PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
2022

PROCESO: GESTIÓN DE LA INFORMACIÓN

UNIDAD ADMINISTRATIVA ESPECIAL DE ALIMENTACIÓN ESCOLAR

BOGOTÁ D.C, ENERO 2022

1. Introducción

El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender está consolidándose bajo la línea de identificación y clasificación de activos de información, los marco normativos y mejores prácticas aplicables. De esta manera, se tiene identificado el "dato" como uno de los activos más valiosos y primordiales, sobre la cual se debe velar porque se conserven los principios de disponibilidad, integridad y confidencialidad, además, con los atributos de que sea oportuno, responsable y seguro.

Bajo este contexto, es importante mencionar que la gestión de los datos ha evolución a tal medida de transformarse en la inteligencia de información de las Entidad, y en el caso de la Unidad no es la excepción, razón por la cual, se debe tener en cuenta que, las amenazas que atentan actualmente contra las infraestructuras tecnológicas y demás procesos de control de seguridad y privacidad de la información han incrementado de manera considerable. Por lo tanto, es evidente que la materialización de los riesgos sobre los activos de información no solo puede generar costos económicos, legales y afectación de su buena imagen, sino que pueden afectar la continuidad del negocio.

La Unidad es consciente de que la protección y aseguramiento de la información que recopila, almacena, gestiona y produce, debe estar bajo un gobierno de TI, estrategia de TI y marco normativo de un Sistema de Gestión Seguridad de la Información con principios, políticas, lineamientos, responsabilidades y obligaciones, para que la Alta Dirección y colaboradores se concienticen del tratamiento necesario para el manejo de la seguridad y privacidad de la información.

En términos generales, con este plan la Unidad busca garantizar que la gestión de los riesgos de seguridad de la información, sean aquellos procesos que reduzcan las pérdidas, permitan la continuidad de la operación y brinden la protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida los procesos de negocio y estar en continuo mejoramiento y evolución.

Finalmente, el presente documento representa la base estructurada del Plan para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la Unidad.

2. Marco normativo

El plan de tratamiento de riesgos de seguridad y privacidad de la información de la Unidad Administrativa Especial de Alimentación Escolar – Alimentos para Aprender, contempla el siguiente marco normativo y mejores prácticas:

- **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 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 1955 de 2019.** Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".

➢ **Decreto 1078 de 2015.** Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.

➢ **Decreto 1499 de 2017**. el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

➢ **Decreto 612 de 4 de abril 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.

➢ **CONPES 3854 de 2016.** Política de Seguridad Digital del Estado Colombiano.

➢ **CONPES 3995 de 2020.** - Política Nacional De Confianza y Seguridad Digital.

➢ **ISO/IEC 27001.** Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de la Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la norma ISO 27002.

➢ **Guía.** Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital año 2020.

➢ **Gobierno Digital.** Estrategia MINTIC, gobierno en línea.

3. Antecedentes

El Gobierno Nacional mediante la Ley 1955 de 2019, expidió el Plan Nacional 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 y mediante Decretos Nacionales 218 y 219 de febrero de 2020, creó la estructura interna de la Entidad y su planta de personal respectivamente; lo que generó que la Entidad iniciara su funcionamiento en el mes de Marzo de 2020 y su operatividad financiera en el mes de Junio de 2020 una vez perfeccionados las gestiones financieras pertinentes ante el Ministerio de Hacienda y Crédito Público.

Por lo anterior, la Subdirección de Información considera que parte de la vigencia 2021 corresponde a un periodo de estructuración, engranaje y consolidación de todos los componentes procedimentales, normativos y tecnológicos de seguridad y privacidad de la información que requiere la entidad, alineado con los planes, programas y proyectos Institucionales.

4. Objetivos

4.1. Objetivo General

Proveer un instrumento con los principios, políticas, lineamiento y mapa de ruta, para el análisis, valoración y tratamiento de los riesgos de seguridad, para el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y cumplimiento normativo en esta materia de la Unidad de Alimentación Escolar del sector educación.

4.2. Objetivos Específicos

- Definir las etapas para establecer la estrategia de seguridad de la información de la Unidad.

- Establecer los lineamientos para la implementación y/o adopción de mejores prácticas de seguridad de la información en la Unidad.

- Definir el modelo de gestión de los eventos de seguridad de la información, seguridad digital, ciberseguridad y continuidad de la operación, para detectar y tratarlos con eficacia y eficiencia, al igual que identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.

- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.

- Identificar, clasificar y mantener actualizado los activos a proteger en la Unidad.

- Identificar las principales amenazas que afectan a los activos.

- Fortalecer la cultura, conocimiento y aplicación en los temas de seguridad y privacidad de la Información en la Unidad.

5. Definiciones

- **Activos de información:** son los recursos necesarios para que una empresa o un negocio funcione y consiga los objetivos que se ha propuesto la alta dirección. (ISO 27001). En relación con la privacidad y seguridad 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 (MSPI - MINTIC). Son, entre otros, las bases de datos, los archivos, los manuales, las aplicaciones, así como el hardware y software que se tiene la Unidad para desarrollar su objeto.
- **Auditoria:** proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del MSPI de una organización.
- **Confidencialidad:** propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** propiedad de la información de ser accesible, utilizable y recuperable a demanda por una entidad.
- **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. En este documento se habla de las Norma Técnica Colombiana ISO27001:2013 e ISO31000:2019.
- **Gestión de riesgos:** proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Incidente de seguridad de la información:** resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.
- **Integridad:** propiedad de la información de ser completa, exacta e inalterada exactitud y completitud.
- **Información**: es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **Inventario de activos:** lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten ser protegidos de potenciales riesgos.
- **ISO 27001:** estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Política de Gobierno Digital.
- **Plan de continuidad del negocio (BCP):** orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles para proteger la misma.
- **Política de seguridad de información:** es el instrumento que adopta una entidad para definir las reglas de comportamiento aceptables en el uso y tratamiento de la información.
- **Riesgo de seguridad y privacidad:** potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.
- **Sistema de Gestión de Seguridad de la Información:** parte del sistema de gestión general de la Unidad, se basa en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

6. Alcance

El Plan de Seguridad de la Información, abarca la definición, identificación y tratamiento de los riesgos de seguridad de la información como lineamiento del nivel Directivo de la Unidad, el cual será de estricta aplicabilidad y cumplimiento por parte de todos los funcionarios, contratistas y terceros que presten sus

servicios o tengan algún tipo de relación con la Entidad; dicho tratamiento de riesgo involucra a todos los procesos de negocio desarrollados por la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos.

7. Metodología A Utilizar

Al ser una entidad en proceso de construcción y consolidación, la definición e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en el ejercicio armónico de: (1) El ciclo PHVA (Planificar, Hacer, Verificar, Actuar); (2) Lo establecido en el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC; y (3) Mejores prácticas y aspectos de la norma ISO 27001. Todo esto se ilustra a continuación:

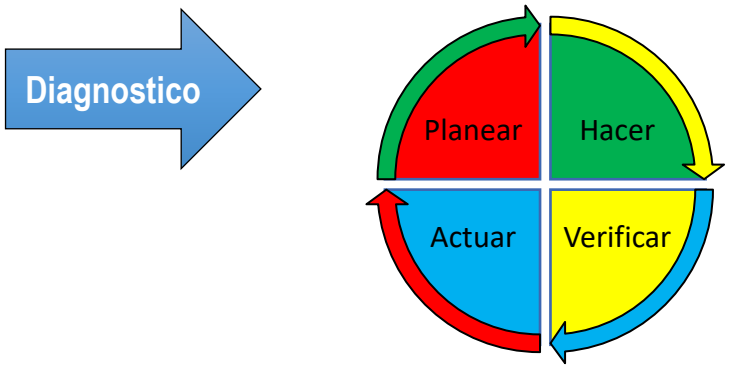

Ilustración N°1. Ciclo PHVA (Elaboración con información pública de la web: https://www. http://www.escolme.edu.co/

Ilustración N° 2. Modelo MSPI (https://www.mintic.gov.co)

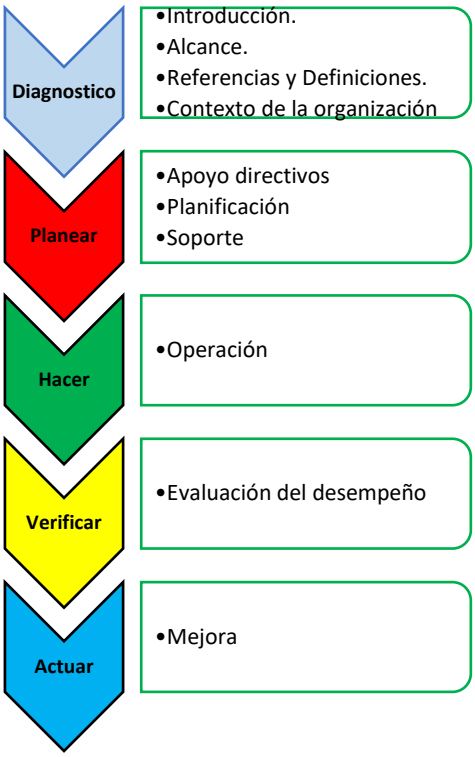

Ilustración N° 3. Modelo ISO 27001, alienado al ciclo de mejora continua (https://www.iso.org)

De manera detallada, la Unidad llevara a cabo las siguientes fases como ciclo de operación para la definición y establecimiento:

- Fase Diagnostico: Permite identificar el estado actual de la Unidad, con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planear: Se establecen los objetivos a alcanzar y las actividades susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- Fase Hacer: Se ejecuta el plan establecido que consiste en implementar las acciones para lograr las mejoras planteadas en la fase de planear.
- Fase Verificar: Una vez implantadas las mejoras, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas en la fase del hacer.
- Fase Actuar: Se analizan los resultados de las acciones implementadas y si estas no cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones, dando un diagnóstico y un nuevo punto de partida en la fase del planear.

Bajo este marco y fases establecidas, es importante mencionar que si bien la norma ISO 27001:2013 (Ilustración N° 3) no determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la estructura de su última versión puede alinearse con el ciclo de mejora continua de los modelos de gestión. De esta manera, trasladando las necesidades del SGSI, al ciclo PHVA definido por la ISO 27001, tendrían las siguientes acciones asociadas:

FASES	ACCIONES
PLANEAR	• Definir la política de seguridad. • Establecer al alcance del SGSI. • Realizar el análisis de riesgos. • Seleccionar los controles. • Definir competencias. • Establecer un mapa de procesos. • Definir autoridades y responsabilidades.
HACER	• Implantar el plan de gestión de riesgos. • Implantar el SGSI. • Implantar los controles de seguridad. • Administrar los dispositivos de seguridad.
VERIFICAR	• Revisar internamente el SGSI. • Realizar auditorías internas del SGSI. • Poner en marcha indicadores y métricas. • Hacer una revisión por parte de la Dirección.
ACTUAR	• Adoptar acciones correctivas • Adoptar acciones de mejora

En cualquier caso, La Unidad ha determinado que el presente plan se dará por cumplido cuando se realicen todas las fases del ciclo de la metodología y el tiempo se determinará una vez iniciado cada fase, componentes o ciclo abordado.

8. Plan de actividades por componente, del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Unidad.

A continuación, se relacionan las actividades por componente:

Componente No. 1 – Activos de información.

➢ Definición y establecimiento de los instrumentos, lineamientos y estrategias para el levantamiento y etiquetado de los activos.
➢ Identificación de activos de los procesos de negocio.
➢ Clasificación y valoración de los activos.
➢ Definición y/o actualización de Instrumentos de gestión de la información pública
➢ Publicación Instrumentos de gestión de la información pública

Componente No. 2 – Riesgos de Seguridad y Privacidad de la Información.

➢ Análisis

- Identificación de los riesgos de seguridad de la información, asociados a la pérdida de confidencialidad, integridad y disponibilidad.
- Identificación de las amenazas y vulnerabilidades

➢ Evaluación

- Valoración del riesgo inherente (probabilidad e impacto)
- Identificación de controles existentes
- Valoración de los controles existentes
- Valoración del riesgo residual (probabilidad e impacto).

➢ Tratamiento

- Definición del tratamiento de riesgos seguridad de la información
- Identificar los riesgos que no aprueban el nivel aceptable.
- Definir el plan de tratamiento de los riesgos no aceptables
- Seguimiento a la implementación de los planes de tratamiento

Componente No. 3 – Capacitación y sensibilización en Seguridad y Privacidad de la Información.

➢ Definición del plan de capacitación y sensibilización en seguridad y privacidad
➢ Implementación del plan de concienciación en seguridad y privacidad.
➢ Apropiación de la cultura en temas seguridad y privacidad de la información.
➢ Análisis de resultados del plan de socialización.

Componente No. 4 – Protección de datos personales

➢ Estructuración y definición del manual de protección de datos personales
➢ Seguimiento a la implementación del manual de protección de datos personales

Componente No. 5 – Sistema de Gestión de Seguridad de la Información.

➢ Definición y establecimiento de la Políticas de Seguridad, en el marco del Sistema de Gestión de Seguridad de la Información.
➢ Definición de lineamientos de seguridad como apoyo a la ejecución de los procesos
➢ Revisión de los controles de la norma ISO 27001:2013
➢ Revisión por la Dirección General y nivel Directivo
➢ Establecimiento del plan de Auditorias al Sistema de Gestión de Seguridad de la Información.
➢ Definición de los planes de mejoramiento en relación con los resultados de las auditorías.
➢ Ejecución de las actividades de los planes de mejoramiento correspondientes al SGSI
➢ Definición, seguimiento y medición de los procesos, procedimientos y/o actividades institucionales que implementen controles de seguridad.

➢ Implementación de los procedimientos para la gestión de incidentes y eventos de seguridad de la Información
➢ Definición, reporte de indicadores y generación de alertas tempranas, asociadas al Sistema de Gestión de Seguridad de la Información
➢ Seguimiento al cumplimiento de los indicadores internos del SGSI.

Componente No. 6 – Continuidad de negocio.

➢ Realizar el análisis de impacto al negocio – BIA para los activos críticos de la DTI
➢ Definir los escenarios de afectación para los servicios de TI
➢ Definición del plan de continuidad de TI
➢ Realizar la planeación y ejecución de las pruebas definidas en el plan de continuidad de TI
➢ Analizar los resultados de la aplicación de la estrategia de continuidad de TI y gestionar las acciones de mejora identificadas con el fin de fortalecer los planes y documentación
➢ Participar en las mesas de trabajo para identificar los aspectos de seguridad de la información que aplican para la definición del plan de continuidad del negocio.

Componente No. 7 – Consolidación, aplicación y estructura organizacional.

➢ No conformidades y acciones correctivas
➢ Mejora continua/Certificación del Sistema de Gestión de Seguridad de la Información – SGSI/Cumplimiento de ley de tratamiento de datos personales.
➢ Establecimiento institucional del SGSI.

HISTORIAL DE CAMBIOS

VERSIÓN	OBSERVACIONES	FECHA
0	Diseño del plan institucional para la vigencia 2022, en atención a los lineamientos del Decreto 612 de 2018	Enero de 2022