Manual.

Manual de Políticas de Seguridad de Información

RT-Ma02

SISTEMA GESTIÓN DE CALIDAD

SENADO DE LA REPÚBLICA

TABLA DE CONTENIDO

1. OBJETIVO
2. ALCANCE
3. TÉRMINOS Y DEFINICIONES
4. DESARROLLO DEL CONTENIDO
4.1 POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN
4.2 REVISIÓN DEL MANUAL
4.3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
4.3.1. Roles y responsabilidades
4.3.2 Contacto con las autoridades
4.3.3. Contactos con grupos de interés
4.3.4. Seguridad de la información en la gestión de proyectos
4.4. DISPOSITIVOS MÓVILES
4.4.1. Política de Dispositivos Móviles Corporativos
4.4.2. Política de uso de dispositivos móviles no corporativos
4.5. TELETRABAJO
4.5.1. Lineamientos para la División de planeación y Sistemas
4.5.2. Lineamientos Generales
4.6. SEGURIDAD DE LOS RECURSOS HUMANOS
4.6.1. Previa vinculación de un funcionario es importante considerar
4.6.2. Previa vinculación de un contratista
4.6.3. Inicio de Ejecución del contrato
4.6.4. Durante la Ejecución del empleo de funcionario o contratista
4.6.5. Terminación o cambio de responsabilidades de empleo
4.6.6. Procesos Disciplinarios
4.6.7. Intercambio de Información
4.7. GESTIÓN DE ACTIVOS
4.7.1. Inventario de activos
4.7.2. Uso aceptable de los activos
4.7.3. Uso de equipos de cómputo
4.7.4. Uso de Internet
4.7.5. Uso del Correo Institucional
4.7.6. Clasificación de la Información
4.7.7. Gestión de Medios Removibles
4.7.8. Disposición de los Medios
4.7.9. Transferencia de Medios Físicos
4.8. CONTROL DE ACCESO
4.8.1. Acceso a Redes y Servicios en Red
4.9.2. Solicitud o Inicio de Acceso
4.9.3. Suspensión o Terminación de Acceso
4.9.4. Revisión o Validación de Accesos 4.9.5. Normas para la Creación de Contraseñas
4.9.6 Control de Acceso a las Aplicaciones y Recursos Tecnológicos
4.9.7. Restricción del Acceso a la Información

4.9.8. Control de Acceso a la Red
4.9.9. ACCESO A DATOS DE PRODUCCIÓN
4.9.10. CONEXIONES REMOTAS
4.10. CONTROLES CRIPTOGRÁFICOS
4.10.1. Firma Digital
4.10.2. Cifrado de la Información
4.10.3. Certificados Digitales
4.11. SEGURIDAD FÍSICA Y DEL ENTORNO
4.11.1. Áreas Seguras
4.11.2. Ubicación y Protección de los Equipos
4.11.3. Servicios de Suministro
4.11.4. Seguridad del Cableado
4.11.5. Mantenimiento de Equipos
4.11.6. Seguridad de los Equipos
4.11.7. Disposición Segura o Reutilización de Equipos
4.11.8. Política de Equipo Desatendido, Pantalla y Escritorio Limpio
4.12. SEGURIDAD DE LAS OPERACIONES
4.12.1. Documentación de Procedimientos Operativos
4.12.2. Control de Cambios
4.12.3. Gestión de Capacidad
4.12.4. Separación de los Ambientes
4.13. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS
4.14. COPIAS DE RESPALDO
4.15. REGISTRO Y SUPERVISIÓN DE EVENTOS
4.15.1. Registro de Eventos
4.15.2. Sincronización de Relojes
4.16. CONTROL DE SOFTWARE OPERACIONAL
4.16.1. Instalación de Software en Sistemas Operativos
4.17. GESTIÓN DE LA VULNERABILIDAD TÉCNICA
4.17.1. Gestión de las Vulnerabilidades Técnicas
4.18. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN
4.18.1. Controles sobre auditorias de sistemas de información
4.19. SEGURIDAD EN LAS COMUNICACIONES
4.19.1. Gestión de la Seguridad en las Redes
4.19.2. Transferencia de Información
4.20. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
4.20.1. Requisitos de Seguridad de los Sistemas de Información.
4.20.2. Seguridad en los Procesos de Desarrollo y Soporte
4.20.3. Ambiente de Desarrollo Seguro
4.20.4. Desarrollo Contratado Externamente
4.20.5. Pruebas de Seguridad de Sistemas
4.20.6. Pruebas de Aceptación de Sistemas
4.21. RELACIÓN CON LOS PROVEEDORES
4.21.1. Seguridad de la Información en las Relaciones con los Proveedores.
4.21.2. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores.
4.22. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

4.23. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
4.24. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO
4.25. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN
5. CUMPLIMIENTO
6. DECLARACIÓN DE APLICABILIDAD
7. BASE LEGAL
8. ANEXOS
9. FORMATOS
10. DOCUMENTOS RELACIONADOS
11. CONTROL DE CAMBIOS

1. OBJETIVO

Establecer y difundir los criterios y comportamientos que deben seguir todos los servidores públicos, 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 establece los lineamientos de seguridad a partir de la definición de cada una de sus políticas y es aplicada para toda la información en cada uno de sus procesos y activos de información del Senado de la República

3. TÉRMINOS Y DEFINICIONES

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Entidad.

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.

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 Dirección general Administrativa mediante la aprobación de esta Política declara su posición y compromiso con el cumplimiento de los requisitos definidos en el marco del MSPI, aspectos en los cuales se involucra directamente la función de seguridad de la información, que tiene como propósito principal mantener un ambiente razonablemente

seguro, alineado a la misión, objetivos estratégicos de la Entidad y requerimientos regulatorios aplicables, definiendo e implementando buenas prácticas que permitan minimizar posibles impactos no deseados que puedan comprometer los principios esenciales de Seguridad de la Información.

4.2 REVISIÓN DEL MANUAL

El manual de políticas de seguridad de la información debe ser revisado al menos una vez al año o cuando surjan cambios relevantes de mejora y de cumplimiento al Modelo de Seguridad y Privacidad de la Información (MSPI) del Senado de la República

La documentación a la que hace llamado cada una de las políticas relacionadas en este manual, hacen parte del proceso de recursos tecnológicos de la División de Planeación y Sistemas, tales como; (procedimientos, instructivos, formatos, etc.) la cual, se ha venido fortaleciendo a través de actualizaciones o creación de algunos de éstos, fundamentales para el cumplimiento de los lineamientos establecidos en este manual.

4.3. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4.3.1. Roles y responsabilidades

Todo el personal que tenga acceso a la información de la entidad es responsable de velar por la seguridad de la información a la que tiene acceso y de cumplir las políticas descritas en este manual; entre ellos están: servidores públicos, contratistas, proveedores, terceros, convenios entre instituciones y visitantes.

La Alta Dirección, es el ente máximo en la entidad y se encuentra representado por los miembros del Comité Institucional de Gestión y Desempeño del Senado de la República, es responsable de revisar y aprobar la política de Seguridad de la Información; revisar la eficacia de la implementación de la política de Seguridad; proporcionar y avalar los recursos necesarios para el desarrollo e implementación de iniciativas de Seguridad; comunicar la importancia de una gestión eficaz de la Seguridad de la Información y Ciberseguridad; promover el cumplimiento de las políticas y normas definidas.

La División de Planeación y Sistemas, es la líder de la implementación y gestión de los controles de ciberseguridad que afecten sistemas de información, aplicaciones, plataformas de apoyo o infraestructura de comunicaciones y seguridad que se encuentre bajo administración de la Jefatura de la División de planeación y Sistemas, es responsable definir políticas, procedimientos de gestión de accesos lógicos y esquema, metodología de construcción de roles y perfiles para los accesos a plataformas e infraestructura de la Entidad; definir procedimientos de gestión de logs; definir líneas base, guías de aseguramiento, etc. para aseguramiento de los sistemas; definir la metodología y procedimientos del ciclo de vida de desarrollo de software

incluyendo requerimientos de seguridad en cada etapa; definir la estrategia de respaldo de información; definir políticas y procedimientos de gestión de cambios; definir el diseño de red y plataformas tecnológicas teniendo en cuenta las necesidades de la Entidad Implementación de planes de remediación de vulnerabilidades; adquirir e implementar herramientas de gestión de logs y correlación; adquirir e implementar tecnologías de seguridad; adquirir, implementar y configurar la red y las plataformas tecnológicas de acuerdo con el diseño propuesto; realizar los ajustes/mejoras necesarias en el proceso de desarrollo de software; ajustes o mejoras a la estrategia de respaldo de información.

Los propietarios de los activos de información, son los líderes de proceso que tienen la responsabilidad de establecer la valoración de los activos, clasificación y respectivo etiquetado teniendo en cuenta el modelo de clasificación de la información en la entidad, igualmente definir el nivel de protección requerido ante accesos no autorizados, pérdida de la confidencialidad, integridad o disponibilidad; realizar el respectivo etiquetado de la información teniendo en cuenta la clasificación definida; mantener actualizada la matriz de activos de información

validando los controles de acceso asignado a los activos; identificar riesgos asociados con la seguridad de la Información en los procesos de los cuales son responsables o tienen participación; reportar oportunamente eventos o incidentes de Seguridad de la Información

4.3.2 Contacto con las autoridades

El Senado de la República, debe mantener contacto actualizado con las autoridades competentes para el cumplimiento de la Ley; como los organismos de control (Procuraduría General de la Nación, Contraloría General de la República, Fiscalía General de la Nación), Fuerzas Militares (Policía Nacional, Comando Conjunto Cibernético).

La División de Planeación y Sistemas debe definir y actualizar el listado de autoridades a contactar en caso de que se sospeche de la violación de la Ley (Normograma), para mantener contacto con organismos de control y autoridades; los funcionarios y contratistas pueden consultar el marco legal aplicable en el Normograma de la Entidad.

4.3.3. Contactos con grupos de interés

El Senado de la República, a través de la División de Planeación y Sistemas debe mantener contacto con grupos de interés especial, foros y asociaciones profesionales en el campo de la seguridad de la información.

Lo anterior con el fin de estar al día con la información relacionada con la seguridad de la información, recibiendo comunicados de actualizaciones de software, notificaciones de ataques de vulnerabilidad día cero, avisos de ciberataques o ataques cibernéticos, reporte de vulnerabilidades y amenazas nuevas.

4.3.4. Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe integrar al procedimiento de gestión de proyectos del Senado de la República, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Esto debe aplicar a cualquier proyecto, independientemente de su naturaleza.

Por lo tanto, es responsabilidad de los líderes de proyectos, de los dueños de proceso, de los funcionarios y contratistas, asegurar que se sigan las siguientes directrices:

- Realizar valoración de los riesgos de seguridad de la información en la fase de estudios previos del proyecto, para identificar los controles necesarios.

- Hacer seguimiento a los riesgos y controles aplicados para tratar los riesgos, durante todas las fases del proyecto.

4.4. DISPOSITIVOS MÓVILES

Los dispositivos móviles corporativos (teléfonos inteligentes, tablet, portátiles), son herramientas de trabajo que se deben utilizar únicamente para el desarrollo de actividades relacionadas con los procesos de la Entidad.

4.4.1. Política de Dispositivos Móviles Corporativos

- Con el fin de minimizar los riesgos de seguridad de la información que implica el uso de dispositivos móviles la DPS debe controlar la conexión de dispositivos móviles tales como Smartphone, tablets y computadores personales de los contratistas a la red corporativa, a excepción de los dispositivos que sean propiedad de la Entidad.

- Las estaciones de trabajo y equipos portátiles que son propiedad de la Entidad cuentan con software licenciado y protección contra código malicioso. Solo el personal de soporte de la DPS está autorizado a instalar software específico en los dispositivos móviles propiedad de la Entidad.

- El Senado de la República se reserva el derecho de revisar cuando se requiera el software instalado y utilizado en equipos de cómputo y servidores, además para los portátiles de los contratistas que se conecten a la red corporativa, se deben validar algunos aspectos de seguridad, entre éstos: antimalware activo y actualizado, sistema operativo actualizado, no permitir que se conecte a internet desde la red de los funcionarios, etc.

- El mantenimiento de dispositivos que son propiedad de la Entidad son responsabilidad de la DPS. Por tanto, los usuarios no deben realizar cambios en el hardware, software o modifique la configuración del equipo sin autorización de la DPS.

- La información de la Entidad que no sea estrictamente necesaria para el desarrollo de las tareas del usuario no debe almacenarse en el dispositivo. Si se accede a la información desde varios dispositivos, esta tiene que estar sincronizada para evitar duplicidades y errores en las versiones. Los funcionarios autorizados por su respectivo jefe deben solicitar a la DPS la creación de los almacenamientos de datos para el intercambio de información al interior de la Entidad.

- Si un funcionario o contratista sospecha la infección por virus u otro software malicioso, se debe notificar a la mayor brevedad posible al personal de soporte de la DPS.

- El computador de la Entidad no debe quedar expuesto a altas temperaturas que puedan dañar sus componentes. El usuario debe impedir que se pueda acceder a la información almacenada en el mismo.

- En ningún caso se debe descuidar el portátil, celular o Tablet si se viaja en transporte público. También debe estar protegidos físicamente contra robo, especialmente cuando se dejan en automóviles y otras formas de transporte, habitaciones de hotel, etc.
- Los dispositivos que contienen información sensible o crítica para la entidad no se deben dejar sin supervisión, y donde sea posible, debe estar protegidos bajo llave o se debe usar guayas para asegurarlos, adicionalmente, los computadores portátiles que salgan de la entidad y de surgir un robo a éste, se debe comunicar inmediatamente a la División de Planeación y Sistemas para seguir los pasos de reporte del incidente y comunicarlo a la Policía Nacional.

- La información sensible o crítica para la entidad no se debe reposar o ser almacenada en los equipos personales de los contratistas.

- El usuario debe aplicar las buenas prácticas de uso del puesto de trabajo que sean relativas al uso de un equipo móvil (obligación de notificar incidentes de seguridad, uso correcto de las contraseñas, bloqueo del equipo, entre otras).

- El usuario es el responsable del equipo portátil o móvil que se le ha facilitado para el desempeño de sus tareas fuera de las instalaciones de la Entidad. Por tanto, es el funcionario el que debe garantizar la seguridad tanto del equipo como de la información que contiene.
- Esta normativa es de obligatorio cumplimiento y debe ser objeto a los acuerdos que se firmen al aceptar el uso de estos dispositivos.

- Los funcionarios que viajan por asuntos de la Entidad son responsables de la seguridad de la información propiedad de la entidad.

4.4.2. Política de uso de dispositivos móviles no corporativos

Todo personal que tenga vínculo laboral con la entidad que utilice equipos de cómputo de su propiedad para el desarrollo del objeto del contrato debe tener y usar solo software legal instalado en su equipo, además de Contar con software antivirus licenciado.

- Los contratistas que tienen información corporativa en sus dispositivos móviles personales son responsables de la seguridad de la información en su poder.
- Es recomendable contar con un software antivirus en su dispositivo móvil.
- Se recomienda solo descargar apps de sitios oficiales (Apple Store, Play Store, Etc.)
- En lo posible se debe evitar almacenar información de la Entidad en los dispositivos móviles personales.

4.5. TELETRABAJO

La implementación del teletrabajo en el Senado de la Republica supone una transformación organizacional, desde sus formas de planear y hacer, hasta sus formas de realizar seguimiento y evaluación. La adopción de esta modalidad y organización laboral requiere del liderazgo del equipo directivo y la participación de un equipo de trabajo coordinado, la utilización de recursos y la movilización hacia un cambio cultural y de procedimientos, que son posibles de alcanzar con el apoyo de las directivas que respalden las iniciativas de aplicar el teletrabajo.

Los lineamientos para la adopción del modelo de teletrabajo en el Senado de la República se especifican en la Resolución 542 de 2023 “Por la cual se adopta la política interna de teletrabajo y se dictan lineamientos generales para su implementación.

4.5.1. Lineamientos para la División de planeación y Sistemas

Contar con las capacidades y disponibilidad de los servicios de VPN, seguridad en los servicios de correo electrónico y el acceso a la información de la Entidad.

- Realizar oportunamente copias de seguridad de los datos en la nube.
- Disponer de protocolos para contar con una clara identificación de roles y responsabilidades del personal de la DPS.
- Contemplar herramientas para la gestión remota en la Entidad.
- Preparar a los funcionarios que prestan el soporte para la instalación y la configuración de los equipos para trabajo remoto.
- Verificar el uso de software licenciado en equipos propios de la entidad.

- Determinar requisitos de seguridad sobre el firewall y de protección contra software malicioso.

4.5.2. Lineamientos Generales

El funcionario o contratista debe haber instalado el cliente de VPN en el computador personal de su hogar, con el fin de conectarse vía remota a los servicios tecnológicos de la Entidad., en el caso que sea necesario.

- Establecida la conectividad, el usuario debe autenticarse con las credenciales normales de acceso brindada por el Directorio Activo. Esto permite que el usuario ingrese a los sistemas de información y recursos compartidos como si estuviera dentro de las oficinas del Senado de la República.
- Por seguridad, el usuario no debe copiar archivos desde su sistema de archivos del computador de la casa hacia el computador al cual está conectado por la VPN y que es propiedad de la Entidad.
- Todos los archivos que gestione el usuario mientras estén conectados por VPN en la estación de trabajo propiedad de la Entidad., no deben ser descargados a las unidades locales o escritorio del computador de la casa.
- Es importante que el usuario no se conecte a internet a páginas como YouTube, streeming, redes sociales, entre otras a través de la VPN y desde la estación de trabajo de la Entidad.
- Se debe realizar desconexión y conexión continua mientras se realizan labores que no requieren de conectividad a la Red de la entidad.
- Todos los usuarios deben usar su espacio en la nube de almacenamiento DRIVE para garantizar copias de respaldo de su información.

4.6. SEGURIDAD DE 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, practicante, judicante 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.

4.6.1. Previa vinculación de un funcionario es importante considerar

Aunque la vinculación en el Senado de la República se rige por la Ley 5ta de 1992. Es importante que la División de Recursos Humanos proporcional a las responsabilidades o al manejo de información sensible de la Entidad, establezca un proceso de verificación de los antecedentes de los candidatos que aspiran a un cargo, el cual se debe llevar a cabo de acuerdo con las leyes y reglamentos, siendo proporcionales a los requisitos dentro de la ENTIDAD, a la clasificación de la información que va a tener acceso y, a los riesgos percibidos.

4.6.2. Previa vinculación de un contratista

La Dirección General Administrativa es la responsable del proceso precontractual y contractual, la cual debe tener en cuenta toda la privacidad pertinente, la protección de la información de datos personales y legislación laboral, y cuando se permita, debe incluir lo siguiente:

- La disponibilidad de referencias satisfactorias, por ejemplo, una comercial y una personal.
- Una verificación (completa y precisa) de la hoja de vida del solicitante.
- Confirmación de las certificaciones y títulos brindados.
- Una verificación de identidad independiente (pasaporte o documento similar).

- Una verificación más detallada, como la información de antecedentes penales.
- Establecer acuerdos o compromisos contractuales con el personal contratista donde se indiquen las responsabilidades en cuanto a la seguridad de la información.
- Firma formato de autorización de tratamiento de datos personales por parte del contratista.

4.6.3. Inicio de Ejecución del contrato

El cumplimiento de las Políticas de Seguridad de la Información por parte de todos los funcionarios, contratistas, proveedores o terceros o cualquier persona que tenga una relación contractual o situacional con la Entidad, o que tengan acceso a los activos de información debe ser informado en el momento que inicie sus actividades contractuales, desde Recursos Humanos para los funcionarios de planta y para los demás colaboradores de la Entidad, desde el supervisor del contrato.

- Todo funcionario, contratista, proveedor o tercero que desde su gestión o alcance del contrato requiera del acceso a un sistema de información o a la red corporativa de la entidad, debe hacer la solicitud vía correo electrónico a la División de Planeación y Sistemas, previa autorización del jefe directo.
- La solicitud debe especificar claramente los permisos que el funcionario, contratista, proveedor o tercero, requiere para sus actividades y acceso a los sistemas de información u otro componente tecnológico, especificando los privilegios a ser asignados en el sistema de información o servidor si es el caso.
- Desde la División de Planeación y Sistemas se debe gestionar el requerimiento descrito dando alcance a cada solicitud con el especialista del sistema de información o componente tecnológico que corresponda.

4.6.4. Durante la Ejecución del empleo de funcionario o contratista

Todos los funcionarios o contratistas a los que se brinde acceso a información confidencial deben firmar un acuerdo de confidencialidad y no divulgación de información, antes de tener acceso a las instalaciones de procesamiento de información, así mismo:

- Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades y derechos con relación a leyes sobre derecho de autor o legislación sobre protección de datos personales.
- Los dueños de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades para la clasificación de la información y la gestión de activos institucionales asociados con información, instalaciones de procesamiento de información y servicios de información que deben ser manejados por el funcionario o contratista.

- Los líderes de proceso deben asegurarse de que los funcionarios y contratistas conozcan las responsabilidades del funcionario o contratista para el manejo de la información recibida de otras Entidades o partes externas.
- La División de Recursos Humanos o el Supervisor del Contrato para los contratistas y/o terceros, deben comunicar a la División de Planeación y Sistemas los cambios de cargo de personal, indicando los cambios en los recursos tecnológicos asignados. Especialmente actualizaciones sobre los accesos a carpetas compartidas y sistemas de información.

4.6.5. Terminación o cambio de responsabilidades de empleo

Se debe informar al personal los deberes y responsabilidades después de la terminación del empleo. Previa emisión de paz y salvo para funcionario o contratista se debe considerar:

- Tener formato de paz y salvo firmado (TH-Fr21)

4.6.6. Procesos Disciplinarios

Dentro de la estrategia de seguridad de la información, El Senado de la República seguirá el proceso establecido en la Ley 734 de 2002 (Código Único Disciplinario).

4.6.7. Intercambio de Información

La entidad debe firmar acuerdos de confidencialidad o compromisos de confidencialidad con los servidores públicos, intercambio de información entre Entidades Públicas u otros Entes Externos, y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial.

- El intercambio de información con organismos de control y autoridades de supervisión debe seguir el Procedimiento Transferencia Segura de Información (RT-Pr07) con los que se intercambie todo tipo de información.

- Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar el grado de sensibilidad de la información de la entidad según el Procedimiento Inventario y Clasificación de Activos de Información (RT-Pr11).

- Es importante gestionar la firma de un acuerdo de intercambio de información por parte de los representantes legales de las partes involucradas.

4.7. GESTIÓN DE ACTIVOS

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.

Es así como, se deben proporcionar niveles de protección a todos los activos de información de la Entidad. Todas estas medidas o lineamientos son basadas para mitigar los posibles riesgos.

4.7.1. Inventario de activos

Cada área debe ser responsable de mantener actualizado el inventario de activos de seguridad de la información, de acuerdo con las directrices del Procedimiento Inventario y Clasificación de Activos de Información (RT-Pr11).

4.7.2. Uso aceptable de los activos

- La información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad del Senado de la República, son activos de la Entidad y se proporcionan a los funcionarios, contratistas y proveedores o terceros autorizados, para cumplir con los propósitos del cargo.

- Los funcionarios, contratistas, proveedores o terceros y, todo aquel que cuente con acceso a la información de la Entidad, debe reportar los eventos de seguridad de la información identificados, de acuerdo con el Procedimiento de Soporte Técnico y Atención de Servicios (RT-Pr01)

4.7.3. Uso de equipos de cómputo

- Está prohibido que personal ajeno a la División de Planeación y Sistemas, destape o retire partes de los equipos de cómputo propiedad del Senado de la República.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo es responsabilidad de la División de Planeación y Sistemas y, por tanto, se debe solicitar soporte a la mesa de servicios para la realización de estas labores.

- Debe respetarse y no modificarse la configuración de hardware y software establecido por la División de Planeación y Sistemas

- Toda actividad informática no autorizada que afecte tanto las redes a nivel LAN y WAN como los sistemas de información, están prohibidas dando lugar a los procesos disciplinarios y/o legales correspondientes.

- Todas las estaciones de trabajo deben apagarse o hibernarse al finalizar la jornada laboral.

- Los equipos de cómputo, servidores, teléfonos IP y equipos de comunicaciones, debe conectarse a los puntos de corriente eléctrica identificados como regulados (Naranjas), con el fin de evitar picos altos que puedan dañar el componente tecnológico.

- Estos puntos de corriente regulada se usan para regular la energía y que bien están soportados igualmente por las UPS en dado caso que se vaya la luz y no se apague abruptamente.

- La conexión eléctrica de equipos personales debe hacerse a través de los puntos eléctricos no regulados. El senado, no se responsabiliza por daños que puedan sufrir estos dispositivos.

- La seguridad física e integridad de los equipos de cómputo que ingresen a las instalaciones del Senado de la República y que no son propiedad de la Entidad, es responsabilidad única y exclusiva de sus propietarios. El Senado, no es la responsable por estos equipos en ningún caso.

4.7.4. Uso de Internet

- No se autoriza conectar módems o celulares para acceder a Internet, dentro de las redes (WAN, LAN, WLAN) de la Entidad.

- No se autoriza a los funcionarios y contratistas acceder a cualquier página o dirección que contenga material pornográfico, o bien páginas que promuevan cualquier tipo de ideas que puedan ser consideradas ofensivas para las normas de la Entidad como violencia, terrorismo, grupos al margen de la Ley, discriminación, entre otras.

- No se autoriza el envío, descarga o visualización de información con contenido que atente contra la integridad moral personal o institucional.

- Con el propósito de minimizar la saturación en la Red, así como interrupción, alteraciones no autorizadas y errores en la red de la Entidad, no se permite el envío o descarga de información masiva como música, videos y software no autorizado.

- Todo usuario es responsable del contenido de toda comunicación e información que se envíe o descargue desde su cuenta de acceso o estación de trabajo.

- Ningún usuario está autorizado para asignar claves de administrador sobre los computadores de la Entidad.

- Los usuarios no deben intentar burlar los sistemas de seguridad y de control de acceso perimetral.

4.7.5. Uso del Correo Institucional

- La Entidad debe proveer a los usuarios un correo electrónico institucional con el dominio Senado.gov.co.

- La cuenta de correo electrónico institucional es personal e intransferible, los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y el buzón asociado a la Entidad.

- El correo electrónico institucional se debe utilizar estrictamente como herramienta de comunicación de la Entidad; esto es para transmitir información relacionada única y exclusivamente con el desarrollo de las funciones.

- El correo electrónico institucional es una herramienta para el intercambio de información necesaria que permita el cumplimiento de las funciones propias de cada cargo, no es una herramienta de difusión masiva de información y no debe ser utilizada como servicio personal de mensajes

- El envío de información masiva a los grupos generados es limitado y solo por las dependencias autorizadas por la Dirección General Administrativa.

- No se debe abrir o ejecutar un correo de origen desconocido, debido a que podría tener código malicioso, lo cual podría atentar contra los sistemas, programas y datos de la Entidad.

- No está permitido abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, es responsabilidad de cada usuario mantener sus sesiones atendidas.

- El usuario debe notificar de cualquier correo sospechoso, a la mesa de servicios helpdesk@senado.gov.co, el correo sospechoso no debe ser abierto ni reenviado a ningún usuario.

4.7.6. 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 con el 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.

4.7.7. Gestión de Medios Removibles

Los medios removibles en los que se almacene información clasificada como información pública clasificada e información pública reservada deben estar cifrados.

La División de Planeación y Sistemas debe establecer herramientas tecnológicas para el cifrado de la información, además:

- Debe proveer el uso de carpetas compartidas en lugar de medios removibles para el intercambio de información al interior de la Entidad.

- Los medios removibles no deben ser utilizados en sitios públicos como un café internet, así mismo, debe tratarse bajo cuidado alejado de daños externos como agua, polvo o fuego.

4.7.8. Disposición de los Medios

- Los medios que contienen información confidencial se deben disponer en forma segura, mediante destrucción o el borrado de datos antes de ser reutilizados o dados de baja, siguiendo el RT-Pr10 Procedimiento de Borrado Seguro de la Información.

- La información en los backups que contienen información pública clasificada o información pública reservada se debe cifrar, además deben estar protegidas en un lugar seguro y vigilado por CCTV como mínimo.

- Se debe guardar varias copias de datos valiosos para la entidad en medios separados, con el fin de evitar la pérdida de información por daño, pérdida o robo de los medios removibles.

- Los backups de los servidores, se deben guardar en una ubicación alterna a la localización de los datos o aplicaciones, para aumentar la seguridad ante posibles impactos de desastres ambientales, accidentes, incendios etc.

- Se debe realizar pruebas a las copias de datos para validar la integridad de la información como mínimo una vez al año.

4.7.9. Transferencia de Medios Físicos

- Para la transferencia de medios físicos (Información en carpetas selladas, computadores, dispositivos móviles, tablets, etc.) se debe tener en cuenta el un adecuado embalaje de la información que mitigue los daños físicos que se puedan presentar en el transporte de esta, protegiendo la exposición al calor, humedad o campos electromagnéticos.

- Se debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte, y el recibo en su destino.

4.8. CONTROL DE ACCESO

4.8.1. Acceso a Redes y Servicios en Red

- La División de Planeación y Sistemas provee un servicio de conectividad a todos los funcionarios y contratistas de la Entidad para la navegación en internet, dicho acceso es controlado por usuario y políticas de navegación.

- Para los usuarios que requieran contar con servicios especiales de mensajería instantánea, páginas de encuentro o descargas, deben ser autorizados por el jefe inmediato, mediante comunicación vía correo electrónico a la División de Planeación y Sistemas formato, justificando la necesidad del acceso.

- La conexión remota a la red de área local o red de servidores de la entidad debe ser realizada a través de una conexión VPN segura, suministrada por la División de Planeación y Sistemas.

- La conexión a servicios en red se controla mediante el directorio activo, a excepción del control de acceso físico mediante acceso biométrico y el servicio de agendamiento.

- La conexión a redes públicas abiertas está prohibida, así como la conexión a redes Wi-Fi públicas.

- Todo acceso o privilegio a sistemas, redes, aplicaciones o información de la entidad debe estar aprobado por los jefes de división y los propietarios de información según aplique.

4.9.2. Solicitud o Inicio de Acceso

El Senado de la República, cuenta con procedimiento para definir y administrar los privilegios de acceso de los usuarios a la información, así mismo los sistemas, recursos y aplicaciones, que procesen cualquier información propietaria deben requerir autenticación y debe tener en cuenta:

- Los jefes de división o dueños de los procesos son los únicos funcionarios autorizados para realizar las solicitudes de acceso a los sistemas de información o delegados formalmente por el jefe para ejecutar esta actividad.

- Los jefes deben realizar las solicitudes de acceso a los sistemas de información requeridos por los funcionarios o colaboradores a su cargo, a la División de Planeación y Sistemas.

- La División de Planeación y Sistemas, asigna a los usuarios los permisos de acceso a la información con base en los roles y perfiles del usuario aprobados por los responsables de cada proceso.

- No debe existir cuentas genéricas para el acceso o gestión sobre los sistemas de información de la Entidad (equipos, aplicaciones, bases de datos, sistemas operativos, entre otros). Cuando por razones del negocio u operación deben ser creadas únicamente como cuentas de servicio y no deben ser utilizadas por ningún funcionario o contratista.

- La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, es decir el uso de las claves de usuarios administradoras, tales como: “root”, “adm” y “system”, entre otros, debe ser controlado por la División de Planeación y Sistemas quienes son los responsables de dichos accesos.

- El acceso de un usuario debe ser limitado sólo a la información requerida para el desarrollo de sus funciones.

- Para los equipos de cómputo se debe establecer bloqueos o terminación de sesiones automáticas en caso de que queden desatendidos, con el propósito de proteger la información.

- La utilización de información compartida en unidades de red debe estar restringida por usuarios, así mismo, El responsable y/o dueño de la información debe definir los accesos a la información únicamente al personal autorizado.

- Se debe considerar la inclusión en los contratos del personal y contratos de servicio con terceros, cláusulas de confidencialidad que especifiquen las sanciones si los colaboradores o terceros intentan un acceso no autorizado.

4.9.3. Suspensión o Terminación de Acceso

- El acceso a los sistemas debe ser suspendido para todo funcionario o colaborador de la entidad que se encuentre en licencia, permisos, vacaciones, entre otras novedades.

- los jefes deben realizar las solicitudes de acceso necesarias a los colaboradores que ejecutaran las actividades, una vez cumplido el plazo se debe solicitar retiro de los permisos, además:

- La División de Planeación y Sistemas debe mantener actualizado el Directorio Activo con la información de los usuarios de funcionarios.

- Se debe definir y aplicar reglas para deshabilitar las cuentas de usuarios de red que no han cambiado la contraseña durante 90 días, igualmente se debe definir qué cuentas deben quedar bloqueadas porque no fueron reactivadas y eliminar aquellas cuentas que no presentan ninguna actividad desde su creación.

- Los usuarios creados con acceso a las bases de datos que no hayan sido utilizados en un período mayor o igual a 3 meses deben ser inhabilitados por los administradores de Base de Datos, así mismo, si éstas no han sido utilizadas en un periodo igual o mayor a 6 meses debe ser eliminadas.

4.9.4. Revisión o Validación de Accesos

- Las autorizaciones de acceso a sistemas y/o aplicaciones debe ser revisadas periódicamente por los administradores de TI y/o propietarios de la información.
- Se debe validar las solicitudes de accesos especiales como VPN, administrador de máquina y acceso remoto.
- Se debe revisar los derechos de acceso de un usuario se deben revisar y reasignar, ya sea por cambio de cargo o traslado de área, dentro de la misma entidad.

4.9.5. Normas para la Creación de Contraseñas

Los usuarios y contraseñas son de uso personal e intransferible, cualquier utilización indebida y/o irregularidad debe ser responsabilidad del funcionario.

Como medida de seguridad los usuarios deben crear y administrar sus contraseñas siguiendo las siguientes normas para la creación y el uso:

- Las contraseñas se consideran como información confidencial y deben ser protegidas como tal.

- La contraseña debe tener al menos ocho (8) caracteres, donde se tengan letras en mayúscula, minúscula y números o caracteres especiales.

- Las contraseñas deben cambiarse mínimo cada 90 días y no se pueden repetir las últimas 5 contraseñas.

- Si se digita más de 3 veces la contraseña de forma inválida, la cuenta del usuario debe ser bloqueada, se deberá solicitar el desbloqueo a través de un requerimiento desde Mesa de Servicios:

- Correo Electrónico: helpdesk@senado.gov.co
- Extensión: 3030
- Portal Autoservicio: https://soporte.senado.gov.co/ASDKV8/

- La contraseña no debe incluir un nombre o palabra común, así misma información como números de tarjeta de crédito, nombres de calles y números telefónicos.

- No utilizar contraseñas por defecto, éstas se deben cambiar una vez se obtengan las credenciales por cambio o creación por primera vez, de igual manera cuando se adquieran equipos de tecnología o sistemas de información nuevos.

- No es permitido compartir usuarios, contraseñas.

- Dispositivos como los Tokens que permitan el acceso a un sistema de información en la Entidad o Entidades externas deben ser almacenados y salvaguardados en lugares seguros, donde solamente el dueño del Token tenga acceso.

- En los casos que se sospeche del compromiso de una contraseña en un posible incidente de seguridad, se debe reportar a la mesa de servicios con el fin de ser cambiada inmediatamente.

- Los usuarios no deben almacenar las claves en ningún proceso de registro automatizado; por ejemplo, almacenado en gestor de contraseñas de los navegadores web como Chrome o Mozilla.

4.9.6 Control de Acceso a las Aplicaciones y Recursos Tecnológicos

- Los accesos a las aplicaciones y recursos tecnológicos deben ser restringidos y monitoreados de acuerdo con las necesidades de la entidad.

- La selección de los mecanismos de control de acceso a las aplicaciones se define de acuerdo con la clasificación de la información de cada proceso.

- Se debe utilizar medidas de seguridad para restringir el acceso a los aplicativos, bases de datos y en general a los recursos tecnológicos.

- Las aplicaciones de la Entidad deben contar con mecanismo para el manejo de contraseñas, deben cumplir con los parámetros de seguridad definidos, para ello debe tener en cuenta:

- Permitir a los usuarios seleccionar y cambiar sus propias contraseñas.
- Se debe tener en cuenta los lineamientos de contraseñas robustas.
- Los aplicativos deben obligar a los usuarios a cambiar las contraseñas temporales en su primer ingreso o registro.
- No mostrar las contraseñas en la pantalla en el momento de ingresarlas.
- Almacenar las contraseñas cifradas con algoritmos fuertes, mediante uso de funciones hash.
- Solicitar la modificación en un periodo definido de las contraseñas de ingreso a los aplicativos.
- Implementar políticas de bloqueo automático del usuario cuando la contraseña se haya ingresado de manera errónea por tres veces como mínimos.

4.9.7. Restricción del Acceso a la Información

- Las restricciones para el acceso a las aplicaciones se deben basar en el rol que el usuario desempeñara, por tal movió, se debe controlar los permisos de acceso de los usuarios: lectura, escritura, modificación y eliminación.

- las restricciones de uso sobre los sistemas operativos por parte de los usuarios, se debe tener en cuenta lo siguiente:

- El administrador de la plataforma es el responsable de otorgar los accesos a los recursos del sistema operativo.
- El uso de herramientas o utilitarios propios de los sistemas operativos deben ser limitado a personal autorizado y su uso está restringido al personal de la División de Planeación y Sistemas.
- Está prohibido el uso de herramientas intrusivas con fines de vulnerar la seguridad del sistema operativo, bases de datos, redes etc.
- Las sesiones que no han presentado ningún tipo de actividad por un período de tiempo determinado deben finalizar automáticamente de acuerdo con la configuración definida; esto mismo aplica para los accesos remotos.
- Todos los funcionarios deben cumplir con las normas de contraseñas.
- Todas las estaciones de trabajo deben estar plenamente identificadas para garantizar la conexión de equipos confiables, esto debe venir acompañado de correctas configuraciones de red que restrinjan la conexión a los equipos de la DMZ o Nube permitiendo solamente las conexiones necesarias.

4.9.8. Control de Acceso a la Red

La División de Planeación y Sistemas debe implementar procedimientos para controlar el acceso a la red del Senado de la República proporcionando a los funcionarios o terceros el acceso a los servicios para los que específicamente se les haya autorizado su uso:

- Para acceder a las redes de datos de la entidad, se requiere autenticación individual.
- Las contraseñas de red de usuario y las contraseñas de usuarios privilegiados deben ser cambiadas periódicamente.
- El senado permite a usuarios externos (proveedores o terceros) acceder a las redes institucionales desde redes externas, bajo ciertas condiciones de seguridad. Dicha autorización debe ser tramitada por el líder del proceso ante La División de Planeación y Sistemas para su aprobación.
- Los líderes de proceso que tienen acuerdos contractuales con proveedores o terceros y, si éstos requieren acceso a los recursos tecnológicos de la Entidad, se debe contar con autorización previa de parte de La División de Planeación y Sistemas. De igual manera se debe asegurar que los proveedores o terceros conozcan y acepten las políticas de Seguridad de la Información y que las normas o acuerdos específicos de seguridad que apliquen para la actividad contractual queden registrados en el documento RT- Plt01 Plantilla Acta de Confidencialidad.

- Se deben definir validaciones o revisiones teniendo en cuenta la criticidad de los proveedores o terceros ante el cumplimiento de la política de Seguridad de la Información, como los acuerdos específicos de seguridad para el desarrollo de las labores con los terceros.

- Cuando los usuarios acceden a datos en redes locales y remotas vía VPN, debe utilizar mecanismos de seguridad para autenticarse ante las redes.

- La División de Planeación y Sistemas debe mantener las redes de datos internas segmentadas por VLANS, grupos de servicios, usuarios y sistemas de información.

- Todas las estaciones de trabajo conectadas a la red del Senado de la República deben contar con herramientas de seguridad, como firewalls, IPS, Filtros de Contenido Web, Antivirus, Endpoint, entre otros.

- El servicio de correo externo no debe ser habilitado para proveedores o terceros y temporales, salvo casos excepcionales por funcionalidad de un servicio.

4.9.9. ACCESO A DATOS DE PRODUCCIÓN

La División de Planeación y Sistemas debe tener en cuenta las siguientes consideraciones respecto al acceso a datos de producción:

- Se deben definir un procedimiento para el control de acceso el cual incluya la aprobación, supervisión etc. a los datos de producción.
- Para todo usuario autorizado, la disponibilidad de la información debe ser limitada.
- Los procedimientos deben ser definidos para conceder el acceso de emergencia de usuarios a datos de producción.
- El acceso a datos de producción debe ser auditable.
- El acceso a los datos de producción debe generar archivos de trazabilidad (logs) que pueden ser auditados, por entes de control.

4.9.10. CONEXIONES REMOTAS

Se define como acceso remoto cualquier conexión establecida desde fuera de la Entidad que requiere acceso a la red o aplicaciones internas del Senado de la República por parte de funcionarios, proveedores entre otros.

Para dichos accesos se debe tener en cuenta las siguientes consideraciones:

- Iniciar la conexión remota de red desde computadores y sitios seguros, evitar conexiones remotas desde computadores públicos o desconocidos como, cafés internet, aeropuertos, hoteles o redes inalámbricas públicas.

- Las conexiones remotas a los recursos de la plataforma tecnológica; deben estar restringidas, únicamente se deben permitir estos accesos a personal autorizado.

- Si es el caso se debe aprobar o aceptar del lado de la Entidad para que el proveedor tome el control remoto. No debe permitirse el acceso y control total de manera automática, sino cuando la entidad lo autorice.

- El trabajo remoto por VPN lo debe solicitar el jefe directo, La Division de Planeación y Sistemas valida la pertinencia de dicha solicitud y otorga el privilegio, evaluando y aplicando las medidas de protección adecuadas que garanticen una conexión segura.

- El acceso remoto a los servidores debe estar controlado por las políticas del Directorio Activo para el ingreso por este servicio, es decir quién puede o no ingresar por este servicio, teniendo presente que este servicio debe ser autorizado únicamente para los administradores de los servidores, los usuarios o proveedores fuera de la oficina no deben tener estos accesos.

- Los sitios Web que se encuentren publicados, deben forzar la autenticación mediante el protocolo de transferencia segura.

4.10. CONTROLES CRIPTOGRÁFICOS

- La División de Planeación y Sistemas debe Determinar los algoritmos criptográficos y protocolos autorizados para su uso en la entidad y configurar los sistemas para permitir únicamente aquellos permitidos, teniendo en cuenta la información de los grupos de interés con el fin de descartar algoritmos de cifrado débil.

- Las llaves criptográficas deben ser cambiadas anualmente o cada vez que se sospeche que han perdido su confidencialidad.

- La administración de llaves criptográficas y certificados digitales están a cargo de La División de Planeación y Sistemas. Sin embargo, la administración de tokens para acceso a SIIF (Sistema Integrado de Información Financiera) y firmas digitales están a cargo de cada uno de los funcionarios o contratistas a quienes les fueron asignados para el desempeño de sus labores.

- Se debe notificar con anterioridad a los dueños de la información, aplicaciones, software que requieran de certificados digitales, la fecha de caducidad de éstos para su renovación.

- Realizar la entrega de los certificados digitales generados con el debido procedimiento para su aplicación y uso.

- Se debe realizar las configuraciones requeridas para el uso y administración de los certificados de firma digital.

- Se deben proporcionar los recursos necesarios para la administración y monitoreo en el uso de controles criptográficos a través de herramientas o software de seguridad.

- Todos los funcionarios o contratistas deben conocer y cumplir la política de uso de controles criptográficos.

- Los funcionarios o contratistas a quienes les fueron asignados tokens de acceso a SIIF, deben almacenarlos bajo llave cuando no hagan uso de éstos, o cuando se van a retirar de sus puestos de trabajo.

4.10.1. Firma Digital

- Los funcionarios autorizados para hacer uso de la Firma Digital son: Senadores, director general, secretario general, Subsecretario, jefes de División, funcionarios de Planta.

- La firma digital se utilizará para cumplir con las normativas legales, para identificar al firmante de manera inequívoca, para certificar la integridad del documento o cuando se requiera proteger un documento o la información (autenticidad e integridad) con un riesgo asociado resultado de una evaluación de riesgos.

- Para el uso de firma digital dentro de la entidad, se ha establecido que éstas deben ser individuales, es decir cada funcionario que esté autorizado para el uso de la firma digital, es responsable único de la firma del documento.

- La firma digital, debe ser verificada a través de una llave pública incluida en un certificado válido emitido por una Entidad certificadora, a la cual, se le debe exigir acuerdos de niveles de servicio para el servicio de certificación o verificación.

- Una vez firmados los documentos con la firma digital, debe conservarse en su estado electrónico para garantizar su validez.

- Una vez firmados digitalmente los documentos, se deben convertir en formato PDF y debe visualizarse a través del sistema de Gestión Documental.

- El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita.

- El uso de firma digital y según la Ley 527 de 1999 establece a su favor tres atributos fundamentales en el aseguramiento jurídico, por lo que es necesario que los funcionarios autorizados para el uso de la firma digital velen por que estos tres atributos se cumplan en su implementación y uso.

- La autenticidad: En la medida que se puede verificar en un mensaje de datos firmado digitalmente quién es su autor, es quién se compromete jurídicamente.
- La integridad: El destinario de ese mensaje de datos podrá verificar si la información ha sido o no alterada en el proceso de comunicación electrónica, lo que es muy útil para determinar la originalidad electrónica del mensaje de datos, especialmente a la luz de los artículos 8 y 9 de la Ley 527 de 1999.
- El no repudio: Quien firma digitalmente se compromete con la suscripción respectiva y posteriormente no le es dado retractarse o refutar dicho acto.

4.10.2. Cifrado de la Información

El Senado de la República debe contar con controles que permitan definir y administrar los mecanismos de cifrado de información, con el fin de poder realizar intercambio de información cifrada:

- Se debe hacer uso de cifrado para la protección de claves de acceso, llaves criptográficas a datos, información clasificada y reservada, y todos aquellos servicios que estén expuestos a internet.

- Cifrado en la transmisión de información clasificada y reservada por los diferentes canales de comunicación que utilice en el Entidad.

- Cifrado en el resguardo de información clasificada y reservada en cualquier medio físico o componente tecnológico, o cuando así surja de la evaluación de riesgos de seguridad de la información.

4.10.3. Certificados Digitales

La División de Planeación y Sistemas, como responsables de los sistemas de información alojados en el Datacenter, debe tener como control un listado de todos los certificados emitidos con la fecha de caducidad y la asignación de éstos en los sistemas de información con el fin de:

- Garantizar la autenticidad del sitio, servicio o aplicativo Web.
- Evitar el riesgo de ataques de suplantación de identidad o phishing de los sitios Web.
- Proteger la confidencialidad de la información intercambiada entre la Entidad y sus ciudadanos o titulares mineros a través del sitio Web.
- Establecer conexiones seguras cifrando la información intercambiada entre los aplicativos y los ciudadanos o titulares mineros.
- Salvaguardar la integridad de la información intercambiada, porque el certificado presenta las características de la Entidad, algoritmo de cifrado, fecha de emisión del certificado, etc.

4.11. SEGURIDAD FÍSICA Y DEL ENTORNO

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido. En consecuencia, debe contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

4.11.1. Áreas Seguras

El Senado de la República en sus sedes Edificio Nuevo, Capitolio y Casa de la Cultura, tiene implementado un sistema de control de acceso físico mediante huella biométrica y tarjeta de proximidad, en las entradas principales cuenta con una recepción donde se controla el ingreso y salida de terceros, y el ingreso y salida de elementos, tanto de funcionarios como de terceros.

A sí mismo la entidad debe exigir a los proveedores que gestionen o procesen información por fuera de las instalaciones, cumplir con las políticas de seguridad de la información.

El Datacenter o centros de cableado debe contar con mecanismos que cumplan los requisitos ambientales (temperatura, humedad, voltaje, entre otros) especificados por los fabricantes de los servidores y equipos de comunicaciones que alberga, igualmente debe contar con sistemas mecánicos para control de incendios, impedir el acceso a personal no autorizado, consumo de alimentos, bebidas o cigarrillo.

El Senado cuenta con un Sistema de Seguridad CCTV, para otorgar la mayor seguridad posible tanto a los ciudadanos como a los funcionarios que ingresan a sus instalaciones. El Sistema de Seguridad CCTV opera bajo las siguientes directrices:

- EL Centro Integrado de Control es la responsable del mantenimiento y soporte de la plataforma tecnológica que soporta el sistema CCTV.

- EL Centro Integrado de Control debe garantizar el funcionamiento del sistema CCTV las 24 horas del día de los 365 días del año. La Policía nacional garantizara la operación y monitoreo.

- El acceso al Centro Integrado de es de carácter restringido. Las únicas personas que tienen permiso de acceder son los operadores, o aquellos funcionarios autorizados por la Dirección General Administrativa.

- Toda solicitud de copias de video debe hacerse mediante comunicación a la División de Planeación y Sistemas.

- Todas las grabaciones tienen una duración mínima de 60 días y después se reescribe.

- Está prohibido dar información de especificaciones técnicas y ubicaciones de cámaras.

- Toda copia de video generada debe ser entregada mediante oficio o mediante cadena de custodia.

- EL Centro Integrado de Control debe brindar un repositorio para almacenamiento de videos históricos garantizado la confidencialidad y disponibilidad de esta información.

- El Senado de la República debe contar con un plan de emergencias definido por la Sección de Bienestar y Urgencia Médica, que debe ser probado anualmente, con el fin de brindar protección contra amenazas externas.

- La carga se recibe y despacha por el sótano 1 del edificio nuevo – costado sur. La recepción y despacho de carga es controlada por la policía nacional y se tienen horarios y días específicos para la realización de estas actividades.

4.11.2. Ubicación y Protección de los Equipos

El Datacenter está ubicado de forma tal que personas no autorizadas no puedan ver la información durante su uso y el acceso físico es controlado por la División de Planeación y Sistemas.

Se hace seguimiento a las condiciones (temperatura, humedad, voltaje, apertura y cierre de puertas) que pueden llegar a afectar adversamente el Datacenter.

4.11.3. Servicios de Suministro

La entidad cuenta con aire acondicionado y UPS de contingencia que asegura el tiempo necesario de 20 minutos de autonomía para que la planta eléctrica entre a soportar la carga o mientras regresa la energía eléctrica.

4.11.4. Seguridad del Cableado

El Datacenter cumple con la normatividad de cableado estructurado. A sí mismo el Senado debe exigir a los proveedores de servicios informáticos, cumplir con las políticas de seguridad establecidas.

4.11.5. Mantenimiento de Equipos

La División de Planeación y Sistemas debe establecer y ejecutar planes anuales de mantenimiento de la infraestructura tecnológica de la entidad.

4.11.6. Seguridad de los Equipos

- Los equipos y medios removibles que son retirados de las instalaciones de la entidad deben tener mecanismo de cifrado activo.

- Los funcionarios y contratistas que retiren equipos o medios removibles de las instalaciones de la entidad deben seguir las siguientes directrices:

- En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo, se debe poner la denuncia ante la autoridad competente e informar inmediatamente al jefe directo para que se inicie el trámite interno correspondiente.

4.11.7. Disposición Segura o Reutilización de Equipos

Cuando una estación de trabajo o equipo portátil vaya a ser reasignado o dado de baja, se debe realizar una copia de respaldo de la información de la entidad que allí se encuentre almacenada (en caso de ser necesario). Posteriormente, el equipo debe ser sometido a un proceso de eliminación segura de la información almacenada con el fin de evitar pérdida de la información y/o recuperación no autorizada de la misma, aplicando el RT-Pr10 procedimiento borrado seguro de la información.

4.11.8. Política de Equipo Desatendido, Pantalla y Escritorio Limpio

Todo funcionario o tercero deben conservar su escritorio libre de información propiedad de la Entidad, que pueda ser alcanzada, copiada o utilizada por terceros o personal que no tenga autorización para su uso o conocimiento, cada vez que se vayan a retirar de sus puestos de trabajo se deben contemplar los siguientes lineamientos:

- Al imprimir documentos de carácter confidencial (información pública clasificada e información pública reservada), estos deben ser retirados de la impresora inmediatamente.

- Los computadores deben cargar por defecto el fondo de pantalla de la entidad, éste no debe ser modificado y debe permanecer activo.

- Los funcionarios y contratistas deben bloquear la pantalla de su computador cuando por cualquier motivo se ausenten del puesto de trabajo (aplique el comando de bloqueo oprimiendo simultáneamente las teclas Windows + L), a su vez, la División de Planeación y Sistemas debe implementar mecanismos para cierres de sesión automáticos.

- Se prohíbe el almacenamiento de información personal en los computadores de la entidad. El escritorio debe estar libre de información pública clasificada e información pública reservada.

- La información de gestión del área deber ser almacenada por los usuarios en carpetas compartidas del área y la información de gestión del usuario en el almacenamiento virtual de Drive.

4.12. SEGURIDAD DE LAS OPERACIONES

4.12.1. Documentación de Procedimientos Operativos

Se debe contar con procedimientos documentados de trabajo debidamente documentados para las actividades operativas asociadas con las instalaciones de procesamiento y comunicación.

4.12.2. Control de Cambios

Los cambios en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información se debe realizar de acuerdo con los lineamientos del RT-Pr04 Procedimiento de Gestión de Cambios de TI.

4.12.3. Gestión de Capacidad

La entidad debe gestionar la capacidad de su plataforma tecnológica (hardware y software).

4.12.4. Separación de los Ambientes

La entidad debe contar con ambientes de desarrollo, pruebas y producción separados por máquinas físicas y máquinas virtuales, de acuerdo con los lineamientos del RT-Pr08 procedimiento separación de ambientes.

4.13. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- Se deben proteger las estaciones de trabajo, equipos portátiles y servidores de la entidad contra códigos maliciosos.

- Los contratistas que hagan uso de sus equipos portátiles personales deben contar con un software antivirus licenciado.

- El servicio de antivirus no requiere de solicitud o autorización para su uso, todos los equipos conectados a la red deben tener el antivirus instalado y activo.

- El único servicio de antivirus autorizado en la entidad es el asignado directamente por la División de Planeación y Sistemas, el cual cumple con todos los requisitos técnicos y de seguridad. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

- El usuario no debe propiciar el intercambio de archivos que hayan sido identificados como infectados por virus o códigos maliciosos o sean sospechosos de estar infectados.

- El usuario no debe instalar o emplear programas no autorizados para manejo de antivirus.

- Los usuarios no deben desactivar o eliminar los archivos que forman parte del programa de antivirus.

- El programa de antivirus debe ser instalado única y exclusivamente por la División de Planeación y Sistemas en los servidores y estaciones de trabajo.

4.14. COPIAS DE RESPALDO

- El Senado de la República debe realizar copias de respaldo de la información y pruebas periódicas a las mismas.

- Se debe seguir los lineamientos del RT-Pr02 procedimiento generación de copias de seguridad y restauración de datos para ambientes virtualizados.

- Los funcionarios y terceros son los responsables de realizar copias de respaldo a las carpetas con información de la entidad (información pública) de los equipos portátiles y/o computadores de escritorio.

- Todas las copias de respaldo deben contemplar un plan de continuidad del negocio, orientado a evitar la pérdida de la información al contemplar un sitio secundario para su preservación.

- Las copias de respaldo deben ser guardadas únicamente con el objetivo de restaurar el sistema cuando por situaciones como: borrado de datos, incidente de seguridad de la información, defectos en los discos de almacenamiento, problemas de los servidores o computadores o por requerimientos legales sea necesario recuperarla.

- Toda la información institucional que se almacena en los equipos asignados a los funcionarios o contratistas es de propiedad de la Entidad, motivo por el cual no debe ser divulgada a terceros.

4.15. REGISTRO Y SUPERVISIÓN DE EVENTOS

4.15.1. Registro de Eventos

Los sistemas operativos, servicios y sistemas de información que hacen parte de la infraestructura para el procesamiento de información y comunicaciones, deben generar archivos de registro de eventos (logs) definidos en conjunto por los responsables de su administración.

4.15.2. Sincronización de Relojes

Los relojes de los diferentes equipos de cómputo, servidores y sistemas de información utilizados por el Senado de la República, debe estar sincronizados utilizando como referencia la hora oficial de Colombia de INM (Instituto Nacional de Metrología) horalegal.inm.gov.co

4.16. CONTROL DE SOFTWARE OPERACIONAL

4.16.1. Instalación de Software en Sistemas Operativos

- El proceso de instalación y desinstalación de software está autorizado exclusivamente al personal de la División de Planeación y Sistemas. Por lo tanto, a los funcionarios o contratistas no le es permitido realizar esta labor.

- El software licenciado debe contar con su respectiva documentación (Licencia) y en el caso del software libre debe estar permitido el uso comercial.

- El instalador debe ser descargado de la página oficial del fabricante.

- Se debe proporcionar capacitación a los usuarios y al personal técnico en los aspectos de operación y funcionalidad de las nuevas adquisiciones de software o mejoras al software existente, antes de su salida a producción.

- Todo el software nuevo y mejorado debe estar completamente soportados por una documentación suficientemente amplia y actualizada, y no debe ser puesto en el ambiente de producción sin contar con la debida documentación:

- Documento de Licencia del Software
- Manual de Instalación del Software

- La División de Planeación y Sistemas debe realizar revisiones como mínimos una vez al año del uso del software instalado en las estaciones de trabajo y servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de 2000 de Derechos de Autor.

- Todo software que viole los acuerdos de licenciamiento debe ser desinstalado inmediatamente y debe ser reportado el hecho como incidente de seguridad por incumplimiento de la política y de los términos y condiciones de uso.

- Toda reproducción del software, transporte, almacenamiento, adquisición para la venta o distribución sin la debida autorización del titular, se constituye como un delito a los Derechos Patrimoniales del Autor.

- La División de Planeación y Sistemas debe comunicar a los funcionarios y contratistas sobre las consecuencias por utilizar software ilegal.

4.17. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- La División de Planeación y Sistemas, es responsable de verificar de manera periódica la información publicada por parte de los fabricantes y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar los sistemas de información de la Entidad, Adicionalmente,

4.17.1. Gestión de las Vulnerabilidades Técnicas

- Se debe contar con un procedimiento y análisis de vulnerabilidades que permitan la identificación y mitigación de las vulnerabilidades identificadas en toda la plataforma tecnológica de la entidad.

- Se debe generar y ejecutar por lo menos una vez al año el plan de análisis de vulnerabilidades y/o Hacking Ético para las plataformas críticas de la Entidad, cuya viabilidad técnica y de administración lo permita.

- Una vez se lleve a cabo la ejecución de escaneos de vulnerabilidad en la plataforma tecnológica de la Entidad, la identificación de estas vulnerabilidades o hallazgos se deben remediar de acuerdo con los lineamientos establecidos desde el Procedimiento de Gestión de Vulnerabilidades.

- Los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de La División de Planeación y Sistemas, para estas remediaciones se debe tener en cuenta las directrices establecidas en el RT-Pr04 Procedimiento de gestión de cambios de TI.

4.18. AUDITORÍAS DE SISTEMAS DE INFORMACIÓN

4.18.1. Controles sobre auditorias de sistemas de información

Para la ejecución de auditorías a los sistemas de información se debe tener en cuenta las siguientes consideraciones:

- Los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con los jefes de las Dependencias involucradas.

- El alcance de las pruebas técnicas de auditoría se debería acordar y controlar.

- Las pruebas de auditoría (incluidas las pruebas de análisis de vulnerabilidades y/o hacking ético) que puedan afectar la disponibilidad del sistema se debe realizar en horario laboral en un ambiente controlado.

- Se debe hacer seguimiento de todos los accesos y logs para producir un rastro de referencia.

- Las pruebas de auditoría se deben limitar a acceso a software y datos únicamente para lectura.

4.19. SEGURIDAD EN LAS COMUNICACIONES

La División de Planeación y Sistemas debe definir e implementar los mecanismos de control que considere apropiados para proteger la confidencialidad, integridad y disponibilidad de la información en las redes definidas en la Entidad, la disponibilidad de los servicios en red y la seguridad en sí de la información que viajan a través de estos canales de redes de comunicaciones.

4.19.1. Gestión de la Seguridad en las Redes

La División de Planeación y Sistemas debe definir e implementar mecanismos de separación de las redes de la entidad con base en los niveles de confianza por dependencias:

- Se debe mantener separadas la red de datos y la red de voz.
- El acceso remoto a las redes de la entidad se debe controlar mediante conexiones VPN.

4.19.2. Transferencia de Información

- La entidad debe firmar acuerdos de confidencialidad con los servidores públicos y debe incluir una cláusula de confidencialidad en los contratos con terceros que tengan acceso a la información y que por alguna razón requieran conocer o intercambiar información restringida o confidencial.

- Todos los lineamientos para la transferencia de información deben aplicarse en toda la Entidad, proveedores y terceros que dentro de sus funciones se establezca la necesidad de intercambio de información física como digital.

- Cuando se realicen acuerdos entre organizaciones para el intercambio de información física o digital, se debe especificar la clasificación de la información y las consideraciones de seguridad sobre la misma.

- Todos los responsables de la información son quienes autoricen la transferencia de la información que esté bajo su responsabilidad, teniendo en cuenta la legislación (Ley 1581 de 2014 y Ley de Habeas Data de 2008).

- El proveedor de servicios en la Nube para los servicios con los que cuenta la entidad debe certificar que se dispone de una transferencia de información segura hacia la Nube.

4.20. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La División de Planeación y Sistemas debe definir los requisitos de seguridad de la información para sistemas de información nuevos o mejoras a los sistemas de información existentes, contratados externamente o desarrollados en la entidad.

Las dependencias que requieran desarrollo de software o adquieran software de terceros, deben apoyarse en la División de Planeación y Sistemas para definir los requisitos de seguridad de la información.

4.20.1. Requisitos de Seguridad de los Sistemas de Información.

- El nivel de confianza requerido con relación a la identificación declarada de los usuarios, para obtener los requisitos de autenticación de usuario.

- Los procesos de suministro de acceso y de autorización para usuarios, al igual que para usuarios privilegiados o técnicos. Por ejemplo, el suministro de datos de acceso por correo electrónico.

- Las necesidades de protección de activos involucrados, en particular acerca de disponibilidad, confidencialidad e integridad (“almacenamiento y envió de información cifrada”)

- Los requisitos obtenidos de los procesos del negocio, tales como los requisitos de ingreso, seguimiento, y no repudio, formularios de autenticación HTTPS, cifrado de contraseñas almacenadas, uso de firmas digitales.

- Los requisitos de trazabilidad (registro de eventos) de las actividades de los usuarios.

- La necesidad de exigir la implementación de metodologías de desarrollo seguro.

- Los desarrolladores propios de la entidad liberan de derechos de autor cualquier desarrollo hecho para el cumplimiento de sus funciones u obligaciones contractuales, siendo estos derechos de autor únicamente del Senado de la República.

4.20.2. Seguridad en los Procesos de Desarrollo y Soporte

- La División de Planeación y Sistemas debe definir e implementar principios de desarrollo seguro para los sistemas de información de la entidad.

- Los principios de desarrollo establecidos se deben revisar con regularidad (al menos anualmente) para asegurar que están contribuyendo a mejorar los estándares de seguridad dentro del proceso.

- Se debe revisar regularmente para que permanezcan actualizados en términos de combatir nuevas amenazas potenciales y seguir siendo aplicables a los avances en las tecnologías y soluciones que se aplican.

- La División de Planeación y Sistemas, debe velar por el desarrollo tanto interno como externo de los sistemas de información, cumplan con los requisitos de seguridad esperados, así como con pruebas de aceptación y seguridad al software desarrollado. Además, debe asegurar que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Entidad.

- Los cambios en sistemas deben realizarse de acuerdo con el RT-Pr04 procedimiento de gestión de cambios de TI.

- Se debe hacer uso de metodologías de desarrollo seguro, que contemplen lineamientos de seguridad en todas las etapas del desarrollo.

4.20.3. Ambiente de Desarrollo Seguro

- La División de Planeación y Sistemas debe aplicar los mismos controles en al ambiente de producción y ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos y separación de ambientes.

- La División de Planeación y Sistemas debe implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo y producción han sido aprobadas, de acuerdo con el RT-Pr04 procedimiento de gestión de cambios de TI.

- La División de Planeación y Sistemas debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.

4.20.4. Desarrollo Contratado Externamente

Cuando se contrata desarrollo externo se debe acordar el cumplimiento de los niveles de soporte requeridos por la entidad. Adicionalmente, se debe acordar la entrega de manuales técnicos, que describan la estructura interna del sistema, así como el diccionario de datos, librerías ejecutables, Entidad relación de la base de datos, manuales funcionales, manual del usuario y manual de instalación, además:

- Se debe asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento en el cual se especifiquen las condiciones de uso del software y los derechos de propiedad intelectual.

- Se debe exigir el suministro de evidencia de que se realizaron pruebas de seguridad al software desarrollado por terceros.

- Los principios de desarrollo seguro se deben aplicar, en donde sea pertinente, a desarrollos contratados externamente.

- Las dependencias que contraten desarrollos externos deben asegurar que se realicen pruebas de aceptación del software, con el fin de verificar el cumplimiento de los requisitos de seguridad acordados.

- Las dependencias deben tener en cuenta e incluir en los acuerdos contractuales la necesidad de que el software cumpla con las leyes aplicables.

- Las dependencias deben incluir en acuerdos contractuales, en donde sea posible, el derecho de la ENTIDAD a realizar auditorías durante el desarrollo del contrato.

4.20.5. Pruebas de Seguridad de Sistemas

Se debe exigir tanto para desarrollos internos como externos la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades conocidas.

4.20.6. Pruebas de Aceptación de Sistemas

Independientemente de que sea un desarrollo interno o un desarrollo contratado externamente, con el fin de validar los requisitos de seguridad de la información y la adherencia a prácticas de desarrollo de sistemas seguros. En estas pruebas se puede hacer uso de herramientas automatizadas, tales como herramientas de análisis de códigos o escáneres de vulnerabilidad, y se debe verificar que se han corregido las brechas de seguridad, además:

- Se debe realizar pruebas de aceptación del software que sea una persona diferente de quien han desarrollado el software, además estas pruebas evidenciadas a través de un documento deben estar firmadas por quienes realizaron las pruebas, en donde se acepte que el software desarrollado cumple con los lineamientos y funcionalidades para su uso.

- De ser posible, las pruebas se deben llevar a cabo en un ambiente de pruebas realista, para asegurar que el sistema no introducirá vulnerabilidades al ambiente productivo de la entidad, y que las pruebas son confiables.

- En donde la funcionalidad de la seguridad no satisface el requisito especificado, antes de comprar el software se debe reconsiderar el riesgo introducido y los controles asociados.

4.21. RELACIÓN CON LOS PROVEEDORES

4.21.1. Seguridad de la Información en las Relaciones con los Proveedores.

La entidad debe establecer mecanismos de verificación de lineamientos de seguridad en sus relaciones con todos los proveedores, especialmente aquellos proveedores críticos para la entidad por el manejo de información crítica o confidencial, con el objetivo de asegurar la información a la que tengan acceso o servicios que sean provistos por los mismos, y que cumplan con las políticas de seguridad de la información.

4.21.2. Tratamiento de la Seguridad dentro de los Acuerdos con Proveedores.

Los supervisores de contratos deben asegurar que se comuniquen las políticas y procedimientos de seguridad de la información a los proveedores y/o contratistas.

La Dirección General debe incluir en los acuerdos con proveedores y/o contratistas, como mínimo, los siguientes requisitos de seguridad de la información:

- Cláusula de confidencialidad (RT-Plt01 plantilla acta de confidencialidad)
- Cumplimiento de los lineamientos de seguridad de la información de la entidad.
- Reporte de eventos de seguridad de la información a través de los canales definidos en el RT-Pr01 procedimiento de soporte técnico y atención de servicios.

Los accesos a los sistemas de información y equipos de cómputo requeridos por los proveedores deben ser solicitados de manera formal a la División de Planeación y Sistemas.

4.22. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- La gestión de incidentes de seguridad debe estar basados de acuerdo con los lineamientos del RT-Pr01 procedimiento de soporte técnico y atención de servicios.

- Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en este manual.

- Cualquier incumplimiento identificado debe remitirse a la, quien debe determinar si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación.

  Categorías de incidentes de seguridad de la información: Si el incumplimiento es sujeto de clasificación teniendo en cuenta las siguientes categorías, se debe considerar como incidente de seguridad de la información:

Fuga de información: Se evidencia divulgación no autorizada de información de la entidad.

Acceso no autorizado:

- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso.
- Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario
- Personal no autorizado ingresa a las instalaciones de la entidad

Ataque:

- Se evidencia intención de afectar un recurso específico.
- Se modifica la imagen institucional en aplicaciones de la entidad.
- No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio (DDoS).
- Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web.

Código dañino:

- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información.
- El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso.

Denegación de servicio:

- El sistema de información no responde por alta cantidad de peticiones.
- El sistema de información se encuentra con latencia o degradación del servicio.

Robo o pérdida:

- Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida.
- Se presenta robo o pérdida de elementos personales en las instalaciones de la ENTIDAD.

Alarmas de sistemas de monitoreo:

- Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas.

Usos inadecuados:

- Si se ingresa texto copiado de internet en documentación oficial de la ENTIDAD, sin registrar la fuente.
- Si se publica comunicados en nombre de la Entidad sin revisión y aprobación del proceso de comunicación estratégica.

4.23. NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Cualquier violación de las políticas de seguridad de la información, se debe notificar inmediatamente a la División de Planeación y Sistemas a través de los siguientes canales.

- E-mail: planeacionysistemas@senado.gov.co
- Mesa de Servicios: extensión: 3030
- Mesa de Servicios: helpdesk@senado.gov.co
- Mesa de Servicios portal autoservicio: https://soporte.senado.gov.co/usdkv8/#!/login/

Así mismo, se debe notificar situaciones tales como: personas ajenas a la entidad en oficinas y centros de cómputo, correos maliciosos o sospechosos, reinicio de los equipos de cómputo o enrutadores, mala utilización de recursos, uso de software ilegal, divulgación, alteración y robo de información.

4.24. GESTIÓN DE LA CONTINUIDAD DE NEGOCIO

El Senado de la República, debe contemplar una estrategia de Continuidad de Negocio basada en los resultados del BIA (Bussines Impact Analisys) y demás documentación que se ha desarrollado que permiten contar con lineamientos para la continuidad de las operaciones de negocio, además:

- Se deben realizar pruebas periódicas a los controles de continuidad de negocio y de continuidad de la Seguridad de la Información implementados.
- La División de Planeación y Sistemas debe asegurar que se actualicen los Planes de Continuidad de Negocio posterior a los cambios en la infraestructura tecnológica.
- Contemplar un sitio alterno, donde los controles implementados en el ambiente de producción deben ser consistentes con el sitio alterno.
- Los cambios de seguridad en el ambiente de producción deben ser aplicados de la misma forma para el ambiente de prueba.

- La entidad debe establecer e implementar un Plan de Recuperación de Desastres (DRP) con el fin de asegurar la redundancia y continuidad de las instalaciones de procesamiento de información.

- La entidad debe realizar pruebas periódicas al DRP, con el fin de asegurar que los controles tecnológicos implementados son válidos y eficaces durante situaciones adversas.

4.25. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

- **Revisión de la Seguridad de la Información**

La Oficina de Control Interno debe realizar auditorías internas de revisión independiente al menos una vez al año. Esta revisión independiente es necesaria para asegurar la conveniencia, la adecuación y la eficacia continuas del enfoque de la Entidad para gestionar la seguridad de la información.

Esta revisión debe incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios en el enfoque hacia la seguridad, incluyendo la política y los objetivos de control

- **Revisión Cumplimiento Técnico**

La División de Planeación y Sistemas debe coordinar la revisión periódica de los sistemas de información para determinar el cumplimiento con las políticas y procedimientos de seguridad de la información. Para ello, se debe determinar a qué sistemas de información se le hará revisión.

5. 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.

6. 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.

7. BASE LEGAL

- 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.
- 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.

8. ANEXOS

RT Plt01 Plantilla acta de confidencialidad

9. FORMATOS

- RT Fr01 Formato Solicitud de Registros y Grabaciones de Seguridad
- RT Fr05 Formato requerimiento para cambios RFC
- RT Fr06 Formato registro copias de seguridad
- RT Fr07 Formato reporte de incidentes de seguridad de la información
- RT Fr08 Formato personal autorizado ingreso áreas seguras

- RT Fr10 Formato inventario, valoración y clasificación de activos de información
- RT Fr11 Formato plan anual de mantenimiento tecnológico

10. DOCUMENTOS RELACIONADOS

- NTC ISO/IEC 27001:2013 - Norma Técnica Colombiana Sistemas de Gestión de Seguridad de la Información.
- NTC ISO/IEC 27002:2013 - Norma Técnica Colombiana Sistemas de Gestión de Controles de Seguridad de la Información.
- Manual de políticas de seguridad de la información – Agencia Nacional de Minería

11. CONTROL DE CAMBIOS

Ver. 004// Rev. 1// FV. 1 de agosto de 2023

Cambios:

1. Actualización del alcance del manual

2.Actualización de términos y definiciones

3. Actualización de políticas generales de seguridad de la información e inclusión de ítems faltantes dentro de la misma.

Justificación: Se solicita la modificación del presente instructivo técnico, con el fin de actualizar el documento, toda vez que la mayoría de las políticas no estaban actualizadas o no se encontraban definidas en el manual. se realizó una definición de más del 90 % del manual, en la que además se incluyen oportunidades de mejora obtenidas en la última auditoria al proceso de recursos tecnológicos y el plan de privacidad y seguridad de la información.
Responsable: Lina María Díaz Rivera
Fecha: 2023-08-01
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: María 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, Términos y definiciones, Políticas generales de seguridad de la información, Políticas 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 Andrés Sánchez Morales

Fecha: 2017-09-26

ELABORÓ	REVISÓ	APROBÓ
Nombre: Aldair Suarez	Nombre: Pablo E. Álzate.	Nombre: Comité Institucional de Gestión y Desempeño
Cargo: Profesional Universitario	Cargo: Jefe División Planeación y Sistemas	No. Acta y Fecha: 23.08 del 27/07/2023