 <p>Agencia Nacional de Seguridad Vial</p>	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GESTIÓN TIC

MAYO 2023




 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

Tabla de contenido

1. INTRODUCCION	4
2. OBJETIVO.....	4
3. ALCANCE Y ÁMBITO DE APLICACIÓN.....	4
4. TÉRMINOS Y DEFINICIONES	5
5. ABREVIATURAS	5
6. RESPONSABILIDAD	5
7. NORMATIVIDAD	6
8. DESARROLLO.....	7
8.1. OBJETIVOS ESPECÍFICOS.....	7
8.2 DECLARACIONES	7
8.3 PRINCIPIOS.....	9
8.4 RECURSOS HUMANOS.....	9
8.4.1 GESTIÓN DEL TALENTO HUMANO.....	9
8.5 ACTIVOS DE INFORMACIÓN	10
8.5.1 GESTIÓN DE LA SEGURIDAD EN LOS ACTIVOS	10
8.5.2 INVENTARIO Y PROPIEDAD DE LOS ACTIVOS	10
8.5.3 CONTROLES A LOS ARCHIVOS DE GESTIÓN.....	10
8.5.4 CLASIFICACIÓN DE LA INFORMACIÓN.....	10
8.5.5 USO ACEPTABLE DE LOS ACTIVOS	11
8.6 CONTROLES DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN.....	14
8.6.1 CONTROL DE ACCESO.....	14
8.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	16
8.8 DISPOSICIONES FINALES.....	17
8.8.1 ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO	17
8.8.2 ADMINISTRACIÓN DEL RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN	17
8.8.3 CAPACITACIÓN Y CREACIÓN DE LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN	18

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

8.8.4	CUMPLIMIENTO	18
8.8.5	SANCIONES.....	18
8.8.6	VIGENCIA Y DEROGATORIA	19
9	CONTROL DE CAMBIOS	19
10	CONTROL DE FIRMAS	19

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

1. INTRODUCCION

La seguridad y privacidad de la información son aspectos esenciales en las entidades públicas. Con la digitalización en constante avance, es crucial contar con una sólida política que proteja los datos sensibles y asegure su confidencialidad, integridad y disponibilidad.

Esta política establece directrices para proteger la información y los sistemas frente a amenazas internas y externas, abordando también la privacidad de los ciudadanos y la gestión adecuada de la información confidencial.

Su propósito es fomentar una cultura de seguridad y responsabilidad en toda la ANSV, asignando roles y responsabilidades claras en la protección de la información. Al implementarla, la entidad busca salvaguardar los datos frente a accesos no autorizados, uso indebido, pérdida, robo o alteración, generando confianza ciudadana y cumpliendo con las regulaciones.


2. OBJETIVO

Adoptar la Política de Seguridad y Privacidad de la Información de la Agencia Nacional de Seguridad Vial, en adelante ANSV la cual buscar proteger la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos digitales y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la ANSV.

3. ALCANCE Y ÁMBITO DE APLICACIÓN

La política de seguridad de la información es un documento que establece las reglas, pautas y procedimientos que debe seguir la entidad para proteger la confidencialidad, integridad y disponibilidad de sus datos y recursos de tecnología de la información.

Esta política se aplica a todos los usuarios y sistemas de la ANSV, así como a los proveedores y entidades externas que acceden o gestionan su información, que en razón del cumplimiento de sus funciones y las de la Agencia Nacional de Seguridad Vial-ANSV, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación. Así mismo, la presente Política aplica a toda la información creada, procesada o utilizada por la ANSV, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

4. TÉRMINOS Y DEFINICIONES

Para efectos de lectura de este documento se tendrán contempladas las siguientes definiciones en la norma ISO 27000, Modelo de Seguridad y Privacidad de la Información-MPSI del Ministerio de las Tecnologías de la Información y Comunicaciones:

1. **Activo [Según ISO 27000]:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
2. **Auditoria [Según ISO 27000]:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoria.
3. **Confidencialidad [Según ISO 27000]:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
4. **Control de acceso [Según ISO 27000]:** Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad.
5. **Disponibilidad [Según ISO 27000]:** Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.
6. **Incidente [Según ISO 27000]:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
7. **Integridad [Según ISO 27000]:** Propiedad de exactitud y completitud
8. **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
9. **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.
10. **Spam:** Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales.
11. **Vulnerabilidad [Según ISO 27000]:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
12. **WAN:** Red de Área Amplia

5. ABREVIATURAS


ANSV: Agencia Nacional de Seguridad Vial

6. RESPONSABILIDAD

Los responsables de la definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información en la Agencia Nacional de Seguridad Vial son:

- a) El Representante de la Alta Dirección de la ANSV, quien velará por el cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información.

Página 5 de 19


 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

- b) El Oficial de seguridad de la información o quien haga sus veces, será designado por la Secretaría General a través del Grupo de Tecnologías de la Información y las Comunicaciones.

No obstante, lo estipulado en el artículo precedente, todos los servidores públicos, contratistas y proveedores de la ANSV son responsables del cumplimiento de la Política de Seguridad y Privacidad de la Información.

7. NORMATIVIDAD

- Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información Pública): Establece el deber de las entidades públicas de garantizar la disponibilidad, integridad y seguridad de la información que generan, obtienen, adquieren, transforman, controlan y custodian. Además, establece la obligación de conservar los documentos y registros en los términos establecidos por la normatividad archivística.
- Ley 1581 de 2012 (Ley de Protección de Datos Personales): Regula el tratamiento de los datos personales por parte de entidades públicas y privadas, estableciendo principios, obligaciones y derechos para garantizar la protección de la información personal.
- Ley 1273 de 2009 – De La Protección de la Información y de los Datos
- Ley 594 de 2000 (Ley General de Archivos): Establece las normas generales para la organización y funcionamiento de los archivos en Colombia, incluyendo los requisitos para el almacenamiento, conservación y protección de los documentos de las entidades públicas.
- Decreto 620 de 2020: Establece disposiciones para el almacenamiento y custodia de archivos de gestión en formato electrónico.
- Decreto 2609 de 2012: Reglamenta la conservación del patrimonio documental en medios electrónicos y se dictan otras disposiciones relacionadas con la gestión documental electrónica en las entidades públicas.
- Decreto 1377 de 2013: Este decreto reglamenta parcialmente la Ley 1581 de 2012 y establece disposiciones adicionales para el manejo de datos personales. Específicamente, establece los requisitos para la elaboración de políticas de tratamiento de datos personales y los procedimientos para el ejercicio de los derechos de los titulares
- Resolución 500 del 2021
- Decreto 620 de 2020: Este decreto establece los lineamientos para la gestión de riesgos en seguridad de la información en el sector público. Define los criterios y las obligaciones para la identificación, análisis y gestión de riesgos, y promueve la implementación de medidas de seguridad en las entidades públicas.

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

- Resolución 3564 de 2015 (Requisitos de seguridad de la información): Establece los requisitos mínimos de seguridad de la información que deben implementar las entidades públicas para proteger los sistemas y datos.

8. DESARROLLO

La política de seguridad de la información tiene como objetivo garantizar el cumplimiento de las normativas legales y sectoriales, prevenir y mitigar los riesgos de ciberseguridad, y fomentar una cultura de responsabilidad y concienciación entre los empleados y colaboradores.

Propender por que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (Confidencialidad), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad) y que sea utilizada para los propósitos que fue obtenida (Privacidad).

8.1. OBJETIVOS ESPECÍFICOS


La Política de Seguridad y Privacidad de la Información de la Agencia Nacional de Seguridad Vial-ANSV tiene como objetivos específicos:

- Establecer mecanismos y lineamientos para el manejo adecuado de la información.
- Mitigar los incidentes de la seguridad y privacidad de la información, seguridad digital en la entidad.
- Gestionar los riesgos digitales asociados a la seguridad y privacidad de la información, seguridad digital que afecten la confidencialidad, disponibilidad y privacidad de la información de La ANSV.

8.2 DECLARACIONES


A partir del Modelo de Seguridad y Privacidad de la Información emanado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, la Agencia Nacional de Seguridad Vial-ANSV declara:

- a) La ANSV establece los roles y responsabilidades relacionados con la presente política de seguridad y privacidad de la información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.
- b) La Entidad protege la información producida, custodiada y transmitida en desarrollo de sus procesos misionales.
- c) La Secretaría General a través del Grupo de Tecnologías de la Información y las Comunicaciones, diseñará e implementará la estrategia para proteger la

 <p>Agencia Nacional de Seguridad Vial</p>	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

información generada, recolectada, procesada y utilizada en el cumplimiento de su misión.

- d) El Grupo de Tecnologías de la Información y las Comunicaciones establecerá los lineamientos para la identificación, clasificación y buen uso de los activos de información, para su protección.
- e) El Grupo de Tecnologías de la Información y las Comunicaciones suministra y gestiona las herramientas de hardware y software para el procesamiento y almacenamiento de la información y a su vez implementa controles para mitigar los riesgos sobre dicha información; los propietarios de la información son los responsables de los procesos institucionales y por ende de la información registrada. De acuerdo a lo anterior serán los únicos que autorizan para realizar cambios y modificaciones a realizar sobre los sistemas de información o su información.
- f) El Grupo de Gestión Documental es el facultado para establecer los lineamientos para la identificación, clasificación y buen uso de los activos de información física, para su protección.
- g) Las dependencias de la Agencia Nacional de Seguridad Vial que tienen la custodia de la información generada en el marco de sus funciones deben aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.
- h) Los activos de información, equipos, bienes, aplicaciones, herramientas tecnológicas y servicios de Tecnologías de la Información y las Comunicaciones en adelante TIC, asignadas por la ANSV son para uso exclusivo del cumplimiento de las funciones designadas; razón por la cual la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos se considera propiedad de la entidad y el uso inadecuado de dichos recursos puede conllevar a sanciones disciplinarias y legales correspondientes.
- i) Es obligación de todos los servidores públicos, contratistas y proveedores adscritos a la ANSV cumplir con la **POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** y propender por la integridad, disponibilidad y confidencialidad de la misma, so pena de que la Entidad tome las medidas disciplinarias, legales y administrativas correspondientes.
- j) Todos los activos de información deben tener un responsable, la creación de cuentas de usuario y/o correo electrónico genéricos (que no estén asociados a un servidor público) no estarán autorizadas.
- k) Es responsabilidad de los servidores públicos y contratistas de la ANSV realizar una copia de seguridad de los archivos más sensibles que se almacenan en los

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

equipos de cómputo asignados; esta copia debe almacenarse en los medios designados por la ANSV tales como servidor de archivos, almacenamiento en la nube, DVD, entre otros. Una vez finalizada la vinculación con la Entidad se deberá entregar toda la información procesada dentro de los equipos a cargo al jefe inmediato o al supervisor de contrato.

- l) Los equipos de cómputo de propiedad de los contratistas deberán cumplir con características mínimas antes de ser conectados en las redes de la Agencia, esto a nivel de seguridad (actualizaciones, antivirus, entre otros) y uso de software legal. En caso de presentarse algún incidente identificado con el equipo del contratista la Entidad tomará las medidas disciplinarias, legales y administrativas correspondientes.

8.3 PRINCIPIOS

La presente política se fundamenta en los siguientes principios:


- a) La información es uno de los activos más importantes de ANSV y por lo tanto se espera que sea utilizada acorde con los requerimientos de sus funciones.
- b) Confidencialidad, la información de la ANSV y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y que sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones.
- c) Integridad, la información de la ANSV debe preservar su integridad independientemente de su residencia temporal o permanente, o la forma en que sea transmitida y que esté protegida contra modificaciones no planeadas, realizadas con o sin intención.
- d) Disponibilidad, la información de la entidad debe estar disponible cuando sea requerida.
- e) Privacidad, la información debe ser preservada y que sea utilizada para los propósitos que fue obtenida.

8.4 RECURSOS HUMANOS

8.4.1 GESTIÓN DEL TALENTO HUMANO

La ANSV a través del Grupo de Gestión del Talento Humano y el Grupo de Gestión Contractual son responsables de divulgar la Política de Seguridad y Privacidad de la Información a todos los servidores públicos o contratistas que se vinculen a la Agencia.

El Grupo de Gestión Contractual debe realizar las tareas pertinentes para que todos los contratos de prestación de servicios incorporen las obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad y Privacidad de la Información, el manejo confidencial de la información, la cesión de derecho de autor a la Entidad y la protección de datos personales.

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

Cuando un servidor público o contratista cese en sus funciones o culmine la ejecución de un contrato en la ANSV, el jefe inmediato o supervisor del contrato será el encargado de la custodia de los recursos de información.

8.5 ACTIVOS DE INFORMACIÓN

8.5.1 GESTIÓN DE LA SEGURIDAD EN LOS ACTIVOS

La ANSV a través del Grupo de Tecnologías de la Información y las Comunicaciones, el Grupo de Gestión Documental y la Oficina Asesora de Planeación, deberán establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

8.5.2 INVENTARIO Y PROPIEDAD DE LOS ACTIVOS

La responsabilidad de la administración, gestión e implementación de controles de los activos de información está en cabeza del propietario de los mismos. Los activos de Información de la ANSV deben ser identificados, clasificados, aceptados y controlados para propender por su uso adecuado, protección y recuperación ante cualquier desastre.

Los propietarios de la información deben propender por mantener actualizado el inventario de sus activos de información y hacer entrega de éste al menos una vez por año. La consolidación de dicho inventario está bajo la responsabilidad de Grupo de Tecnologías de la Información y las Comunicaciones y el Grupo de Gestión Documental.

Con el objeto de implementar los controles de seguridad, las dependencias que tienen la custodia de la información en el marco de su función se encargarán de proteger la información, mantener y actualizar el inventario de activos de información.


8.5.3 CONTROLES A LOS ARCHIVOS DE GESTIÓN

El Grupo de Gestión Documental, debe implementar controles para garantizar que los archivos de gestión de la entidad cuenten con los mecanismos de seguridad que salvaguarden y conserven dicha información, conforme lo establecido en la normatividad aplicable.

8.5.4 CLASIFICACIÓN DE LA INFORMACIÓN

Los propietarios de los activos de información deben documentar la clasificación de seguridad de los activos de los que son responsables y designarán un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la ANSV se debe realizar con base en la normatividad vigente.


 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

8.5.5 USO ACEPTABLE DE LOS ACTIVOS

Los recursos tecnológicos al igual que los archivos, carpetas, bases de datos, aplicaciones y documentos, son activos de información que pertenecen a la ANSV, por lo cual su uso es exclusivamente institucional y es responsabilidad de aquel a quien se asigne o corresponda su uso, propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso. Se constituyen como recursos tecnológicos:

a. **CORREO ELECTRÓNICO:** El correo electrónico institucional asignado es un servicio para la comunicación y colaboración de los servidores públicos y contratistas de la ANSV, de uso personal e intransferible, que debe utilizarse responsablemente cumpliendo como mínimo con los siguientes lineamientos:

- El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales, económicos, comerciales, propaganda, campañas, invitaciones y cualquier otro ajeno a los propósitos de la Entidad.
- El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @ansv.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
- Está prohibido el envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través del correo del Director(a) General, el (la) Secretario General y el (la) jefe de la Oficina Asesora de Comunicaciones.
- Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar al Grupo de Tecnologías de la Información y las Comunicaciones a través de la mesa de servicios y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM por parte de los colaboradores de la entidad.
- Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados al Grupo de Tecnologías de la Información y las Comunicaciones a través de la mesa de servicio y serán tratados como incidentes de seguridad de la información.
- La cuenta de correo institucional no podrá ser utilizada para el registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales, casinos, concursos, sitios de citas o cualquier otro ajeno a las funciones que tengan directa relación con el objeto misional de la ANSV.
- Está expresamente prohibido el uso del correo para el envío de contenidos insultantes, información de agremiaciones, ofensivos, injuriosos, obscenos, violatorios de los derechos fundamentales, derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
- Está expresamente prohibido distribuir información de la ANSV que no sea considerada de uso público a otras entidades o ciudadanos, sin la debida autorización de dueño del activo de información.
- El correo electrónico institucional deberá contener junto con la firma un mensaje de

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26


confidencialidad, que deberá ser aprobado por el Grupo de Tecnologías de la Información y las Comunicaciones. Las cuentas de correo electrónico se asignarán de acuerdo a la nomenclatura definida por el Grupo de Tecnologías de la Información y las Comunicaciones.

a. INTERNET: Si bien el Grupo de Tecnologías de la Información y las Comunicaciones establece controles a la navegación de acuerdo a las políticas y perfiles establecidos, es responsabilidad de todos los servidores públicos y contratistas de la ANSV hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí establecidas:


- La ANSV, en cabeza del Grupo de Tecnologías de la Información y las Comunicaciones, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
- La ANSV, a través del Grupo de Tecnologías de la Información y las Comunicaciones se reserva el derecho de monitorear, hacer seguimiento y auditoría al uso que los usuarios le den, para verificar que se haga un uso responsable y racional de dicho recurso.
- El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales dentro del marco institucional y se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, ofensivo, injurioso, obsceno, pornográfico, violatorio de los derechos de autor y todo aquel que atente contra la integridad moral y seguridad de la Entidad.
- El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación están totalmente prohibidos y su detección será tratada como un incidente de seguridad.
- Descargar archivos provenientes de Internet implica un riesgo para la seguridad de la información, así como un riesgo de infracción al régimen legal de derechos de autor, por lo cual se solicita que únicamente se haga cuando sea necesario; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, .pig.

b. EQUIPOS DE CÓMPUTO Y OTROS DISPOSITIVOS: La ANSV podrá hacer entrega a los servidores públicos y contratistas de computadores de escritorio, portátiles, Tablet, teléfonos IP, teléfonos inteligentes o dispositivos similares para el desarrollo de sus labores; el manejo de dichos equipos por parte de éstos conlleva responsabilidades y deben ajustarse a las siguientes directrices generales:

- La clave de acceso de aquellos dispositivos que la requieran es de uso personal y no podrá ser compartida, razón por la cual la responsabilidad de un posible mal uso del dispositivo recaerá sobre el servidor público o contratista a quien se asignó dicho usuario y contraseña.
- Los dispositivos asignados solo podrán usarse para fines laborales relacionados con las funciones y obligaciones designadas, razón por la cual no hay autorización de instalar software diferente al autorizado por el Grupo de Tecnologías de la Información

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

- y las Comunicaciones y debidamente licenciado.
- Los dispositivos de cómputo y móviles que sean asignados a los servidores públicos y contratistas serán para uso institucional exclusivamente e intransferibles y la responsabilidad de su uso recaerá sobre la persona a la que le fue asignado.
 - La ANSV se reserva el derecho de monitorear el contenido y software instalado en los equipos de la Agencia para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, video, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del servidor público o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
 - Los únicos autorizados para la instalación de software adicional a las aplicaciones base es el personal técnico que designe el Grupo de Tecnologías de la Información y las Comunicaciones, previa solicitud a través de la mesa de servicio y luego de la aprobación respectiva (se debe constatar la necesidad de su uso y que la ANSV cuente con el respectivo licenciamiento).
 - Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por el Grupo de Tecnologías de la Información y las Comunicaciones previa solicitud a través de la mesa de servicio.
 - Es responsabilidad de los servidores públicos y contratistas de la ANSV mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas en custodia al jefe inmediato o supervisor del contrato al finalizar la vinculación con la Entidad.
 - No está permitido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos tales como computadores de escritorio, portátiles entre otros.
 - El Grupo de Tecnologías de la Información y las Comunicaciones en cabeza del equipo de mesa de servicio deberá aprovisionar los computadores antes de ser entregados, garantizando que:
 - Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.
 - El software instalado sea el software base definido por el Grupo de Tecnologías de la Información y las Comunicaciones y cuente con el respectivo licenciamiento.
 - Los sistemas operativos y demás aplicativos tengan instaladas las últimas actualizaciones liberadas a la fecha de entrega del equipo.
 - El antivirus este actualizado, funcionando y administrado desde consola.
 - Los equipos deberán quedar apagados cada vez que el servidor público o contratista no se encuentre en la oficina durante la noche, por seguridad y ahorro de energía, salvo en aquellos casos dada la necesidad del servicio
 - El Grupo de Tecnologías de la Información y las Comunicaciones, debe implementar servidores para el despliegue de actualizaciones y parches de seguridad y diseñar estrategias que permitan mantener actualizada toda la plataforma computacional de la ANSV.

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

- c. CABLEADO ESTRUCTURADO:** Las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas de energía eléctrica regulada color naranja y bajo ninguna circunstancia se puede conectar otros elementos en dichas tomas.

En los puntos de red de los usuarios no está permitido realizar conexiones de switches, hub, acces point u otros dispositivos para realizar derivaciones, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

- d. SISTEMAS DE INFORMACIÓN:** Las credenciales de acceso a la red y a recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los servidores públicos y contratistas de la ANSV no deben revelar éstas a terceros ni utilizar claves ajenas. Todo servidor público y contratista será responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

Cuando se presenten ausencias de servidores públicos o contratistas por incapacidades, licencias no remuneradas o suspensión de contrato, será bloqueado el acceso a los equipos de cómputo asignados, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. Es responsabilidad del Grupo de Gestión del Talento Humano y el Grupo de Gestión Contractual notificar este evento con una solicitud al Grupo de Tecnologías de la Información y las Comunicaciones a través de la mesa de servicio.


Solo podrán publicarse aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a la ANSV; las demás aplicaciones son de uso interno y su acceso desde fuera de la Entidad se debe realizar a través de conexiones seguras con previa autorización por parte del Grupo de Tecnologías de la Información y las Comunicaciones.

8.6 CONTROLES DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

8.6.1 CONTROL DE ACCESO

La ANSV a través del Grupo de Servicios Administrativos, propende por implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad, deberá garantizar la correcta identificación del personal que pretende el ingreso a las instalaciones.

La ANSV a través del Grupo de Gestión del Talento Humano y el Grupo de Gestión Contractual deben establecer los mecanismos para comunicar al Grupo de Tecnologías de la Información y las Comunicaciones las novedades de ingreso y retiro de los servidores públicos y contratistas de la ANSV para gestionar los derechos de acceso a los sistemas de información, recursos y servicios tecnológicos de la Agencia.

 <p>Agencia Nacional de Seguridad Vial</p>	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

El Grupo de Tecnologías de la Información y las Comunicaciones debe implementar controles, procedimientos e instructivos para proveer el acceso físico y lógico de los recursos informáticos a usuarios autorizados para el cumplimiento de sus funciones estos serán los siguientes:

- a. CONTROLES CRIPTOGRÁFICOS:** La ANSV a través del Grupo de Tecnologías de la Información y las Comunicaciones debe implementar lineamientos o directrices del uso adecuado de controles criptográficos, con el fin de establecer un lineamiento que permita servir como guía bajo las mejores prácticas.

Los propietarios de los activos de información deben identificar las necesidades de criptografía de información de acuerdo al grado de criticidad y privacidad de la misma e informar de dicha necesidad al Grupo de Tecnologías de la Información y las Comunicaciones quien debe analizar y si es procedente aprobar.


El Grupo de Tecnologías de la Información y las Comunicaciones debe asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información que así lo requiera.

- b. SEGURIDAD FÍSICA Y DEL ENTORNO:** La ANSV a través del Grupo de Servicios Administrativos, debe implementar controles para proteger el perímetro de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructuras de soporte a los sistemas de información y comunicaciones.), además mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Todos los servidores públicos, contratistas y visitantes que se encuentren en las instalaciones de la ANSV deberán estar debidamente identificados, con un documento que acredite su tipo de vinculación el cual se deberá portar en un lugar visible.

- c. SEGURIDAD DE LAS OPERACIONES:** La ANSV a través del Grupo de Tecnologías de la Información y las Comunicaciones se debe encargar de la operación y administración de los recursos tecnológicos que soportan la operación de la Agencia y propender por la implementación de los controles asociados a éstos para mitigar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información; para este fin debe cumplir con los siguientes lineamientos:

- Implementar controles para mitigar los riesgos inherentes a códigos maliciosos, sin embargo, los usuarios no pueden instalar software en los equipos de propiedad de la Entidad.
- Implementar un procedimiento para la gestión o control de cambios de las TIC donde los cambios en la configuración de los equipos, redes, sistemas de

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

información, bases de datos, aplicaciones o cualquier activo de información de Tecnologías de Información-TI sean revisados, evaluados y aprobados.

- Implementar controles para auditar el acceso y uso de datos a los sistemas de información designados por el Grupo de Tecnologías de la Información y las Comunicaciones para el control de los servidores públicos y contratistas, adicionalmente se reserva el derecho de monitorear la actividad donde se sospecha que se ha producido o pueda producir una violación de la política, asegurando el debido proceso y el respeto por los derechos de las partes involucradas.
- Proveer los recursos necesarios para la implementar controles requeridos para la seguridad de las operaciones.

- d. SEGURIDAD DE LAS COMUNICACIONES:** La ANSV a través del Grupo de Tecnologías de la Información y las Comunicaciones establecerá los Acuerdos de Niveles de Servicios-ANS requeridos para que el proveedor de servicios de tecnologías de Información-TI que permita la disponibilidad de las redes WAN e Internet.


La ANSV a través del el Grupo de Tecnologías de la Información y las Comunicaciones debe implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos de la Entidad propendiendo la integridad y confidencialidad de la información.

- e. CONTROLES EN LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS:** El Grupo de Tecnologías de la Información y las Comunicaciones será la única área autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de aplicaciones, sistemas de información o cualquier componente de TIC. De igual forma el Grupo de Tecnologías de la Información y las Comunicaciones velará porque la adquisición, desarrollo interno o externo de sistemas de información incorpore las buenas prácticas para el desarrollo seguro de software y estándares de seguridad informática.

- f. CONTROLES EN LAS RELACIONES CON LOS PROVEEDORES:** La ANSV a través del Grupo de Tecnologías de la Información y las Comunicaciones y el Grupo de Gestión Contractual, definirán mecanismos de control que aseguren que la información a la que tenga acceso un tercero cuente con un nivel de protección adecuado y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

8.7 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La ANSV, a través del Grupo de Tecnologías de la Información y las Comunicaciones se encarga de definir, documentar, mantener, publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos de seguridad de la información. De igual forma el Grupo de Tecnologías de la Información y las Comunicaciones deberá promover el reporte

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

de eventos de seguridad de la información para reducir la probabilidad e impacto del riesgo inherente a ellos.

Los eventos e incidentes de seguridad de la información serán investigados por el Grupo de Tecnologías de la Información y las Comunicaciones de acuerdo al procedimiento de incidentes de seguridad de la información.

Para la consecución efectiva de lo establecido en el presente ítem, se debe diseñar, construir y aplicar un protocolo referente al reporte de incidentes de seguridad de la información.

8.8 DISPOSICIONES FINALES

8.8.1 ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO

Se espera que la Política de Seguridad y privacidad de la Información se preserve en el tiempo. Sin embargo, se deberá hacer una revisión anual o ante cambios estructurales y tecnológicos que afecten a la ANSV, para asegurar que ésta cumple con el cambio de las necesidades de la Entidad. El oficial de Seguridad de la Información es responsable de desarrollar esta revisión y llevarla a cabo considerando los lineamientos institucionales.


Cualquier miembro de la ANSV puede identificar la necesidad de modificar la Política de Seguridad y privacidad de la Información. Dichas inquietudes y sugerencias deben ser comunicadas al oficial de Seguridad de la Información, responsable por el mantenimiento de esta.

8.8.2 ADMINISTRACIÓN DEL RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

La información de la ANSV se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, a través de la Oficina Asesora de Planeación se realizará periódicamente un análisis respecto al impacto en seguridad de la información, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable.

Establecidos el nivel de riesgo y el valor de la información, se debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos en la Entidad.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de la ANSV y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información.

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

8.8.3 CAPACITACIÓN Y CREACIÓN DE LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN

La ANSV debe contar con un programa permanente que permita asegurar que los servidores públicos, contratistas, usuarios y terceros estén informados acerca de sus responsabilidades en Seguridad de la Información y de las continuas amenazas que ponen en riesgo la información de la Entidad a cargo del Grupo de Talento Humano.

Los servidores públicos, contratistas, usuarios y terceros deben estar enterados de los procedimientos de seguridad y privacidad de la información que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo.

8.8.4 CUMPLIMIENTO

La Agencia Nacional de Seguridad Vial velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

La ANSV, implementará y mantendrá los controles necesarios para proteger la información de servidores públicos, contratistas, beneficiarios, proveedores y demás terceros de los cuales reciba y administre información de conformidad con la Ley de Protección de Datos Personales.

La ANSV implementará y mantendrá los controles necesarios para dar cumplimiento a las disposiciones legales sobre derechos de autor, propiedad intelectual, ley de transparencia y Política Gobierno Digital.


Los servidores públicos, contratistas y proveedores que violen los requisitos contenidos en esta norma pueden estar sujetos a medidas disciplinarias, penales y administrativas según el caso.

La Política de Seguridad y Privacidad de la Información deberá revisarse y actualizarse cada año o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.

Así mismo, esta Política que da las directrices generales estará reglamentada por los lineamientos contenidos en un manual de seguridad de la información y demás documentación que apoye la estrategia de seguridad y privacidad de la información.

8.8.5 SANCIONES

El incumplimiento de la política de seguridad y privacidad de la información por parte de los servidores públicos de la Agencia de Seguridad Vial puede llevar a la adopción de sanciones disciplinarias de conformidad con la Ley 734 de 2002 y 1952 de 2019 “Código Disciplinario

 Agencia Nacional de Seguridad Vial	GESTIÓN TIC		
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
	Código: ANSV-TIC-PO-04	Versión: 02	Fecha: 2023-05-26

Único". Así mismo, el incumplimiento por parte de los aprendices, practicantes, proveedores, visitantes, organizaciones o entidades cooperantes y miembros del público que utilicen los servicios de información proporcionada por la Entidad puede generar en la terminación de los contratos y de las relaciones interinstitucionales y/o la suspensión de los servicios y/o dar lugar al inicio de acciones legales de conformidad con la Ley.

8.8.6 VIGENCIA Y DEROGATORIA

La presente política se aprobó en el Comité Institucional de Gestión y Desempeño de fecha 27 de noviembre de 2019 y rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

9 CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
2018-06-18	Se crea la primera versión del cambio	00
2019-11-27	Actualización del documento	01
2023-05-26	Se actualiza alcance, se crea introducción, normatividad y abreviaturas	02

10 CONTROL DE FIRMAS

Firma

CARLOS FREDY CARMONA RAMIREZ
Secretario General

Elaboró: Javier Alejandro Pereira Vargas – Contratista Grupo TIC 

Revisó: Erika Jazmin Ladino Garzon - Contratista Grupo TIC 