Diseño de un SGSI basado en la ISO/IEC 27001 para el liceo Moderno José Celestino Mutis de San Sebastián de Mariquita

Elaborado por:

Héctor Fabio Amaya Díaz

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnologías de la Información

2022

Diseño de un SGSI basado en la ISO/IEC 27001 para el Liceo Moderno José Celestino Mutis de San Sebastián de Mariquita

Elaborado por:

Héctor Fabio Amaya Díaz

Asesor:

Andrés Felipe Millán Cifuentes

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería – ECBTI

Maestría en Gestión de Tecnologías de la Información

2022

Dedicatoria

Este trabajo está dedicado a la memoria de mi madre Rosita Diaz de Amaya y a mi padre Pablo Emilio Amaya, por ser mi motivación para superarme personal y profesionalmente, porque sus recuerdos siempre estarán conmigo hasta el día que Dios me lleve con ellos.

Resumen

Las entidades públicas que desean ajustarse a la Estrategia de Gobierno en Línea requieren adoptar el Modelo de Seguridad y Privacidad de la información planteado por el Ministerio de las TIC, cumpliendo con estándares que permitan controlar sus procesos y salvaguardar la información generada. De la misma manera, este es un referente importante para las organizaciones privadas como las instituciones educativas de carácter privado que son monitoreadas y controladas por el Ministerio de Educación Nacional.

Por este motivo, se presenta el diseño de un Sistema de Gestión de Seguridad de la Información SGSI en el Liceo Moderno José Celestino de San Sebastián de Mariquita. Este proyecto incluye el análisis y diagnóstico de los procesos tanto académicos, como administrativos que se realizan en la institución, identificando los activos de información, los riesgos y su valoración, con el fin de determinar las diferentes estrategias de gestión del riesgo y la selección de los controles de seguridad de la información.

Así mismo, en este proyecto se formularon políticas de seguridad de la información para los activos de información presentes en la organización de estudio aprobadas por el comité de seguridad de la información, que involucran a los diferentes actores interesados de la institución como colaboradores, proveedores, terceros y comunidad en general y a los procesos administrativos y académicos donde estos intervienen.

Palabras Clave: SGSI, ISO 27001, activos de información, Seguridad de la información, Institución Educativa.

Abstract

Government entities that wish to comply with the Colombia´s Online Government Strategy need to adopt the Information Security and Privacy Model proposed by the Ministry of ICT, using standards that allow them to control their processes and information safeguarded. In the same way, this is an important reference for private organizations such as private educational institutions that are monitored and controlled by the Ministry of National Education.

For this reason, the design of an ISMS Information Security Management System is presented at the Liceo Moderno José Celestino in San Sebastián de Mariquita. This project includes the analysis and evaluation of academic and administrative processes that are carried out in the institution, identifying information assets, risks and their evaluation, in order to determine the different risk management strategies and the selection of information security controls.

Likewise, in this project, information security policies were formulated for the information assets present in the study organization and approved by the information security committee, which involve the different stakeholders of the institution such as collaborators, suppliers, third parties and the community in general and the administrative and academic processes where they participate.

Key words: ISMS, ISO 27001, information assets, information security, educational institution.

Tabla de Contenido

Índice de tablas

Índice de figuras

Introducción

La definición de un Sistema de Gestión de Seguridad de la Información SGSI en una institución de educación sea pública o privada, busca identificar los riesgos y elaborar un análisis y evaluación de estos, con el objetivo de formular políticas de seguridad y seleccionar los controles requeridos que salvaguarden la integridad de los activos de información.

Actualmente, las instituciones educativas hacen uso de las tecnologías de la información, como una herramienta que facilita los procesos de aprendizaje en los estudiantes, accediendo a bibliotecas virtuales, uso de software didáctico, además de los procesos de gestión de la institución. Todo esto alineado con los objetivos institucionales y los retos externos como el impacto con el medio ambiente. Por ende, debe tenerse en cuenta que el mal uso de las herramientas tecnológicas, el mal manejo de la información y la falta de cultura en las organizaciones sobre el uso de las Tecnologías de la información, pueden convertirse en riesgos que afectan el cumplimiento de los objetivos institucionales, hasta la integridad de los funcionarios que componen dichas instituciones educativas.

En particular, la información del Liceo Moderno José Celestino Mutis constituye uno de los activos de más valor de la organización, por lo tanto, es de vital importancia, brindarle control, monitoreo y seguridad a esta información, con el fin de evitar, que sea utilizada por otras personas o empresas para actos malintencionados o para obtener ventaja competitiva en el mercado. Por esta razón durante el desarrollo de esta investigación, se comprobó como el diseño de un SGSI apoyado en la norma ISO/IEC 27001 optimiza la gestión de los activos de información de las instituciones de educación. Además, el proyecto permitió aplicar la norma ISO 27001 para la definición del sistema propuesto de gestión de seguridad de la información logrando evidenciar la importancia de este “enfoque sistemático para establecer, implementar,

operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización y lograr sus objetivos comerciales y/o de servicio” (ISO27000.es, s.f.).

Justificación

En el mercado actual de la educación, es imperativo elevar la calidad de las instituciones educativas, lo cual involucra un mejoramiento continuo de los procesos que conforman estas organizaciones. Esto permite alcanzar el logro de misión institucional en la formación de personas y profesionales idóneos.

Como lo manifiesta Benavides y Blandón (2018, p.86), “el gobierno de Colombia incluye en la carta magna de 1991, las normas que reglamentan la educación, por cuanto es importante analizar la relación y los puntos de convergencia entre los requerimientos de seguridad de la información emanados por el MINTIC a través de la estrategia de Gobierno en Línea, el MEN y los requisitos de la norma NTC ISO/IEC 27001”.

Por ende, la aplicación de las mejores prácticas en las organizaciones asegura que las características de seguridad de los sistemas de información que se usan a diario, sean gestionados de una forma estandarizada, garantizando ciertos niveles de calidad. Para que la institución pueda mejorar sus procesos, es necesario implementar tecnologías de información que permitan mejorar la calidad, alcanzando un mayor nivel de eficiencia mediante el diseño de un SGSI.

Dentro de este contexto, la aplicación de políticas de seguridad en la gestión de los activos de información asegura la aplicación de criterios de calidad y se obtienen resultados fiables y válidos, que se soportan en directrices alineadas a las necesidades de la organización y a los requerimientos del sistema educativo. De esta manera, se puede lograr la misión institucional y la misión del Ministerio de Educación Nacional que busca que “la educación sea la principal herramienta de transformación social cumpliendo estándares de calidad y así lograr que Colombia sea el país más educado de América Latina en el año 2025” (Ministerio de Educación Nacional, s.f.)

Para la ejecución de este proyecto se contó con el total apoyo de las directivas de la institución, las cuales se encargaron de socializar y sensibilizar a todas las partes interesadas, acerca de la importancia de desarrollar todas las actividades consignadas en él.

Definición del problema

El problema principal de este proyecto es la falta de controles de protección a los activos de información del Liceo Moderno José Celestino Mutis causados por la falta de personal experto, el bajo presupuesto y la ausencia de procesos bien definidos. Así mismo, se lograron identificar los siguientes hallazgos de la situación actual de seguridad de la información:

- No se cuenta con un diagnóstico tanto de aspectos internos como externos relacionados con seguridad, desconociendo sus vulnerabilidades y la forma de subsanarlas.
- Se evidencia que en las labores diarias hay mucha información que se maneja o se genera, la cual no posee una normatividad aplicada a su disponibilidad, confidencialidad y accesibilidad.

Por lo anterior, el interrogante al cual se le quiso dar respuesta con este proyecto es: ¿Cómo mejorar la gestión de la seguridad de los sistemas de información del Liceo Moderno José Celestino Mutis?

Objetivos

Objetivo general

Diseñar un SGSI basado en la norma ISO/IEC 27001 para el Liceo Moderno José Celestino Mutis de San Sebastián de Mariquita.

Objetivos específicos

Analizar el estado actual de la gestión de seguridad, incluyendo los sistemas de información con que cuenta la institución.

Identificar los activos de información con sus amenazas y vulnerabilidades; y los controles de seguridad existentes.

Diseñar políticas de seguridad adecuadas a los requerimientos de la institución.

Formular un plan de implementación del SGSI acorde con la estrategia de seguridad propuesta.

Línea de investigación

Gestión de Sistemas.

Marco Referencial

Marco Teórico

SGSI

La información en una organización está presente de muchas formas, debemos tener en cuenta que no solo está impresa en papel, se puede presentar en forma digital en dispositivos como memorias USB, discos duros, correos electrónicos, o en la nube. Por ende, la OCDE (2004, p.9) propone la importancia del diseño de la seguridad al decir que "los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas, así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas".

Para la ISOTools (2015) Excellence SGSI es: "la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System".

De tal manera, la seguridad de la información pretende conservar los activos de información de una entidad, teniendo en cuenta ciertos aspectos en el tratamiento que reciben, para ISO 27001.ES (s.f., p.3), los aspectos a tener en cuenta en la seguridad de la información son:

- “Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran”.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados que incluyen la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de estos.

Figura 1.

Fases de implementación de un SGSI norma ISO 27001.

Fuente: ISO27000.es

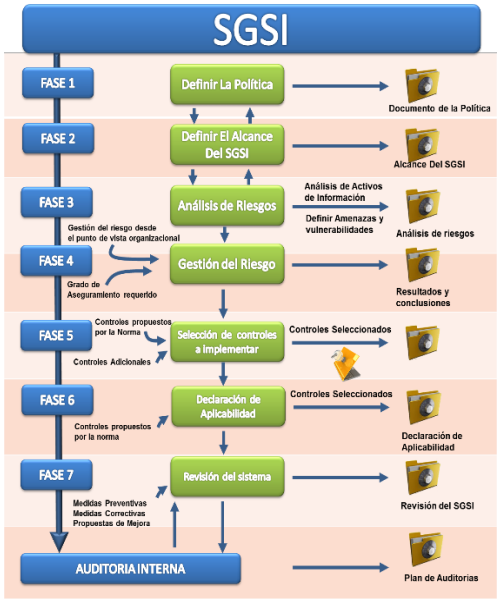
De tal manera, el Sistema de Gestión de la Seguridad de la Información (SGSI) establece procedimientos que se relacionan con las metas de la organización, logrando mantener un nivel bajo de riesgo. Por ende, la responsabilidad de implementar un SGSI, recae en el compromiso de los directivos y en la toma de decisiones, donde se evalúan los riesgos de los sistemas de información, su ocurrencia, impacto y su posible mitigación, involucrando todas las áreas y recursos tanto humanos como económicos.

La gobernanza de seguridad de la información describe el proceso por el cual se aborda la seguridad de la información desde un nivel ejecutivo en la organización. Varios autores (Posthumus; Von-Solms, 2004; Von-Solms; Von-Solms, 2005), muestran que la seguridad de la información debe ser una prioridad de la dirección ejecutiva; por lo tanto, debe comenzar como una responsabilidad de gobierno corporativo. Esto establece la necesidad de integrar la seguridad de la información en la dirección corporativa a través del desarrollo de un marco de gobierno de la seguridad de la información (Cárdenas, Martínez y Becerra, 2016, p.940).

Para la implementación de un SGSI la Norma ISO 27001, propone las fases que se muestran en la figura 2.

Figura 2.

Fases de implementación de un SGSI norma ISO 27001.



Fuente: ISO27000.es

Modelo de Seguridad y Privacidad de la Información MSPI

El Ministerio de Tecnologías de la Información y las Comunicaciones, publicó el Modelo de Seguridad y Privacidad de la Información (MSPI), como un componente TIC de la estrategia de Gobierno en Línea, para MINTIC: "El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables" (2016, p. 20).

Teniendo en cuenta, que dicho documento se generó para servir de guía en buenas prácticas en seguridad y privacidad para entidades del estado, este modelo se puede utilizar como

referente para implementar dichas prácticas en instituciones educativas privadas vigiladas por el Ministerio de Educación Nacional.

Para la implementación del MSPI, se proponen varios instrumentos, de los cuales se utilizaron algunas guías para el desarrollo de este proyecto, como son:

- Guía 2 - Política General MSPI v1
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 14 - Plan de comunicación, sensibilización, capacitación

Para un mejor alcance de la implementación de este modelo en una entidad, se tomó la Guía para MIPYME, con el objetivo de proporcionar un panorama empresarial de la seguridad de la información y su administración. Para MINTIC las entidades deben enfocarse en sus sistemas de información ya que, "Las MIPYMES suelen tener una débil comprensión de la seguridad de la información, tecnologías de seguridad y medidas de control, y suelen dejar el análisis de riesgos o el desarrollo de las políticas de seguridades olvidadas. De ahí la gran importancia de divulgar esta guía al interior de las empresas de nuestro país" (2016, p. 3).

Norma ISO/IEC 27001

La familia ISO 27000 comprende un conjunto de estándares, que proponen un marco de gestión de la seguridad de la información. Siendo la 27001 la norma que deben seguir las organizaciones que quieran adoptar un SGSI.

Según la ISO, la norma ISO /IEC 27001 es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados (ISO 27000.es, s.f.).

En la última actualización de la norma realizada en el 2013, la norma ISO 27001 propuso lo siguiente:

La norma ISO 27001:2013 ha sido desarrollada con base al Anexo SL, en la que se proporciona un formato y un conjunto de alineamientos que siguen el desarrollo documental de un Sistema de Gestión sin que le importe el enfoque empresarial, se alinean bajo la misma estructura todos los documentos que se relacionan con el Sistema de Gestión de Seguridad de la Información y así se evitan problemas de integración con otros marcos de referencia. La nueva estructura queda así:

- **Introducción**

  En la **norma ISO 27001:2013** el cambio más significativo es la eliminación de la sección “Enfoque del proceso” que sí contenía la versión 2005, donde se

describía el modelo PHVA, considerándose el corazón del **Sistema de Gestión de Seguridad de la Información** (**SGSI**).

- **Alcance**

  En la **norma ISO 27001:2013** se establece como obligatorio el cumplimiento de los requisitos especificados entre los capítulos 4 a 10 de dicho documentos, para poder obtener una conformidad de cumplimiento y así poder certificase.

- **Referencias normativas**

  El estándar ISO 27002 ya no será referencia normativa para la **norma ISO 27001:2013**, aunque se puede considerar necesario el desarrollo de una declaración de aplicabilidad.

  La **norma ISO 27001:2013** se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

- **Términos y definiciones**

  Los términos y las definiciones que se encontraban en la ISO 27001:2005 los trasladaron y fueron agrupados en la sección 3 de la **norma ISO 27001:2013** "Fundamento y vocabulario", con el fin de contar con una sola guía de términos y definiciones que sea consistente.

- **Contexto de la organización**

  Durante esta cláusula de la **norma ISO 27001:2013** se identifican todos los problemas externos e internos que rodean a la empresa:

- Se intuyen todos los requisitos para definir el contexto del **SGSI** sin importar el tipo de empresa que sea y el alcance que tenga.
- Se introduce una nueva figura como un elemento primordial para definir el alcance del SGSI
- Se establece la prioridad de identificar y definir todas las necesidades de las partes interesadas con relación a la seguridad de la información y las expectativas creadas por el **Sistema de Gestión de Seguridad de la Información**, ya que esto determinó las políticas de Seguridad de la Información y todos los objetivos a seguir para el proceso de gestión de riesgos.

- **Liderazgo**

Se realiza un ajuste de la relación y las responsabilidades de la gerencia de la organización con respecto al **Sistema de Gestión de Seguridad de la Información**, destacando como se deberá demostrar el compromiso, como por ejemplo:

- Garantizar que los objetivos del **SGSI** y la política de seguridad de la información, antes se conocía como la política del SGSI.
- Se debe garantizar la disponibilidad de todos los recursos para la implantación del SGSI.
- Se garantiza que los roles y las responsabilidades para la seguridad de la información se asignan y se comunican de forma adecuada.

- **Planeación**

  En este apartado de la **norma ISO 27001:2013** se enfoca a la definición de los objetivos de seguridad como un todo, los cuales deben estar claros y se deben contar con planes específicos para conseguirlos.

  Se puede presentar grandes cambios en el proceso de evaluación de riesgos:

  - El proceso para evaluar los riesgos ya no se encuentra enfocado a los activos, las vulnerabilidades y las amenazas.
  - La metodología se enfoca con el objetivo de identificar todos los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información.
  - El nivel de riesgos se determina con base a toda probabilidad de que ocurra un riego y las consecuencias generadas, si el riesgo se materializa.
  - Se elimina el término propietario del activo y se adopta el término propietario del riesgo.
  - Los requisitos no han sufrido transformaciones significativas.

- **Soporte**

  Los requisitos del soporte para el establecimiento de la implementación y mejora del **SGSI**, que incluye:

  - Recursos
  - Personal competente
  - Conciencia y comunicación de todas las partes interesadas.

Se incluye una nueva definición que es “información documentada”, ésta sustituye a los términos “documentos y registros”, establece el proceso de documentar, mantener, controlar y conservar la documentación que corresponde al **Sistema de Gestión de Seguridad de la Información**.

La **norma ISO 27001:2013** se enfoca en el contenido de los documentos y no en que existe un determinado número de éstos.

- **Operación**

Establece todos los requisitos para medir el funcionamiento del **Sistema de Gestión de Seguridad de la Información**, todas las expectativas de la gerencia de la organización y la retroalimentación sobre estas, además de cumplir con la **norma ISO 27001:2013**.

Además, la organización se plantea y controla las operaciones y los requisitos de seguridad, el pilar de este proceso se centra en realizar las evaluaciones de riesgos de seguridad de la información de forma periódica por medio de un programa elegido.

Todos los activos, las vulnerabilidades y las amenazas ya no son la base principal de la evaluación de riesgos. Solo se requiere para realizar la identificación de los riesgos, que están asociados a la confidencialidad, la integridad y la disponibilidad.

- **Evaluación del desempeño**

  La base para poder realizar la identificación y la medición de la eficiencia y el desempeño que realiza el **Sistema de Gestión de Seguridad de la Información** continúa siendo las auditorías internas y las revisiones del **SGSI**.

  Se tiene que considerar el estado en el que se encuentran los planes de acción para poder atender las **no conformidades** como es debido, además se establece la necesidad de definir quién y cuándo realiza las evaluaciones, además de quien tiene que analizar la información que se ha recolectado.

- **Mejora**

  El principal elemento del proceso de mejora son las **no conformidades** identificadas, las cuales tiene que contabilizarse y compararse con las accione correctivas para asegurarse de que no se repitan y que las acciones correctoras que se realicen sean efectivas (ISOTools Excellence, 2015**).**

ISO/ IEC/27002

Esta norma complementa la norma ISO/27001, con la definición de controles a aplicar en la implementación de un SGSI. Publicada desde el 1 de Julio de 2007, renombra la norma ya publicada ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005 (ISO 2700.ES, s.f.).

El contenido de las políticas se basa en el contexto en el que opera una empresa y suele ser considerado en su redacción todos los fines y objetivos de la empresa, las estrategias adoptadas para conseguir sus objetivos, la estructura y los procesos utilizados por la empresa. Además, de los objetivos generales y específicos relacionados con el tema de la política y los requisitos de las políticas procedentes de niveles mucho más superiores y que se encuentran relacionadas. La estructura típica de los documentos de políticas puede ser:

- Resumen: se establece una visión general de una extensión breve, uno o dos frases y que pueden aparecer fusionadas con la introducción.
- Introducción: se establece una pequeña explicación del asunto principal de la política.
- Ámbito de aplicación: es la descripción de los departamentos, áreas o actividades de la empresa en las que aplica la política. Pueden ser necesario mencionar otras políticas relevantes a las que se pretende ofrecer cobertura desde ésta.
- Objetivos: es la descripción de la intención de la política.
- Principios: se describen las reglas que conciernen a las acciones o decisiones para conseguir los objetivos. En algunos casos puede ser de utilidad identificar de forma previa los procesos calve que están asociados a un asunto principal de la política para después identificar las reglas de operación de los procesos.
- Responsabilidades: descripción de quién es el responsable de qué acciones pueda cumplir con los requisitos de la política. En algunos casos, esto puede incluir una descripción de los mecanismos organizativos, además de las responsabilidades de las personas que tienen sus roles asignados.

- Resultados clave: describe todos los resultados relevantes para las actividades de la empresa que se obtienen cuando se cumplen los objetivos.
- Políticas relacionadas**:** se describen las políticas relevantes para cumplir con los objetivos, se indican detalles adicionales en relación con los temas específicos.

La política de alto nivel se encuentra relacionada con un Sistema de Gestión de Seguridad de la Información que suele estar apoyada por políticas de bajo nivel, específicas para aspectos concretos en temáticas como el control de accesos, la clasificación de la información, la seguridad física y ambiental, utilizar activos, dispositivos móviles y protección contra los malware. Si partimos del principio típico en seguridad "lo que no está permitido está prohibido" cada empresa debe detectar las necesidades de los usuarios y valorar los controles necesarios que fundamentan las políticas aplicables, que se aplican en una mejor estructura y relaciones entre ellas para su gestión (ISOTools Excellence, 2017).

Diseño de un SGSI para entidades públicas y privadas

Para Figueroa (2018, p,84) "dado que la información es uno de los activos más importantes al interior de las organizaciones porque son parte fundamental en la toma de decisiones, en la medida en que se realizan ejercicios de gestión en este ámbito, es posible consolidar los demás aspectos que implica la administración eficaz y eficiente de una entidad"

Por ende, definir un SGSI dentro de cualquier entidad permite controlar la seguridad de su información, conservando su confidencialidad, integridad y disponibilidad. Para las entidades del estado es importante establecer y determinar las políticas de seguridad con que se cuenta, ya que son estas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la misma, así mismo las políticas permitirán que se trabaje bajo las mejores prácticas y lineamientos de seguridad de la información y cumpla con los requisitos legales vigentes a los cuales esté obligada a cumplir la entidad (De Leon ,2019, p. 92). De tal manera, la información en cualquier entidad pública o privada, juega un papel importante en su gestión, ya que los procesos que se llevan a cabo deben contar con datos seguros y confiables.

Es importante reconocer que en la actualidad la información de las organizaciones se constituye como uno de los activos más importantes de competitividad y empoderamiento la gestión de seguridad de la misma es tal vez uno de los retos a los que se enfrentan hoy en día, dado que controlar variables internas y externas en un sistema que requiere que cada día sea más dinámico capaz de responder a los constantes cambios, procesos de mejora continua, actualizaciones tecnológicas y sociales; exige que un proyecto de gestión de seguridad informática desde las etapas de formulación, implementación e implantación se realicen procesos rigurosos de investigación, análisis y documentación que garantice que el Sistema Integrado de seguridad informática sea suficientemente completo de tal forma garantice el cumplimiento y total cobertura de los sistemas de información de toda organización e involucre el mayor número posible de agentes funcionales que intervienen en la gestión de la información, Sin embargo los procesos de implementación gradual para organizaciones pequeñas resultan ser una buena alternativa dado que en la media de su crecimiento el sistema se puede ir adaptando a las

necesidades y así mismo las variables tecnológicas, funcionales, culturales, sociales, normativas con más fácil control y cobertura (Celis & Franco, 2016, p 409).

Marco Conceptual

En este apartado, se exponen conceptos que ayudaran a una mejor comprensión del desarrollo del documento.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Controles: 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 .

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos.

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 por tanto ser protegidos de potenciales riesgos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información (ISO27001.es).

Aspectos metodológicos

Para la presente investigación, se adoptó el modelo PDCA que traduce Plan-DO-Check-Act o también conocido como PHVA, planear, hacer, verificar y actuar, el cual se tiene en cuenta dentro de la norma ISO 27001:2005.

La norma define el enfoque del proyecto como el modelo Planificar-Hacer-Verificar-Actuar (PDCA) para estructurar las tareas necesarias para introducir un SGSI eficaces. Si bien esto ya no es estrictamente el mandato de ISO 27001.es, sigue siendo un enfoque válido y eficaz.

El ciclo PDCA se puede resumir como:

- Planifique lo que debe hacer para lograr el objetivo (que incluye definir cuál es ese objetivo).
- Haga lo que planeó.
- Compruebe que lo que ha hecho logra lo que había planeado para lograrlo e identifique cualquier brecha o deficiencia (es decir, comprobar si ha cumplido con los objetivos).
- Actuar sobre los resultados de la fase de verificación para abordar las lagunas y/o mejorar la eficiencia y eficacia de lo que tiene en su lugar.

Por lo general, esta última etapa implicó hacer un plan, hacer lo que ese plan implica, verificar que los objetivos se alcanzaron, identificar cualquier déficit y luego actuar sobre los hallazgos creando una vez más un plan. Y así, con la introducción de un ISMS usando P-D-C-A, se realiza el ciclo inicial de mejora continua (Watkins, 2013, p. 21).

Análisis, interpretación y Presentación de resultados

Fase de Análisis y diagnóstico del estado actual

En esta fase se analizó el estado actual de la institución educativa, se determinó el estado de los activos de información y los controles existentes, esto con el fin de desarrollar las políticas de seguridad para el SGSI.

Para realizar el análisis de la información, se inició con su recolección, en esta etapa se realizó trabajo de campo (visitas) y entrevistas personales a cada uno de los integrantes de la institución educativa (personal administrativo y académico), se revisaron cada uno de los procesos que se llevan a cabo, el tipo de información que se genera y de qué forma se maneja. Se hizo una identificación del contexto organizacional, grupos de interés tanto internos como externos.

Contexto Organizacional

En este Ítem se desarrolla el contexto de la empresa seleccionada para la aplicación del SGSI, donde se realiza un reconocimiento y análisis con el fin de identificar el estado actual de la información en el colegio Liceo Moderno José Celestino Mutis, basado en la norma ISO/IEC 27001:2013, donde se evalúa el cumplimiento de los dominios descritos en la norma anteriormente mencionada.

En el reconocimiento de la organización se realiza la descripción de esta, detallando su estructura organizacional e infraestructura del colegio Liceo Moderno José Celestino Mutis como lo son los equipos, red de datos, servicios y aplicaciones con los que cuenta la institución.

- **Descripción**

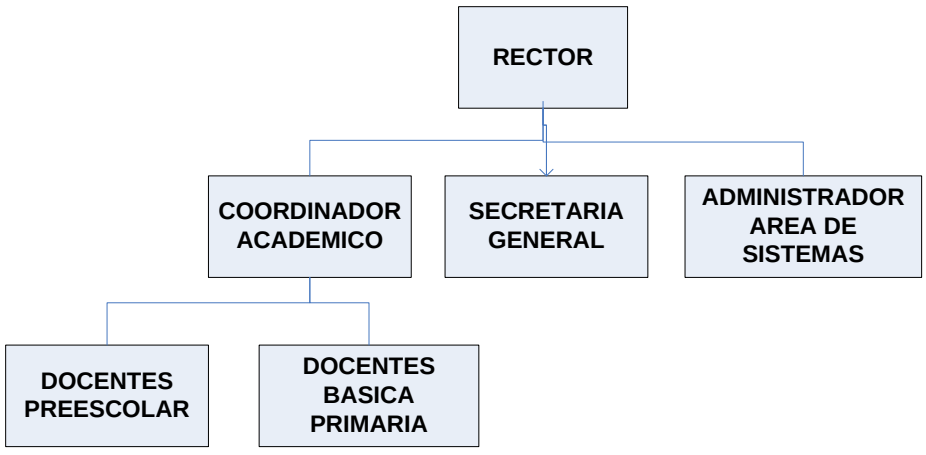
El Liceo Moderno José Celestino Mutis es una Institución Educativa privada, con reconocimiento oficial por la Secretaría de Educación y Cultura del departamento del Tolima, mediante resolución 2214 del 17 de diciembre 2008, para los grados de preescolar en los niveles de pre jardín, Jardín y Transición, y en los grados de 1º a 5º de básica primaria, calendario A, jornada única. Su domicilio principal está ubicado en la calle 4 Nº 1-31 Barrio el Centro, Municipio de San Sebastián de Mariquita del Departamento del Tolima.

- **Estructura Organizacional**

La estructura organizacional del colegio Liceo Moderno José Celestino Mutis, está dada jerárquicamente.

Figura 3.

Organigrama Liceo Moderno José Celestino Mutis.



Fuente. Elaboración propia

- **Identificación de grupos de interés**

Los grupos de interés del Liceo JCM están representados por: clientes internos están constituidos por el personal administrativo, académico, estudiantes, padres de familia y egresados al servicio de la Institución. Los clientes externos están conformados por Secretaria de Educación de Mariquita, Secretaria de Educación del Tolima y Ministerio de Educación Nacional (MEN).

- **Productos y servicios**

Los servicios que ofrece el liceo son de índole educativo en una jornada única escolar de 8:00 a.m. a 12:00 m en los niveles de: Preescolar (Jardín y Transición) y Básica Primaria primero a quinto, de 6:30 a.m. a 12:00 m.

- **Recursos**

Planta física propia, con 8 salones, un salón de audiovisuales, biblioteca, dos oficinas, dos patios para recreación, 9 unidades sanitarias.

- ✓ Recursos Humanos.

Una docente Auxiliar técnica en docencia

Dos docentes Técnicas en educación preescolar

Una docente Licenciada en educación infantil y preescolar

Una docente Licenciada en artes plásticas para la educación básica

Una docente Licenciada en artes plásticas para la educación básica

Una docente Licenciada en preescolar con énfasis en ingles

Una docente Licenciada en preescolar con énfasis en educación infantil

Un docente Ingeniero de Sistemas Especialista en Educación

Una asistente Administradora financiera

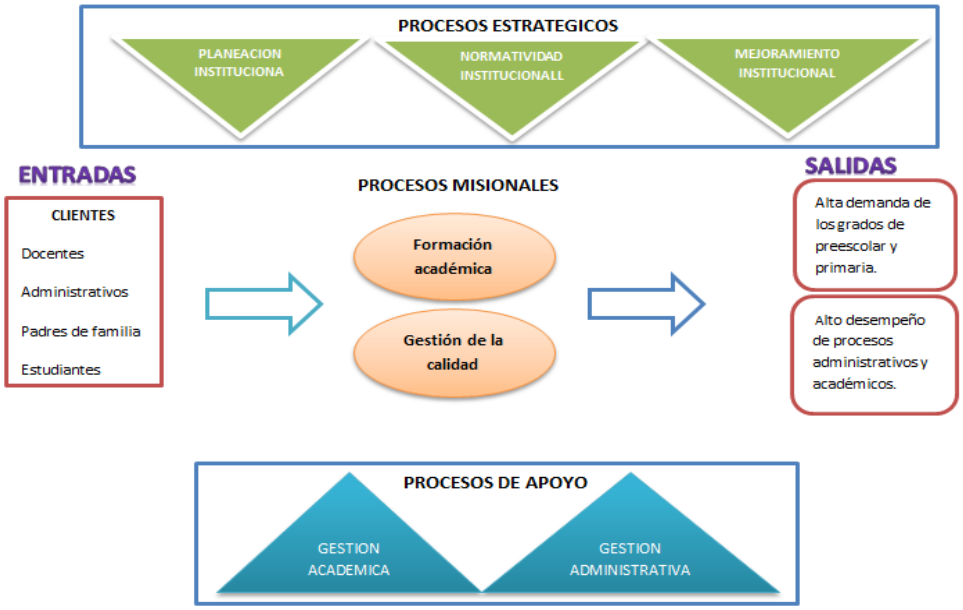
El Rector Licenciado y Magister en Neuropsicología

- **Procesos**

Los Macroprocesos, son las acciones encadenadas que la institución debe realizar a fin de cumplir con sus objetivos, misión y visión. Existen entonces diferentes tipos de Macr procesos: Procesos Estratégicos, Procesos Primarios u Operativos y Procesos de soporte. Ver figura 4.

Figura 4.

Mapa de procesos Liceo Moderno José Celestino Mutis.



Fuente: elaboración propia.

- **Infraestructura Tecnológica**

Actualmente la institución cuenta con una conectividad de 4 Mbps de ancho de banda, a 20 equipos en sala de sistemas, 1 equipo en la rectoría, 1 equipo secretaria general, 1 equipo en la coordinación académica. Un Access point para la conexión de los equipos de la sala de cómputo. Cableado estructurado UTP para conexión de los demás equipos.

Clasificación Activos de información

En la siguiente tabla se muestran los activos tecnológicos (información, software, hardware) con los que cuenta la institución, a su vez que identifica el responsable o persona a la que le ha sido asignado cada activo con el que cuenta el colegio.

Tabla 1

Inventario Activos de información Liceo Moderno José Celestino Mutis

Activo	Cantidad	Descripción	Estado físico/digital	Responsable
Información	NA	Informe académico periódico	Físico/Digital	Docentes, Coordinación académica
		Hojas de matriculas	Físico	Secretaría General
		Libro consolidado de matriculas	Físico	Secretaría General
		Libro consolidado de notas	Físico/Digital	Secretaría General

		Archivo hojas de vida alumnos	Físico	Secretaría General
		Archivo hojas de vida empleados	Físico	Secretaría General
		Observador del estudiante	Físico	Coordinación académica
		Informes financieros	Físico	Secretaría General
		Facturas	Físico	Secretaría General
		Correspondencia	Físico/Digital	Secretaría General
		Actas de comités	Físico	Secretaría General
		Actas de reuniones	Físico	Secretaría General
		PEI	Físico/Digital	Coordinación académica
		Movimientos bancarios	Físico	Secretaría General
Software	1	Antivirus ClamAV (GNU)	NA	Docente sistemas
	1	Sistema operativo LINUX (GNU)	NA	Docente sistemas
	1	Staroffice (GNU)	NA	Docente sistemas
Hardware	20	Computadores portátiles	NA	Docente sistemas
	1	Impresora multifuncional	NA	Dirección, Coordinación académica, secretaría general

	1	Accespoint	NA	Docente sistemas
	1	Computador portátil		Rectoría
	2	Computadores de escritorio	NA	Coordinación académica, secretaría general
	1	Router	NA	Docente sistemas
	2	Memoria USB	NA	Secretaría General
	1	Disco duro externo	NA	Secretaría General

Nota: Descripción inventario activos de información Liceo JCM.

Identificación de los Activos de Información

En la identificación de los activos de información, se inicia con la valoración en tres dimensiones, teniéndose en cuenta una escala numérica de valoración, lo que permite comparar riesgos, en este caso se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo).

Dimensiones de valoración: Son características que le dan valor a los activos de información de una organización.

- **Confidencialidad**: garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma. (NTC-ISO /IEC 27001, 2013)

- **Integridad**: salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. (NTC-ISO /IEC 27001, 2013)

- **Disponibilidad**: garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. (NTC-ISO /IEC 27001, 2013)

Tabla 2

Escala de valoración de activos

Valor		Criterio
10	extremo	daño considerablemente peligroso
9	muy alto	daño muy peligroso
6-8	alto	daño peligroso
3-5	medio	daño significativo
1-2	bajo	daño moderado
0	despreciable	Sin efectos prácticos

Nota: valoración aplicada a activos de información para determinar su importancia dentro de las dimensiones

Tomando las dimensiones y criterios de valoración de activos, se realiza su aplicación a los activos del Liceo Moderno José Celestino Mutis:

Tabla 3

Valoración activos del Liceo Moderno José Celestino Mutis

Descripción	Disponibilidad	Integridad	Confidencialidad
Hojas de vida docentes	9	2	4
Informe académico periódico	9	2	4
Hojas de matriculas	9	2	7
Libro consolidado de matriculas	9	7	7
Libro consolidado de notas	9	2	7
Hojas de vida alumnos	9	4	7
Observador del estudiante	9	4	7
Informes financieros	9	7	7
Facturas	9	4	4
Correspondencia	9	4	4
Actas de comités	9	7	7
Actas de reuniones	9	7	7
PEI	9	9	7
Movimientos bancarios	4	2	9
Manual de convivencia	4	2	4
Manual de emergencias	4	2	4
Antivirus ClamAV (GNU)	4	2	2
Sistema operativo LINUX (GNU)	4	2	2
Staroffice (GNU)	4	2	2

Computadores portátiles	9	9	4
Computadores de escritorio	9	9	9
Accespoint	9	9	2
Router	9	9	2
Impresora multifuncional	4	9	2
Video Beam	4	7	2
Oficinas	9	9	9
Aulas	9	9	7
Internet	6	4	2
Red inalámbrica	9	7	2
Red cableada	9	7	7
Disco duro externo	9	9	9
Memoria USB	4	4	7
Extintores	9	2	2
Docente profesional sistemas	9	7	9
Secretaria general	7	7	9
Director	9	9	9
Coordinador académico	7	7	9
Docentes	4	4	7

Nota: valor del activo dentro de las tres dimensiones.

Identificación de amenazas

La identificación de las amenazas se realiza con el propósito de evaluar las brechas de seguridad, errores o situaciones que puedan causar perdida de información o afectación a los activos de información de la institución. A continuación, se listan las amenazas comunes:

D= Deliberadas, **A**= Accidentales, **E**= Ambientales

Tabla 4

Amenazas comunes

Tipo	**Amenaza**	**Origen**		
		A	**D**	**E**
Daño físico	Fuego	X	X	X
	Agua	X	X	X
	Contaminación	X	X	X
	Accidente Importante	X	X	X
	Destrucción del equipo o medios	X	X	X
	Polvo, corrosión, congelamiento	X	X	X
Eventos naturales	Fenómenos climáticos			X
	Fenómenos sísmicos			X
	Fenómenos volcánicos			X
	Fenómenos meteorológico			X
	Inundación			X
	Fallas en el sistema de suministro de agua o aire acondicionado			X

Perdida de los servicios esenciales	Perdida de suministro de energía		X
	Falla en equipo de telecomunicaciones		X
Compromiso de la información	Interceptación de señales de interferencia comprometida		X
	Espionaje remoto		X
	Escucha encubierta		X
	Hurto de medios o documentos		X
	Hurto de equipo		X
	Recuperación de medios reciclados o desechados		X
	Divulgación		X
	Datos provenientes de fuentes no confiables		X
	Manipulación con hardware		X
	Manipulación con software		X
	Detección de la posición		X
Fallas técnicas	Fallas del equipo	X	
	Mal funcionamiento del equipo	X	
	Saturación del sistema de información	X	
	Mal funcionamiento del software	X	
	Incumplimiento en el mantenimiento del sistema de información.	X	
Acciones no autorizadas	Uso no autorizado del equipo		X
	Copia fraudulenta del software		X

	Uso de software falso o copiado	X
	Corrupción de los datos	X
	Procesamiento ilegal de datos	X
Compromiso de las funciones	Error en el uso	X
	Abuso de derechos	X
	Falsificación de derechos	X
	Negación de acciones	X
	Incumplimiento en la disponibilidad del personal	X

Nota: tomado de Guía de gestión de riesgos MinTIC (2016).

Es importante tener en cuenta, que además de las amenazas comunes también existen amenazas humanas, de las cuales se debe conocer la fuente y la motivación, a continuación, se listan las amenazas humanas:

Tabla 5

Amenazas humanas

Fuente de la amenaza	**Motivación**	**Acciones amenazantes**
Pirata informático, intruso ilegal	Reto Ego Rebelión	Piratería Ingeniería Social

	Estatus Dinero	Intrusión, accesos forzados al sistema Acceso no autorizado
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador Acto fraudulento Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/Terrorismo Guerra de la información Ataques contra el sistema Penetración en el sistema Manipulación en el sistema
Espionaje industrial(inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja política Explotación económica Hurto de información Intrusión en privacidad personal Ingeniería social

		Penetración en el sistema Acceso no autorizado al sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Interceptación Código malicioso Venta de información personal Errores en el sistema Intrusión al sistema Sabotaje del sistema Acceso no autorizado al sistema.

Nota: tomado de Guía de gestión de riesgos MinTIC (2016).

Identificación de los controles existentes

Se procede a la identificación de los controles existentes, su implementación y utilización, se aplicó una lista de chequeo desarrollando los dominios con sus objetivos de control respectivos, según el anexo A de la norma ISO 27001:2013.

Tabla 6.

Cumplimiento controles Anexo A norma ISO 27001:2013 en el Liceo Moderno José Celestino Mutis

	Dominio - Control		Controles Implementados (SI/NO /PARCIALMENTE)
N° A6	**Política de seguridad de la información**		
A.5.1	Dirección de gestión para la seguridad de la información		
A.5.1.1	Política para la seguridad de la información	La dirección ha publicado y aprobado las políticas sobre la Seguridad de la Información acordar con los requisitos del negocio	**NO**
A.5.1.2	Revisión de las políticas para la seguridad de la información	Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información	**NO**
A6	**Organización de la seguridad de la información**		
A.6.1	Organización Interna		

A.6.1.1	Asignación de responsabilidades para la seguridad de la información.	Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización	**PARCIALMENTE**
A.6.1.2	Segregación de tareas.	Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos	**PARCIALMENTE**
A.6.1.3	Contacto con las autoridades	Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información	**NO**
A.6.1.4	Contacto con grupos de interés especial.	Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad	**NO**

A.6.1.5	Seguridad de la información en la gestión de proyectos	Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la organización	**NO**
A6.2	**Dispositivos móviles y teletrabajo**		
A.6.2.1	Política para dispositivos móviles	Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles	**NO**
A.6.2.2	Teletrabajo	Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el teletrabajo.	**NO**
A7	**Seguridad de los recursos humanos**		
A7.1	**Antes de asumir el empleo**		
A.7.1.1	Investigación de antecedentes.	Se investigan los antecedentes de los candidatos -Formación -	**SI**

		Experiencia - Titulación - Referencias	
A.7.1.2	Términos y condiciones de contratación.	Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo	**NO**
A.7.2	**Durante la vigencia del empleo**		
A.7.2.1	Responsabilidades de gestión.	El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas	**SI**
A.7.2.2	Concienciación, educación y capacitación en seguridad de la información	Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información	**NO**
A.7.2.3	Proceso disciplinario.	Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las	**NO**

		políticas de la Seguridad de la Información	
A.7.3	**Terminación o cambio de empleo**		
A.7.3.1	Cese o cambio de puesto de trabajo.	Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato como por ejemplo cuestiones relativas a la confidencialidad de la Información	**NO**
A.8	**Gestión de activos**		
A8.1	**Responsabilidad por los activos**		
A.8.1.1	Inventario de activos	Se ha realizado un inventarios de activos que dan soporte al negocio y de Información	**PARCIALMENTE**
A.8.1.2	Propiedad de los activos	Se ha identificado al responsable de cada activo en cuanto a su seguridad	**NO**
A.8.1.3	Uso aceptable de los activos	Se han establecido normas para el uso de activos en relación a su seguridad	**PARCIALMENTE**

A.8.1.4	Devolución de activos	Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato	**NO**
A.8.2	**Clasificación de la información**		
A.8.2.1	Directrices de clasificación	Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas	**NO**
A.8.2.2	Etiquetado y manejo de información	Los activos de información son fácilmente identificables por su grado de confidencialidad o el nivel de clasificación	**NO**
A.8.2.3	Manejo de activos	Existen procedimientos para el manipulado de la información de acuerdo a su clasificación	**NO**
A.8.3	**Manejo de medios**		
A.8.3.1	Gestión de soportes extraíbles.	Existen controles establecidos para aplicar a soportes extraíbles.	**PARCIALMENTE**

		-Uso -Cifrado -Borrado -Etc.	
A.8.3.2	Eliminación de soportes.	Existen procedimientos establecidos para la eliminación de soportes	**PARCIALMENTE**
A.8.3.3	Soportes físicos en tránsito.	Existen procedimientos para el traslado de soportes de información para proteger su seguridad. -Control de salidas -Cifrado etc.	**NO**
A.9	**Control de acceso**		
A 9.1	**Requisito del negocio para el control de acceso**		
A.9.1.1	Política de control de accesos.	Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo	**PARCIALMENTE**

A.9.1.2	Control de acceso a las redes y servicios asociados.	Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados	**SI**
A.9.2	**Gestión de acceso de usuarios**		
A.9.2.1	Gestión de altas/bajas en el registro de usuarios.	Existen procesos formales de registros de usuarios	**NO**
A.9.2.2	Gestión de los derechos de acceso asignados a usuarios.	Existen procesos formales para asignación de perfiles de acceso	**NO**
A.9.2.3	Gestión de información confidencial de autenticación de usuarios.	Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos	**NO**
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Se ha establecido una política específica para el manejo de información clasificada cono secreta. en cuanto a: -Autenticación -Compromisos	**NO**

A.9.2.5	Revisión de los derechos de acceso de los usuarios.	Se establecen periodos concretos para renovación de permisos de acceso	**NO**
A.9.2.6	Retirada o adaptación de los derechos de acceso	Existe un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos	**NO**
A.9.3	**Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta	Se establecen normas para la creación y salvaguarda de contraseñas de acceso	**NO**
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricciones de acceso a la información	Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar	**NO**
A.9.4.2	Procedimiento de ingreso seguro	Se han implementado procesos de acceso seguro para el inicio de sesión considerando	**SI**

		limitaciones de intentos de acceso, controlando la información en pantalla etc.	
A.9.4.3	Sistema de gestión de contraseñas	Se establecen medidas para controlar el establecimiento de contraseñas seguras	**NO**
A.9.4.4	Uso de los programas utilitarios privilegiados	Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad	**NO**
A.9.4.5	Control de acceso a códigos fuente de programas	Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar	**NO**
A.10	**Criptografía**		
A.10.1	**Controles criptográficos**		
A.10. 1.1	Política sobre el uso de controles criptográficos	Existe una política para el establecimiento de controles criptográficos	**NO**

A.10. 1.2	Gestión de llaves	Existe un control del ciclo de vida de las claves criptográficas	**NO**
A.11	**Seguridad física y del entorno**		
A.11.1	**Áreas seguras**		
A.11.1.1	Perímetro de seguridad física.	Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso	**SI**
A.11.1.2	Controles de acceso físico	Existen controles de acceso a personas autorizadas en áreas restringidas	**SI**
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo	**SI**
A.11.1.4	Protección contra amenazas externas y ambientales	Se controla o supervisa la actividad de personal que accede a áreas seguras	**SI**
A.11.1.5	Trabajo en áreas seguras	Se controlan las áreas de Carga y descarga con procedimientos	**SI**

		de control de mercancías entregadas etc.	
A.11.2	**Seguridad de los Equipos**		
A.11.2.1	Ubicación y protección de los equipos	Se protegen los equipos tanto del medioambiente como de accesos no autorizados	**SI**
A.11.2.2	Servicios de suministro	Se protegen los equipos contra fallos de suministro de energía	**PARCIALMENTE**
A.11.2.3	Seguridad del Cableado	Existen protecciones para los cableados de energía y de datos	**SI**
A.11.2.4	Mantenimiento de equipos	Se planifican y realizan tareas de mantenimiento sobre los equipos	**SI**
A.11.2.5	Retiro de activos	Se controlan y autorizan la salida de equipos, aplicaciones etc. Que puedan contener información	**SI**
A.11.2.6	Seguridad de los equipos fuera de las instalaciones	Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa	**SI**

A.11.2.7	Disposición segura o reutilización de equipos	Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados	**SI**
A.11.2.8	Equipos de usuario desatendido	Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo	**SI**
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo	**SI**
A.12	**Seguridad de las operaciones**		
A.12.1	**Procedimientos operacionales y responsabilidades**		
A.12. 1.1	Procedimientos de operación documentados	Se documentan los procedimientos y se establecen responsabilidades	**NO**
A.12. 1.2	Gestión de cambios	Se controla que la información sobre procedimientos se mantenga actualizada	**NO**

A.12. 1.3	Gestión de capacidad	Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos	**NO**
A.12. 1.4	Separación de los ambientes de desarrollo, pruebas y operación.	Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas	**NO**
A.12.2	**Protección contra códigos maliciosos**		
A12.2.1.	Controles contra códigos maliciosos	Existen sistemas de detección para Software malicioso o malware	**SI**
A12.3.	**Copias de Respaldo**		
A12.3.1.	Respaldo de la Información	Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas	**SI**
A12.4.	**Registro y Seguimiento**		
A12.4.1.	Registro de eventos	Se realiza un registro de eventos -Intentos de acceso fallidos/exitosos	**NO**

		-Desconexiones del sistema -Alertas de fallos Etc.	
A12.4.2.	Protección de la información de registro.	Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad	**NO**
A12.4.3.	Registros del administrador y del operador	Se protege convenientemente y de forma específica los accesos o los de los administradores	**NO**
A12.4.4.	Sincronización de Relojes	Existe un control de sincronización de los distintos sistemas	**NO**
A12.5.	**Control de Software Operacional**		
A12.5.1.	Instalación de software en sistemas operativos	Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación.	**SI**
A12.6.	**Gestión de la vulnerabilidad técnica**		

A12.6.1.	Gestión de las vulnerabilidades técnicas	Se conoce oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.	**SI**
A12.6.2.	Restricciones sobre la instalación de software.	Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales	**SI**
A13.	**Seguridad de las Comunicaciones**		
A13.1.	**Gestión de la seguridad de las redes**		
A.13.1.1.	Controles de redes	En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados	**SI**
A13.1.2.	Seguridad de los servicios de red.	Se establecen condiciones de seguridad en los servicios de	**SI**

		red tanto propios como subcontratados	
A 13.1.3.	Separación en las redes.	Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos	**SI**
A13.2.	**Transferencia de información**		
A13.2.1	Políticas y procedimientos de transferencia de información.	Se establecen políticas y procedimientos para proteger la información en los intercambios	**SI**
A13.2.2.	Acuerdos sobre transferencia de información.	Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades	**SI**
A13.2.3.	Mensajería electrónica	Se establecen normas o criterios de seguridad en mensajería electrónica	**SI**
A13.2.4.	Acuerdos de confidencialidad o de no divulgación.	Se establecen acuerdos de confidencialidad antes de realizar intercambios de	**SI**

		información con otras entidades	
A14.	**Adquisición y Mantenimiento de Sistemas**		
A14.1.	**Requisitos de seguridad de los sistemas de información**		
A14.1.1.	Análisis y especificación de requisitos de seguridad de la información.	Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de información	**SI**
A14.1.2.	Seguridad de servicios de las aplicaciones en redes públicas.	Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información	**SI**
A14.1.3.	Protección de transacciones de los servicios de las aplicaciones	Se establecen medidas de protección para transacciones Online	**SI**
A14.2.	**Seguridad en los procesos de desarrollo y de soporte**		
A14.2.1.	Política de desarrollo seguro.	Se establecen procedimientos que garanticen el desarrollo seguro del Software	**NO**
A14.2.2.	Procedimiento de control de cambios en sistemas.	Se gestiona el control de cambios en relación al impacto	**NO**

		que puedan tener en los sistemas	
A14.2.3.	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones	**NO**
A14.2.4.	Restricciones en los cambios a los paquetes de software	Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros	**NO**
A14.2.5.	Principios de construcción de los sistemas seguros.	Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas	**NO**
A14.2.6.	Ambiente de desarrollo seguro.	Se realiza una evaluación de riesgos para herramientas de desarrollo de Software	**NO**
A14.2.7.	Desarrollo contratado externamente	Se acuerdan los requisitos de seguridad de la Información para Software desarrollado por terceros	**NO**

A14.2.8.	Pruebas de seguridad de Sistemas	Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción	**NO**
A.14.2.9.	Prueba de aceptación de Sistemas	Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones	**NO**
A14.3.	**Datos de prueba**		
A14.3.1.	Protección de datos de prueba.	Se utilizan datos de prueba en los ensayos o pruebas de los sistemas	**NO**
A15.	**RELACIONES CON LOS PROVEEDORES**		
A15.1.	**Seguridad de la información en las relaciones con los proveedores**		
A15.1.1.	Política de seguridad de la información para las relaciones con proveedores.	Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa	**NO**

A15.1.2.	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Se han establecido requisitos de seguridad de la información en contratos con terceros	**NO**
A15.1.3.	Cadena de suministro de tecnología de información y comunicación.	Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministro	**NO**
A15.2.	**Gestión de la prestación de servicios de proveedores**		
A15.2.1.	Seguimiento y revisión de los servicios de los proveedores.	Se controla el cumplimiento de los requisitos establecidos con proveedores externos	**NO**
A15.2.2.	Gestión de cambios en los servicios de los proveedores.	Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos	**NO**
A16.	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACION**		
A16.1.	Gestión de incidentes y mejoras en la seguridad de la información		
A16.1.1.	Responsabilidades y procedimientos.	Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información	**NO**

A16.1.2.	Reporte de eventos de seguridad de la información.	Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información	**NO**
A16.1.3.	Reporte de debilidades de seguridad de la información	Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información	**NO**
A16.1.4.	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información	**NO**
A16.1.5.	Respuesta a incidentes de seguridad de la información.	Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información	**NO**
A16.1.6.	Aprendizaje obtenido de los incidentes de seguridad de la información.	La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas	**NO**
A16.1.7.	Recolección de evidencia.	Existe un proceso para recopilar evidencias sobre los	**NO**

		incidentes en la seguridad de la Información	
A17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE**		
A17.1.	Continuidad de seguridad de la información		
A17.1.1.	Planificación de la continuidad de la seguridad de la información.	Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información	**NO**
A17.1.2.	Implementación de la continuidad de la seguridad de la información.	Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio	**NO**
A17.1.3.	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio	**NO**
A17.2.	Redundancias		
A17.2.1.	Disponibilidad de instalaciones de procesamiento de información.	Se ha evaluado la necesidad de redundar los activos críticos de la Información	**NO**
A18.	**CUMPLIMIENTO**		

A18.1.	Cumplimiento de requisitos legales y contractuales		
A18.1.1.	Identificación de la legislación aplicable y de los requisitos contractuales.	Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento. -Leyes para comercio Electrónico - Transacciones Bancarias -Información Protegida -Otras propias del negocio -Ley general de Telecomunicaciones	**SI**
A18.1.2.	Derechos de propiedad intelectual.	Existen procedimientos implementados sobre la propiedad intelectual	**SI**
A18.1.3.	Protección de registros.	Se establecen criterios para clasificación de registros y medidas de protección según niveles	**SI**
A18.1.4.	Privacidad y Protección de información de datos personales.	Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente	**SI**

A18.1.5.	Reglamentación de controles criptográficos.	Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación	**NO**
A18.2.	Revisiones de seguridad de la información:		
A18.2.1.	Revisión independiente de la seguridad de la información.	Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles	**NO**
A18.2.2.	Cumplimiento con las políticas y normas de seguridad.	Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información	**NO**
A18.2.3.	Revisión del cumplimiento técnico	Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información	**NO**

Nota: Identificación del estado actual de los dominios en el Liceo JCM. Tomado del Test de cumplimiento Anexo A de la ISO 27001

Hallazgos

Después de analizar los controles aplicados a los activos de información del Liceo Moderno José Celestino Mutis, se describen a continuación los hallazgos relacionados con estos:

- Se evidencia que no existe un documento de política de seguridad de la información para la institución, o ningún tipo de norma establecida para orientar los procesos de seguridad.
- La institución cuenta con un inventario de activos, pero no existe un procedimiento formal donde se realice la asignación de responsabilidades sobre los activos, no existen normas sobre el uso aceptable de la información y sus activos, no existe procedimiento para la devolución de activos a la finalización de un puesto de trabajo o contrato.
- El uso de dispositivos móviles y el teletrabajo son actividades que no están permitidas dentro de la institución conforme a su labor educativa.
- No se incluyen cláusulas relativas a la Seguridad de la Información, ni de confidencialidad dentro de la contratación del personal, no existen procedimientos de capacitación al personal, no existen manuales de procedimientos, las capacitaciones son realizadas por algún otro empleado de la institución, no existe un plan disciplinario para aplicar a empleados como consecuencia del incumplimiento sobre las políticas de la Seguridad de la Información.
- No existe una debida clasificación de información en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización, además no hay establecidos procedimientos adecuados para el etiquetado y el manejo de la información según su clasificación.

- La seguridad en las áreas que contienen información y servicios de procesamiento de información es deficiente, los controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado son insuficientes.
- No existen controles para la gestión de acceso de usuarios, la institución en el momento no cuenta con sistemas informáticos para la gestión de procesos.
- Los equipos y las redes de energía y telecomunicaciones no cuentan con la protección suficiente, su instalación no es muy adecuada, están expuestos a amenazas del entorno y accesos no autorizados, es necesario llevar registro de los mantenimientos realizados a la infraestructura tecnológica.
- Dentro de la institución no existen los siguientes dominios y controles: Servicios de comercio electrónico, acceso de usuarios remotos, grupos de servicios de información, enrutamiento en las redes, actividades de trabajo remoto (teletrabajo), aislamiento de sistemas sensibles, ambientes de desarrollo, pruebas y operación.
- El personal conoce que está prohibido descargar cualquier tipo de archivo o programa sin autorización, utilización de medios extraíbles ajenos a la institución.
- El administrador del área de sistemas, aunque realiza la configuración y mantenimiento adecuado de las redes, no cuenta con un manual de procedimientos formalizado.
- No existen procedimientos formales sobre el manejo, protección, almacenamiento y eliminación de medios removibles. La información está a cargo del área que la produce.
- No existen procedimientos formales documentados sobre los procesos que se realizan dentro de la institución.
- No hay procedimientos formales, sobre el tratamiento de la información privada de la institución y el manejo de datos personales, La institución prohíbe la salida de los

medios físicos de la institución en cualquier circunstancia, no existe control para la información contenida en la mensajería (correo electrónico), ni procedimientos de protección de la información asociada con la interconexión de los sistemas de información.

- los usuarios conocen que el uso de la red es solo para las actividades académicas y administrativas de la institución, que no debe realizarse ninguna actividad personal. Los únicos equipos que se conectan a la red son de la institución, no hay autorización para que otro dispositivo tenga acceso. El acceso lógico y físico a los puertos de configuración y de diagnóstico lo realiza el administrador de sistemas quien realiza la identificación de los equipos dentro de la red, ninguno de estos procesos está formalizados o estandarizados.
- No existen controles establecidos para el acceso al sistema operativo y el uso de programas utilitarios, los usuarios de los equipos están logeados como invitados, pero no está formalizado un procedimiento adecuado de gestión de usuarios y contraseñas de acceso.
- Los únicos equipos móviles utilizados dentro de la institución son USB y portátiles, los equipos no pueden salir de las instalaciones y su uso está restringido para impartir las clases de sistemas, donde no se accede a internet.
- No existe control para los incidentes de seguridad que se presentan, solo se notifica al administrador del área de sistemas, quien realiza las actividades pertinentes para su tratamiento. A lo anterior se suma que no se realiza monitoreo de los tipos, volúmenes y costos de los incidentes y no se lleva ningún registro de dichos eventos, siendo importante en el caso de ser necesario la aplicación de una acción legal.

- La institución no cuenta en el momento con servicios de terceros donde tengan acceso a los activos de información.
- Aunque se conoce el manejo y las medidas para la protección de datos personales y la información, no existe un procedimiento formalizado.

Recomendaciones

- Crear un comité de seguridad de la información, conformado por miembros de la organización.
- Definir la "Política de Seguridad de la Información", publicarlo y comunicarlo a la comunidad educativa, realizar capacitaciones y charlas a todo el personal,
- Establecer un procedimiento de revisión de la política de seguridad.
- Realizar la asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información dentro de la institución.
- Crear una política de seguridad para el control de los recursos humanos de la institución.
- Crear manuales de procedimientos, manuales de funciones e instructivos que direccionen las actividades del cargo.
- Realizar capacitaciones a personal sobre funciones, procedimientos y políticas de seguridad establecidas.
- Establecer una política para gestionar los activos de información, donde se dicten reglas sobre el uso aceptable de la información y sus activos.
- Complementar el inventario de activos, con la identificación del responsable de este.

- Establecer una política de seguridad donde se clasifique la información en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización y un procedimiento de etiquetado de la misma.
- Crear una política de seguridad de la información, estableciendo controles de acceso apropiados, controles de seguridad física y normas de despacho y acceso público.
- implementar perímetros de seguridad en las áreas pertinentes, adquirir elementos de seguridad y desarrollar brigadas de acción ante emergencias.
- Establecer una política de seguridad de la información, creando normas para la protección del cableado de energía eléctrica y de telecomunicaciones.
- Diseñar un procedimiento de instalación, soporte y mantenimiento de equipos, que cumpla con los requerimientos de seguridad.
- Se sugiere que los dominios y controles que no están presentes en la actualidad, hacia el futuro sean implementados dentro de la organización.
- Se deben establecer medidas de protección contra códigos maliciosos, dictar charlas educativas al personal sobre las medidas de protección contra códigos maliciosos.
- Establecer normas y procedimientos documentados para la configuración y mantenimiento adecuado de las redes.
- Dentro de la Política de Seguridad de la Información, se debe establecer la normatividad para la gestión de los medios removibles y el acceso a la documentación del sistema, diseñar procedimientos para la eliminación de los medios.
- En el documento de Política de Seguridad de la Información se deben establecer políticas de intercambio de información, políticas de protección para la mensajería

electrónica y; políticas y procedimientos para la protección de información asociada con la interconexión.

- En el documento Política de Seguridad de la Información se debe establecer la restricción y control de la asignación de privilegios, proceso de control de contraseñas y la revisión periódica de los derechos de acceso de los usuarios: y diseñar un procedimiento para el alta y baja de usuarios a los servicios y sistemas de información de la institución.
- Crear una política de seguridad donde se establezcan las buenas prácticas de seguridad que los usuarios de la institución deben darle al uso de las contraseñas y la protección de los equipos desatendidos, establecer la política de escritorio y pantalla despejada.
- Se sugiere implementar un software de identificación automática de equipos en la red, además de establecer una política de restricción de usuarios a la red
- Establecer políticas de seguridad para la identificación de acceso de usuarios, de acceso al código fuente del sistema o programas utilitarios de la institución y de desconexión automática de sesión de usuarios
- Establecer una política de seguridad de medios extraíbles para portátiles y USB.
- Crear una política de seguridad donde se establezca la comunicación de eventos y debilidades en el tema de seguridad de la información.
- Crear políticas de seguridad estableciendo el procedimiento sobre manejo de incidentes de seguridad de la información, además de su cuantificación, registro y monitoreo.

Resultados estado de madurez capacidades AS IS

Luego de realizar el diagnóstico del estado actual de las capacidades relacionadas con el tema de la seguridad de la información, se procede a realizar una tabla con su estado, en una escala de 1 a 5 de grado de madurez, los resultados obtenidos son los siguientes:

Tabla 7

Estado de madurez capacidades AS IS

Capacidad	Estado de madurez
Definición y aplicación de Políticas de Seguridad de la Información de la entidad.	1. No existe
Formación del personal de la institución sobre la adopción de políticas de información.	1. No existe
Gestión de activos de información	2. Capacidad aislada
Control de Acceso y responsabilidades de los usuarios a los activos de información	2. Capacidad aislada
Gestión de Responsabilidades y procedimientos de operación	2. Capacidad aislada
Gestión de incidentes de Seguridad de la Información	1. No existe

Nota: Identificación del estado actual de las capacidades.

Fase de Planeación estado futuro

En esta fase se realizan las actividades que permitirán cerrar las brechas del sistema de seguridad de la institución.

Políticas para el SGSI

Un Sistema de Gestión de Seguridad de la Información (SGSI) tiene como finalidad preservar la información de una organización, brindando confidencialidad, integridad y disponibilidad, para realizar estas actividades es necesario diseñar políticas de seguridad que cubran los requerimientos específicos de cada organización. Lo anterior con miras a definir controles, procesos y procedimientos, que eviten o permitan el tratamiento de amenazas y riesgos a los activos de información.

La Norma ISO 27002 es un estándar para la seguridad de la información, que proporciona buenas prácticas para la gestión de la información dentro de una organización, esta norma trabaja bajo 14 dominios, 35 objetivos de control y 114 controles.

- **Objetivo General**

Establecer políticas y controles de seguridad en el Sistema de Gestión de Seguridad de la Información en el Liceo Moderno José Celestino Mutis, con el fin de preservar los activos de información, realizando una descripción detallada de los elementos que conforman este documento.

- **Objetivos de las Políticas de Seguridad de la Información**

  - ✓ Minimizar el riesgo en las funciones más importantes de la institución.

  - ✓ Cumplir con los principios de seguridad de la información.

- ✓ Cumplir con los principios de la función administrativa y académica.
- ✓ Mantener la confianza de los clientes, empleados y entidades del orden público.
- ✓ 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 del Liceo Moderno José Celestino Mutis.
- ✓ Garantizar la continuidad del negocio frente a incidentes.
- ✓ El Liceo Moderno José Celestino Mutis 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 del negocio, y a los requerimientos regulatorios (MINTIC, 2016, pp. 9-10).

- **Alcance**

Las políticas de seguridad de la información, se aplicón a los activos de información presentes en la organización de estudio “Liceo Moderno José Celestino Mutis” del municipio de San Sebastián de Mariquita, a la organización como tal, sus funcionarios, contratistas, terceros y comunidad en general. Intervendrá en todos los procesos tanto administrativos como académicos, donde los usuarios tendrán la obligación de cumplir las políticas aprobadas por el comité de seguridad de la información.

- **Requerimientos**

Para el cumplimiento, aplicación y sostenimiento de las Políticas de Seguridad de la Información en la organización, se requiere el compromiso total del Liceo Moderno JCM, sus directivas, empleados y todo aquel que haga parte de él. Asegurando la provisión de todos los recursos que se necesiten (económicos, físicos y humanos).

- **Definición de violaciones**

Dentro de las políticas se establecerá un documento de declaración de violaciones en las que pueden incurrir los diferentes usuarios de los activos de información de la organización, al no cumplir o respetar estas políticas, ya sea intencionalmente o por negligencia. Dicha declaración asegura la aplicación de sanciones disciplinarias y/o legales, previamente establecidas por las autoridades competentes.

- **Responsabilidades de los usuarios**

Los usuarios o en este caso la comunidad educativa del Liceo Moderno José Celestino Mutis, serán informados sobre las responsabilidades individuales en la protección de los activos de información dentro de la organización y de ser necesario, si el comité de seguridad lo decide, los usuarios tendrán que firmar un documento de declaración del usuario (Versión abreviada de la política de seguridad).

Tabla 8

Políticas obligatorias de seguridad de la información del Liceo Moderno José Celestino Mutis

CONTROL	GUIA DE IMPLEMENTACIÒN
Políticas de seguridad de la información de la institución educativa.	Se debe definir el conjunto de políticas o directrices para la seguridad de la información de la institución educativa, las cuáles deben obedecer y soportar cada una de las actividades, servicios o productos que ofrece la empresa; estas políticas deben ser socializadas por el departamento de seguridad de la información de la empresa, para que cada uno de los funcionarios pueda conocerla y aplicarla en sus labores diarias.
Política de control de acceso a la información a través de mecanismos de autenticación.	Se deben generar políticas de seguridad, relacionadas con el acceso de los funcionarios de la institución educativa a cada software implementado por la empresa
Políticas de usuarios y claves de acceso para los funcionarios que laboran en la institución educativa, y	Se deben generar y adoptar políticas que permitan el uso adecuado de los usuarios y claves de acceso a los portales de la institución educativa, garantizando la seguridad de la información y la mejora en la calidad de los procesos. Las claves y usuarios serán personales e intransferibles, por lo

con la cual se protegerá la información de la empresa.	tanto cada usuario responderá por el incorrecto uso que se le dé.
Políticas para la manipulación de la información relacionada con la generación de matrículas estudiantiles, certificado de notas y manipulación de información del estudiante.	Se deben implementar políticas que permitan salvaguardar los datos e información de cada uno de los usuarios, en este caso, los estudiantes, que forman parte de la institución educativa y los que se encuentran haciendo el proceso de matrícula para ingresar a alguno de los grados ofertados.
Políticas para la manipulación de la información a través de los equipos de cómputo de la institución educativa.	Se deben generar y adoptar políticas de seguridad que permitan proteger la información en cada uno de los equipos de la institución educativa, con el fin de evitar caer en manos de personas malintencionadas que puedan usarla para hacer daño a la institución o al propio cliente.
Políticas de Backup	Se deben generar y adoptar políticas de respaldo de la información, con el fin de poder protegerla y recuperarla en caso de ser borrada de los equipos fuente, o en caso de posibles ataques o daños a los equipos o redes de infraestructura, garantizando con ello la disponibilidad de la información.
Políticas de desarrollo seguro	Se deben aplicar y generar reglas para el desarrollo e implementación de software por parte de la institución educativa.

Nota. Actividades por desarrollar, para implementar las Políticas obligatorias de seguridad de la información en el Liceo JCM.

Además de las políticas de seguridad definidas por la norma ISO 27001, se definen otras políticas de seguridad para ser aplicadas en la institución educativa Liceo Moderno José Celestino Mutis. Estas políticas se relacionan a continuación:

- ✓ Políticas de seguridad de los funcionarios que laboran en la institución educativa
- ✓ Políticas de seguridad para los equipos de cómputo, redes de infraestructura, medios de almacenamiento de la información y otros equipos.
- ✓ Política de seguridad para administración de la información y su clasificación o categorización.
- ✓ Política de seguridad de bases de datos
- ✓ Políticas de seguridad de uso de aplicaciones o correo electrónico corporativo
- ✓ Políticas de seguridad relacionadas con el uso del internet en la institución.

- **Sanciones**

Todas las políticas de seguridad descritas anteriormente deben ser cumplidas y aplicadas por cada uno de los funcionarios, actores o usuarios que componen la institución educativa Liceo Moderno, por tal motivo el incumplimiento de alguna de estas políticas conllevó a sanciones, las cuales se describen a continuación:

- ✓ Retiro de la institución educativa

- ✓ Sanciones económicas según sea la infracción a las políticas de seguridad.
- ✓ Suspensión temporal de la institución educativa, según sea la infracción.
- ✓ Reubicación laboral en otra área de la organización con menor manejo de información con alta categoría.
- ✓ Otras que imponga el área de seguridad de tecnología en acuerdo con las normas y estándares nacionales.

- **Responsabilidades de los usuarios**

Los usuarios o en este caso la comunidad educativa del Liceo Moderno José Celestino Mutis, serán informados sobre las responsabilidades individuales en la protección de los activos de información dentro de la organización y de ser necesario, si el comité de seguridad lo decide, los usuarios tendrán que firmar un documento de declaración del usuario (Versión abreviada de la política de seguridad).

Políticas generales

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI del Liceo Moderno José Celestino Mutis:

El Liceo Moderno José Celestino Mutis 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 del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

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

- El Liceo Moderno José Celestino Mutis protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- El Liceo Moderno José Celestino Mutis 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.
- El Liceo Moderno José Celestino Mutis protegerá su información de las amenazas originadas por parte del personal.
- El Liceo Moderno José Celestino Mutis protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- El Liceo Moderno José Celestino Mutis controló la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- El Liceo Moderno José Celestino Mutis implementó control de acceso a la información, sistemas y recursos de red.
- El Liceo Moderno José Celestino Mutis garantizó que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- El Liceo Moderno José Celestino Mutis garantizó 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.

- El Liceo Moderno José Celestino Mutis garantizó la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- El Liceo Moderno José Celestino Mutis garantizó el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

> El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la institución, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere (MINTIC, 2016, pp. 12-13)

Se consideran uso inadecuado de los recursos informáticos de la empresa cuando el funcionario practica conductas inapropiadas, las cuales se mencionan a continuación:

a. Dar a conocer información a personas o entidades que no están autorizadas por la institución educativa.

b. Emplear la información para beneficios propios o de terceros para obtener beneficios diferentes a los planeados o definidos por la institución educativa.

c. Acceder a información sin tener la autorización de la empresa para la categoría de la información

d. Ocultar información de forma maliciosa, con el propósito de causar daño a la institución educativa.

e. Hurtar información privada o confidencial de la empresa, para fines malintencionados.

f. Alterar los activos informáticos de la institución educativa, para conseguir beneficios propios o de terceros.

g. Hacer uso del internet o programas de la empresa para enviar o recibir información no autorizada.

h. Hacer uso de los recursos informáticos de la institución educativa, para imprimir, enviar, visualizar, compartir, almacenar material pornográfico.

i. Violar las leyes y normas establecidas por la institución en cuanto a las políticas de seguridad de la información.

j. Atacar los activos informáticos de la institución educativa con cualquier tipo de virus o software de computadora malintencionado cuyo fin es destructivo.

- ✓ Los funcionarios de la institución educativa no podrán hacer uso de los equipos de cómputo, internet y otros activos de la organización, para comercializar productos propios, para juegos, cadenas y envío de mensajes de correos electrónicos personales, además no podrán utilizar de forma inadecuada los recursos eléctricos y el internet de la empresa.
- ✓ Otras políticas que tenga a bien definir la institución educativa Liceo Moderno José Celestino Mutis.

Gestión de los activos de información

Para la implementación del SGSI, la institución debe tener actualizado el inventario de activos de información, donde se recojan los activos importantes, incluyendo la siguiente información:

- **Identificación**: código ordenado.
- **Tipo**: categoría a la que pertenece, según el MEN, esta clasificación se realiza según la descripción de los activos de información:
  - ✓ Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.
  - ✓ Aplicaciones: El software que se utiliza para la gestión de la información.
  - ✓ Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.
  - ✓ Servicios: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo, la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo, la comercialización de productos).
  - ✓ Tecnología: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)
  - ✓ Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)

- ✓ Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.), (MINTIC, 2016, p. 23)

- **Descripción**: breve descripción del activo para su identificación.
- **Propietario**: Persona responsable del activo.
- **Usuario**: Persona que lo usa
- **Ubicación**: dependencia o lugar físico donde se encuentra.

Para realizar esta tarea se propone un formato ver anexo 2. Inventario y clasificación de activos de información.

Roles y Responsabilidades

Para las entidades que desean implementar un SGSI, es importante definir los roles y sus responsabilidades dentro de su equipo de trabajo, para realizar esta labor se deben definir los siguientes perfiles:

- **Responsable de Seguridad de la información**: será el líder del proyecto, escogido dentro del equipo mencionado anteriormente en cada entidad y tendrá las siguientes responsabilidades:
  - ✓ Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

- ✓ Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- ✓ Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- ✓ Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- ✓ Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- ✓ Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- ✓ Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- ✓ Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- ✓ Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- ✓ Trabajar de manera integrada con el grupo o áreas asignadas.
- ✓ Asegurar la calidad de los entregables y del proyecto en su totalidad.
- ✓ Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- ✓ Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.

- ✓ Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto (MINTIC, 2016, pp. 12-13).

- **Equipo del Proyecto**: con el fin de asegurar que toda la información de la institución esté disponible durante el desarrollo de este proyecto, debe conformarse un equipo conformado por personal perteneciente al área directiva y áreas misionales, cumpliendo con la transversalidad de este. Dicho equipo debe estar conformado de la siguiente manera:

  - ✓ Personal de seguridad de la información.
  - ✓ Un representante del área de Tecnología.
  - ✓ Un representante del área administrativa.
  - ✓ Un representante del área de Dirección.
  - ✓ Un representante de sistemas de Gestión de Calidad.
  - ✓ Un representante del área Jurídica.
  - ✓ Docente, padre de familia y proveedor

  Las responsabilidades del equipo del proyecto son las siguientes:

  - ✓ Apoyar al líder de proyecto al interior de la entidad.
  - ✓ Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
  - ✓ Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.

- ✓ Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- ✓ Las que considere el líder del proyecto o el comité de seguridad de la entidad

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante el desarrollo del proyecto, a pesar de que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo a la Ley de Protección de Datos Personales se debe tener muy presente el rol de responsable del tratamiento de los datos personales.

Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- ✓ Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- ✓ Tramitar las consultas, solicitudes y reclamos.
- ✓ Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- ✓ Respetar las condiciones de seguridad y privacidad de información del titular.

- ✓ Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente (MINTIC, 2016, pp. 16-17).

- *Comité de seguridad*: encargado de orientar la implementación de la estrategia de Gobierno en línea, asegurando la gestión y desarrollo de las iniciativas sobre seguridad de la información. En este caso la institución debe emitir una resolución para la creación del comité de seguridad de la información.

Análisis y Evaluación del Riesgo

La institución educativa debe definir criterios de riesgo detallando los niveles de riesgo, estos criterios serian la probabilidad y el impacto, los cuales se entienden como la posibilidad de que suceda un riesgo y el daño que puede ocasionar la ocurrencia de un riesgo, respectivamente

Según MINTIC, en su guía de gestión de riesgos la evaluación del riesgo "se hace de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos (MINTIC, 2016, p. 32)". Ver figura Matriz de Calificación, Evaluación y respuesta a los Riesgos.

Figura 5

Matriz de Calificación, Evaluación y respuesta a los Riesgos

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada*: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Nota: Guía de Riesgos DAFP

Resultados fase de planeación

Luego de realizar la etapa de planeación, se espera que como mínimo el estado futuro de las capacidades relacionadas con el tema de la seguridad de la información este en la escala 3, Capacidad sirviendo, para alcanzar este nivel se deben realizar ciertas acciones que cierren la brecha entre el estado actual y el estado futuro, alcanzando como mínimo capacidades sirviendo. A continuación, se muestran dichas acciones:

Tabla 8

Análisis de brecha AS IS – TO BE

Proceso	AS IS	TO BE	ACCIONES PARA CERRAR LA BRECHA
Definición y aplicación de Políticas de Seguridad de la Información de la entidad.	1. No existe	3. Capacidad sirviendo	Definición y aplicación de Políticas de Seguridad de la Información a los procesos misionales, de gestión y de apoyo de la institución.
Formación del personal de la institución sobre la adopción de políticas de información.	1. No existe	3. Capacidad sirviendo	Adelantar plan de capacitación, sensibilización y comunicación de al personal involucrado
Gestión de activos de información	2. Capacidad aislada	3. Capacidad sirviendo	Realizar el Inventario y clasificación de activos de información
Control de Acceso y responsabilidades de los usuarios a los activos de información	2. Capacidad aislada	3. Capacidad sirviendo	Aplicación de políticas específicas de seguridad de la información
Gestión de Responsabilidades y procedimientos de operación	2. Capacidad aislada	3. Capacidad sirviendo	Aplicación de políticas específicas de seguridad de la información

Gestión de incidentes de Seguridad de la Información	1. No existe	3. Capacidad sirviendo	Aplicación de políticas específicas de seguridad de la información

Nota: Identificación de actividades a realizar para alcanzar el estado futuro.

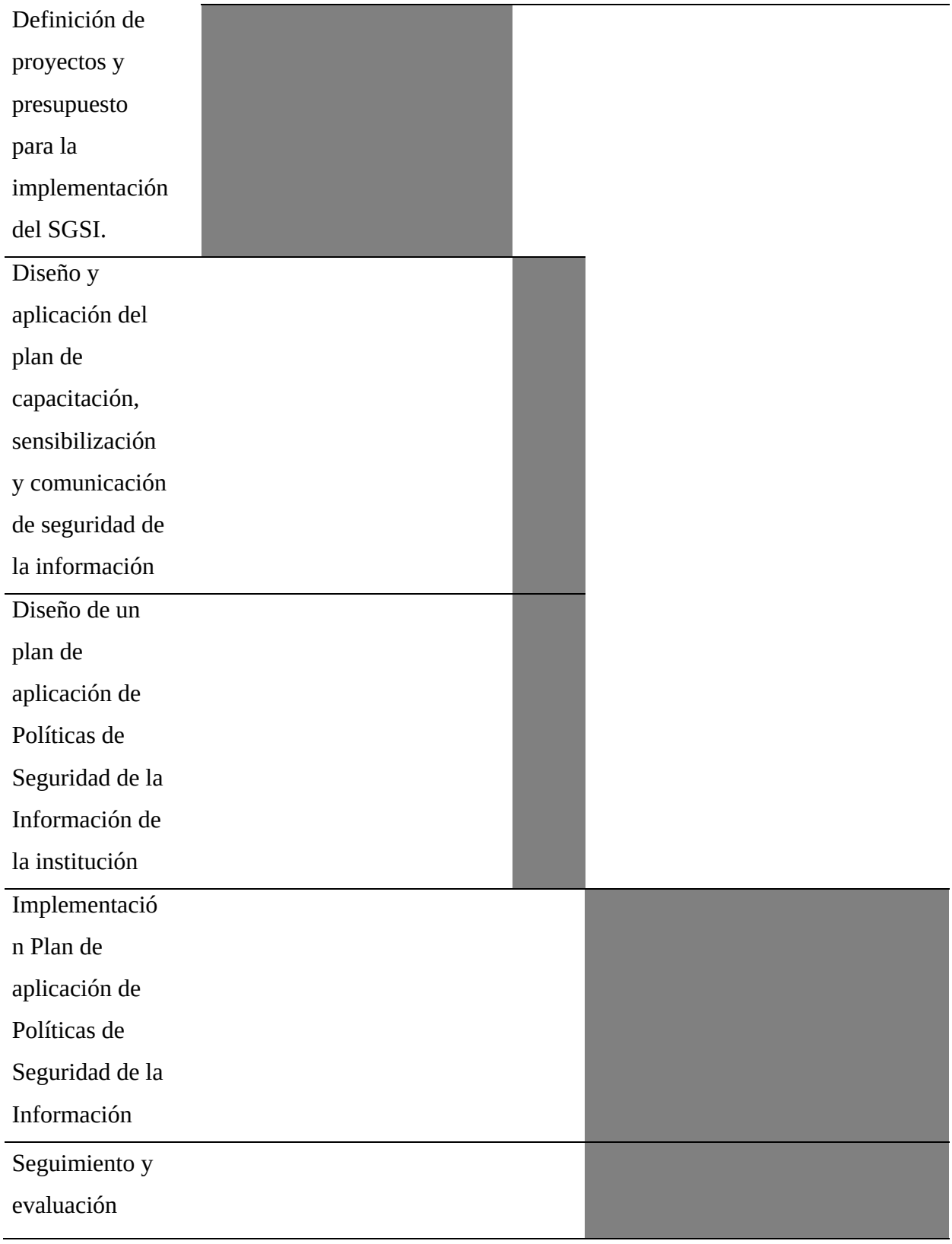
Plan de implementación del SGSI

Se propone que la fase de implementación de SGSI dentro de la institución educativa, se lleve a cabo en dos años, a partir de la fecha en la que se finalizó el presente trabajo y se entreguen los resultados a la institución, ver tabla, Cronograma de actividades. Por lo anterior, se debe tener en cuenta la clasificación de los activos y los riesgos que revisten un tratamiento urgente, duración de la aplicación de la política, costo y capacidad del personal existente.

Tabla 9

Cronograma de actividades

ACTIVIDAD	**MES**																							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**
Crear un comité de seguridad de la información, formado por miembros de la institución.																								



Nota: Programación de actividades a realizar en un plazo de 24 meses.

Crear un comité de seguridad de la información, formado por miembros de la institución.

Para iniciar con la implementación del SGSI en la institución, el primer paso es la conformación del Comité de Seguridad de la Información con el objetivo de orientar la implementación de la estrategia de Gobierno en línea en una institución educativa, asegurando el cumplimiento de las políticas de seguridad de la información.

Resultado: una resolución de conformación de dicho comité, aprobado por la dirección y publicado.

Indicador: Número de personas que conforman el comité, directivos, docentes y administrativos de la institución.

Definición de proyectos para la implementación del SGSI.

Dentro del SGSI, se deben desarrollar ciertos proyectos, que garanticen la seguridad de los activos de información, dichos proyectos tienen como objetivo general velar por un nivel de seguridad aceptable que cubra los riesgos mínimos a los que están expuestos los activos. Ver tabla Proyectos de seguridad.

Tabla 10

Proyectos de seguridad.

Proyecto: Desarrollo de políticas de seguridad				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Desarrollar el conjunto de	Implementar normatividad	2 horas semanales del	Valor hora/salario	Numero de políticas

políticas obligatorias para la seguridad de la información de la institución, siendo las encargadas de velar el cumplimiento de los servicios ofrecidos.	para el uso de los sistemas de seguridad de la información en la institución.	Comité de Seguridad de la Información	del personal responsable.	obligatorias documentadas después de 15 meses

Proyecto: Gestión de Backup de información

Descripción	Objetivo	Recursos	Costos	Indicador
La información se copia de forma organizada en medios extraíbles como memorias usb, discos duros, es importante implementar una backup en la nube, teniendo en	Implantar un sistema de copias de seguridad de la información, que permita recuperar la información en caso de un incidente.	Adquisición de un hosting con las características necesarias.	$150.000 por año	Número de copias de seguridad de la información institucional después de 18 meses

cuenta las guías de gestión documental que realiza el centro.				
Proyecto: Gestión de soporte eléctrico para infraestructura tecnológica				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Polo a tierra que provea seguridad a los equipos tecnológicos de la institución, cuando se presenten fallas eléctricas, batería de respaldo UPS que proporcione la energía suficiente para que los equipos sean apagados correctamente (21 laptops, 2 desktop, 1	Proteger equipos de descargas eléctricas, electrostática y de rayo, que se presenten en la institución. Permitir que los usuarios gestionen adecuadamente los equipos ante una falta de fluido eléctrico.	Malla a tierra (polo a tierra) UPS aprox. 3000 watts de Protección eléctrica.	$2’000.000 $3’500.000	Numero de equipos protegidos con polo a tierra y UPS después de 18 meses

impresora, 1 router, 1 accespoint).				
Proyecto: Seguridad de software				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Adquisición de software antivirus, antimalware y antispyware.	Brindar seguridad a los sistemas de información contra programas malintencionados que buscar dañar o robar la información.	Antivirus multidispositivo con vigencia de 1 año.	$250.000	Numero de equipos protegidos con antivirus después de 18 meses
Proyecto: Control de acceso físico				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Instalación y cambio de puertas en el área de sistemas, oficina de coordinación	Restringir el acceso a los equipos tecnológicos por parte de personal no autorizado	3 puertas en madera 2 horas semanales del Comité de	$600.000 Valor hora/salario del personal responsable.	3 puertas con llave instaladas en los espacios asignados, después de 15 meses.

académica y rectoría. Establecer controles de acceso a los espacios de producción de información.	Seguridad de la Información.			

Proyecto: Control de acceso lógico

Descripción	Objetivo	Recursos	Costos	Indicador
Implementación de mecanismos para proteger sistemas de información de accesos y usos indebidos. Gestionar los servicios de red, los perfiles de usuario de los sistemas.	Mantener la seguridad de la información y los sistemas.	2 horas semanales del líder de sistemas	Valor hora/salario del personal responsable	Numero de equipos con acceso restringido y Numero de perfiles de usuarios creados, después de 15 meses.

Proyecto: Acuerdos de confidencialidad				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Redactar acuerdos de confidencialidad para todo el personal académico, administrativo y terceros, definición de la normatividad y procedimientos disciplinarios.	Implantar medidas legales que protejan la información de la institución, evitando daños y fuga.	2 horas semanales del Comité de Seguridad de la Información.	Valor hora/salario del personal responsable.	Numero de acuerdos de confidencialidad formalizados, después de 15 meses.

Proyecto: Gestión de Eventos de seguridad de la información				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Realizar un registro de eventos -Intentos de acceso fallidos/exitosos -Caídas del	Establecer un procedimiento de registro y seguimiento de eventos.	2 horas semanales del Comité de Seguridad de la Información.	Valor hora/salario del personal responsable.	Número total de eventos encontrados y Número total de eventos cerrados.

sistema -Alertas de fallos entre otras.				

Proyecto: Mejoramiento procesos de operación				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Formalizar y documentar procedimientos sobre los procesos que se realizan dentro de la institución, elaborando documentos guía que reúnan toda la información de que área y de qué forma se deben realizar las distintas tareas, tanto administrativas	Lograr que los procesos desarrollados por el personal de la institución estén definidos y documentados, permitiendo elevar la calidad de los productos y su seguimiento.	2 horas semanales del Comité de Seguridad de la Información y personal responsable del área encargada.	Valor hora/salario del personal responsable.	Numero de procesos institucionales documentados y formalizados después de 18 meses.

como académicas.				
Proyecto: Formalización de responsabilidades para el personal				
Descripción	**Objetivo**	**Recursos**	**Costos**	**Indicador**
Asignar y definir las responsabilidades del personal, según el área de desempeño, tareas y actividades, reorganizando el organigrama institucional.	Mejorar el desempeño organizacional, asignando y definiendo las responsabilidades de cada área.	2 horas semanales del Comité de Seguridad de la Información.	Valor hora/salario del personal responsable.	Número de personas con su respectivo rol asignado después de 18 meses.

Nota: Identificación de proyectos que apoyan la implementación del SGSI

Diseño y aplicación del plan de capacitación, sensibilización y comunicación de seguridad de la información

Para el desarrollo de este plan se tuvo en cuenta las recomendaciones realizadas por el MINTIC:

Según MINTIC, en su guía 14 del Modelo de Seguridad y privacidad de la información, Un

> programa efectivo de sensibilización, capacitación y comunicación en seguridad de la información debe explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que generalmente están plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema.
>
> Cualquier incumplimiento a las políticas, debe llevar a la imposición de una sanción, siempre y cuando el usuario haya sido adecuadamente capacitado e informado sobre todo el contenido de seguridad correspondiente a su rol y responsabilidades dentro de la Entidad (MINTIC, 2016, p.10)

Para el diseño de este plan se deben tener en cuenta la misión, las necesidades y prioridades que tenga la institución, respecto al entrenamiento y sensibilización del personal. Cuando esta tarea de identificación de necesidades esta lista, se construye el plan en sí, el cual según el MINTIC, debe contener los siguientes elementos.

a. Políticas para que se ejecute un plan de capacitación y sensibilización, que deberán estar incluidas en la política de seguridad de la información (Ver *guía de Implementación de políticas de seguridad de la información*).
b. El alcance del programa.
c. Roles y responsabilidades de quienes diseñaran, desarrollaran, implementaran y mejoran continuamente el programa y el material.

d. Metas para cumplir con el programa desarrollado.
e. Audiencias objetivo para cada aspecto, quienes deben ser sensibilizados, quienes capacitados o entrenados.
f. Cursos obligatorios para todo el personal.
g. Temas a ser tocados en cada sesión o cada curso.
h. Métodos a desplegar para brindar las capacitaciones respectivas.
i. Frecuencia de las capacitaciones o las situaciones en las que será necesaria una capacitación (reinducciones o capacitaciones para personal nuevo, etc.).
j. Documentación y evidencia de cada aspecto del programa (incluyendo evaluaciones).
k. Evaluación y renovación del material creado (MINTIC,2016, p. 17).

Indicador: Número de errores o incumplimientos, presentados en los eventos de evaluación de la sensibilización. Total, del personal a capacitar.

Diseño de un plan de aplicación de Políticas de Seguridad de la Información de la institución

Para iniciar la implementación de seguridad de la información en los procesos de la institución, se deben tener en claro las siguientes fases:

- **Desarrollo de las políticas**: se crean, se estructuran, se redactan, se revisan y se aprueban.
- **Cumplimiento**: las políticas son implementadas y debidamente relacionadas con los controles de seguridad de la información.

- **Comunicación**: se socializa con todos los usuarios la existencia de las políticas y su obligatoriedad.
- **Monitoreo**: se verifica su efectividad y cumplimiento
- **Mantenimiento**: políticas ajustadas y debidamente actualizadas.
- **Retiro**: la política se elimina cuando ya cumplió su objetivo o ya no es necesaria.

A continuación, se propone de forma general como se debe desarrollar la planificación del SGSI para la institución:

Según el Modelo de Seguridad y Privacidad de la Información de MINTIC, las fases a seguir son:

- **Política de seguridad y privacidad de la información.**

  La Política de Seguridad y Privacidad de la información está contenida en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. La política debe contener una declaración general por parte de la administración, donde se especifique sus objetivos, alcance, nivel de cumplimiento.

  La política debe ser aprobada y divulgada al interior de la entidad.

- **Políticas de Seguridad y Privacidad de la Información.**

  Manual de políticas, donde se describe los objetivos, alcances y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas

para la gestión de la seguridad de la información. En el manual de políticas de la entidad, se debe explicar de manera general, las políticas, los principios de seguridad y la normatividad pertinente. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

- **Procedimientos de Seguridad de la Información.**

  En este Ítem se debe desarrollar y formalizar procedimientos que permitan gestionar la seguridad de la información en cada uno de los procesos definidos en la entidad.

  Para desarrollar esta actividad, la Guía No 3 - describe los procedimientos mínimos que se deberían tener en cuenta para la gestión de la seguridad al interior de la entidad.

- **Roles y Responsabilidades de Seguridad y Privacidad de la Información.**

  La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de la Entidad. Para desarrollar estas actividades, la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información, brinda información relacionada para tal fin.

- **Inventario de activos de información.**

  La entidad debe desarrollar una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios. La Guía No 5 - Gestión De Activos, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

- **Integración del MSPI con el Sistema de Gestión documental.**

  La entidad deberá alinear la documentación relacionada con seguridad de la información con el sistema de gestión documental generado o emitido conforme a los parámetros emitidos por el archivo general de la nación. La Guía No 6 - Gestión Documental, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente.

- **Identificación, Valoración y Tratamiento de Riesgos.**

  La entidad debe definir una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, asi como la declaración de aplicabilidad. Para conseguir una integración adecuada entre el MSPI y la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, se recomienda emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Para definir la

> metodología, la entidad puede hacer uso de buenas prácticas vigentes tales como: ISO 27005, Margerit, Octave, ISO 31000 o la Guía No 7 - Gestión de Riesgos emitida por el MinTIC. Para la elaboración del plan de tratamiento de riesgos y la declaración de aplicabilidad, puede emplearse la Guía No 8 - Controles de Seguridad (MINTIC, 2016, p 26).

Indicador: Numero de Políticas verificadas del total de políticas planteadas para el SGSI.

Implementación Plan de aplicación de Políticas de Seguridad de la Información

La dirección de la institución deberá iniciar la implementación en aquellos procesos misionales o procesos que se consideren la base fundamental. Además de incluir dentro de su normatividad las sanciones a las cuales están sujetos el personal que no cumpla las políticas establecidas. Para ayudar con el desarrollo de las políticas se propone un formato para la creación del Comité de Seguridad de la Información, ver anexo 3; formato de política de Seguridad y Privacidad de la Información, ver anexo 4;

Indicador: Porcentaje de implementación del SGSI en la institución después de 18 meses.

Seguimiento y evaluación

El proceso de seguimiento y monitoreo del SGSI, se hace con base a los resultados que arrojan los indicadores de la seguridad de la información, propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

Indicador: Numero de reportes de evaluación del SGSI.

Conclusiones

Se logró analizar el estado actual de la gestión de seguridad, incluyendo los sistemas de información con que cuenta la institución, identificando los activos de información: hardware, software, las amenazas y vulnerabilidades a las que están expuestas; y los controles de seguridad existentes. Los controles de seguridad de la información se presentan como normas que aseguran la confidencialidad, disponibilidad, confiabilidad e integridad de la información, frente a todas aquellas amenazas internas, externas, accidentales o deliberadas a las que se exponga la institución.

A partir del trabajo adelantado en el análisis de la situación actual frente a las normas de seguridad de la información, se diseñó la política general de seguridad y privacidad de la información, adecuadas a los requerimientos de la institución y acordes a sus objetivos misionales. La adopción de un Sistema de Gestión de Seguridad de la Información es una decisión que la dirección de cualquier organización toma, teniendo en cuenta las necesidades, objetivos organizacionales y procesos, garantizando que los riesgos a los cuales estén sujetos los activos de información se conozcan, se gestionen y se minimicen de forma eficiente.

Se proponen formatos que sirvan de guía para la futura implementación del SGSI diseñado para el Liceo Moderno José Celestino Mutis en este trabajo, los cuales están apegados al documento de seguridad y privacidad de la información, del Modelo de Seguridad y Privacidad de la Información en el marco de la Estrategia de Gobierno en Línea, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones.

Recomendaciones

Uno de los elementos básicos para el éxito de un SGSI, es la formación y concientización en seguridad de la información de todo el recurso humano de una organización, es por esto, que se recomienda realizar jornadas de socialización antes y durante la implementación del SGSI, asignando responsabilidades en las actividades de seguridad, que contribuirán al cumplimiento de los objetivos.

Si la institución decide continuar con la implementación del Sistema de Gestión de Seguridad de la Información, se recomienda diseñar un plan de sensibilización, capacitación y comunicación en seguridad de la información, dirigido a todo el personal que conforma la institución educativa, con el objetivo de mejorar los procesos de seguridad de la información.

Referencias Bibliográficas

Benavides Sepúlveda, A., Blandón Jaramillo, C. (2018). *Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico* https://www.redalyc.org/journal/849/84956661012/html/

Cárdenas Solano, L. J., Martínez Ardila, H., & Becerra-Ardila, L.E. (2016). *Gestión De Seguridad De La Información: Revisión Bibliográfica*. El Profesional de La Información, Vol. 25 n. 6, pag. 940. https://doi-org.bibliotecavirtual.unad.edu.co/10.3145/epi.2016.nov.10

Celis, C. A. & Franco, O. (2016). *Implementación del Sistema de Gestión de Seguridad de la Información – SGSI, en el proceso de apoyo "Gestión Tecnológica y de la Información" del Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON.*. [info:eu-repo/semanTIC/bachelorThesis, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/11482.

CourseHero. doc_sgsi_all.pdf - Sistema de Gestión de la Seguridad de la Información. https://www.coursehero.com/file/38441412/doc-sgsi-allpdf/

De León, J. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) Basado en la Norma ISO/IEC 27001 Para Entidades Del Estado.*

https://repository.unad.edu.co/bitstream/handle/10596/27821/%20%09jcdeleonc.pdf?sequence=3&isAllowed=y

Figueroa, C. (2018). *Diseño de un sistema de gestión de seguridad de la información para el colegio Germán Arciniegas I.E.D., bajo la norma técnica colombiana ntc ISO/IEC 27001:2013*. https://repository.unad.edu.co/bitstream/handle/10596/25633/%20fccarolina.pdf?sequence=1&isAllowed=y%20-#page=26&zoom=100,148,169

ISOTools Excellence. (2015, 28 de julio). ¿Qué es SGSI?. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la información. https://www.pmg-ssi.com/2015/07/que-es-sgsi/#:~:text=%C2%BFQu%C3%A9%20es%20un%20SGSI%3F,a%20Information%20Security%20Management%20System.

ISOTools Excellence. (2017, 3 de agosto). Norma ISO 27002: El dominio política de seguridad. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. https://www.pmg-ssi.com/2017/08/norma-iso-27002-politica-seguridad/

ISOTools Excellence. (2015, 18 de agosto). *La norma ISO 27001:2013 ¿Cuál es su estructura?*. SGSI Blog especializado en Sistemas de Gestión de Seguridad de la Información. https://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/

ISO27000.ES. (s.f.). *Glosario. ISO27000.ES*. https://www.iso27000.es/glosario.html

ISO2700.ES. (s.f.). *¿Qué es un SGSI?. SGSI*. https://www.iso27000.es/sgsi.html

ISO27000.ES. (s.f.). *Serie "27000".* http://www.iso27000.es/page8.html

ISO 2700.ES. (s.f.). *Otros, Relación de algunos de los estándares que pueden integrarse con SGSIs*. https://www.iso27000.es/iso27000.html

MinTIC. (2016). *Elaboración de la política general de seguridad y privacidad de la información.* https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MinTIC. (2016*). Guía de gestión de riesgos*. https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MinTIC. (2016*). Guía para la Implementación de Seguridad de la Información en una MIPYME*. https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

MinTIC. (2016*). Modelo de Seguridad y Privacidad de la Información.* https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

MinTIC. (2016). *Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información*. https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

MinTIC. (2016). *Roles y Responsabilidades*. https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

OCDE. *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad.* https://www.oecd.org/sti/ieconomy/34912912.pdf

Watkins, S. (2013). *An Introduction to Information Security and ISO27001:2013 : A Pocket Guide: Vol. 2nd ed. ITGP*. http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=nlebk&AN=838719&lang=es&site=eds-live&scope=site

Anexos

Anexo1. Controles ISO 27002

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO27000.es

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta. Octubre-2013

Anexo 2. Inventario y clasificación de activos de información.

	LICEO MODERNO JOSE CELESTINO MUTIS	Codigo: SGSI-F-002
	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION	Fecha: 01 de octubre de 2020
		Version 001
	FORMATO: INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN	

INVENTARIO					CLASIFICACION (confidencialidad)	Fecha de ingreso/Fecha de retiro (dd/mm/aaaa - dd/mm/aaaa)
Codigo	Nombre Activo	Descripción / Observaciones	Tipo (informacion, software, hardware, servicio, RRHH)	Ubicación		

Anexo 3. Formato creación del Comité de Seguridad de la Información

RESOLUCIÓN XX DE XXXX

"Por la cual se conforma el Comité de Seguridad de la Información del Liceo Moderno José Celestino Mutis y se definen sus funciones".

EL RECTOR DEL LICEO MODERNO JOSE CELESTINO MUTIS

En ejercicio de sus facultades legales, en especial las conferidas por …, y

CONSIDERANDO:

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el 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 en el artículo 2.2.9.1.2.1., define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que la Norma Técnica NTC- ISO-IEC 27001 del 2013 contempla los lineamientos a tener en cuenta en el diseño de las políticas en: Las Tecnologías de la Información, Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

.

Que de acuerdo a las recomendaciones de la Norma ISO27001 y el Modelo de Seguridad y privacidad de la Información establecido por el Ministerio de tecnologías de la Información y las Comunicaciones de Colombia MINTIC, se hace necesario conformar el Comité de Seguridad de la Información, el cual validará las Políticas de Seguridad de la Información para el uso adecuado de los activos de información, con el fin de asegurar la información del Liceo Moderno José Celestino Mutis y la implementación del Sistema de Gestión de Seguridad de la Información SGSI.

Que, en mérito de lo expuesto, se hace necesario la conformación del Comité de Seguridad de la Información.

RESUELVE:

Artículo 1°. Conformación del Comité de Seguridad de la Información. Créase el Comité de Seguridad de la Información de Nombre de la entidad. El Comité estará integrado así:

1. El Directivo del área de informática o su delegado.
2. El Directivo del área de Planeación o su representante.
3. El Directivo del área Jurídica (según corresponda por distribución Orgánica de la entidad) o su delegado.
4. El Directivo encargado de los sistemas de Gestión de Calidad (según corresponda por distribución Orgánica de la entidad) o su delegado
5. El Directivo encargado de la Gestión Documental (según corresponda por distribución Orgánica de la entidad) o su delegado.
6. El Directivo encargado (según corresponda por distribución Orgánica de la entidad) de Control Interno o su delegado.
7. El responsable de Seguridad de la información de la entidad.

Parágrafo 1º. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del comité. El Comité de Seguridad de la Información de la Nombre de la entidad tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad.
4. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad.
5. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
6. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
7. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
10. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
11. Las demás funciones inherentes a la naturaleza del Comité.

Parágrafo. Una vez conformado el Comité de Seguridad de la Información, este podrá expedir su reglamento, en el cual fijará el alcance de cada una de las funciones operativas señalas en el presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada XXXX (X) meses.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soporte.
5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del Secretario Técnico del Comité.

Artículo 8°. Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dado en XXXX, a los X días del mes de XXXX de XXXX

_____

XXXXXXXXXXXXXXXX
Rector

Anexo 4. Formato de política de Seguridad y Privacidad de la Información

RESOLUCIÓN XXXX DE XXXX

"Por la cual se dicta la Política General de Seguridad y Privacidad de la Informacion del Liceo Moderno José Celestino Mutis ".

EL RECTOR DEL LICEO MODERNO JOSE CELESTINO MUTIS

En ejercicio de sus facultades legales, en especial las conferidas por …, y

CONSIDERANDO:

Que el artículo 15 de la Constitución Política consagra que "todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. // En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley (…)"

Que la 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", tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.

Que la ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, la cual busca proteger la información de las personas que esté en poder de empresas públicas o entidades privadas, las cuales tienen la responsabilidad de adaptar sus procesos con el fin de realizar un manejo adecuado de sus bases de datos.

Que el Decreto 1377 de 2013, "por el cual se reglamenta parcialmente la Ley 1581 de 2012", establece en su artículo 13 que los responsables del tratamiento de la información deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los encargados del tratamiento de datos den cabal cumplimiento a las mismas.

Que el Conpes 3854 de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia.

Que el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el 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 en el artículo 2.2.9.1.2.1., define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que la Norma Técnica NTC- ISO-IEC 27001 del 2013 contempla los lineamientos a tener en cuenta en el diseño de las políticas en: Las Tecnologías de la Información, Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información.

Que, en mérito de lo expuesto, se hace necesario la creación de la Política General de Seguridad y Privacidad de la Información.

RESUELVE:

POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección de LICEO MODERNO JOSÉ CELESTINO MUTIS, 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, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para LICEO MODERNO JOSÉ CELESTINO MUTIS, la protección de la información busca 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 LICEO MODERNO JOSÉ CELESTINO MUTIS*
- *Garantizar la continuidad del negocio frente a incidentes.*
- *LICEO MODERNO JOSÉ CELESTINO MUTIS 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 del negocio, y a los requerimientos regulatorios.*

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de LICEO MODERNO JOSÉ CELESTINO MUTIS:

*• 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**.*

*• LICEO MODERNO JOSÉ CELESTINO MUTIS **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.*

*• LICEO MODERNO JOSÉ CELESTINO MUTIS **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.*

- *LICEO MODERNO JOSÉ CELESTINO MUTIS **protegerá su información** de las amenazas originadas por parte **del personal**.*

*• LICEO MODERNO JOSÉ CELESTINO MUTIS **protegerá las instalaciones** de procesamiento y la infraestructura tecnológica **que soporta sus procesos críticos**.*

*• LICEO MODERNO JOSÉ CELESTINO MUTIS **controlará la operación** de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.*

*• LICEO MODERNO JOSÉ CELESTINO MUTIS **implementará control de acceso** a la información, sistemas y recursos de red.*

• LICEO MODERNO JOSÉ CELESTINO MUTIS garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
• LICEO MODERNO JOSÉ CELESTINO MUTIS 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.

• LICEO MODERNO JOSÉ CELESTINO MUTIS ***garantizará la disponibilidad*** *de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.*

• LICEO MODERNO JOSÉ CELESTINO MUTIS garantizará el cumplimiento de las ***obligaciones legales, regulatorias y contractuales establecidas.***

La presente Resolución rige a partir de la fecha de su expedición y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dado en la ciudad de San Sebastián de Mariquita, a los XXX días del mes de XXXXXXXXX de XXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Rector y Representante legal del Liceo Moderno José Celestino Mutis