POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS 2021

PROCESO: GESTIÓN DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR

BOGOTÁ D.C, FEBRERO 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de la **Unidad Administrativa Especial de alimentación Escolar – Alimentos para Aprender** (en adelante UapA) y para garantizar la integridad, confidencialidad y disponibilidad de la Información.

La definición e implementación de políticas, metodologías, directrices y recomendaciones basadas en estándares y mejores prácticas, todas orientadas con procesos de TI, fortalecerán los procesos de negocio y garantizarán el aprovechamiento de los recursos informáticos en la Entidad. Así mismo, se facilitará la incorporación y uso efectivo de las tecnologías emergentes de última generación, se aprovecharán mejor las herramientas informáticas y demás servicios de TI requeridos para la integración y el intercambio de la información.

En tal sentido, la Subdirección de Información está consolidando la gestión tecnológica de la Unidad, mediante la definición de los principios, políticas y lineamentos de las diferentes líneas de acción de TI, buscando que se genere un valor agregado sobre las actividades de los usuarios la Entidad. Ahora bien, el mapa de ruta para la definición, estructuración e implementación, parte de la alineación con los objetivos estratégicos establecidos por el Ministerio de Educación Nacional en su plan estratégico sectorial y atendiendo los lineamientos propuestos para el desarrollo educativo. De esta manera, una Institucionalidad moderna y tecnificada genera acciones transversales sobre los pilares de la Unidad, al igual que garantiza el cumplimiento a las políticas establecidas por el Departamento Administrativo de la Función Pública para el mejoramiento de la Gestión y el Desempeño de la institucionalidad del Sector.

En razón de lo anterior y considerando la necesidad de incorporar estrategias y controles en el ámbito de las Tecnologías de la Información y las Comunicaciones (en adelante TI), necesarias para el cumplimiento de las metas institucionales, se hace indispensable trazar y comprometer la implementación de la política de gestión de seguridad de la información y protección de datos, la cual proporcione un marco de confianza en el ejercicio de sus deberes con la institucionalidad, el estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Unidad.

En ese sentido y de acuerdo con los principios de tecnología adoptados por la Unidad, con el fin de mantener un control eficiente de las tecnologías de información y

comunicaciones aportando valor a la Entidad, se estructura el presente documento de Política de Seguridad en la Información.

El respectivo contenido y sus actualizaciones serán informados a directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la Unidad, a través de la Dirección General o su delegado y se publicarán en la Intranet.

2. MARCO NORMATIVO

El Principio de estrategia de TI de la Unidad Administrativa Especial de Alimentación Escolar- Alimentos para Aprender, contempla el siguiente marco normativo:

- **Constitución Política de Colombia** 1991, artículos 15 y 20.

- **Ley 1266 de 2008**, "Por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países 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 1403 de 2010,** "Sobre derechos de autor."

- **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."

- **Decreto 943 de 2014** "Por el cual se actualiza el Modelo Estándar de Control Interno (MECI)".

- **Decreto 2573 de 2014**, "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones."

- **Resolución No. 253 de 2015** de 27 de febrero de 2015, "Por la cual se establecen los requisitos para la viabilidad, seguimiento y control de los proyectos para el financiamiento de la infraestructura, en el Sector de Tecnologías de la Información y las Comunicaciones, de acuerdo con el artículo 6 del decreto 2048 de 2014."

- **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 415 de 2016**, "Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones."

- **CONPES 3859 de 2016**, "Política para la adopción e implementación de un catastro multipropósito rural - urbano."

- **Decreto 1008 de 14 jun 2018**: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título.

- **Directiva Presidencial N° 02 del 02 de abril de 2019**. Simplificación de la interacción digital entre los ciudadanos y el estado. Integración con Gov.co.

- **Directiva Presidencial N° 03 del 02 de abril de 2019**: Lineamientos para la definición de la estrategia institucional de comunicaciones, objetivos y contenidos de las entidades de la rama ejecutiva del orden nacional.

- **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.

- **Ley 1955 de 2019**, expidió el plan de desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad” en su artículo 189 creó la Unidad Administrativa Especial de Alimentación Escolar con autonomía administrativa, personería jurídica y patrimonio independiente, adscrita al Ministerio de Educación Nacional.

- **Decretos Nacionales 218 y 219 de febrero de 2020**, Crea la estructura interna de la Unidad Administrativa Especial de Alimentación Escolar y su planta de personal respectivamente.

- **Decreto 620 de mayo 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.

- **Decreto 2106 de 22 de noviembre de 2020**: Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. Capítulo General de Transformación Digital para una gestión Pública efectiva.

- **CONPES 3975:** Este documento CONPES formula una política nacional para la transformación digital e inteligencia artificial. Esta política tiene como objetivo potenciar la generación de valor social y económico en el país a través del uso estratégico de tecnologías digitales en el sector público y el sector privado, para impulsar la productividad y favorecer el bienestar de los ciudadanos, así como generar los habilitadores transversales para la transformación digital sectorial, de manera que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial (4RI).

3. GLOSARIO

▪ **ACTIVIDADES**: Son el conjunto de operaciones mediante los cuales se genera valor al utilizar los insumos, dando lugar a un producto determinado.

▪ **APLICACIONES**: Son programas de computador que están diseñados con capacidades lógicas y matemáticas para procesar información. El término Aplicación se utiliza para agrupar un conjunto de programas que responden a requerimientos particulares del negocio o área de negocio.

- **ARQUITECTURA**: Según ISO/IEC 42010: "Proceso de concebir, expresar, documentar, comunicar, certificar la implementación, mantener y mejorar la arquitectura a través de todo el ciclo de vida de un sistema.

- **ARQUITECTURA EMPRESARIAL**: Es una práctica estratégica (una capacidad) que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones (el negocio, la información, las aplicaciones, la infraestructura, etc.), con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión y/o los objetivos de la entidad.

- **AUTORIZACIÓN**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **BASE DE DATOS**: Conjunto organizado de datos personales que sea objeto de Tratamiento.

- **DATO PERSONAL:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **ENCARGADO DEL TRATAMIENTO**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realiza el tratamiento de datos personales por cuenta del responsable del tratamiento.

- **ESTANDAR**: Regla que específica una acción o respuesta que se debe seguir a una situación dada; son orientaciones obligatorias que buscan hacer cumplir las políticas; se diseñan para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

- **GUÍA**: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- **MADUREZ**: Indica el grado de confiabilidad que el negocio puede tener en un proceso, gracias a la capacidad del mismo para alcanzar las metas y objetivos deseados.

- **MEJOR PRÁCTICA**: Una regla de seguridad específica o una plataforma que es aceptada, en la industria al proporcionar el enfoque más efectivo para una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad en la entidad.

- **PAE - Programa de Alimentación Escolar**: El Programa de Alimentación Escolar consiste en el suministro organizado de un complemento nutricional con alimentos, a los niños, niñas y adolescentes matriculados en el sistema educativo público, y el desarrollo de un conjunto de acciones alimentarias, nutricionales, de salud y de formación, que contribuyen a mejorar el desempeño de los escolares y apoyar su vinculación y permanencia en el sistema educativo.

- **Plan Nacional de Desarrollo - PND**: Documento base que establece los lineamientos estratégicos de las políticas públicas formuladas por el Presidente de la Republica a través de su equipo para su periodo de gobierno. Su elaboración, socialización, evaluación y seguimiento es responsabilidad directa del DNP. El marco legal que rige el PND está consignado dentro de la ley 152 de 1994, por la cual se estableció la Ley Orgánica del Plan de Desarrollo.6

- **PETI**: Plan Estratégico de Tecnologías de la Información y las Comunicaciones.

- **POLÍTICA:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

- **PROCEDIMIENTO**: Los procedimientos definen específicamente las actividades a realizar de manera ordenada en concordancia con las políticas, estándares, mejores prácticas y guías. Los procedimientos son independientes de la tecnología y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema; los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

- **RESPONSABLE DEL TRATAMIENTO**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

- **SGSI**: Sistema de Gestión de Seguridad de la Información.

- **TIC**: Tecnologías de la Información y las Comunicaciones.

- **TITULAR**: Persona natural cuyos datos personales sean objeto de Tratamiento.

- **TRATAMIENTO**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Establecer la Política de Seguridad de la información, tratamiento y protección de datos personales como referente para el manejo, uso, procesamiento, recibo, recolección, almacenamiento, circulación, actualización, transmisión y/o generación de la información de la UApA, con el fin de minimizar los riesgos asociados y mantener la integridad, disponibilidad y confidencialidad al interior de la Entidad.

Esta política está compuesta de lineamientos de seguridad que serán entregados y actualizados conforme exista mayores niveles de madurez en la entidad y también cuando se presenten cambios regulatorios que ameriten su actualización.

4.2. ALCANCE

La presente política se debe aplicar en cada una de las áreas de trabajo de la UApA y debe ser de conocimiento de los directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la Unidad, en especial para quienes:

- Accedan a información de la UApA.
- Operen equipos informáticos y/o de comunicaciones dentro de la red de la Unidad.

- Diseñen, construyan, prueben y/o utilicen sistemas de información, bases de datos o servicios colaborativos de la UApA.
- Accedan de manera física o lógica a las instalaciones.
- Directivas y demás roles de máxima autoridad de la UApA que atiendan procesos que soportan la política de Alimentación Escolar.

5. ORGANIZACIÓN

La coordinación de las actividades referidas a la gestión de la Política de seguridad de la Información y protección de datos personales, serán lideradas por la Subdirección de Información y apoyadas por la Subdirección de Gestión Corporativa y Oficina de Planeación de la Unidad.

6. VIGENCIA, RESPONSABILIDADES Y ACTUALIZACIÓN DE LA POLITICA

Es responsabilidad de la Subdirección de Información realizar todas las acciones relacionadas con la seguridad de la información y continuidad de la operación. De esta manera, deberá realizar las acciones para su implementación, mantenimiento, actualización y supervisión de esta política, así como de brindar asistencia técnica seguridad informática y de comunicaciones hacia las dependencias de la UApA.

Cualquier excepción a lo establecido en esta política, deberá contar con la aprobación formal del Comité de Desarrollo Institucional de la Unidad Administrativa Especial de Alimentación Escolar. Mediante resolución interna y con la publicación en la intranet de la versión aprobada de este documento, donde entra en vigencia la Política de seguridad de la Información y protección de datos personales y se entiende incorporada a las obligaciones de los directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la UApA.

Esta política es de estricto cumplimiento y su desacato se considerará un incidente de seguridad que, dependiendo de la gravedad, dará lugar a un proceso disciplinario en el caso de los funcionarios y causal válida de terminación de contrato con los terceros, sin perjuicio de la iniciación de otro tipo de acciones.

La política seguirá un proceso de revisión y actualización periódica, como mínimo una vez al año, y para esto se tendrán en cuenta los resultados de la Arquitectura Empresarial, las modificaciones a la infraestructura tecnológica, los cambios

organizacionales, culturales del entorno y operativos, y las normas que se expidan al respecto.

7. DECLARACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

7.1 Consideraciones transversales en Seguridad de la Información

La protección de la información en la Unidad de Alimentación Escolar, busca la disminución del impacto que generan sobre sus activos los riesgos identificados de manera sistemática; su propósito es mantener un nivel de exposición que permita responder por la integridad, la confidencialidad y la disponibilidad de la información, acorde con las necesidades de los diferentes grupos de interés identificados, mediante el cumplimiento normativo e implementación de un sistema de gestión de seguridad de la información - SGSI, planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del mismo.

Bajo este contexto, a continuación se describe la situación objetivo para gestionar la seguridad y habilitar las actividades relacionadas con la arquitectura de información de la UApA, con la cual se podrán estructurar proyectos orientados a explotar el valor de los datos para generar información y conocimiento de manera segura.

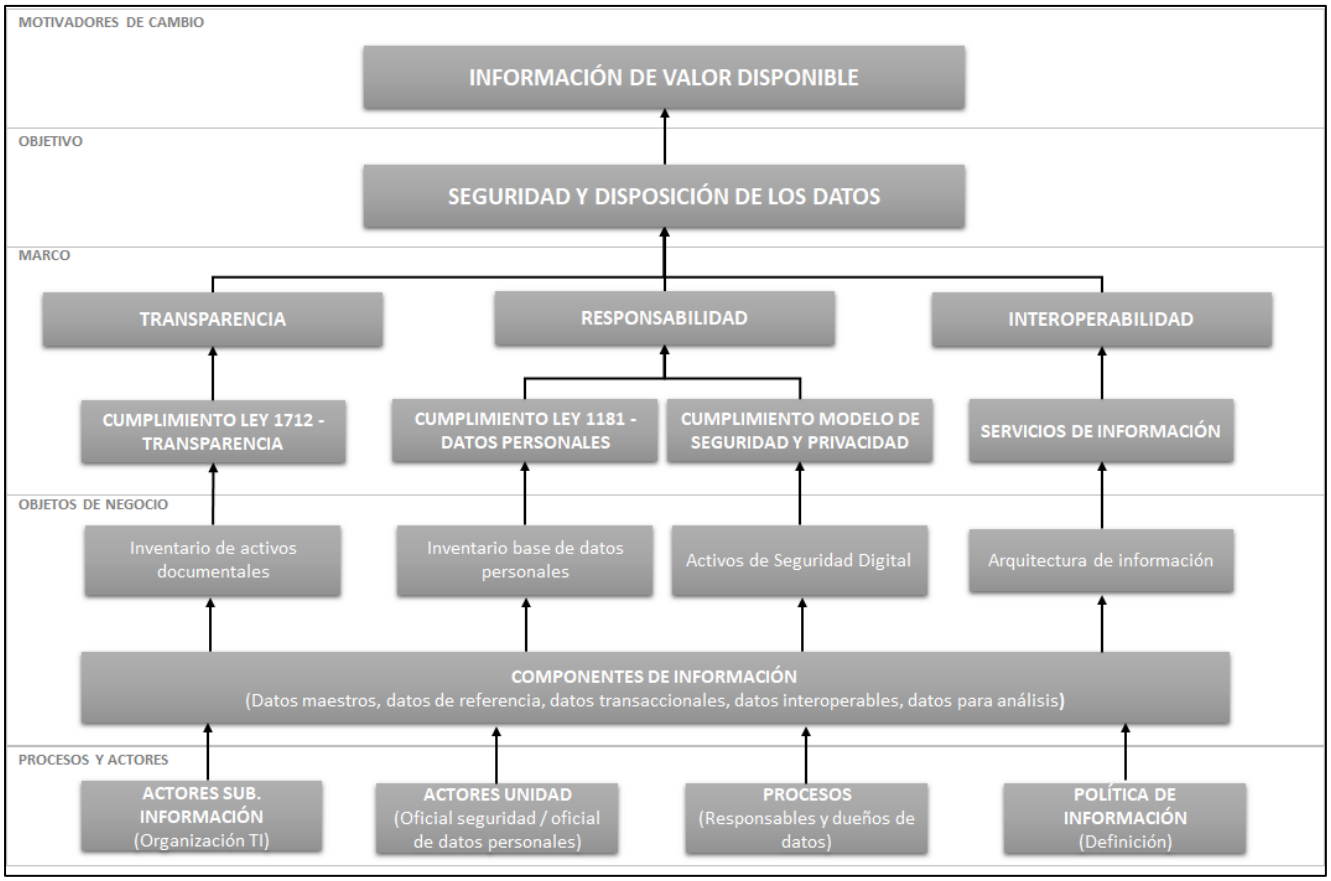

Diagrama No. 1. Situación objetivo de la gestión de información segura UAPA
(Elaboración propia, Equipo Sub. Información - 2021)

En esta misma línea, el desarrollo de las acciones y la toma de decisiones con relación al SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la UApA.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función pública en su Ley de Transparencia.
- Mantener la confianza de los usuarios, socios estratégicos y servidores públicos.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la cultura de seguridad de la información en los funcionarios, contratista, colaborador o tercero de la Unidad.

- Garantizar la continuidad del negocio frente a incidentes.

- Definir, implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información.

- La UApA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos, del riesgo que se genera por los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- La Unidad protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La UApA protegerá su información de las amenazas originadas por parte del personal encargado de su administración, manejo y custodia.

- La Unidad protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La UApA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- La Unidad implementará control de acceso a la información, sistemas y recursos de red.

- La UApA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- La Unidad garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- La UApA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- La UApA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7.2 Consideraciones transversales en protección de datos

El responsable de tratamiento y protección de datos será:

- Entidad: Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender.
- Dirección: Calle 24 No.7-43, Bogotá, Colombia
- Página Web: www.alimentosparaaprender.gov.co
- Correo electrónico: info@alimentosparaaprender.gov.co, atencionalciudadano@alimentosparaaprender.gov.co

De acuerdo con lo anterior, la UApA será responsable del tratamiento y protección de los datos personales que registren y almacenen y hará uso de estos únicamente para las finalidades para las que se encuentra legalmente facultado y en especial las señaladas a continuación, contando previamente con la autorización del titular de los datos personales:

- Para los fines administrativos y misionales de la Entidad.

- Caracterizar ciudadanos y grupos de interés, para adelantar estrategias de mejoramiento en los trámites y en la prestación del servicio.

- Gestionar y dar respuesta a las peticiones, quejas, reclamos, denuncias, sugerencias y/o felicitaciones presentados a la Unidad.

- Conocer y consultar la información del titular del dato que repose en las bases de datos de entidades públicas o privadas.

- Adelantar encuestas de satisfacción de usuarios.

- Enviar información de interés general.

- Enviar mensajes con contenidos institucionales, notificaciones, información relevante para el titular y demás información relativa al portafolio de servicios de la Unidad, a través de correo electrónico y/o mensajes de texto al teléfono móvil.

Nota. Cualquier otro tipo de finalidad que se pretenda dar a los datos personales registrados por la Unidad, deberá ser informado previamente en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato, según sea el caso, teniendo en cuenta los principios legales para el tratamiento de los datos personales.

De igual manera y tomando como base la ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, se definen unas políticas técnicas detalladas que, de ahora en adelante se llamarán **Lineamientos.**

Los Lineamientos de Seguridad de la Información, Tratamiento y Protección de Datos Personales, que se desarrollan para la presente política, son parte integral del SGSI y contemplan los aspectos relacionados con:

- Finalidad de los datos
- Derechos de los titulares de los datos personales.
- Responsables de Gestionar las peticiones, quejas y reclamos sobre el tratamiento de datos personales.
- Gestión de la Política de tratamiento y protección de datos
- Actualización y rectificación de datos
- Datos Personales de niños, niñas y adolescentes
- Datos personales sensibles
- Supresión de datos
- Almacenamiento de datos personales
- Modificaciones a las Políticas de tratamiento de datos personales
- Revelación de la Información

En caso de requerir actualización, rectificación, supresión, tener alguna queja o reclamo, los canales de comunicación y el procedimiento para su solicitud se definen en el documento de lineamientos.

7.3. Organización interna en seguridad de la información y protección de datos

Se deberá conformar gradualmente un grupo interdisciplinar para la implementación del gobierno de TI, la gestión de los datos institucionales y demás componentes propios del modelo seguridad de la información. De esta manera, estarán involucradas al menos las siguientes áreas o perfiles:

- Subdirector de Información o su delegado
- Oficial de seguridad de la información
- Oficial de protección de datos personales
- Líder de gestión de información
- Subdirector de Gestión Corporativa y/o Líder de Gestión Documental
- Asesor de Planeación o su delegado.

7.4. Plan de implementación de la seguridad de la información y protección de datos

El modelo de seguridad y privacidad de la información contemplará un ciclo de operación que consta de cinco fases;

1. Diagnostico.
2. Planear.
3. Implementación.
4. Evaluación desempeño.
5. Mejora Continua.

Dicho modelo permiten que la entidad pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información. Así mismo, se realice la implementación de los controles definidos anteriormente.

Por otro lado, se deberá tener en cuenta que dentro del modelo de Gobierno de TI y SGSI, para el cumplimiento de los principios y políticas de TI, se definen políticas y técnicas detalladas, que conforme al modelo de Gobierno de TI diseñado para la UapA, proporcionan lineamientos generales.

Dichos lineamientos de Seguridad de la Información contemplan los aspectos relacionados con:

- Gestión de activos.
- Seguridad física y ambiental.
- Control de accesos.
- Comunicaciones.
- Operaciones.
- Control de acceso a la información.
- Llaves criptográficas (Firma Digital y certificados SSL).
- Intercambio de información.
- Computación en la nube.
- Dispositivos móviles.
- Relaciones con proveedores.
- Teletrabajo.
- Escritorio Limpio y Pantalla Limpia.
- Copias de respaldo.
- Desarrollo de software.
- Protección de datos personales.
- Correo electrónico.
- Acceso a Internet.
- Uso aceptable de activos de información.
- Traiga su propio dispositivo (BYDO).
- Gestión para la protección y tratamiento de datos personales.

Los documentos que establecen dichos lineamientos serán realizados, socializados y gestionados por la Subdirección de Información y su generación será acorde al avance en la implementación de SGSI y Plan Estratégico de Tecnologías de Información – PETI.

8. CUMPLIMIENTO

8.1. Cumplimiento de las Obligaciones Legales

Los directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la Unidad, deben cumplir con la legislación aplicable en la materia.

8.2. Derechos de propiedad intelectual

Los directivos, funcionarios, contratistas, proveedores, colaboradores y terceros que presten sus servicios o tengan alguna relación con la Unidad, deben cumplir con la reglamentación de propiedad intelectual. La Unidad realizará revisiones periódicas para cerciorarse que se cumplan los lineamientos sobre derechos de propiedad intelectual.

8.3. Revisiones de Seguridad de la Información

La Subdirección de Información será responsable de la ejecución del Sistema de Gestión de Seguridad de la Información y tratamiento de datos personales, esto en el marco de los procesos definidos en el Sistema Integrado de Gestión Institucional de la Unidad, por lo cual, podrá realizar o delegar, la verificación del cumplimiento de esta política, mediante revisiones periódicas a la ejecución de los procesos y procedimientos, dentro del marco de las políticas, normas y cualquier otro requisito de seguridad aplicable.

HISTORIAL DE CAMBIOS

VERSIÓN	OBSERVACIONES	FECHA
1	Se crea el documento	Febrero de 2021