistemas de Información:

- La División de Planeación y Sistemas deberá realizar pruebas de funcionamiento y de seguridad a las

aplicaciones en ambiente de pruebas, nuevos sistemas y actualizaciones, con el fin de validar la necesidad y operatividad de estos, previo a la aprobación e implementación en la entidad.

- La División de Planeación y Sistemas será la encargada de establecer los requerimientos técnicos y no funcionales para la adquisición de sistemas de información.
- las dependencias o áreas serán las encargadas de definir los requerimientos funcionales de los sistemas de información que se requieren.
- La División de Planeación y Sistemas implementa reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información del Senado de la República.
- Todo software o sistema de información que se adquiera deberá quedar licenciado a nombre del Senado de la República.
- La División de Planeación y Sistemas realizará las solicitudes de mantenimiento y soporte de los sistemas de información.
- Para actividades de desarrollo de software, el Senado de la República realizará la contratación de servicios profesionales cumpliendo con las normas relacionadas con derecho de autor

5.22. Política de respaldo y restauración de información

La División de Planeación y Sistemas definirá los medios de respaldo adecuados para asegurar que la información en los activos de TI se pueda restablecer, garantizando su restauración en caso de una falla o incidente.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por entidad. De igual manera, las directrices de respaldo y restauración de Información, se encuentran definidas en el **Procedimiento Generación de Copias de Seguridad y Restauración de Datos para Ambientes Virtualizados RT-Pr02)**

5.23. Política para la realización de copias en estaciones de usuario final

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe realizar un análisis previo por el software antivirus que se encuentra en cada uno de los equipos de cómputo.

El usuario final debe realizar copias de la información contenida en la estación de trabajo que se encuentren bajo su uso, teniendo en cuenta lo referente en el esquema de clasificación de la información.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la mesa de servicios vía correo electrónico a helpdesk@senado.gov.co o vía extensión 3030 y el acceso directo en el escritorio de las estaciones.

A través de los lineamientos de borrado seguro se deben definir los medios que vayan a ser eliminados o que cumplan el periodo de retención

El administrador de la plataforma de Backup de la entidad, deben generar mensualmente tareas de restauración aleatorias de la información y deben ser documentadas.

5.24. Política transferencia de información

- **Transferencia de información en medio físico**

  La transferencia en medios físicos se realizará de acuerdo a lo establecido por la Entidad en el **Programa de Gestión Documental (GD-pg01).**

- **Transferencia de información digital**

  Para la realización de transferencias de información digital de forma interna o externa de la entidad, se debe tener en cuenta el **Procedimiento Transferencia Segura de la Información (RT-Pr07)**

- **Características mínimas para la transferencia de información.**

  El acuerdo de transferencia de información con organizaciones deberá contener cláusulas donde se establezcan las herramientas a utilizar para asegurar la transferencia de información.

  Definir los mecanismos a utilizar para evitar la interceptación, copiado, modificación y destrucción de información.

Establecer en el acuerdo de transferencia de información quienes asumirán los costos de servicios y licenciamiento necesarios.

Incluir acuerdos de confidencialidad de la información, compromiso y reserva, el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información.

El Senado de la República se reservará el derecho de suspender de manera unilateral los servicios que hacen parte del objeto del acuerdo, así como la terminación unilateral del mismo.

El acatamiento total de la política de seguridad de la información establecida por el Senado de la República es de obligatorio cumplimiento, el cual deberá ser notificado y acatado por los funcionarios que tengan acceso a las actividades del acuerdo de transferencia de información.

La transferencia de información digital será liderada por la División de Planeación y Sistemas, con la coordinación del Área u oficina que manifieste la necesidad.

5.25. Política de uso de correo electrónico

Se definen las pautas generales para asegurar una adecuada protección de la información de la entidad, en el uso del servicio de correo electrónico por parte de los usuarios.

Las directrices de uso de correo electrónico se encuentran definidas en el **Manual de Políticas de Gestión de Recursos Tecnológicos (RT-Ma01)**.

5.26. Política de Relación Con los Proveedores

Se deben establecer criterios de selección que contemplen la experiencia de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la empresa, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Todos los proveedores y terceros, deben firmar un acuerdo de confidencialidad, en el cual se indique los lineamientos a seguir, la privacidad y uso de la tecnología, al igual que las consecuencias jurídicas y legales en caso de incumplirse

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información del Senado de la República, las cuales deben se divulgadas por los funcionarios responsables de la realización y firma de contratos o convenios.

La División de Planeación y Sistemas deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y contratistas a los sistemas de información de la entidad.

Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

5.27. Política de gestión de vulnerabilidades

El Senado de la República se compromete a realizar gestión de las vulnerabilidades anualmente, con el fin de identificarlas y realizar un análisis para su prevención o corrección.

5.28. Política de gestión de los incidentes de seguridad de la información

El Senado de la República establecerá responsables y seguirá el **Procedimiento Soporte Técnico y Atención de Servicios (RT-Pr01)**, para la atención de incidentes de seguridad de la información asegurando una respuesta oportuna y eficaz, implementando las acciones necesarias para evitar su repetición.

5.29. Política de cumplimiento de requisitos legales y contractuales

El Senado de la República respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.

La División de Planeación y Sistemas deberá garantizar que todo el software que se ejecute en los activos de información que cumpla con los derechos de autor. Los usuarios y funcionarios de la entidad deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.

5.30. Política de revisiones de seguridad de la información

Se debe implementar el Modelo de Seguridad y Privacidad de la información (MSPI) de acuerdo a las políticas y

procedimientos implementados en el Senado de la República.

La Oficina Coordinadora de Control Interno realizará auditorías al Modelo de Seguridad y Privacidad de la información (MSPI), para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.

Los Altos Directivos, secretarios, Jefes de División, Asesores, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

6. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de la Entidad podrán ser restaurados dentro de escalas de tiempo razonables.

El Senado de la República deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La Dirección General Administrativa será la responsable de ejecutar la implementación y cumplimiento de las medidas relativas a este plan.

La División de Planeación y Sistemas es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas y se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio.

7. CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas, practicantes, judicantes y proveedores del Senado de la República. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por descuido, la entidad tomará las acciones disciplinarias y legales correspondientes.

8. CONTROLES

El Manual de la Política de Seguridad de Información del Senado de la República está soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología de la Entidad pueden consultar los procedimientos a través de la División de Planeación y Sistemas y a través del Sistema de Gestión de Calidad.

9. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en el numeral 6.1.3d del estándar ISO/IEC 27001, menciona los controles existentes al momento de definir el Sistema de Gestión de Seguridad de la Información y realizar el análisis de riesgos, así como los controles y objetivos de control que han sido seleccionados con base en el análisis y evaluación de riesgos, en los requerimientos de seguridad identificados y por ende, en las definiciones dadas en el plan de tratamiento del riesgo.

La declaración de aplicabilidad debe ser documentada y actualizada cuando cambien las condiciones de la Entidad, los procesos, la infraestructura tecnológica, el análisis de riesgos, entre otros.

10. BASE LEGAL

- Manual de la política de seguridad de la información M-TI-01 – Presidencia de la República
- Constitución Política de Colombia 1991
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal. • Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.

- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”
- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

11. ANEXOS

No aplica

12. FORMATOS

No aplica

13. DOCUMENTOS RELACIONADOS

No aplica

14. CONTROL DE CAMBIOS

Control de Cambios

7. Ver. 001// Rev. 5// FV. 12 de septiembre de 2017
   Cambios: Versión inicial del documento
   Justificación:
   Responsable: Arley Andres Sánchez Morales
   Fecha: 2017-09-26

8. CONTROL DE CAMBIOS

Control de Cambios

- Ver. 003// Rev. 1// FV. 26 de noviembre de 2021

  Cambios:

  Se solicita la modificación del presente procedimiento, con el fin realizar actualización y revisión ya que su última versión era del año 2019 y adicionar temas de virtualidad debido a la pandemia.

  - Se modificó la redacción en diferentes partes del documento
  - Se agrega en políticas generales de seguridad de la información que se debe revisar y actualizar las políticas de seguridad de la información, mínimo una vez cada año.
  - Se incluyen los formatos a tener en cuenta en las siguientes políticas: Política de Seguridad para los Recursos Humanos, Política de seguridad física, Política de seguridad física y Política transferencia de información.
  - Se cambia la declaración de aplicabilidad.

Justificación:

Responsable: Maria Paula Vesga Ospina

Fecha: 2021-11-26

- Ver. 002// Rev. 1// FV. 8 de mayo de 2019

Cambios:

Se realiza actualización del documento, en lo que refiere a los siguientes puntos:

-Objetivo

-Alcance

-Terminos y definiciones

-Politicas generales de seguridad de la información.

-Politicas de Seguridad de la información

-Gestión de la continuidad del negocio

-Cumplimiento

-Controles

-Declaración de aplicabilidad.

Justificación:

Responsable: Yenni Yanire Yela Yela

Fecha: 2019-05-08

- Ver. 001// Rev. 1// FV. 12 de septiembre de 2017

Cambios: Versión inicial del documento

Justificación:

Responsable: Arley Andres Sanchez Morales

Fecha: 2017-09-26

ELABORÓ	REVISÓ	APROBÓ
Nombre: Aldair Suarez	Nombre: Diana Rocio Plata Arango.	Nombre: Grupo Evaluador de Documentos
Cargo: Profesional Universitario	Cargo: Jefe División Planeación y Sistemas	No. Acta y Fecha: 31 de 22 de noviembre de 2021