Proceso: Seguridad y privacidad de la información
POLÍTICA: POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Versión: 3

1. OBJETIVO

Establecer los lineamientos definidos por la Dirección y las Subdirecciones de la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL —AND, para la seguridad de la información, 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.

2. ALCANCE

La Política de Seguridad y Privacidad de la Información, aplica a todos los niveles funcionales y organizacionales en la CORPORACIÓN AGENCIA NACIONAL DE GOBIERNO DIGITAL —AND, 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.

3. DEFINICIONES

Las definiciones de la Política General de Seguridad y Privacidad de la Información de la Corporación Agencia Nacional de Gobierno Digital —AND, 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[1].

3.1 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:

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

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).

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).

3.2. 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, Titulo 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.

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 /as 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 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 Corporación Agencia Nacional Digital -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.

4. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Corporación Agencia Nacional de Gobierno Digital —AND, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

La Corporación Agencia Nacional de Gobierno Digital —AND en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos

- Fortalecer la cultura de seguridad de la información en los empleados de planta, terceros y clientes de la AND.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Minimizar el riesgo de todos los procesos de la entidad.
- Mejorar continuamente el sistema de gestión de seguridad de la información.

- Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

5. COMPROMISO DE LA DIRECCIÓN Y LAS SUBDIRECCIONES

La Dirección y las Subdirecciones de Corporación Agencia Nacional de Gobierno Digital —AND 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 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.

6. CUMPLIMIENTO

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a toda la entidad, servidores públicos, contratistas y terceros de la Corporación Agencia Nacional de Gobierno Digital —AND

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

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

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN)
Dirección y Las Subdirecciones	Proporcionar los recursos necesarios para la implementación y mantenimiento 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.
Profesional 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

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES CON LA SEGURIDAD DE LA INFORMACIÓN)
y/o Oficial de Seguridad de la Información	seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. ➢ Apoyar en 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 sistemas de gestión de seguridad de la información (SGSI).Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
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.
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.
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).
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.

8. REVISIÓN, VIGENCIA Y DEROGATORIA

Lineamientos de las Políticas de Seguridad de la Información

Todas las políticas identificadas en este documento se deberán desarrollar de manera detallada 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 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 Profesional 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).

- Incidentes de seguridad de la información que requieran que la política requiera cambios.

Vigencia y Derogatoria. La presente política es adoptada por medio de la resolución 008 del 4 de 02 de 2025 y rige a partir de esta fecha.

9. 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 Organización de la Seguridad de la Información (Roles Y Responsabilidades) y la actualización al cumplimiento de estándar ISO/IEC 27001:2022.

Revisó y aprobó: Comité Institucional de Gestión y Desempeño, acta sesión 023 del 20 de diciembre del 2024

Revisó: Manuel Geovanny Rueda Camino, Profesional TI AND 
Elaboró: Catherine Suarez Rodriguez, Profesional de seguridad de la Información, AND