PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

PROCESO: Gestión de la Información

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR

BOGOTÁ D.C, ENERO 2021

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender para la vigencia 2021, se define atendiendo las directrices del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, las líneas operacionales de seguridad de la entidad y las siguientes funciones:

- Diseñar y gestionar el sistema de información del Programa de Alimentación Escolar y articularlo con los sistemas de información públicos que recogen datos relativos a la política de alimentación escolar, y su implementación en el territorio.

- Brindar asistencia técnica a las eentidades tterritoriales para la adecuada implementación de la política de alimentación escolar.

- Establecer canales de comunicación para facilitar la gestión del conocimiento sobre la implementación de la política de alimentación escolar en campo, para identificar las particularidades de los diferentes contextos regionales y promover la transferencia de buenas prácticas y lecciones aprendidas entre entidades territoriales.

- Promover la participación ciudadana o cualquier otra modalidad de control social que constituya o integre la ciudadanía, para que contribuyan a la transparencia en la prestación del servicio de alimentación escolar en el país.

- Absolver consultas en relación con la aplicación de normas sobre alimentación escolar y expedir lineamientos para su implementación.

- Difundir las políticas públicas, planes, programas, normas, instrumentos y herramientas que faciliten la implementación de la política de alimentación escolar.

Por lo anterior, la entidad a través de la Subdirección de Información, emprenderá acciones orientadas a la gestión y protección de la información, en el marco del Plan de acción institucional y del Sistema Integrado de Gestión.

2. MARCO NORMATIVO

El Estado colombiano cuenta con normatividad vigente, que obliga al adecuado tratamiento de la información manejada por las entidades del estado en términos de confidencialidad, integridad y disponibilidad. Entre los documentos de referencia se citan:

- **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 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.

- **Resolución 2999 del 2008.** Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.

- **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 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.

- **Ley 1437 de 2011.** Capítulo IV, “utilización de medios electrónicos en el procedimiento 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.

- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.

- **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 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **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 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- **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.

- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.

- **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 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.

- **Ley 2015 de 2018.** Por la cual se modifica la Ley 23 de 2082 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- **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.

- **Ley 2052 de 2020.** Por medio de la cual se expide el código general disciplinario.

- **Ley 2055 de 2020.** Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".

3. OBJETIVO

Establecer las actividades del Modelo de Seguridad y Privacidad de la Información que manejará la Unidad Administrativa Especial de Alimentación Escolar - Alimentos para Aprender, a través de la implementación sistemática de las políticas y controles de seguridad digital, en el marco del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC.

3.1. OBJETIVOS ESPECÍFICOS

- Establecer las políticas, lineamientos, buenas prácticas y recomendaciones de seguridad de la información en la entidad y con las partes interesadas.

- Definir los lineamientos necesarios para el manejo de la información tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.

- Constituir del Modelo de Seguridad y Privacidad de la Información.

- Mitigar los incidentes de seguridad y privacidad de la información, y de seguridad digital de forma efectiva, eficaz y eficiente.

- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información.

- Generar conciencia para el cambio organizacional requerido para la apropiación de la seguridad y privacidad de la información.

- Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

- Definir controles de seguridad que permitan fortalecer el aseguramiento de la información en las entidades territoriales, departamentos y municipios, donde tiene alcance la Unidad.

4. ALCANCE

Las disposiciones contenidas en la política de seguridad de la información y las políticas complementarias, aplican para todos los procesos de la entidad (estratégicos, misionales, y de apoyo) que son soportados en la sede central, entidades territoriales, y demás escenarios en donde se desarrollen actividades de la Unidad tales como: el teletrabajo y trabajo en casa, la gestión de proveedores y terceras partes interesadas, que dependan o interactúen con la misma.

Adicionalmente, aplica a toda la información creada, procesada y respaldada de los diferentes procesos, sin importar el medio, formato, presentación o lugar en el cual se encuentre; incluyendo, pero no limitando a:

- Información de bases de datos, computadores, dispositivos de almacenamiento masivo.

- Respaldo en centros de datos.

- Almacenamiento en la nube Pública o Privada.

- Información transmitida a través de redes públicas o privadas.

- Información impresa o escrita a mano en papel o en tableros u otro medio semejante.

- Información enviada por Scanner/fax o por cualquier otro medio similar.

- Archivo físico.

- Información grabada a través de los diferentes medios de comunicación y vigilancia.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Unidad entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La protección de la información, pretende la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la

disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI, estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- 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, terceros, aprendices, practicantes y clientes de la entidad.
- Garantizar la continuidad del negocio frente a incidentes.

- La Unidad ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades y a los requerimientos regulatorios.

6. PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SISTEMA DE GESTIÓN Y DE SEGURIDAD DE LA INFORMACIÓN

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

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

- Se 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 Subdirección de Información protegerá la información de las amenazas originadas por parte del personal.

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

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

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

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

- Se garantizarán a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva del modelo de seguridad.

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

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

7. DISEÑO

7.1. DESCRIPCIÓN DE ACTIVIDADES

En la Subdirección de Información de la Unidad se adopta el MSPI Modelo de Seguridad y Privacidad de la Información de MinTIC, como guía para la construcción del Subsistema de Gestión de Seguridad de la Información - SGSI, modelo basado en el Marco de Referencia de Arquitectura TI, el cual fue propuesto para el desarrollo de las arquitecturas empresariales sectoriales, institucionales y territoriales, convirtiéndose en el soporte para la transformación de la Estrategia de Gobierno en Línea a la nueva Política de Gobierno Digital.

Este modelo contempla un ciclo de operación que consta de cinco (5) fases:

1. Diagnostico: en esta fase se identifica el estado actual de la organización para determinar las actividades que se deben tener en cuenta para avanzar en la implementación y mejora del MSPI.

2. Planificación: en este paso se tienen en cuenta el contexto de la Entidad, los procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, plan de comunicaciones y las interrelaciones del modelo con otros procesos.

3. Implementación: en esta fase se llevará a cabo lo descrito en la fase de planificación, donde se deberán implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan ejecutar acciones determinadas en el plan de tratamiento de riesgos. Por otra parte, se definirán y establecerán indicadores de gestión que medirán la efectividad, eficiencia y eficacia de las acciones implementadas en seguridad de la información.

4. Evaluación de Desempeño: en este paso se realizará el monitoreo, medición, análisis y evaluación de las acciones implementadas, así como también las auditorías internas al Sistema de Gestión de Seguridad de la Información - SGSI.

5. Mejora continua: en esta etapa se consolidarán los resultados obtenidos en la fase de evaluación de desempeño, para diseñar el plan de mejoramiento dirigido la seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas, cerrando de esta forma el ciclo.

8. METAS

- Establecer el estado actual y nivel de madurez a través de un diagnóstico al Subsistema de Gestión de Seguridad de la Información - SGSI, a través de la implementación de indicadores.

- Establecer las principales líneas de acción a seguir en el corto y mediano plazo, para la implementación y mantenimiento del SGSI.

- Mejorar continuamente el Sistema de Gestión de Seguridad de la Información, a partir de la evaluación de la eficacia de los controles asociados a los activos de información y demás herramientas del Sistema.

9. MEDICIÓN

La medición se realizará de manera proporcional por cobertura de aplicación en los procesos, servicios, sistemas de información, bases de datos, servidores o canales de comunicación de la entidad, relacionados con el determinado control.

- **Nivel 1:** Inexistente.
- **Nivel 2:** Inicial 20%: si la Entidad reconoce la necesidad de implementar el MPSI
- **Nivel 3:** Repetible 40%: si los procedimientos y controles se ejecutan de manera no oficial, pero regularmente.
- **Nivel 4:** Efectivo 60%: Si los procedimientos y controles están documentados y comunicados.
- **Nivel 5:** Gestionado 80%: Si se miden los procedimientos y controles.
- **Nivel 6:** Optimizado 100%: si los procedimientos y controles se aplican como mejor práctica y siguen la mejora continua.

10. PLAN DE TRABAJO

El logro de los objetivos específicos definidos en el presente documento, requiere la definición de actividades detalladas y categorizadas, según el ámbito de ejecución indicado en la siguiente tabla.

ACTIVIDADES	ENTREGABLES	ESTADO	FECHA DE FINALIZACIÓN
Diagnostico: identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información	Herramienta de diagnostico	Abierto	30/06/2021
Política de Seguridad y Privacidad de la Información: desarrollar las Políticas de Seguridad y Privacidad de la Información.	Políticas de Seguridad y Privacidad de la Información	Abierto	31/03/21
Procedimientos de Seguridad: generar el plan de trabajo para la creación, formalización y divulgación de los procedimientos asociados a seguridad de la información relacionados en el MSPI y que apliquen a Alimentos para Aprender	Documento plan con las actividades relacionadas a la creación de los procedimientos de seguridad de la información.	Abierto	31/05/21
Alta dirección: desarrollar la resolución, donde se establece la política de seguridad y privacidad de la información de UApA	Acto administrativo a través del cual se crea la resolución, donde se establece la PSPI	Abierto	31/07/21

Plan de Riesgos: identificación de riesgos en la Unidad y generación del plan de tratamiento de los mismos	Documento plan de riesgos	Abierto	31/08/21
Plan de sensibilización y comunicación: mesas de trabajo con las diferentes subdirecciones, comunicación de los hallazgos de seguridad a los colaboradores y dependencias, actividades de sensibilización SGPI	Actas de las mesas de trabajo, documento plan de sensibilización y comunicación	Abierto	31/08/21
Protección de datos personales: desarrollar la política de protección de datos y establecer los controles que se requieran de acuerdo la lo requerido por la ley	Política de protección de datos personales	Abierto	30/09/21
Plan de tratamiento de datos: recolección y revisión de bases de datos, así como también registro y actualización	Bases de datos, documento de revisión y actualizaciones de las bases de datos	Abierto	30/07/21
Activos de Información: desarrollar los activos de Información y determinar los responsables para establecer controles de acuerdo con la criticidad del activo	Matriz de identificación y valoración de los activos de información	Abierto	31/10/21
Evaluación de desempeño: incluir en el alcance de la auditoría interna, los avances del SGPI	Documento con el plan de ejecución de auditorías del SGSI	Abierto	30/11/21

Mejora continua: plantear el plan de mejoramiento Continuo	Plan de mejoramiento	Abierto	30/11/21
Gestión de Incidentes: elaboración del procedimiento de gestión de incidentes de Seguridad	Plan de gestión de incidentes	Abierto	31/08/21
Eventos de vulnerabilidad: realizar informes de eventos asociados al SGSI	Informes de vulnerabilidad	Abierto	31/12/21
Gestión de Cambio: elaborar el plan de gestión del cambio y cultura de seguridad y privacidad de la información	Plan de gestión del cambio y cultura de seguridad y privacidad de la información	Abierto	30/11/21
Requisitos legales: creación de la matriz de requisitos legales de seguridad de la información	Matriz de requisitos legales	Abierto	30/03/21
Gobierno Digital: desarrollar el documento de diagnostico de la entidad en la implementación de Seguridad y privacidad de la información	Documento diagnostico	Abierto	30/05/21

HISTORIAL DE CAMBIOS

VERSIÓN	OBSERVACIONES	FECHA
1	Se crea el documento	Enero de 2021