PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR – ALIMENTOS PARA APRENDER

PROCESO: MANTENIMIENTO Y SOPORTE DE TECNOLOGÍA

BOGOTÁ D.C, ENERO DE 2026

Tabla de contenido **Pág.**

1. Introducción

El presente documento define las medidas que se desarrollarán e implementarán durante la vigencia 2026 del plan de tratamiento de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital en la UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR – UApA, medidas que permitan mitigar los riesgos presentes (perdida de confidencialidad, integridad, disponibilidad, privacidad en los activos de información e interrupción), evitando situaciones que generen incertidumbre en el cumplimiento de los objetivos de la Entidad.

Las actividades se definieron teniendo en cuenta la metodología de gestión de riesgos adoptada por la entidad en cuanto a la seguridad y privacidad de la información y seguridad digital y basados en la Guía para la gestión integral del riesgo en entidades públicas, proporcionando las herramientas necesarias para identificar sus características y definir los pasos a seguir para su ejecución.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información y Seguridad Digital de la UApA se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, al CONPES 3995 de 2020 que establece la política nacional de confianza y seguridad digital, al Modelo de Seguridad y Privacidad del MINTIC - MSPI y lo establecido en el decreto 1008 de 2018; adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001, ISO 31000:2018 y la Guía para la gestión integral del riesgo en entidades públicas del Departamento Administrativo de la Función Pública - DAFP.

2. 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.

3. 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.

4. Alcance

Este plan aplica para todos los procesos (estratégicos, misionales, apoyo y de evaluación) que hacen parte del modelo de operación por procesos de la UApA, brindando una eficiente gestión de riesgos de Seguridad y Privacidad de la información y Seguridad Digital, y proporcionando buenas prácticas que contribuyan a la toma de decisiones, previniendo incidentes que puedan afectar el logro de los objetivos de la entidad.

El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por la UApA, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

5. 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 y Gobierno Digital permitiendo fortalecer las capacidades de la Unidad y grupos de valor para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

6. Avances o logros - Programado vigencia 2025

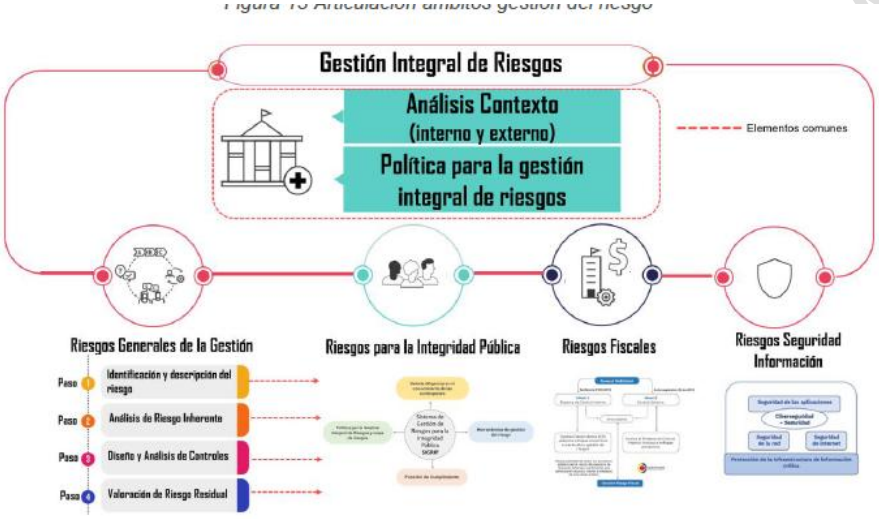
Durante la vigencia 2025 se avanzó en lo siguiente frente a la gestión de riesgos de seguridad y privacidad de la información:

- Definición de la metodología para la administración de riesgos de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para aprender (UApA), incluyendo los lineamientos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.
- Actualización del contexto interno y externo de los procesos de la Entidad.
- Se realizó entrenamiento al personal de la Entidad y medición del impacto, simulando un ataque de ingeniería social – Phishing.
- Se realizó análisis de vulnerabilidades de la infraestructura tecnológica y los sistemas de información de la Unidad.
- Se inició con la identificación de los riesgos de seguridad y privacidad de la información y seguridad digital en el proceso de Gestión de información y Tecnología.

7. Metodología

7.1. Desarrollo metodológico

La UApA, acogerá la metodología establecida por el Departamento Administrativo de la Función Pública, descrita en la Guía para la gestión integral del riesgo en entidades públicas versión 7.



Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2025.

Para dar cumplimiento a las etapas establecidas en dicha metodología se establece el siguiente cronograma de actividades, el cual se le hará seguimiento a través del plan de acción Institucional, con la línea estratégica "Definir y ejecutar un plan estratégico de seguridad y privacidad de la información - PESI, alineado al MSPI del MinTIC con el fin de fortalecer la postura en seguridad digital en la UApA":

Actividades	Tareas	Responsable de la Tarea	Fecha Inicio	Fecha Final
Revisión de los lineamientos de riesgos de seguridad y privacidad de la información y seguridad digital	Revisar la política, metodología y lineamientos de la gestión de riesgos.	Oficina Asesora de Planeación. Oficial de seguridad y Privacidad de la Información.	2-feb-26	31-mar-26
Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Identificar y/o actualizar el Contexto interno y externo de los procesos	Oficial de seguridad y Privacidad de la Información Líderes de los procesos	01 abr-26	30-jun-26
	Identificar, Analizar y Evaluar los Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.	Oficial de seguridad y Privacidad de la Información Líderes de los procesos	01 abr-26	30-jun-26
Aceptación y aprobación de Riesgos Identificados	Aceptar y aprobar los riesgos identificados y los planes de tratamiento	Líderes de los procesos	01 abr-26	30-jun-26
Seguimiento fase de tratamiento	Realizar seguimiento a la implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Oficial de seguridad y Privacidad de la Información	01-jul-26	23-dic-26
Vulnerabilidades	Ejecutar las pruebas de vulnerabilidades y pentest	Oficial de seguridad y Privacidad de la Información	02-feb-26	30-jun-26

Actividades	Tareas	Responsable de la Tarea	Fecha Inicio	Fecha Final
	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pentest	Oficial de seguridad y Privacidad de la Información Subdirección de Información	02-feb-26	30-jun-26
Entrenamiento	Realizar ejercicio de Ingeniería Social	Oficial de seguridad y Privacidad de la Información	02-feb-26	23-dic-26

8. Recursos

La UApA, para la gestión de riesgos de Seguridad y Privacidad de la información y Seguridad Digital, dispondrá de los siguientes recursos:

Recursos	Variable
Humanos	Responsables de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la gestión de riesgos de seguridad y privacidad de la información y seguridad digital.
Técnicos	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital en su última versión. Herramienta para la gestión de riesgos.
Logísticos	Cronograma para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos con los procesos de la entidad.
Financieros	El Presupuesto que implique la ejecución de los planes de tratamiento de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles

Recursos	Variable
	definidos.

9. Medición

La medición se realiza con un indicador que está orientado principalmente a determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en el sistema de gestión de seguridad y privacidad de la información de la entidad.

Historial de cambios

VERSIÓN	OBSERVACIONES	FECHA
0	Se crea el documento, en atención a los lineamientos del Decreto 612 de 2018.	Enero de 2026