COLOMBIA POTENCIA DE LA VIDA

Alimentos para Aprender

Plan de Seguridad y Privacidad de la Información 2024

Proceso: Gestión de la Tecnología e Información

Unidad Administrativa Especial de Alimentación Escolar
Alimentos para Aprender

Tabla de contenido **Pág.**

1. Introducción

En Colombia se viene adelantando la implementación de la política pública de Gobierno Digital, tal como lo establece el decreto 1008 de 2018, donde en su artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera el Decreto 767 de 2022 en el artículo 2.2.9.1.2.1 define la estructura a través de un esquema que articula los elementos que la componen, a saber: gobernanza, innovación pública digital, habilitadores, líneas de acción, e iniciativas dinamizadoras, con el fin de lograr su objetivo. Así mismo, el numeral 3.2 del mismo artículo define la 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, lo anterior articulado con el Modelo Integrado de Planeación y Gestión - MIPG, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo.

En la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender (en adelante UApA) mediante la Resolución 020 de 2021, se adoptó el Modelo Integrado de Planeación y Gestión – MIPG, y en su artículo 4 expresa que (…) Conforme a las 7 Dimensiones y 18 Políticas de Gestión y Desempeño definidas para la operación del Modelo Integrado de Planeación y Gestión, se efectúa la asignación de responsabilidades al interior de la Unidad, que (…) La política de Gobierno digital (en donde se encuentra como habilitador el Modelo de Seguridad y Privacidad de la Información) serán responsables de la implementación el proceso de Gestión de la Tecnología e Información, así como de la política de Seguridad digital.

El manual interactivo de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como objetivo impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del

territorio nacional y la competitividad del país, 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 y permitir 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, que son habilitados por cuatro elementos: Arquitectura, Cultura y apropiación, seguridad y privacidad de la información, arquitectura y servicios ciudadanos digitales. El manual en mención, precisa que el habilitador de seguridad y privacidad de la información desarrolla 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 datos.

De igual manera el 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, en el parágrafo del artículo 16 indica que (…) Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones (…).

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de 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, y de la resolución 746 del 11 de marzo de 2022, por la cual se fortalece este modelo y se definen lineamientos adicionales a los establecidos en la resolución 500; por lo anterior, la Subdirección de Información de la UApA, y dando cumplimiento a 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 para continuar adoptando el Modelo de Seguridad y Privacidad de la información de la UApA, que permita la

protección de los activos de información que soportan la prestación de servicios digitales de la entidad, logrando fortalecer la confianza de sus funcionarios, ciudadanos, usuarios, proveedores y demás partes interesadas.

3. Alcance

El presente plan, es la hoja de ruta para la vigencia 2024 de la UApA, y su planeación se enfocará en fortalecer la implementación de acciones de acuerdo con los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados al cumplimiento de las acciones en Seguridad y Privacidad de la información, teniendo en cuenta las capacidades y recursos disponibles, para mejorar la confianza de sus 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:

Constitución Política de Colombia

- Artículos 15, 20, 23 y 74.

Leyes

- **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 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 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 la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019,

y el artículo 9° 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 Titulo 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.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020**. Confianza y Seguridad Digital
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
  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.

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 controlar 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 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.

7. Avances o logros - Programado vigencia 2023

Durante la vigencia 2023 se avanzó en lo siguiente frente a la seguridad y privacidad de la información:

- Contratación de profesional especialista en seguridad y privacidad de la información.
- Adopción de la política de seguridad y privacidad de la información y seguridad digital bajo la resolución No. 063 de 2023.

- Adopción de las políticas de protección de tratamiento de datos personales bajo la resolución No. 064 de 2023.
- Designación del oficial de seguridad y privacidad de la información y de datos personales bajo la resolución 123 del 15 de junio de 2023.
- Implementación de controles del Anexo de la Norma ISO 27001:2013 sobre las plataformas tecnológicas de la Unidad.
- Se identificaron los activos de información de la Unidad
- Inclusión de la seguridad y privacidad de la información y seguridad digital en la gestión contractual
- Se estableció la documentación necesaria para la alineación con el Modelo de seguridad y privacidad y seguridad digital de la información del MinTIC.
- Fortalecimiento de la cultura en seguridad y privacidad de la información y seguridad digital en los colaboradores de la entidad

8. Plan de implementación de seguridad y privacidad de la información

8.1 Política general de seguridad y privacidad de la información y seguridad digital

Preservar y administrar la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiablidad de la información digital y física, que se produce en el marco de la operación de sus procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, promoviendo el desarrollo, la implementación y seguimiento a la Política Pública de Alimentación Escolar.

8.2 Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital de la UApA.

1. Establecer mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, privacidad, legalidad y confiabilidad de la información de la Unidad.
2. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y seguridad digital en la Unidad.
3. Gestionar los riesgos de seguridad y privacidad de la información y de seguridad digital.
4. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de gestión de seguridad y privacidad de la información.
5. Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
6. Definir y operar la continuidad de la operación de los servicios de la Unidad.

La UApA ha adoptado la política de seguridad y privacidad de la información, como parte de su Sistema Integrado de Gestión, y para lograr su implementación y fortalecimiento ha diseñado un conjunto de actividades que dan cumplimiento a las políticas públicas de gobierno y seguridad digital.

El logro de los objetivos específicos de la política de seguridad y privacidad de la información definidos en el presente documento, requiere la definición de actividades detalladas categorizadas según el ámbito de ejecución en la siguiente estructura de plan de trabajo. A continuación, se presenta el plan para fortalecer la implementación del modelo de seguridad y privacidad en la UApA para la vigencia 2024, el cual se le hará seguimiento a través del plan de acción Institucional, con la línea estratégica "Migrar e implementar los componentes que hacen parte del Sistema de Gestión de Seguridad y Privacidad de la Información de la UApA según la normativa vigente":

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Activos de información	Definir lineamientos para el levantamiento de activos de información	Actualizar la metodología o la documentación de la gestión de levantamiento de activos de información, en el caso que aplique	Oficial de Seguridad y Privacidad de la Información	12-feb-24	20-dic-24
	Levantamiento activos de información	Socializar la metodología de activos de información.	Oficial de Seguridad y Privacidad de la Información	12-feb-24	16-feb-24
		Identificar activos de información en cada dependencia	Enlace de cada proceso, Oficial de Seguridad y Privacidad de la Información	19-feb-24	29-mar-24
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Oficial de Seguridad y Privacidad de la Información	01-abr-24	08-abr-24
		Realizar correcciones a los instrumentos de activos de información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	01-abr-24	19-abr-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		Actualización del inventario de activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, adición de actividades al proceso, inclusión de un nuevo activo, cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, materialización de riesgos que cambien la criticidad del activo.	Enlaces de cada proceso	19-abr-24	27-dic-24
		Validar y aceptar los activos de información por cada líder de proceso para su publicación	Enlace de cada proceso, Oficial de Seguridad y Privacidad de la Información	19-abr-24	30-abr-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
	Publicación de Activos de Información	Consolidar el instrumento de activos de Información.	Oficial de Seguridad y Privacidad de la Información	19-abr-24	30-abr-24
		Publicar los instrumentos de activos de información consolidado en el SIG	Oficial de Seguridad y Privacidad de la Información, Oficina Asesora de Planeación, Subdirección de Información	19-abr-24	30-abr-24
	Registros activos de información ley 1712	Consolidar el instrumento de Registro Activos de Información, el índice de información Clasificada y Reservada, y el inventario de datos abiertos, con el insumo de la matriz de activos de Información.	Oficial de Seguridad y Privacidad de la Información	30-abr-24	27-dic-24
		Publicación del Registro Activos de Información, el índice de información Clasificada y Reservada, y el inventario de datos abiertos en el sitio web de la Entidad.	Oficial de Seguridad y Privacidad de la Información, Oficina Asesora de Planeación, Subdirección de Información	30-abr-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	**Fecha final**
	Reporte datos personales	Reportar las bases de datos con datos personales.	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
Gestión de Riesgos	Revisión de los lineamientos de riesgos de seguridad y privacidad de la información	Revisar la política, metodología y lineamientos de la gestión de riesgos	Oficina Asesora de Planeación. Oficial de seguridad y Privacidad de la Información	6-may-24	29-nov-24
	Sensibilización	Socialización de lineamientos y herramienta - Gestión de riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de Seguridad y Privacidad de la Información	8-may-24	16-may-24
	Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Identificación y/o actualización del contexto interno y externo de los procesos, identificación, análisis y evaluación de riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de seguridad y Privacidad de la Información	20-may-24	21-jun-24
		Realimentación, revisión y verificación	Oficial de Seguridad y Privacidad de la Información	20-may-24	21-jun-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		de los riesgos identificados.			
	Aceptación y aprobación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Líderes de los procesos	1-jul-24	19-jul-24
	Publicación	Publicación mapas de riesgos de los procesos	Oficial de Seguridad y Privacidad de la Información Oficina Asesora de Planeación	1-jul-24	31-jul-24
	Seguimiento Fase de Tratamiento	Seguimiento a la implementación de controles y planes de tratamiento de los riesgos identificados (verificación de evidencias)	Oficial de Seguridad y Privacidad de la Información	01-ago-24	27-dic-24
	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento	Oficial de Seguridad y Privacidad de la Información	01-ago-24	27-dic-24
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Oficial de Seguridad y Privacidad de la Información	01-ago-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Gestión de Incidentes de Seguridad y Privacidad de la Información	Publicar y socializar el procedimiento de incidentes de seguridad de la información	Creación y/o actualización del procedimiento de incidentes de seguridad y privacidad de la información	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
		Socializar el procedimiento de incidentes de seguridad y privacidad de la información a todos los interesados	Oficial de Seguridad y Privacidad de la Información	04-mar-24	08-mar-24
	Gestionar los incidentes de seguridad de la información identificados	Seguimiento a los incidentes de seguridad de la información reportados a la mesa de servicio de acuerdo con lo establecido en el procedimiento definido	Profesional Subdirección de Información. Oficial de Seguridad y Privacidad de la Información	01-ene-24	31-dic-24
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSPI	Profesional Subdirección de Información. Oficial de Seguridad y	12-feb-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
			Privacidad de la Información		
Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar el plan de cambio y cultura de Seguridad y Privacidad de la Información y Seguridad Digital	Elaborar y/o actualizar la documentación del plan de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital, en el caso que aplique	Oficial de Seguridad y Privacidad de la Información	12-feb-24	29-feb-24
		Publicar y divulgar el plan de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital con los gestores de procesos.	Oficial de Seguridad y Privacidad de la Información	29-feb-24	29-feb-24
	Ejecutar el plan de cambio, Cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Implementar las estrategias del plan de cambio, cultura y apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de Seguridad y Privacidad de la Información, Gestor de procesos	01-mar-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Elaborar y/o actualizar la matriz de verificación de requisitos legales de Seguridad y Privacidad de la Información	Elaborar la matriz de verificación de requisitos Legales de Seguridad de la Información	Oficial de Seguridad y Privacidad de la Información, Oficina Asesora de Planeación	12-feb-24	27-dic-24
	Revisar y publicar la matriz de verificación de requisitos legales de Seguridad y Privacidad de la Información	Solicitar las evidencias del cumplimiento de los requisitos legales de Seguridad y Privacidad de la Información	Oficial de Seguridad y Privacidad de la Información Todos los procesos	12-feb-24	27-dic-24
		Publicar la matriz de requisitos legales en el SIG	Oficial de Seguridad y Privacidad de la Información Oficina Asesora de Planeación	12-feb-24	27-dic-24
Plan de Continuidad de la operación de los servicios	Documentación del plan de continuidad de la operación	Crear documentación del plan de continuidad de la operación	Oficial de Seguridad y Privacidad de la Información	12-feb-24	30-dic-24
		Aprobación del plan de continuidad de la operación	Oficial de Seguridad y Privacidad de la Información	12-feb-24	30-dic-24
	Revisión manual políticas de Seguridad de	Crear y/o actualizar los manuales, políticas,	Oficial de Seguridad y Privacidad de	12-feb-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
Planeación	la Información y Resolución de Seguridad y Privacidad de la Información	resoluciones, y demás documentación estratégica del Sistema de Gestión de Seguridad y privacidad de la Información.	la Información.		
		Actualizar el plan de Seguridad y Privacidad de la Información y el plan de tratamiento de riesgos.	Oficial de Seguridad y Privacidad de la Información y equipo implementador	18-nov-23	31-ene-24
Gobierno Digital	Implementar la política pública de Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
		Revisar y alinear la documentación del SGSPI de la Entidad al MSPI, de acuerdo con la normatividad vigente.	Oficial de Seguridad y Privacidad de la Información	12-feb-24	28-jun-24
		Implementar el Plan de Seguridad Digital en la Entidad	Oficial de Seguridad y Privacidad de la Información	12-feb-24	30-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	**Fecha final**
		Revisar e implementar los lineamientos que define el FURAG en cuanto a las políticas de Gobierno Digital y Seguridad Digital.	Oficial de Seguridad y Privacidad de la Información	12-feb-24	30-dic-24
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno nacional	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
Auditorías Internas y/o Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el PAAI	Todos los procesos	15-feb-23	30-dic-23
Revisión de los controles de la norma ISO 27001	Revisión de los controles de la norma ISO 27001:2013	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información y Seguridad Digital	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
Indicadores SGSI	Creación y provisión de información a los indicadores	Formular, Implementar y alimentar los	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
	de medición del SGSPI	indicadores del SGSPI			
Vulnerabilidades	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo con el alcance y la metodología establecida	Pentester	12-feb-24	27-dic-24
	Ejecutar plan de remediación	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, OTI	12-feb-24	27-dic-24
Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24
	Registro de las bases de datos	Registrar o actualizar las bases de datos en el aplicativo RNBD de la SIC, teniendo en cuenta la información suministrada	Oficial de Seguridad y Privacidad de la Información	12-feb-24	27-dic-24

Gestión	Actividades	Tareas	Responsable de la tarea	Fechas Programación Tareas	
				Fecha inicio	Fecha final
		por las áreas y el levantamiento de activos de información			

Los responsables adelantarán las actividades concernientes con el propósito de aportar a la implementación del modelo de seguridad y privacidad de la información de la UApA sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; lo anterior, de acuerdo con la disponibilidad presupuestal oportuna, al interés institucional y a las orientaciones de la alta dirección que se adopten para afrontar el desarrollo y cumplimiento de las actividades planificadas.

9. Documentos de referencia

- Norma técnica colombiana NTC- ISO IEC 27001:2013
- Modelo de Seguridad y Privacidad de la Información (MSPI), MinTIC
- Guía N° 17, Guía de Mejora Continua, MinTIC.
- Sistemas de Gestión de la Seguridad de la Información (SGSI), MinTIC.
- Manual de Gobierno Digital, Implementación de la Política de Gobierno Digital, Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2), MinTIC.

Historial de cambios

VERSIÓN	OBSERVACIONES	FECHA
0	Se crea el documento, en atención a los lineamientos del Decreto 612 de 2018.	Diciembre de 2023