

PLAN DE TRATAMIENTO DE RIESGOS 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.....	3
2.1 Objetivos específicos.....	3
3. Alcance	3
4. Marco normativo	4
5. Términos y definiciones	7
6. Política del MIPG con la cual se articula el plan	8
6.1. Resultados del Índice de Desempeño Institucional - Vigencia 2023	8
7. Avances o logros - Vigencia 2024.....	8
8. Acciones estratégicas 2025	9
Anexo. Plan de implementación	

1. Introducción

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital de la UApA se fundamenta en una estrategia integral orientada a cultivar una cultura preventiva en toda la organización. Esta cultura es esencial para que los miembros de la entidad comprendan el concepto de riesgo en su totalidad, así como el contexto en el que opera la UApA. Al fomentar este entendimiento, se pueden diseñar y planificar acciones proactivas que reduzcan significativamente el impacto negativo en la organización en caso de que dichos riesgos se materialicen.

Este enfoque no solo se centra en la protección de los activos de información, sino que también garantiza el cumplimiento riguroso de la normativa vigente en Colombia. Esto incluye el CONPES 3995 de 2020, que establece la política nacional de confianza y seguridad digital, así como el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) conocido como MSPI, y el Decreto 1008 de 2018, que regula aspectos cruciales de la gestión de seguridad digital.

El marco de referencia para la gestión de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital de la UApA se basa en la guía del Departamento Administrativo de la Función Pública (DAFP) y en el Anexo 4: Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. Estos lineamientos proporcionan un enfoque estructurado y coherente para identificar, evaluar y mitigar los riesgos asociados con la seguridad digital en el contexto de las entidades públicas.

Además, la UApA se compromete a adoptar buenas prácticas que se alineen con estándares internacionales reconocidos, como ISO 27001, que se enfoca en la gestión de la seguridad de la información, e ISO 31000:2018, que proporciona directrices sobre la gestión de riesgos. Estos estándares permiten establecer un marco robusto para la identificación, evaluación y mitigación de riesgos, asegurando que la UApA esté preparada para enfrentar los desafíos que puedan surgir en el ámbito digital.

2. Objetivo general

Definir y aplicar los lineamientos para tratar de manera integral los riesgos de seguridad y privacidad de la información y seguridad digital a los que la UApA pueda estar expuesta, de acuerdo con el contexto establecido en la Entidad, y a los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.

2.1 Objetivos específicos

- Realizar un diagnóstico de la situación actual de la entidad en materia de riesgos de seguridad digital.
- Optimizar los recursos de la entidad en la aplicación del plan de tratamiento de riesgos seguridad y privacidad de la información.
- Caracterizar los riesgos de seguridad en los procesos del Sistema Integrado de Gestión de la entidad.

3. Alcance

Este plan es aplicable a todos los procesos de la UApA (Estratégicos, misionales, de apoyo y de evaluación), que conforman el modelo de operación por procesos de la entidad. Su propósito es

facilitar una gestión eficiente de los riesgos relacionados con la Seguridad y Privacidad de la Información y la Seguridad Digital, implementando buenas prácticas que apoyen la toma de decisiones informadas y que contribuyan a la prevención de incidentes que puedan comprometer el cumplimiento de los objetivos institucionales.

El Plan de Tratamiento de Riesgos considerará todos los tipos de riesgos, prestando especial atención a aquellos clasificados en niveles Moderado, Alto y Extremo, según los lineamientos establecidos por la UApA. Los riesgos identificados en niveles inferiores serán aceptados por la entidad, asegurando así un enfoque equilibrado y estratégico en la gestión de riesgos.

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 2082 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 884 de 2012.** Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 2364 de 2012.** Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica 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 1068 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **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 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 en 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)
- ANEXO 4 Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas

5. Términos y definiciones

- **Activo de información:** Conocimiento o información que tiene valor para la organización.
- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Identificación del riesgo:** Etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.
- **Información:** Datos relacionados que tienen significado para la entidad.
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas

por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

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 UApA y sus grupos de valor para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

6.1. 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.

De acuerdo con lo anterior, se informan las siguientes acciones estratégicas adelantadas:

- Se llevó a cabo la contratación del profesional especialista en seguridad y privacidad de la información.
- Se realizó la designación del Oficial de Seguridad y Privacidad de la Información y de Protección de Datos.
- Se implementaron controles de seguridad que ayudaron a mitigar riesgos.
- Se configuró la firma digital en la entidad.
- Se verificaron y actualizaron documentos de los procesos.
- Se fortalecieron los controles del anexo de la Norma ISO 27001 sobre las plataformas tecnológicas de la UApA.

7. Avances o logros - Vigencia 2024

Teniendo en cuenta el plan de tratamiento de riesgos 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 y aprobación de los riesgos de seguridad de la información.
- Se revisó la eficacia de los controles de seguridad física de la entidad.

8. Acciones estratégicas 2025

El plan de tratamiento de riesgos 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:

- *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