

## **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - VIGENCIA 2025**

### **PROCESO: GESTIÓN DE LA TECNOLOGÍA E INFORMACIÓN**

### **UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR - ALIMENTOS PARA APRENDER**

**BOGOTÁ D.C, NOVIEMBRE DE 2024**

Tabla de contenido	Pág.
1. Introducción .....	3
2. Objetivo general.....	4
2.1 Objetivos específicos.....	4
3. Alcance .....	4
4. Marco normativo .....	4
5. Términos y definiciones .....	7
6. Política del MIPG con la cual se articula el plan .....	9
7. Resultados del del Índice de Desempeño Institucional - Vigencia 2023.....	9
8. Avances o logros - Vigencia 2024.....	10
9. Acciones estratégicas 2025 .....	10
Anexo. Plan de implementación	

## 1. Introducción

En Colombia, se está llevando a cabo la implementación de la política pública de Gobierno Digital, tal como establece el Decreto 1008 de 2018. En su artículo 2.2.9.1.1.3, se define la seguridad de la información como un principio fundamental de esta política. Asimismo, el Decreto 767 de 2022, en su artículo 2.2.9.1.2.1, establece una estructura que articula elementos como la gobernanza, la innovación pública digital, los habilitadores, las líneas de acción y las iniciativas dinamizadoras para alcanzar los objetivos propuestos.

El numeral 3.2 del mismo artículo destaca la Seguridad y Privacidad de la Información como un habilitador clave, instando a los sujetos obligados a desarrollar capacidades mediante la implementación de lineamientos específicos 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. Este enfoque se articula con el Modelo Integrado de Planeación y Gestión (MIPG), que actúa como una herramienta para cumplir con las metas de las políticas de desarrollo administrativo.

En la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender (UApA), se adoptó el Modelo Integrado de Planeación y Gestión (MIPG) mediante la Resolución No. 0020 de 2021. En su artículo 4, se expresa que, conforme a las siete dimensiones y dieciocho políticas de gestión y desempeño definidas para la operación del Modelo, se efectúa la asignación de responsabilidades al interior de la Unidad. En este contexto, la política de Gobierno Digital, que incluye el Modelo de Seguridad y Privacidad de la Información como habilitador, asigna la responsabilidad de implementación al proceso de Gestión de la Tecnología e Información, así como a la política de Seguridad Digital.

El manual interactivo de la política de Gobierno Digital, expedido por el Ministerio de Tecnologías de la Información y de las Comunicaciones, establece que esta política tiene como objetivo impactar positivamente la calidad de vida de los ciudadanos y, en general, de los habitantes del territorio nacional, así como mejorar la competitividad del país. Esto se logra promoviendo la generación de valor público a través de la transformación digital del Estado de manera proactiva, confiable, articulada y colaborativa entre los grupos de interés, permitiendo además el ejercicio de los derechos de los usuarios del ciberespacio.

Según el manual, la implementación de la política de Gobierno Digital se ha definido en dos componentes: gobernanza e innovación pública digital, habilitados por cuatro elementos: arquitectura, cultura y apropiación, seguridad y privacidad de la información, y arquitectura y servicios ciudadanos digitales. El manual precisa que el habilitador de seguridad y privacidad de la información desarrolla capacidades a través de la implementación de lineamientos de seguridad y privacidad en todos los procesos, trámites, servicios, sistemas de información, infraestructura y activos de información, con el objetivo de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

De igual manera, el Decreto 2106 de 2019, que dicta normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios en la administración pública, establece en el parágrafo del artículo 16 que las autoridades deben contar con una estrategia de seguridad digital, siguiendo los lineamientos emitidos por el Ministerio de Tecnologías de la Información y de las Comunicaciones.

Por otro lado, la Resolución No. 0500 del 10 de marzo de 2021, expedida por el Ministerio de Tecnologías de la Información y de las Comunicaciones, establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, cuyo propósito es servir como guía para la mejora de los estándares de seguridad en las entidades nacionales. La Resolución No. 746 del 11 de marzo de 2022 fortalece este modelo y define lineamientos adicionales a los establecidos en la Resolución 500. Por lo anterior, la Subdirección de Información de la UApA, cumpliendo con lo establecido en el Decreto 612 de 2018, actualiza el Plan de Seguridad y Privacidad de la Información al interior de la Unidad.

## 2. Objetivo general

Establecer un marco de acción que facilite la adopción continua del Modelo de Seguridad y Privacidad de la Información en la UApA, garantizando la protección de los activos de información que sustentan la prestación de los servicios digitales de la entidad. Esto permitirá fortalecer la confianza de funcionarios, ciudadanos, usuarios, proveedores y demás partes interesadas.

### 2.1 Objetivos específicos

- Planificar el desarrollo y seguimiento de las actividades que conforman el Sistema de Gestión de Seguridad Digital.
- Realizar la evaluación del Modelo de Seguridad y Privacidad de la Información – MSPI.
- Probar la efectividad de los controles definidos para mitigar riesgos.
- Sensibilizar a los funcionarios y contratistas de la entidad en temas de seguridad de la información.

## 3. Alcance

El presente plan constituye la hoja de ruta para la vigencia 2025 de la UApA. Su planificación se centrará en fortalecer la implementación de acciones alineadas con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientadas al cumplimiento de las medidas en Seguridad y Privacidad de la Información. Este enfoque tendrá en cuenta las capacidades y recursos disponibles, con el objetivo de mejorar la confianza de funcionarios, ciudadanos, usuarios, proveedores y demás partes interesadas.

## 4. Marco normativo

A continuación, se referencian las normas y leyes colombianas que aplican en el ámbito de seguridad y privacidad de la información; si cualquier disposición de estas condiciones pierde validez por cualquier razón, todas las demás conservan su fuerza obligatoria:

**La Constitución Política de Colombia**, promulgada en 1991. A continuación, se proporciona un resumen de los artículos que son relevantes para la seguridad de la información y la protección de datos:

- **Artículo 15:** Este artículo protege el derecho a la intimidad personal y familiar, así como el derecho al buen nombre, lo que implica que la información personal debe ser manejada con respeto a la privacidad de las personas.

- **Artículo 20:** Este artículo garantiza la libertad de expresión, incluyendo el derecho a recibir y difundir información. Este derecho es fundamental para la transparencia y el acceso a la información, aunque debe equilibrarse con el respeto a otros derechos, como la intimidad.
- **Artículo 23:** Este artículo consagra el derecho de petición, permitiendo a cualquier persona solicitar información a las autoridades. Este derecho es esencial para la rendición de cuentas y el acceso a la información pública.
- **Artículo 74:** Este artículo establece el derecho de acceso a la información pública, garantizando que los ciudadanos puedan acceder a documentos y registros de las entidades públicas, lo que contribuye a la transparencia y a la correcta administración de la información.

#### Leyes Colombianas:

- **Ley 23 de 1982.** Sobre derechos de autor.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 962 de 2005.** Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- **Ley 1221 del 2008.** Por la cual se establecen normas para promover y regular el teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Ley 1712 de 2014.** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- **Ley 1753 de 2015.** Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país".
- **Ley 1755 de 2015.** Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario.

- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.

#### Decretos

- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7º de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- **Decreto 884 de 2012.** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto reglamentario del sector comercio, industria y turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 1068 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 612 de 2018.** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1008 del 2018.** 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.
- **Decreto 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020.** Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de y el artículo 9º del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **Decreto 88 de 2022.** Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 Y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea

- **Decreto 338 de 2022.** Por el cual se adiciona el Título 21 a la parte 2 del libro 2 del Decreto Único 1078 de 2015, reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- **Decreto 767 de 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.

## Resoluciones

- **Resolución 1519 de 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- **Resolución 500 de 2021.** Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital
- **Resolución 746 de 2022.** Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
- **Resolución 063 de 2023.** Por la cual se adopta la Política de seguridad y privacidad de la información y seguridad digital, como uno de los elementos habilitadores de la Política de Gobierno Digital
- **Resolución 064 de 2023.** Por la cual se adopta la Política para la Protección y Tratamiento de Datos Personales de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender.

## Otras

- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos
- **CONPES 3701 de 2011** - Lineamientos de Política para Ciberseguridad y Ciberdefensa: Es la base para muchas de las políticas y estrategias posteriores en ciberseguridad en Colombia.
- **CONPES 3854 de 2016** - Política Nacional de Seguridad Digital: Establece directrices para la protección de la infraestructura crítica y la seguridad digital en el país.
- **CONPES 3995 de 2020** - Política Nacional de Confianza y Seguridad Digital: Tiene como objetivo promover la confianza en el uso de tecnologías digitales en Colombia, estableciendo estrategias para fortalecer la seguridad en el ciberespacio.
- **Directiva 26 de 2020.** Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- Guías del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MInTIC)

## 5. Términos y definiciones



- **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) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo de información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Dato abierto:** Son información pública dispuesta en formatos que permiten su uso y reutilización bajo licencia abierta y sin restricciones legales para su aprovechamiento.
- **Dato personal:** Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos impersonales no se sujetan al régimen de protección de datos de la presente ley. Cuando en la presente ley se haga referencia a un dato, se presume que se trata de uso personal. Los datos personales pueden ser públicos, semiprivados o privados.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000:2009].
- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).
- **Mejora continua:** Es el procedimiento que tiene como finalidad buscar un mayor rendimiento de los procesos o actividades.
- **Oficial de protección de datos personales:** Colaborador que se encarga de la gestión de las funciones establecidas en la Ley 1581 de 2012 y sus decretos reglamentarios.
- **Oficial de seguridad de la información:** Designación dada a un colaborador para cumplir con los temas relacionados frente a la jefatura y gerencia de la seguridad de la información de la Entidad.
- **Requisito legal:** Requisito obligatorio especificado por un organismo legislativo, ejecutivo y/o judicial.
- **Requisito reglamentario:** Requisito obligatorio especificado por una autoridad que recibe el mandato de un órgano legislativo.
- **Riesgos de seguridad de la información:** 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 que afecta la confidencialidad, integridad o disponibilidad de la información

- **RNBD:** Registro Nacional de Bases de datos, es el directorio público de las bases de datos sujetas a tratamiento que operan en el país, el cual es administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

## 6. Política del MIPG con la cual se articula el plan

El plan de tratamiento de riesgos de seguridad y privacidad de la información y seguridad digital se articula con las políticas de seguridad digital y gobierno digital del Modelo Integrado de Planeación y Gestión (MIPG), permitiendo fortalecer las capacidades de la Unidad y sus grupos de valor para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

## 7. Resultados del Índice de Desempeño Institucional - Vigencia 2023

A partir de la medición que realizó en la vigencia 2024 el Departamento Administrativo de la Función Pública (DAFP) al estado de la gestión y desempeño durante la vigencia 2023 por parte de las entidades públicas del orden nacional y territorial, bajo los criterios y estructura del Modelo Integrado de Planeación y Gestión (MIPG), se obtuvo una calificación en la política de seguridad digital correspondiente a 80 puntos. Este resultado representa un incremento de 25,4 puntos respecto a la medición realizada en la vigencia 2023 sobre la gestión del año 2022.

Con relación al subíndice de despliegue de controles se destaca que se obtuvieron 100 puntos en la vigencia, mientras que para el subíndice correspondiente a implementación de políticas de seguridad digital se obtuvieron 76,7 puntos.

Adicionalmente, se efectuaron las siguientes acciones:

- Se realizó la designación del Oficial de Seguridad y Privacidad de la Información y de Protección de Datos.
- Se llevó a cabo la contratación de profesional especialista en seguridad y privacidad de la información.
- Se fortalecieron los controles del anexo de la Norma ISO 27001:2013 sobre las plataformas tecnológicas de la Unidad.
- Se identificaron y se publicaron los activos de información de la Unidad.
- Se fortaleció una cultura en seguridad y privacidad de la información y seguridad digital en los colaboradores de la entidad.

## 8. Avances o logros - Vigencia 2024

Teniendo en cuenta el plan de seguridad y privacidad de la información formulado para la vigencia 2024, a continuación, se presentan los resultados alcanzados:

- Se realizó la actualización y publicación de los activos de información
- Se realizó la identificación de riesgos de seguridad de la información.
- Se revisó la eficacia de los controles de seguridad física de la entidad.
- Se realizó la prueba de continuidad tecnológica.
- Se realizaron sensibilizaciones en temas de seguridad y privacidad de la información y seguridad digital para los colaboradores de la entidad.

## 9. Acciones estratégicas 2025

El plan de seguridad y privacidad de la información establece la siguiente acción estratégica, la cual se encuentra alineada con el Plan de Acción Institucional de la UApA formulado para la vigencia 2025, con el fin de fortalecer la postura del Sistema de Gestión de Seguridad y Privacidad de la Información de la Entidad:

- *Definir e implementar un plan de trabajo alineado a los controles de la ISO 27001 con el fin de fortalecer la postura del Sistema de Gestión de Seguridad y Privacidad de la Información de la UApA.*

Esta acción se desarrollará a través de la ejecución de las actividades propuestas en el **anexo** que define el plan de implementación, para el correspondiente seguimiento por parte del Comité Institucional de Gestión y Desempeño.

## Historial de cambios

VERSIÓN	OBSERVACIONES	FECHA
0	Se elabora el documento para la vigencia 2025, en atención a los lineamientos del Decreto 612 de 2018.	Noviembre de 2024