



MINISTERIO DE EDUCACIÓN
NACIONAL

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 0

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR – ALIMENTOS PARA APRENDER

Gestión de la Información

Subdirección de Información

2023



Tabla de contenido	Pág.
1. Introducción.....	3
2. Objetivo	4
2.1. Objetivos específicos de la política de seguridad y privacidad de la información y seguridad digital de la UApA.....	4
3. Alcance.....	4
4. Marco normativo.....	5
5. Glosario.....	7
6. Política general de seguridad y privacidad de la información y seguridad digital	8
7. Plan de implementación de seguridad y privacidad de la información	8
8. Documentos de referencia	14



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, como una herramienta dinamizadora para cumplir las metas de las políticas de desarrollo administrativo.

En la 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 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 desarrollar 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 párrafo 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 de la Información de las entidades nacionales; 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 UApA,

2. Objetivo

El presente documento, tiene como objetivo establecer un marco de acción para adoptar la implementación del 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.

2.1 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 UApA.
2. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y seguridad digital en la UApA.
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 UApA.

3. Alcance

El presente plan, es la hoja de ruta para la vigencia 2023 de la UApA, y su planeación se enfocará en fortalecer la implementación de acciones de acuerdo a los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados al cumplimiento de las acciones en torno a la Seguridad y Privacidad de la información institucional, 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.
- **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 23 de 1982.** Sobre derechos de autor
- **Ley 44 de 2093.** 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).
- **Decisión Andina 351 de 1993.** Régimen común sobre derecho de autor y derechos conexos
- **Ley 527 de 2099.** 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.
- **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
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **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.
- **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.
- **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 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- **Ley 1450 de 2011.** Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.
- **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 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **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.
- **CONPES 3854 de 2017.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Confianza y Seguridad Digital
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **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 1287 de 2020.** Por el cual se reglamenta el Decreto Legislativo 491 del 28 de marzo de 2020, en lo relacionado con la seguridad de los documentos firmados durante el trabajo en casa, en el marco de la Emergencia Sanitaria.
- **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.
- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario
- **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 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 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 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 1068 de 2015.** por medio del cual se expide el Decreto Único Reglamentario del Sector Hacienda y Crédito Público.
- **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 884 de 2012.** por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **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.
- **Ley 2088 de 2021.** Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- **Resolución 0279 de 2022.** Por la cual se adopta la política de Seguridad y privacidad de la información y se definen los lineamientos frente a su uso y manejo.
- **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
- **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.
- **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
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.

5. Glosario

- **Acciones correctivas:** Acción por medio de la cual se elimina la causa de la no conformidad, evitando que se repita.
- **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).
- **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.
- **Mejora continua:** Es el procedimiento que tiene como finalidad buscar un mayor rendimiento de los procesos o actividades.
- **No conformidad:** Es el incumplimiento de un requisito.
- **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 general de seguridad y privacidad de la información y seguridad digital

La UApa protege, preserva y administra la integridad, confidencialidad, disponibilidad, privacidad, legalidad y confiabilidad 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 así, a través de una política pública, por el acceso y la permanencia de los niños, niñas, adolescentes y jóvenes en el sistema educativo oficial, a una alimentación saludable con calidad, oportunidad e integralidad, basada en la eficiencia, eficacia y transparencia.

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

La UApa ha adoptado la Política de Seguridad 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 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 2023, el cual se le hará seguimiento mes a mes:

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
Activos de Información	Levantamiento 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	15-feb-23	22-dic-23
		Socializar la metodología de activos de Información.	Oficial de Seguridad y Privacidad de la Información	15-feb-23	17-feb-23
		Identificar activos de información en cada dependencia	Enlace de cada proceso, Oficial de Seguridad y Privacidad de la Información	20-feb-23	24-mar-23
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Oficial de Seguridad y Privacidad de la Información	24-mar-23	31-mar-23
		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Enlaces de cada proceso	31-mar-23	14-abr-23
		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	14-abr-23	30-dic-23

Publicación de Activos de Información	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	14-abr-23	28-abr-23
	Consolidar el instrumento de activos de Información.	Oficial de Seguridad y Privacidad de la Información	14-abr-23	28-abr-23
	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	14-abr-23	28-abr-23
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	28-abr-23	22-dic-23
	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 Prensa, Oficina de TI	28-abr-23	22-dic-23
Reporte Datos Personales	Reportar las bases de datos con datos personales.	Oficial de Seguridad y Privacidad de la Información	28-abr-23	22-dic-23
Definición de lineamientos de riesgos	Definir y establecer la política, metodología y lineamientos de la gestión de riesgos	Oficial de seguridad y Privacidad de la Información	2-may-23	30-nov-23
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-23	8-may-23
Identificación de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Identificación del Contexto 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	15-may-23	28-jul-23

Gestión de Riesgos		Realimentación, revisión y verificación de los riesgos identificados.	Oficial de Seguridad y Privacidad de la Información	15-may-23	28-jul-23
	Aceptación y aprobación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Líderes de los procesos	1-ago-23	18-ago-23
	Publicación	Publicación mapas de riesgos de los procesos	Oficial de Seguridad y Privacidad de la Información Oficina Asesora de Planeación	1-ago-23	31-ago-23
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Oficial de Seguridad y Privacidad de la Información	31-ago-23	22-dic-23
	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	31-ago-23	22-dic-23
	Mejoramiento Monitoreo y Revisión	Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones presentadas.	Oficial de Seguridad y Privacidad de la Información	31-ago-23	22-dic-23
		Medición, presentación y reporte de indicadores	Oficial de Seguridad y Privacidad de la Información	31-ago-23	22-dic-23
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	15-feb-23	22-dic-23
		Socializar el procedimiento de incidentes de seguridad y privacidad de la información a todos los interesados	Oficial de Seguridad y Privacidad de la Información	01-mar-23	03-mar-23
	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	1-mar-23	31-dic-23

	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad y Privacidad de la Información	15-feb-23	22-dic-23
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSPI	Profesional Subdirección de Información. Oficial de Seguridad y Privacidad de la Información	15-feb-23	22-dic-23
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	15-feb-23	28-feb-23
		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	28-feb-23	28-feb-23
	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	28-feb-23	22-dic-23
	Analizar el Plan de Cambio, Cultura y Apropiación de Seguridad y Privacidad de la Información y Seguridad Digital	Analizar los instrumentos de medición 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	28-feb-23	22-dic-23
	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	15-feb-23
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	15-feb-23	22-dic-23

		Publicar la Matriz de Requisitos Legales en el SIG	Oficial de Seguridad y Privacidad de la Información Oficina Asesora de Planeación	15-feb-23	22-dic-23
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	15-feb-23	30-dic-23
		Aprobación del Plan de continuidad de la Operación	Oficial de Seguridad y Privacidad de la Información	15-feb-23	30-dic-23
Oportunidades de mejoras del SGSPI	Realizar seguimiento a los planes de mejoramiento producto de revisiones internas y externas a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Oficial de Seguridad y Privacidad de la Información y equipo implementador	15-feb-23	22-dic-23
Planeación	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad y Privacidad de la Información	Crear y/o actualizar los Manuales, Políticas, Resoluciones, y demás documentación estratégica del Sistema de Gestión de Seguridad y privacidad de la Información.	Oficial de Seguridad y Privacidad de la Información.	15-feb-23	22-dic-23
		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	17-nov-22	31-ene-23
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	15-feb-23	31-may-23
		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	15-feb-23	31-may-23
		Implementar el Plan de Seguridad Digital en la Entidad	Oficial de Seguridad y Privacidad de la Información	15-feb-23	30-dic-23
		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	15-feb-23	30-dic-23
	CCOCI	Cumplimiento requerimientos infraestructuras críticas del gobierno nacional	Oficial de Seguridad y Privacidad de la Información	1-mar-23	22-dic-23

Auditorías Internas y 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	15-feb-23	22-dic-23
Indicadores SGSI	Creación y Provisión de información a los indicadores de medición del SGSPI	Formular, Implementar y alimentar los indicadores del SGSPI	Oficial de Seguridad y Privacidad de la Información	15-feb-23	22-dic-23
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-may-23	30-nov-23
	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-may-23	30-nov-23
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	15-feb-23	30-jun-23
	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 por las áreas y el levantamiento de activos de información	Oficial de Seguridad y Privacidad de la Información	15-feb-23	22-dic-23

Los responsables adelantarán las actividades concernientes con el propósito de aportar al fortalecimiento 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.

8. 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 2022