POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AGENCIA NACIONAL DE HIDROCARBUROS - ANH

Versión 4.0

Bogotá D.C., Marzo de 2026

Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Sandra Mireya Ramírez	Pablo Yesid Fajardo Benitez
Experto G3-5 Oficial de Seguridad de la Información ANH	Jefe Oficina de Tecnologías de la Información (e)	Presidente ANH Comité Institucional de Gestión y Desempeño Acta de Comité del 11/03/2026

Tabla de contenido

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. PROPÓSITO

Definir la Política General de Seguridad y Privacidad de la Información como una declaración general por parte de la Alta Dirección, donde se establece la postura, objetivos, alcance, nivel de cumplimiento, aprobación y divulgación al interior de la Entidad de los lineamientos que pretenden proteger la información, en línea con lo establecido en la resolución 266 de 2018[1].

2. 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 organización[2].
- **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades
- **Confidencialidad:** Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados[3].
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada[4].
- **Incidente de seguridad**: Evento único o serie de eventos inesperados, no deseados, que poseen una probabilidad significativa de comprometer las operaciones de la entidad y amenazar la Seguridad de la Información[5].
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[6].
- **Información pública**: Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal[7].
- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. Esta se alinea a la definición de NIST Sistema y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos.[8]
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud[9].
- **No repudio:** El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido)[10].
- **Política:** Intenciones y dirección de una organización, expresada formalmente por su alta dirección[11]
- **Privacidad:** Se entiende como el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar que genera la obligación de proteger dicha información en observancia del marco legal vigente[12].
- **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[13].
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información[14].
- **Sistema de Gestión de Seguridad de la Información**: Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad

[1] Agencia Nacional de Hidrocarburos, Resolución 266 de 2018, por la cual se adopta el sistema de gestión de seguridad de la información, las políticas específicas de seguridad de la información y la política de protección de datos personales.
[2] ISO 27000:2018
[3] Ibidem
[4] ISO 27000:2018
[5] Ibidem
[6] Ley 1712 de 2014
[7] Ibidem
[8] NIST SP 800-30 Rev.1
[9] ISO 27000:2018
[10] Ibidem
[11] ISO 27000:2018
[12] MINTIC, Modelo de Seguridad y Privacidad de la Información MSPI vigente
[13] ISO 27000:2018
[14] Ibidem

Editado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Sandra Mireya Ramírez	Pablo Yesid Fajardo Benitez
Experto G3-5 Oficial de Seguridad de la Información ANH	Jefe Oficina de Tecnologías de la Información (e)	Presidente ANH Comité Institucional de Gestión y Desempeño Acta de Comité del 11/03/2026

3. DECLARACIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Teniendo en cuenta los aspectos enunciados, la misión y visión de la Entidad, se declara la siguiente Política General de Seguridad y Privacidad de la Información:

La Alta Dirección de la Entidad, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la información- SGSI buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la sociedad y las empresas del sector, en estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad, mediante las siguientes premisas:

- *Proteger la información como activo de gran valor para la Entidad*[15]
- *Emprender las acciones necesarias para preservar la confidencialidad, integridad, disponibilidad y no repudio de su información, mediante la formulación de objetivos, definición de lineamientos, procedimientos y la implementación de controles para gestionar y mitigar de manera efectiva los riesgos de seguridad de la información.*
- *Fomentar la formación de una cultura de seguridad y privacidad de la información*
- *Velar por la asignación de los recursos necesarios para la implementación de la política y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información-SGSI.*
- *Cumplir los requisitos legales vigentes en materia de seguridad y privacidad de la información, así como de protección de datos personales.*

4. OBJETIVOS.

4.1. Proteger los activos de información de la Entidad y la tecnología utilizada en su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio de la información, con especial enfoque en los activos de información críticos e Infraestructura Crítica Cibernética.

4.2. Prestar servicios de confianza, generando protección de la información de los ciudadanos y partes interesadas.

4.3. Gestionar y mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

4.4. Fomentar la cultura de seguridad y privacidad de la información en todos los usuarios o actores[16] que usen, tengan acceso, diseñen, administren, operen o sea responsables por la gestión de información en forma manual o computarizada en el marco de la misión de la Entidad.

4.5. Dar cumplimiento a la normatividad vigente sobre seguridad y privacidad de la información, protección de datos personales, derechos de autor y conexos.

4.6. Establecer, socializar, revisar y mantener actualizada la Política de Seguridad y privacidad de la Información de la Entidad, asegurando su divulgación, vigencia y aplicación efectiva.

4.7. Promover el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información – SGSI.

[15] En este marco se destaca la protección de los activos de información críticos, así como su relación con la infraestructura crítica cibernética de la Entidad
[16] Actores comprende tanto personal interno como contratistas por prestación de servicios, personas jurídicas, terceros, proveedores, visitantes y otras partes interesadas.

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información -SGSI; así mismo, se compromete a revisar el avance de la implementación de manera periódica, garantizar los recursos suficientes (tecnológicos y talento humano calificado) para su implementación y mantenimiento e incluir dentro de las decisiones estratégicas, la seguridad de la información.

6. ALCANCE.

La política de seguridad y privacidad de la información aplica a:

6.1. Todos los activos de información de la Entidad -sin importar el medio en el que se encuentren[17] - a través de su ciclo de vida, incluyendo creación, distribución, almacenamiento y disposición final, priorizando su protección acorde con las evaluaciones de riesgos y conforme lineamientos gubernamentales vigentes.

6.2. Todos los ambientes de procesamiento de información (desarrollo, pruebas[18], preproducción, producción).

6.3. Todos los niveles jerárquicos, dependencias y procesos de la Entidad, así como a todos los servidores públicos, colaboradores y/o terceros que tengan vínculo con la Entidad.

6.4. Todos los usuarios o actores que usen, tengan acceso, diseñen, administren, operen o sea responsables por la gestión de información en forma manual o computarizada en el marco de la misión de la Entidad.

7. ORGANIZACIÓN DE LA SEGURIDAD Y RESPONSABLES

La Entidad define los Roles y Responsabilidades dentro del Sistema de Gestión de Seguridad de la Información -SGSI; estos y los demás instrumentos aplican en toda la Entidad y hacen parte de la implementación del sistema.

El Comité Institucional de Gestión y Desempeño (o su equivalente) ejerce el liderazgo y compromiso para conseguir los objetivos definidos en la adopción, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información- SGSI.

Los líderes de proceso son responsables de gestionar los riesgos de seguridad y privacidad de la información de sus activos de información.

El responsable u Oficial de seguridad tiene a su cargo liderar y gestionar la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información – SGSI en la Entidad.

El Oficial de Protección de Datos Personales o quien haga sus veces, tiene a su cargo la función de estructurar, diseñar y administrar el programa que permita a la Entidad cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

Todo el personal y los usuarios o actores que usen, tengan acceso, diseñen, administren, operen o sean responsables por la gestión de información en forma manual o computarizada en el marco de la misión de la Entidad, son responsables de aplicar las políticas y lineamientos de seguridad y privacidad de la

17 La información contenida o gestionada en medios digitales, adicionalmente a las políticas de seguridad de la información, estará sujeta a las políticas de seguridad digital
18 Incluye Pruebas de Concepto, de Contingencia, simulaciones, Demos, etc.

Información que imparta la Entidad; así como de participar en la implementación del Sistema de Gestión de Seguridad de la Información – SGSI.

8. NIVEL DE CUMPLIMIENTO

Todos los responsables deberán dar cumplimiento y aplicación a las Políticas de Seguridad y Privacidad de la Información y al Sistema de Gestión de Seguridad de la Información – SGSI de la Entidad, so pena de las consecuencias y posibles sanciones por acciones que se deriven de la negligencia, intención deliberada que genere daños, interrupción o afectación a los activos de información de la Entidad. Lo anterior, de acuerdo con los reglamentos internos, de aplicación a los servidores públicos, la Constitución Política, leyes[19] y estatutos de la ley colombiana y, demás normatividad vigente.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

La Entidad realizará revisiones periódicas de la adopción del Sistema de Gestión de Seguridad de la Información – SGSI; así mismo evaluará el desempeño de seguridad de la información y la eficacia.

10. APROBACIÓN Y DIVULGACIÓN

La Política General de Seguridad y Privacidad de la Información de la Entidad será propuesta por el responsable u Oficial de Seguridad y presentada al Comité Institucional de Gestión y Desempeño para su aprobación.

La revisión y/o actualización de la Política General de Seguridad y Privacidad de la Información de la Entidad podrá darse por cambios tecnológicos, normativos, organizacionales o procedimentales, entre otros.

La Política General de Seguridad y Privacidad de la Información de la Entidad es de carácter público y su divulgación se realizará a través de los medios de comunicación oficiales dispuestos por la Entidad.

11. MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la adecuada implementación de la Política de Seguridad y Privacidad de la Información, la Entidad define las políticas específicas que se derivan de ésta y que son de obligatorio cumplimiento, en el "*Manual de Políticas Específicas de Seguridad y Privacidad de la Información*".

El Manual de Políticas Específicas de Seguridad y Privacidad de la Información de la Entidad surtirá el mismo procedimiento de aprobación de la Política General. En razón a su detalle en cuanto a la postura de seguridad de la Entidad, su divulgación será primordialmente con alcance interno y a los actores que así lo requieran.

12. VIGENCIA

La Política General de Seguridad y Privacidad de la Información, así como el Manual de Políticas Específicas de Seguridad y Privacidad de la Información, entrarán en vigor una vez sean aprobadas, publicadas y divulgadas a través de los medios establecidos.

[19] Como lo es La Ley de Delitos Informáticos vigente.

13. REFERENCIAS

La Política de Seguridad y Privacidad de la Información se alinea a la legislación vigente en la materia, así como a la normativa de Habeas Data, Protección de Datos Personales y las directrices emitidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, además de buenas prácticas relacionadas.

14. CONTROL DE CAMBIOS

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Septiembre de 2013	Creación del documento	1
Agosto de 2017	Actualización	2
Julio de 2018	Actualización y alineación a MSPI	3
Marzo de 2026	Actualización y alineación conforme Resolución 500 de 2021, modificada por la Resolución 746 de 2022 y actualizada por la Resolución 2277 de 2025, expedidas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC.	4