Agencia Nacional Digital

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTÁ D.C., OCTUBRE 2026

Proceso: Seguridad y privacidad de la información
POLÍTICA: POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 5

Tabla de contenido

1. Introducción 3
2. Objetivo 3
3. Alcance 3
4. Definiciones 3
5. Términos Asociados A Seguridad De La Información 4
6. Términos Asociados A Documentación Y Procesos Administrativos 6
7. Marco Normativo 6
9. Política General De Seguridad Y Privacidad De La Información.....11
10. Compromiso Institucional.....12
11. Cumplimiento 12
12. Organización De La Seguridad De La Información (Roles Y Responsabilidades) 13
13. Revisión, Vigencia Y Derogatoria 15
14. Documentos De Referencia 15
15. Control De Cambios 15

Fecha 15
Descripción Del Cambio 15

Proceso: Seguridad y privacidad de la información
POLÍTICA: POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 5

1. INTRODUCCIÓN

La Corporación Agencia Nacional de Gobierno Digital o Agencia Nacional Digital (AND), en la gestión de seguridad de la información establece condiciones adecuadas para la óptima operación de los activos de información y la infraestructura tecnológica que soporta los procesos de la entidad, para fortalecer la confidencialidad, disponibilidad, e integridad de la información. Así mismo propende por el cumplimiento de las directrices del Gobierno Nacional relacionadas con la seguridad y privacidad de la información, incluyendo la seguridad digital, ciberseguridad y la protección de los datos personales, el habeas data, manejo de la imagen de la entidad, de proveedores y terceros con los que la Entidad tenga vínculos aplicando metodologías de valoración y tratamiento de los riesgos según la normatividad vigente. El presente documento muestra el compromiso de la Dirección y de todas sus áreas con la seguridad de la información y con su sistema de gestión con el propósito de mantener una cultura organizacional a través de la aplicación de buenas prácticas y el cumplimiento de requisitos legales, contractuales y funcionales con las partes interesadas.

2. OBJETIVO

Establecer el marco general para la gestión de la seguridad definidos por la Dirección y las Subdirecciones de la AND, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad Digital y Gobierno Digital y demás requisitos legales y necesidades de las partes interesadas.

3. ALCANCE

La Política General de Seguridad y Privacidad de la Información, aplica a todos los niveles funcionales y organizacionales en la Agencia, a todos sus empleados de planta, contratistas, proveedores y operadores, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la AND compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

De igual manera, esta política aplica a toda la información creada, procesada o utilizada por la AND, sin importar el medio, formato, presentación o lugar en el cual se encuentre en conformidad a los requisitos normativos, comprende a todos los procesos de la entidad en la implementación del Modelo de Seguridad y Privacidad de la Información.

4. DEFINICIONES

Las definiciones de la Política General de Seguridad y Privacidad de la Información de la Corporación Agencia Nacional de Gobierno Digital, tiene fundamento en el estándar

internacional ISO/IEC 27001:2022 - Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información - Requisitos[1].

5. TÉRMINOS ASOCIADOS A SEGURIDAD DE LA INFORMACIÓN

Con el propósito de facilitar la comprensión de la política se deben tener en cuenta las siguientes definiciones asociadas a la seguridad de la información:

a. **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados (Ley 1712, 2014).

b. **Activo:** 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, etc.) Que tenga valor para la organización. (Modelo de Seguridad y Privacidad de la Información, 2021).

c. **Amenaza:** Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).

d. **Análisis de riesgos:** Proceso de comprender la naturaleza del riesgo y determinar su nivel de riesgo. (Modelo de Seguridad y Privacidad de la Información, 2021).

e. **Confidencialidad:** propiedad de que la información no se pone a disposición ni se revela a personas, entidades o procesos no autorizados. (ISO/CEI 27000, 2018).

f. **Control:** Medida que modifica el riesgo. Sinónimo salvaguarda (ISO/CEI 27000, 2018).

g. **Disponibilidad:** propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (ISO/CEI 27000, 2018).

h. **Gestión de incidentes de seguridad de la información:** Conjunto de procesos para detectar, informar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/CEI 27000, 2018).

[1] https://www.iso.org/es/contents/data/standard/08/28/82875.html

i. **Gestión de riesgos:** Actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (ISO/CEI 27000, 2018).

j. **Incidente de seguridad de la información:** único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información, (ISO/CEI 27000, 2018).

k. **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712, 2014).

l. **Integridad:** La propiedad de salvaguardar la exactitud y complejidad de la información. (ISO/CEI 27000, 2018).

m. **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (Modelo de Seguridad y Privacidad de la Información, 2021).

n. **Riesgo:** La posibilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daño a una organización. (ISO/CEI 27000, 2018).

o. **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/CEI 27000, 2018).

p. **Seguridad digital:** es la situación de normalidad y de tranquilidad en el entorno digital(ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (Política Nacional de Confianza y Seguridad Digital [Documento CONPES 3995], 2020).

q. **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley Estatutaria 1581. Art 3, 2012).

r. **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas (ISO/CEI 27000, 2018).

6. TÉRMINOS ASOCIADOS A DOCUMENTACIÓN Y PROCESOS ADMINISTRATIVOS

Con el propósito de facilitar la comprensión de la política se deben tener en cuenta las siguientes definiciones asociadas a la documentación y procesos administrativos:

Archivo. Es el conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 1712, 2014).

Datos Abiertos. Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos. (Ley 1712, 2014).

Documento de archivo. Es el registro de información producida o recibida por una entidad pública o privada en razón de sus actividades o funciones. (Ley 1712, 2014).

7. MARCO NORMATIVO

La Constitución Política de Colombia en su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

El artículo 17 de la Ley Estatutaria 1581 de 2012, "Régimen General de Protección de Datos Personales", y el artículo 2.2.2.25.3.1. Del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

La Ley 1712 de 2014, sobre transparencia y derecho de acceso a la información pública nacional, adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos

de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

ARTÍCULO 2.2.9.1.2.1. Del decreto 767 del 2022 Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones que dentro de la estructura tiene el 3.2 Seguridad y Privacidad de la Información: como habilitador que busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

La Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, establece lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. Del Decreto 1078 de 2015.

El artículo 5 de la misma Resolución establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. Del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue. Así como, adoptar el Modelo de Seguridad y Privacidad de la Información - MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital.

El Documento CONPES 3854 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Proceso: Seguridad y privacidad de la información
POLÍTICA: POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 5

El Documento CONPES 3995 de 2020 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

A su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

Que en el artículo 2.2.22.3.2. Del Decreto 1083 de 2015, se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el "Marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan /las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

Ley 1952 del 2019 por la cual se expide el código general disciplinario que deroga la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario. Artículo 38 deberes. Son deberes de todo servidor público: ‟5. Utilizar los bienes y recursos asignados para el desempeño de su empleo cargo función, las facultades que les sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines que están afectos. 6. Custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o función conserve bajo su cuidado OA la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.

Que la adopción del modelo de seguridad de la información (MSPI), es una decisión estratégica para una organización. El establecimiento e implementación del modelo de seguridad de la información de una entidad como es la AND, están influenciados por las necesidades y objetivos de la Entidad, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la entidad.

La Política General de Seguridad y Privacidad de la Información de la Agencia se fundamenta en el siguiente marco normativo, el cual se aplica con sus modificaciones, adiciones, subrogaciones o derogatorias. El detalle de la normativa aplicable a la entidad se mantiene actualizado en el Normograma Institucional.

Constitución y leyes. El artículo 15 de la Constitución Política de Colombia consagra el derecho de todas las personas a su intimidad personal y familiar y a su buen nombre, así como a conocer, actualizar y rectificar las informaciones recogidas sobre

ellas en bancos de datos y archivos de entidades públicas y privadas. La Ley Estatutaria 1581 de 2012 establece el régimen general de protección de datos personales y, en su artículo 17, impone a los responsables del tratamiento el deber de adoptar políticas y procedimientos internos. La Ley 1712 de 2014 regula la transparencia y el derecho de acceso a la información pública, y la Ley 594 de 2000 dicta la Ley General de Archivos. La Ley 1273 de 2009 tipifica los delitos informáticos contra la protección de la información y de los datos. La Ley 1952 de 2019 (Código General Disciplinario), en su artículo 38, establece como deberes de los servidores públicos utilizar la información reservada exclusivamente para los fines de su función, así como custodiar la documentación e información a su cargo y evitar su sustracción, destrucción, ocultamiento o utilización indebidos. El Decreto Ley 2106 de 2019, en el parágrafo de su artículo 16, dispone que las autoridades que adelanten trámites y procedimientos por medios digitales deben contar con una estrategia de seguridad digital, conforme a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Decretos reglamentarios. El Decreto 1074 de 2015 (Capítulos 25 y 26) compila la reglamentación de la Ley 1581 de 2012, incluido el artículo 2.2.2.25.3.1 sobre políticas de tratamiento de datos personales. El Decreto 103 de 2015 reglamenta la Ley 1712 de 2014, y el Decreto 1080 de 2015 (Libro 2, Parte 8, Títulos IV y V) desarrolla la gestión de la información clasificada y reservada y los instrumentos de gestión de información pública. El Decreto 1083 de 2015 establece las políticas de gestión y desempeño institucional, entre ellas Gobierno Digital y Seguridad Digital (artículo 2.2.22.2.1), y define el Modelo Integrado de Planeación y Gestión (artículo 2.2.22.3.2). En el sector TIC, el Decreto 1078 de 2015 es el decreto único reglamentario. El Decreto 767 de 2022 establece los lineamientos de la Política de Gobierno Digital y, en el artículo 2.2.9.1.2.1, define la seguridad y privacidad de la información como habilitador de la política. El Decreto 338 de 2022 fortalece la gobernanza de la seguridad digital, incluidos el modelo de gestión de riesgos y atención de incidentes y el CSIRT de Gobierno. El Decreto 1263 de 2022 adiciona el Título 22 al Decreto 1078 de 2015 con lineamientos y estándares de transformación digital pública. El Decreto 620 de 2020 y la Resolución 1951 de 2022 regulan los Servicios Ciudadanos Digitales, en los cuales la AND actúa como articulador.

Modelo de Seguridad y Privacidad de la Información (MSPI). La Resolución 500 de 2021 de MinTIC establece los lineamientos y estándares de la estrategia de seguridad digital y adopta el MSPI como habilitador de la Política de Gobierno Digital. La Resolución 746 de 2022 fortalece el MSPI con lineamientos adicionales, entre ellos los relativos a proveedores y a la protección de datos personales. La Resolución 02277 del 3 de junio de 2025 actualiza el Anexo 1 de la Resolución 500 de 2021 (MSPI), alineándolo con la norma ISO/IEC 27001:2022, y reemplaza las versiones anteriores del modelo.

Política pública. El Documento CONPES 3854 de 2016 formuló la Política Nacional de Seguridad Digital, y el Documento CONPES 3995 de 2020 formula la Política

Nacional de Confianza y Seguridad Digital. Documento CONPES 4144 de 2025 y lineamientos del MSPI para sistemas de IA.

Estándares técnicos de referencia. Las normas ISO/IEC 27001:2022 (con su Enmienda 1:2024) e ISO/IEC 27002:2022 son el fundamento del Sistema de Gestión de Seguridad de la Información. **[Citar ISO/IEC 27000 en su edición vigente como fuente de definiciones.]**

Normativa interna. La Resolución 035 de 2023 integra y establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño, instancia responsable de asegurar la implementación de las políticas de seguridad digital y de la información, conforme a lo señalado en el numeral 7 de este documento.

8. PRINCIPIOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Corporación Agencia Nacional de Gobierno Digital (AND) orientará la gestión de la seguridad y privacidad de la información bajo los siguientes principios:

- Confidencialidad: La información solo será accesible a personas, procesos o entidades debidamente autorizadas, protegiéndola contra la divulgación no autorizada.

- Integridad: La información deberá mantenerse completa, exacta, consistente y protegida contra modificaciones no autorizadas durante todo su ciclo de vida.

- Disponibilidad: La información y los servicios que la soportan deberán estar disponibles y accesibles para los usuarios autorizados cuando se requieran para el cumplimiento de la misión institucional.

- Gestión basada en riesgos: La seguridad de la información se gestionará a partir de la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar los activos de información y los procesos institucionales.

- Cumplimiento normativo: La Corporación garantizará la observancia de los requisitos legales, regulatorios, contractuales e institucionales aplicables en materia de seguridad de la información, protección de datos personales y seguridad digital.

- Mejora continua: La seguridad y privacidad de la información se fortalecerán de manera permanente mediante el seguimiento, evaluación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

- Responsabilidad compartida: La protección de la información es una responsabilidad de todos los colaboradores, contratistas, proveedores y terceros que accedan, procesen o administren información de la entidad.

9. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La AND reconociendo la importancia de la seguridad y privacidad de la información para el cumplimiento de su misión institucional, se compromete a proporcionar los recursos necesarios para la implementación, mantenimiento y mejora continua del SGSI, con el propósito de proteger la confidencialidad, integridad y disponibilidad de los activos de información, gestionar adecuadamente los riesgos, vulnerabilidades e incidentes de seguridad de la información, y fortalecer la confianza digital de los ciudadanos, entidades del Estado y demás grupos de interés.

Asimismo, la AND velará por el cumplimiento de los requisitos legales, regulatorios, contractuales e institucionales aplicables, promoviendo una cultura de seguridad de la información y mejora continua en todos sus procesos.

Objetivos de Seguridad y Privacidad de la Información

Los siguientes objetivos orientan la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información, en concordancia con la norma ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos institucionales aplicables:

1. Mantener la disponibilidad, integridad y continuidad de los Servicios Ciudadanos Digitales y de los servicios críticos de la AND.
2. Proteger la confidencialidad y la privacidad de los datos personales de ciudadanos, colaboradores, contratistas y demás titulares de información, en cumplimiento de la normatividad aplicable en materia de protección de datos personales.
3. Integrar la seguridad de la información durante todo el ciclo de vida de las soluciones tecnológicas y desarrollos de software implementados o gestionados por la entidad.
4. Gestionar los riesgos de seguridad asociados a proveedores, servicios en la nube, terceros y tecnologías emergentes, incluida la inteligencia artificial, utilizadas en el desarrollo de la innovación pública.
5. Proteger los activos de información y la propiedad intelectual asociados a proyectos de Ciencia, Tecnología e Innovación (CTeI), durante todas sus fases de ejecución.
6. Fortalecer la cultura, conciencia y competencias en seguridad y privacidad de la información de colaboradores, contratistas, proveedores y terceros que interactúen con los activos de información de la entidad.
7. Gestionar los riesgos, vulnerabilidades e incidentes de seguridad de la información, manteniendo los niveles de riesgo dentro de los criterios de aceptación establecidos por la entidad.

8. Mantener y mejorar continuamente la eficacia del Sistema de Gestión de Seguridad de la Información, asegurando el cumplimiento de los requisitos legales, regulatorios y normativos aplicables.

Seguimiento y medición

El cumplimiento de los objetivos de seguridad y privacidad de la información será evaluado mediante indicadores, métricas, auditorías, revisiones por la dirección, seguimiento a riesgos, vulnerabilidades e incidentes de seguridad de la información, así como los demás mecanismos definidos dentro del Sistema de Gestión de Seguridad de la Información. Los resultados obtenidos serán utilizados para la toma de decisiones y la mejora continua del SGSI.

Indicadores asociados

- Disponibilidad de los Servicios Ciudadanos Digitales.
- Servicios críticos con pruebas de recuperación ejecutadas durante la vigencia.
- Bases de datos personales con cumplimiento normativo.
- Solicitudes de titulares atendidas dentro de los tiempos establecidos.
- Soluciones de software liberadas con revisión de seguridad.
- Contratos con inclusión de cláusulas de seguridad de la información.
- Proyectos de CTeI con identificación y gestión de activos y riesgos.
- Personal capacitado y sensibilizado en seguridad de la información.
- Incidentes de seguridad atendidos dentro de los tiempos definidos.
- Riesgos altos y extremos con planes de tratamiento implementados.
- Cumplimiento del Plan de Seguridad y Privacidad de la Información.
- Hallazgos de auditoría cerrados dentro de los plazos establecidos.

10. COMPROMISO INSTITUCIONAL

La Dirección y las Subdirecciones de la AND se comprometen a: apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información; así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado), para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

11. CUMPLIMIENTO

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas, proveedores y terceros de la Agencia.

El incumplimiento a la Política General de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa vigente.

12. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

A continuación se realcionan los roles y las responsabilidad que tienen cada uno:

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN)
Dirección y las Subdirecciones	Proporcionar los recursos necesarios para la implementación, mantenimiento y mejora continua del Modelo de seguridad y privacidad de la información (Recursos económicos, formación y recursos tecnológicos).
Comité Institucional de Gestión y Desempeño	"Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información". Establecido en el Artículo Tercero: - Funciones. Ítem 6, de la resolución número 035 de 2023.
Profesional de TI y/o Grupo TI	Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información y minimizar los riesgos de seguridad de la información.
Profesional de seguridad de la información y/o Oficial de Seguridad de la Información	• Analizar, definir, documentar y gestionar el plan de seguridad de la información y proponer las acciones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidos y aprobados por la entidad. • Apoyar, definir, gestionar la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Modelo de seguridad y privacidad de la Información MSPI. • Realizar la planificación, implementación, seguimiento y evaluación de los SGSI. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad. • Responsable del mantenimiento e la Declaración de Aplicabilidad (SOA).
Gestión Talento Humano	Coordinar con el Oficial de Seguridad el plan de inducción, capacitación y sensibilización en seguridad de la información en la AND, para la toma conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN)
Gestión Documental	Coordinar con el Oficial de Seguridad de la Información la gestión documental relacionados con la información que se maneja en el SGSI.
Gestión Administrativa	Coordinar con el Oficial de Seguridad de la Información el monitoreo y control de seguridad de las áreas físicas (sistemas de control de incendios, emergencias, entre otros), que hacen parte de las operaciones de la AND.
Profesional o delegado de Protección de Datos	Coordinar y apoyar al Oficial de Seguridad de la Información con los lineamientos y controles para el tratamiento de datos personales en cumplimiento de la legislación y buenas prácticas vigentes en la AND.
Control Interno	• Incluir la seguridad de la información en los planes de auditoría institucionales. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Comunicaciones	Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la AND, teniendo en cuenta los lineamientos de comunicación ya establecidos por la entidad.
Jurídica / Contratación	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Líderes de proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del MSPI (Por ejemplo: gestión de activos, gestión de riesgos, controles entre otros). • Responsable de la identificación y tratamiento de riesgos de los activos de información de su proceso.
Empleados de planta, contratistas y terceros	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir las políticas y procedimientos de seguridad de la información definidos y aprobados. • Informar sobre cualquier incidente de seguridad de la información por los canales establecidos y asistir a las sensibilizaciones en temas de Seguridad de la Información. • Utilizar los activos de información exclusivamente para el desempeño de sus funciones y obligaciones dentro y fuera la AND.

13. REVISIÓN, VIGENCIA Y DEROGATORIA

La Política General de Seguridad y Privacidad de la Información se deberá desarrollar de manera específica y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad y Privacidad de la Información de la AND, que deberán ser publicados en el Sistema de Información del Modelo Integrado de Gestión de la entidad.

Esta política será efectiva desde su aprobación. La revisión de esta política se hará en las siguientes condiciones:

- La Política General de Seguridad y Privacidad de la Información de la AND, será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el Oficial de Seguridad de la Información o quien la Dirección de AND delegue.

- Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).

14. DOCUMENTOS DE REFERENCIA

De acuerdo con la política general se asocian los siguientes documentos de referencia:

- Norma ISO 27001:2022. Sistema de gestión de seguridad de la información. Requisitos.
- Manual de políticas de seguridad y privacidad de la información.
- Normograma.

15. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	19/07/02022	Emisión del documento.
2	13/12/2023	Se incluye lineamiento para revisiones y actualizaciones de la política general del SGSI. Se incluye el compromiso de la Alta Dirección con la mejora continua del SGSI.
3	20/12/2024	Se actualiza al cambio de formato documental de la AND e inclusión del Manual de Políticas de Seguridad y Privacidad de la Información de la AND, las definiciones de compresión de la Política, así como la

Proceso: Seguridad y privacidad de la información
POLÍTICA: POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 5

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
		Organización de la Seguridad de la Información (Roles Y Responsabilidades) y la actualización al cumplimiento de estándar ISO/IEC 27001:2022.
4	04/12/2025	Se actualiza el nombre de la política, dejando en su título Política General de Seguridad y Privacidad de la Información. Así mismo, se complementan roles de seguridad de la información (Gestión Administrativa, Gestión Documental y Profesional o delegado de Protección de Datos Personales. Otros cambios de forma. Se actualizan los objetivos del SGSI y se ajusta incluyendo la gestión de riesgos, incidentes y continuidad de la seguridad.
5	05/11/2026	Se alinean y actualizan los objetivos frente los objetivos de la Agencia Nacional Digital Se ajusta actualiza normativa de la política conforme con el cronograma.

Elaboró	Revisó	Aprobó
Andrés Mariño Ramírez Contratista - Gerente Anexo 01 Subdirección de Servicios Ciudadanos Digitales	Claudia P. Castaño S. Profesional de Planeación Tatiana Guerrero R. Profesional líder de comunicaciones Lady Gilari Torres Becerra	Maricela Torrenegra Directora (E) AND

	Líder transversal – Subdirección de Servicios Ciudadanos Digitales  Denis Fernando Montealegre Oficial de seguridad de la información	