# POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## Tabla de contenido

## 1. OBJETIVO GENERAL

La presente política tiene por objetivo determinar los lineamientos y directrices que permitan la protección de los activos de información de la Agencia Nacional de Infraestructura.

## 2. OBJETIVOS ESPECÍFICOS

- Asegurar la confidencialidad, integridad y disponibilidad de los activos de información que soportan el cumplimiento de la misión en la ANI.
- Mantener la cultura de protección y uso adecuado de los activos de información al interior de la ANI.
- Mitigar o eliminar los incidentes de seguridad de la información que afecten de manera negativa los activos de información de la ANI.
- Gestionar los riesgos de seguridad digital en la ANI.
- Contribuir al fortalecimiento de la política de transparencia.
- Definir los parámetros bajo los cuales se trata y administra los datos personales recogidos y almacenados dentro las bases de datos y los procedimientos para la garantía de los derechos de los titulares de los datos

## 3. ALCANCE

La política de Seguridad y Privacidad de la información son de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad. Aplican a toda la información que es producida y administrada producto de la ejecución de los procesos y proyectos a cargo de la ANI en cumplimiento de sus funciones.

## 4. GLOSARIO

**Autorizaciones:** Es el consentimiento dado por el dueño o titular de información que se pretende incluir en una base de datos, dicha autorización debe informarle cuáles datos personales serán recolectados, así como las finalidades para las cuales será usado el dato.

**Activo de información**: elemento que es de valor para el cumplimiento de la función de la Entidad, tales como: software, servicios web, redes, hardware, información física o digital (archivos, bases de datos), recurso humano, entre otros.

**Aviso de Privacidad:** Es el instrumento a través del cual se le comunica al titular de la información que la entidad cuenta con las políticas de tratamiento de información que le serán aplicables; éste

debe ser entregado a más tardar "al momento de la recolección de los datos personales". Debe incluir mínimo lo siguiente:

- ✓ Datos del responsable del tratamiento
- ✓ Derechos del titular
- ✓ Canales dispuestos para que el titular conozca la política de tratamiento de datos personales de la Agencia Nacional de Infraestructura

**Base de datos personales:** Se entiende como el conjunto de datos personales pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

**Clasificación de Información:** acto de asignar a la información alguna de las categorías definidas por la Entidad.

**Confidencialidad**: Propiedad que la información sea concedida o accedida por quienes están autorizados.

**Contratos de Transmisión de Datos:** Es el acuerdo que debe suscribir el responsable y el encargado del tratamiento de datos personales bajo su control y responsabilidad, señalando los alcances, las actividades que el encargado realizará por cuenta del responsable y las obligaciones con el titular y el responsable.

**Control**: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

**Datos personales:** Hace referencia a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables; pueden ser clasificados en cuatro grandes categorías: públicos, semiprivados, privados y sensibles.

**Dato privado:** Es la información de naturaleza íntima o reservada que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones, así como por decisión del titular de los mismos. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

**Datos públicos:** Son todos aquellos que no son de naturaleza semiprivada o privada, como también los contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, y los relativos al estado civil de las personas. Entre los datos de naturaleza pública a resaltar se encuentran: los registros civiles de nacimiento, matrimonio y defunción, y las cédulas de ciudadanía apreciadas de manera individual y sin estar vinculadas a otro tipo de información.

**Dato semiprivado:** Es aquella información que no es de naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como es el caso de los datos financieros, crediticios o actividades comerciales.

**Datos sensibles:** Es la información que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tal es el caso del origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

**Disponibilidad**: Propiedad que la información sea accesible y utilizable en el momento en que se requiera.

**Dispositivo Móvil**: Tipo de equipo de cómputo de tamaño pequeño, con capacidades de procesamiento, almacenamiento, con posibilidad de conexión a internet, con memoria, que pueden llevar a cabo diferentes funciones.

**Encargado del Tratamiento:** Es la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros realiza el tratamiento de datos personales en virtud de la delegación o mandato por parte del responsable. Entre dichos encargos se encuentran la obtención de autorizaciones por parte de los ciudadanos y la verificación de cumplimiento de la finalidad en la recolección por parte de la Entidad.

**Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

**Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

**Incidente de Seguridad**: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

**Información crítica:** Información necesaria para llevar a cabo una acción determinada y para evaluar su grado de cumplimiento.

**Información sensible:** Datos que por su conocimiento o divulgación no autorizado podría traer efectos indeseados a la Entidad.

**Integridad**: Propiedad que la información o activo de información asegure su estado de exactitud y completitud.

**Inventario de activos de información**: es una lista ordenada y documentada de los activos de información pertenecientes a la Agencia.

**Modelo de Seguridad y Privacidad de la información:** Es un modelo que conduce a las Entidades a la preservación de la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar los datos, mediante la aplicación de un proceso de gestión del riesgo; pretende facilitar el proceso de construcción de una política de privacidad por parte de la Entidad.

**Norma Técnica Colombiana ISO/IEC 27001:2013:** Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico

**Política de Seguridad de la Información:** Es un conjunto de directrices y lineamientos pertinentes a la seguridad de la información.

**Propietario de la información**: es la unidad organizacional, proceso donde se crean los activos de información o rol designado.

**Recursos tecnológicos**: son aquellos componentes de hardware y software tales como: equipos servidores (de aplicaciones y de servicios de red), equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas para el buen funcionamiento y la optimización del trabajo al interior de la ANI.

**Responsable del Tratamiento**: Es toda persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, tenga poder de decisión sobre las bases de datos y/o el Tratamiento de los datos, entendiendo por tratamiento: “Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión”. Tiene entre sus actividades las de definir la finalidad y la forma en que se almacenan, recolectan y administran los datos, así como solicitar y conservar la autorización en la que conste el consentimiento expreso del titular de la información.

**Riesgo:** Efecto de la incertidumbre en el cumplimiento de los objetivos.

**Sistemas de información**: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la ANI o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

**Titular de la información**: Persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

**Tratamiento de datos o de información**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

**Usuario:** Persona natural o jurídica pública o privada que, en los términos y circunstancias previstos en la presente ley, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información.

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

## 5. RESPONSABILIDADES DE LA ALTA DIRECCIÓN

Frente a los lineamientos antes enunciados, la alta dirección de la ANI, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de estándares de seguridad y privacidad de esta, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad. De igual manera garantiza la disposición de los recursos necesarios para que la entidad en términos de seguridad de la información pueda acoplar sus procesos al modelo MSPI.

Es así como la alta dirección de la ANI aprueba la política de seguridad y privacidad de la información y protección de datos personales, como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento y mejora continua de políticas y lineamientos consecuentemente orientados a salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

## 6. RESPONSABILIDAD DE FUNCIONARIOS, CONTRATISTAS Y TERCEROS

**Es responsabilidad de los funcionarios, contratistas y terceros** salvaguardar la información institucional de la Agencia, garantizando así la confidencialidad, integridad y disponibilidad de la información y la protección de datos personales, teniendo como responsabilidades:

i. Cumplir las políticas de seguridad y privacidad de la información descritas en el presente documento.
ii. Reportar los incidentes de seguridad de la información a la mayor brevedad mediante los procedimientos establecidos.
iii. Utilizar los sistemas de información, el acceso a la red y la información únicamente para las funciones a su cargo y los propósitos establecidos en las políticas de seguridad de la información.
iv. Incorporar la seguridad de información como parte de las actividades y tareas bajo su responsabilidad.
v. Utilizar únicamente software y demás recursos tecnológicos autorizados.

## 7. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A continuación, se dictan los lineamientos que conforman la Política de seguridad de la información:

PSI 1. Organización de la Seguridad de la Información:

- La ANI establece y lidera la gestión de seguridad y privacidad de la información a través de la identificación de una estructura de roles y responsabilidades compartidas y aceptadas por los servidores públicos, proveedores, o terceros con quien la ANI tenga una relación laboral o contractual.

PSI 2. Gestión de Activos de Información:

- La ANI protege los activos de información y vigila la efectividad de los mecanismos de control de acceso físico que aseguren las instalaciones físicas de la entidad. Así mismo, controla las vulnerabilidades y las condiciones medioambientales de sus oficinas. 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 cumplimiento de la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, los activos de información de la ANI deberán ser identificados y registrados en un “Inventario de activos de Información”.

- Es responsabilidad de cada líder de proceso mantener actualizado el inventario de activos de información.

PSI 3. Clasificación de la Información:

- La clasificación, tratamiento y control de la información se realiza por todos los procesos en concordancia con la legislación colombiana vigente para las entidades estatales.

- Los documentos que se tienen en la ANI estarán etiquetados de acuerdo con las tablas de retención documental y el índice de información clasificada y reservada adoptado. A su vez, el manejo, custodia y préstamo de dichos documentos se debe realizar de acuerdo con las medidas definidas por la Vicepresidencia Administrativa y Financiera de la Entidad.

- El criterio que adopta la ANI para la clasificación de activos de información está basado en el nivel de accesibilidad, integridad y confidencialidad de la siguiente manera:

    - **Confidencialidad**: la información debe estar disponible solamente para los individuos, entidades o procesos autorizados por los líderes de proceso y/o responsables de la información que se defina al interior de la ANI.
      Se definen como niveles de acceso a la información para esta clasificación:

- Información pública – reservada.
- Información pública – clasificada.
- Información pública y no clasificada.

- **Integridad**: la información debe ser exacta, precisa y completa desde su creación hasta su destrucción. Se definen niveles para esta clasificación: alta, media, baja y no clasificada.

- **Disponibilidad**: la información debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizado cuando así lo requiera. Se definen niveles para esta clasificación:

  - Alta
  - Media
  - Baja
  - No clasificada.

PSI 4. Gestión de control de acceso:

- La ANI adopta mecanismos de autenticación para el acceso y/o uso de los activos de información, los cuales son personales e intransferibles. Los funcionarios públicos, contratistas y terceros son responsables de tomar precauciones para mantener por preservar la confidencialidad de la información.

PSI 5. Uso de dispositivos móviles:

- La ANI establece directrices y mecanismos para autorizar, configurar y asignar responsabilidad frente al uso de dispositivos móviles. Los usuarios deberán adoptar y mantener toda precaución necesaria para asegurar la confidencialidad, integridad y disponibilidad de la información.

PSI 6. Acceso y uso de información:

- El acceso a la información es autorizado por el responsable del tratamiento de esta y será controlado por mecanismos tecnológicos (Herramientas de control de acceso como validación de contraseñas) y no tecnológicos (aplicación de políticas y verificación de procedimientos de T.I.) que garantizan confidencialidad, integridad, disponibilidad, control y auditoría.

- Todos los servidores públicos, contratistas y terceros firmarán un acuerdo de responsabilidad en cuanto al uso y confidencialidad de la información a la cual tendrá acceso, donde, además se reconozca los criterios de propiedad de la información, uso o explotación de sobre los derechos de autor o patrimoniales de la Agencia, acciones ante incumplimiento del acuerdo y, tiempo de caducidad de este.

PSI 7. Disposición de información, medios y equipos de cómputo:

- La ANI definirá lineamientos para las actividades de eliminación segura de la información de equipos de cómputo por posibles estados de obsolescencia, daño o reutilización de equipos de cómputo.

- Es responsabilidad de los líderes de proceso (dueños de los activos de información), asegurar que toda la información en medio físico esté debidamente salvaguardada de acuerdo con la políticas internas de manejo de los documentos y aquella que se encuentre en medio digital esté almacenada en la infraestructura dispuesta por la entidad (correo institucional, sistemas de información misional y de apoyo, carpetas compartidas y herramienta Microsoft OneDrive, entre otras) de tal forma que pueda ser protegida por la políticas configuradas en los activos tecnológicos de la entidad.

PSI 8. Uso de los equipos de cómputo:

- En los equipos de cómputo de propiedad de la ANI no se permite la instalación y uso de software no licenciado o no autorizado por el GIT de Tecnologías de la Información y las Comunicaciones.
- Los equipos de cómputo y recursos tecnológicos al servicio de los usuarios de la Agencia no deberán ser utilizados para actividades que no correspondan o tengan relación con el cumplimiento de las funciones de la entidad, entre ellas, divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política o, cualquier otro uso que no esté autorizado.

PSI 9. Gestión de desarrollo, adquisición y mantenimiento de sistemas de información:

- La ANI garantiza que la seguridad de la información sea parte integral del ciclo de vida de los sistemas de información, bien para su desarrollo, adquisición o mantenimiento, por tanto, áreas con la responsabilidad de adquirirlos, desarrollarlos o mantenerlos deberán asegurar que dichos sistemas de información cumplan con los propósitos y buenas prácticas de seguridad y privacidad de la información.
- El uso de sistemas de información o aplicaciones o instalación de cualquier tipo de software y/o herramientas informáticas en los equipos de cómputo de la entidad deberán ser aprobados por el G.I.T. de Tecnologías de la Información, ello con el fin de validar las características técnicas, el cumplimiento de derechos de autor y las políticas de seguridad de la información.

PSI 10. Gestión de incidentes de seguridad de la información:

- La ANI establecerá el procedimiento para que los incidentes de seguridad de la información sean reportados, registrados y atendidos de manera oportuna, en consecuencia, todos los servidores públicos, contratistas y terceros que tengan acceso a la información de la entidad, están obligados a reportar cualquier incidente que afecte o ponga en riesgo la seguridad de la información.

PSI 11. Gestión de seguridad en la continuidad del negocio:

- La Agencia identificará las necesidades y requisitos de seguridad de la información para su integración con las estrategias de continuidad de negocio, de modo que, ante situaciones de crisis o desastres, no se descuiden los niveles de protección y seguridad necesarios para evitar incurrir en impactos colaterales indeseados.

PSI 12. Capacitación y sensibilización de seguridad y privacidad de la información:

- La ANI realiza sesiones de capacitación y sensibilización de seguridad y privacidad de la información, a cargo del GIT de Tecnologías de la Información y las telecomunicaciones para lograr niveles de apropiación y adecuados comportamientos por parte de los servidores públicos y contratistas, acerca de los aspectos y propósitos de seguridad y privacidad de la información al interior de la Agencia.

PSI 13. Servicios de Acceso remoto:

- Para el acceso remoto a los servicios tecnológicos que provee la ANI, de acuerdo con el al servicio tecnológico requerido el de Tecnologías de la Información y las Comunicaciones proveerá el tipo de conexión más adecuada
- La conexión remota que sea provista deberá garantizar la seguridad de la información a nivel de recursos tecnológicos. La responsabilidad de la información que se utilice en la conexión será del usuario de la conexión.

PSI 14. Uso de los servicios de Red e Internet:

- La infraestructura, servicios y tecnologías usados para acceder a Internet son propiedad de la ANI, por lo tanto, la entidad realizará monitoreo del uso de estos servicios a través del GIT de Tecnologías de la Información y las Comunicaciones.

- El uso de Internet, incluida la descarga de archivos por parte de los servidores públicos, contratistas y terceros debe realizarse con propósitos laborales. Por tal razón, la navegación en sitios con contenidos como: pornografía, drogas, alcohol, terrorismo, segregación racial o cualquier otra página que vaya en contra de la ética o moral, de las leyes vigentes o de políticas establecidas por la ANI, contrarios a la ley o a las políticas de la Agencia o que representen peligro, está prohibida.

PSI 15. Transferencia de Información:

- La ANI deberá establecer los mecanismos de transmisión y/o transferencia de la información que permitan garantizar la seguridad de esta, así como también la aplicación de métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

- Se deberán establecer acuerdos de confidencialidad y no divulgación para los casos en donde la clasificación de la información que se transfiere lo amerite. Estos acuerdos deberán revisarse periódicamente y mantenerse actualizados, definiendo claramente la información

a proteger, la duración del acuerdo, responsables, propietarios y acciones en casos de incumplimiento.

## 8. POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES

La política de datos personales tiene por objeto definir los parámetros bajo los cuales se da tratamiento y administración a todos los datos personales recogidos y almacenados dentro de sus bases de datos, y los procedimientos para la garantía de los derechos de los titulares de los datos.

Esta política tiene fundamento jurídico en la Ley estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales desarrolla el derecho constitucional a conocer, actualizar y rectificar la información recogida en bases de datos y los demás derechos, libertades y garantías a que se refieren los artículos 15 y 20 de la Constitución Política (derecho a la intimidad y derecho a la información, respectivamente).

La citada ley se aplica a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por parte de entidades públicas o privadas. Considerando el modo de conservación de una base de datos, se puede distinguir entre bases de datos automatizadas y bases de datos manuales o archivos.

La presente política se aplica a todas las bases de datos personales generadas por concepto de ingreso y/o accesibilidad a las instalaciones la Agencia Nacional de Infraestructura dentro de todas y cada una de sus dependencias, por parte de todos los encargados del tratamiento de dichos datos, por lo anterior se dictan los lineamientos que describen en los siguientes capítulos.

### 8.1 CREACIÓN DE LAS BASES DE DATOS

#### 8.1.1 Finalidad de la recolección

Cuando una dependencia de la Agencia Nacional de Infraestructura requiera recolectar datos personales para crear una base de datos, debe identificar claramente el ¿Por qué? necesita esa información. Es necesario que la finalidad esté relacionada con las funciones atribuidas a la entidad y debe ser incluida en el formato de autorización**.**

La dependencia deberá identificar previamente los datos que solicitará y los debe clasificar en: pública, semiprivada, privada y sensible, lo anterior de acuerdo con el glosario descrito en el presente documento

#### 8.1.2 Límite temporal para utilizar la información

Una vez definida la finalidad, se debe establecer el periodo de tiempo dentro del cual se hará uso de la información no es necesario establecer fechas exactas, se puede asociar a circunstancias o condiciones que agoten la finalidad.

#### 8.1.3 Designar al responsable o encargado de la base de datos

La entidad designará a un colaborador o área responsable de la administración de la base de datos, el cual debe estar relacionado con el manejo constate de la información.

Al responsable o encargado de la base de datos se le hará entrega de un reglamento que contenga las responsabilidades de su rol y las consecuencias en caso del mal manejo de la información.

**NOTA:** El responsable o encargado de la base de datos es diferente al responsable y encargado del Tratamiento de los datos:

- **Encargado:** Realiza el tratamiento en virtud de la delegación o mandato del responsable. Como por ejemplo la obtención de las Autorizaciones y verificación del cumplimiento de la finalidad.
- **Responsable:** Tiene poder de decisión sobre las bases de datos, define la forma en que se almacenan, recolectan y administran las bases de datos; así como las finalidades. Tiene la obligación de solicitar y conservar la autorización del ciudadano, así como, mantenerlo informado sobre la finalidad.

### 8.2 TRATAMIENTO DE LAS BASES DE DATOS

#### 8.2.1 Responsable de las bases de datos

El rol del responsable consiste en tomar las decisiones sobre las bases de datos y/o el Tratamiento de los datos. Define la finalidad y la forma en que se recolectan, almacenan y administran los datos. Asimismo, está obligado a solicitar y conservar la autorización en la que conste el consentimiento expreso del titular de la información.

#### 8.2.2 Derechos de los ciudadanos titulares de la información

- Conocer, actualizar y rectificar sus datos personales. Ejerciendo este derecho, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada, salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto al Ley 1581 de 2012.

- Cuando lo solicite ser informado frente al uso que se le ha dado a sus Datos Personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en las normas relacionadas con la protección de datos personales.
- Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento se ha incurrido en conductas contrarias a esta ley y a la Constitución.
- Acceder en forma gratuita, según lo establecido en el artículo 21 del Decreto 1377 de 2013, a sus datos personales que hayan sido objeto de tratamiento.

#### 8.2.3 Responsable de atender las PQRSD que se presenten ante la entidad

Una vez radicada la petición del titular relacionado con el tratamiento de los datos personales, el área responsable y/o encargada del tratamiento de datos debe analizarla, dar respuesta dentro de los términos legales.

**NOTA:** Teniendo en cuenta que las peticiones en materia de protección de datos personales tienen reglas especiales, se deben tener en cuenta los siguientes términos para dar respuesta. (Ley 1266 de 2008)

- Peticiones o Consultas: 10 días hábiles prorrogables por 5 días.
- Peticiones y Reclamos: 15 días hábiles prorrogables por 8 días.

Los colaboradores que tendrán acceso a la base de datos: El área responsable del tratamiento de los datos personales definirá los colaboradores que accederán a las bases de datos; así como, las contraseñas y procedimientos que sean necesarios

### 8.3 CIERRE DE LA BASE DE DATOS

#### 8.3.1 A solicitud del titular de la información

En este punto es importante resaltar que durante el tratamiento de los datos personales los titulares de la información pueden solicitar la supresión de estos.
Una vez radicada esta solicitud, se debe indicar al titular los tiempos de respuesta que existen para dar trámite a esta.

**NOTA**: Mientras se resuelve la solicitud se debe escribir una leyenda sobre el dato objeto del requerimiento que diga: “petición, queja o reclamo en trámite” de la misma manera como se haría si existe una exigencia para actualizar los datos personales.

### 8.3.2 Finalidad

Teniendo en cuenta que para la recolección de la información se debe establecer su finalidad, es claro que cuando ésta deja de existir no es procedente seguir con el tratamiento de los datos personales; no obstante, si el término que se había establecido inicialmente no es suficiente y se requiere prorrogarlo, es necesario contar nuevamente con la autorización del titular de la información.
Con el objeto de cerrar la base de datos, bien sea por que el titular de la información lo requirió o por que se agotó su finalidad, se deben llevar a cabo la anonimización de la información. Este es un procedimiento mediante el cual se "expresa un dato relativo a entidades o personas, eliminando la referencia a su identidad".

## 8.4 REGISTRO DE LA BASE DE DATOS

La Agencia Nacional de Infraestructura debe incluir las bases de datos creadas en el Registro Nacional de Bases de datos de la Superintendencia de Industria y Comercio, que debe contener la siguiente información:

- Finalidad
- Población a la cual se recopiló la información
- Descripción básica de los tipos de datos solicitados
- Área encargada de la administración de la base de datos
- Herramientas para que el titular de la información cancele, rectifique o modifique sus datos personales
- Medidas de seguridad aplicable

## 8.5 DIVULGACIÓN Y CAPACITACIÓN DE LA POLITICA DE DATOS PERSONALES

La Agencia Nacional de Infraestructura definirá los procesos de divulgación y capacitación del contenido de esta Política a través de la Coordinación de la Gerencia Administrativa y Financiera, para lo cual se programarán cuando así lo dispongan capacitaciones sobre política de tratamiento de información y datos personales.

## 8.6 MEDIDA INMEDIATA

En el tratamiento de los datos personales, la Agencia Nacional de Infraestructura actualiza de manera inmediata y permanente las bases de datos personales que tiene en su poder, con el lleno de los requisitos legales. Para tal propósito solicita la autorización de los titulares de los datos de conformidad con lo establecido en la ley 1581 de 2012. El uso de dichas bases de datos está restringido estrictamente para los fines propios para los cuales se hayan recogido de su titular y de acuerdo con la manifestación libre, previa, expresa e informada del titular de la información.

### 8.7 CONSULTA DE LA POLÍTICA DE LA POLITICA DE DATOS PERSONALES

La Agencia Nacional de Infraestructura, pone a disposición de los titulares de los datos personales esta política de tratamiento de datos, en sus oficinas y en su página web www.ani.gov.co, redes sociales y demás medios de comunicación.

## 9 MODELO PARA LA IMPLEMENTACIÓN DE LA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Modelo de Seguridad y Privacidad que se implementará en la Agencia Nacional de Infraestructura se encuentra alineado al definido por el Ministerio de Tecnologías de la Información y las Comunicaciones, denominado: "***MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI***", correspondiente al decreto único reglamentario 1078 de 2015 y su actualización de mayo de 2018 publicado en la página oficial del MINTIC (https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf)

La política de seguridad de la información aquí mencionada está alineada con la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG), la norma NTC ISO/IEC 27001:2013 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

Mediante la adopción del Modelo de Seguridad y Privacidad se busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

El Modelo de Seguridad y Privacidad de la Información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permitirán a la ANI gestionar adecuadamente la seguridad y privacidad de sus activos de información: **i) diagnóstico**, el cual ya fue realizado en la ANI y actualmente se hace retroalimentación permanente mediante el ejercicio "Autodiagnóstico de Gobierno Digital" que se reporta trimestralmente al MinTIC y también el ejercicio de Evaluación de la implementación del modelo MSPI que se reporta trimestralmente al Ministerio de Transporte**. ii) planeación, iii) implementación, iv) evaluación del desempeño y v) mejora continua.**

El presente documento hace parte de la fase de planificación y las siguientes fases se desarrollarán progresivamente de acuerdo con lo establecido en el modelo.

## 10 ESTRATEGIA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la implementación de la presente política, ésta se publicará en la página web de la entidad a fin que sea conocida y consultada por todos los funcionarios, contratistas y terceros que tengan relación con la entidad, así mismo las dependencias deberán articularse para llevar a cabo las actividades descritas en cumplimiento de las políticas aquí descritas, de acuerdo con la naturaleza de su función y responsabilidad de participación y/o liderazgo; complementariamente y cuando se determine necesario se dispondrán de documentos tales como procedimientos, instructivos y/o formatos (en medio digital cada vez que sea posible) para apoyar el cumplimiento de lo aquí definido.

## 11 SEGUIMIENTO

El seguimiento permanente al cumplimiento de la política de seguridad y privacidad de la información estará a cargo del responsable de la seguridad de la información y los líderes de cada proceso de acuerdo con la naturaleza de su función.

## 12 SANCIONES POR EL INCUMPLIMIENTO A LA POLÍTICA.

El no cumplimiento a la presente política acarreará las acciones disciplinarias establecidas por la ANI o las sanciones específicas en la Ley 1952 de 2019 y demás normas que reglamentan los procesos disciplinarios para los funcionarios públicos, contratistas y terceros. El incumplimiento será evaluado de acuerdo con el impacto generado y al criterio de las instancias de control, pudiendo éste, ser aplicado con medidas correctivas administrativas, disciplinarias o legales.

## 13 CONTROL DE CAMBIOS

| VERSIÓN | FECHA | DESCRIPCIÓN DEL CAMBIO |
|---|---|---|
| 001 | 28/08/2015 | Creación del Documento |
| 002 | 28/05/2019 | Actualización de la Política, cumplimiento Estrategia de Gobierno Digital |
| 003 | 28/05/2020 | Actualización al nuevo proceso de Gestion Tecnológica y la integración de la política de protección de datos |

**APROBACIÓN**

| | Nombre | Cargo | Firma |
|---|---|---|---|
| **Elaborado** | Guillermo Cadena Ronderos | Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones | Aprobado en sesión de Comité Institucional de Gestión y Desempeño **Acta No. 64** |
| **Revisado** | Erika Díaz Abella | Contratista G.I.T. Tecnologías de la Información y las Telecomunicaciones | |
| **Revisado** | Andrés Francisco Boada Icabuco | Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones | |
| **Aprobado** | Comité Institucional de Gestión y Desempeño | Comité Institucional de Gestión y Desempeño | |
| **Vo.Bo. Calidad** | Daniela Mendoza Navarrete | Contratista G.I.T. Planeación | |