Título:

Esquema de ciberseguridad y recomendaciones para el manejo de información de PYMES en Colombia.

Carlos Alberto Peña Montenegro

Wilmer Alberto Gil Moreno
Asesor interno por parte de Universidad de Antioquia
Yeyson Jehu Hernández Gallego
Asesor interno de práctica de parte de Bancolombia

Universidad de Antioquia
Facultad de ingeniería, escuela de ingeniería de sistemas, Corporación UdeA
Pregrado
Medellín
2023

Cita	Peña Montenegro [1]
Referencia Estilo IEEE (2020)	[1] C. Peña Montenegro, "Esquema de ciberseguridad y recomendaciones para el manejo de información de PYMES", grado presencial, pregrado en ingeniería de sistemas UdeA, Universidad de Antioquia, Medellín, 2023.

creative commons BY NC SA

Créditos al escenario de las prácticas en Bancolombia y el entorno LDC Seguridad de los datos que me acompañó en el proceso.

UNIVERSIDAD DE ANTIOQUIA
Vicerrectoría de Docencia

Sistema de Bibliotecas

Centro de documentación de ingeniería (CENDOI)

Repositorio Institucional: http://bibliotecadigital.udea.edu.co

Universidad de Antioquia - www.udea.edu.co

Rector: Jhon Jairo Arboleda Céspedes

Decano de la facultad de ingeniería: Julio César Saldarriaga Molina

Jefe departamento: Diego José Luis Botia

El contenido de esta obra corresponde al derecho de expresión de los autores y no compromete el pensamiento institucional de la Universidad de Antioquia ni desata su responsabilidad frente a terceros. Los autores asumen la responsabilidad por los derechos de autor y conexos.

Dedicado a mi familia, a mi padre, a mis ángeles y todos aquellos que han sido mi soporte incondicional y estable en el tiempo.

Agradecimientos a
Universidad de Antioquia
Wilmer Gil
Equipo de Bancolombia LDC Seguridad de los Datos

TABLA DE CONTENIDO

LISTA DE FIGURAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

PYME:	Pequeña y mediana empresa
SME:	Small and medium-sized enterprise o subject matter expert
ISO:	International Organization for Standardization
RUT:	Registro Único Tributario
DIAN:	Dirección de Impuestos y Aduanas Nacionales
SGSI:	Sistema de Gestión de Seguridad de la Información
NIST:	National Institute of Standards and Technology
COBIT:	Control Objectives for Information and Related Technologies
FFIEC:	Federal Financial Institutions Examination Council
OWASP:	Open Web Application Security Project

RESUMEN

En el marco de las prácticas realizadas en Bancolombia en el primer periodo de 2023, se comprometió con la entidad bancaria realizar un desarrollo en el entorno de ciberseguridad el cual solo lo conocería el banco, para salvaguardar la información y los conocimientos de banco se comprometió con Universidad de Antioquia un escrito dónde se revisa lo que debe seguir una empresa PYME en Colombia para poder establecer un esquema de ciberseguridad desde el campo de manejo de sistemas de información, se revisa la normativa ISO 27001, este escrito contiene esa información.

Palabras clave — Ciberseguridad, ISO 27001, PYME.

ABSTRACT

Within the framework of the internship carried out in Bancolombia in the first season of 2023, it was promised to the bank to carry out a development in the cybersecurity environment, which would only be known to the bank, to safeguard the information and knowledge of the bank, it committed to University of Antioquia a writing where what an SME company in Colombia must follow is reviewed in order to establish a cybersecurity scheme from the field of information systems management, the ISO 27001 standard is reviewed, the current document contents this information.

Keywords — Cybersecurity, ISO 27001, SMEs.

I. INTRODUCCIÓN

Este trabajo se desarrolla en el primer periodo de 2023 dentro el marco de las practicas académicas en la Universidad de Antioquia, en ellas se realizó las prácticas en el entorno de ciberseguridad y la línea de conocimientos de Seguridad de los Datos de la entidad bancaria Bancolombia. Con la entidad bancaria se comprometió mejorar un desarrollo que venía siendo trabajado por un practicante anterior, se realizó labores del día a día del equipo de trabajo y se entregó tanto el desarrollo con su código fuente como la configuración de las maquinas del entorno para el despliegue del mismo, sus respectivos manuales técnico y de usuario, sin embargo, para proteger la información del banco se pactó con los asesores internos tanto de banco como de Universidad de Antioquia la entrega de una revisión de la norma ISO 27001 para la gestión de seguridad de pequeñas empresas.

Las PYME en Colombia tienen un marco legal que rige desde su establecimiento hasta su funcionamiento, la variedad de empresas que se pueden crear es ilimitada, cada campo tiene su respectiva legislación que se debe seguir, esta revisión aborda las PYME de manera muy general ya que existe un amplio espectro para hablar de ellas y basa la información que se presenta en el manejo de sistemas de información en ellas.

En ese documento se aborda alguno de los requisitos que se debe seguir para considerar una empresa PYME organizada, una vez que ello esté bien definido y establecido desde su constitución se sugiere que se inicie con la gestión de la seguridad de la información abordando paulatinamente los conceptos necesarios para la implementación de ello.

JUSTIFICACIÓN

La ciberseguridad es un factor clave para la competitividad y el desarrollo de las PYMES en Colombia, ya que les permite proteger su información, su reputación, su continuidad y su innovación. La información es el activo más valioso de las pymes, y su pérdida o compromiso puede tener consecuencias graves para su negocio. También es un requisito legal y normativo para las PYMES, ya que deben cumplir con las disposiciones vigentes en materia de protección de datos personales, ciberseguridad y demás aspectos relacionados con la gestión de la información. El incumplimiento de estas disposiciones puede acarrear sanciones legales y reputacionales para las pymes. La seguridad de los datos desafío constante para las PYMES, ya que se enfrentan a amenazas cada vez más sofisticadas y variadas, que pueden provenir de actores maliciosos internos o externos, o de errores humanos o técnicos. Las PYMES deben estar preparadas para prevenir, detectar y responder a estos incidentes, y recuperarse de ellos.

Implementar sistemas de gestión de activos a las PYMES les permite mejorar su calidad, su eficiencia y su valor agregado. Al implementar un esquema de ciberseguridad basado en ISO 27001 y normativa colombiana, las PYMES pueden demostrar su compromiso con las mejores prácticas de seguridad de la información, y generar confianza y satisfacción en sus clientes, proveedores, empleados y demás partes interesadas

II. OBJETIVOS

A. Objetivo general

Presentar una propuesta de esquema general con el uso de buenas prácticas de ciberseguridad en el manejo de datos, información y activos de información een sistemas que utilicen grandes volúmenes de datos.

B. Objetivos específicos

- Establecer pautas mínimas de ciberseguridad para el manejo da datos que puedan ser implementadas desde PYMES y que puedan escalarse a grandes empresas.
- Identificar el impacto y los riesgos que existe en el manejo de procesos inteligentes que puedan incluir automatizaciones en sistemas que utilicen volúmenes de datos.

III. MARCO TEÓRICO

Las PYME son las siglas de Pequeñas y Medianas Empresas. Son aquellas que tienen un número limitado de trabajadores, un valor de activos y unos ingresos por actividades ordinarias que no superan ciertos umbrales establecidos por la ley.[1]

Las PYMES se clasifican en tres categorías:

- Microempresas
- Pequeñas empresas
- Medianas empresas.

Cada categoría tiene sus propios criterios de tamaño, según el sector económico al que pertenezcan.

Las PYME son muy importantes para la economía y el desarrollo del país, ya que representan el 90% de las empresas colombianas y generan el 65% del empleo formal. Según Confecámaras, en el año 2020 había cerca de 1.7 millones de PYME registradas en el país, de las cuales el 96% eran microempresas, el 3.4% eran pequeñas empresas y el 0.6% eran medianas empresas. La mayoría de las PYMES se concentran en los sectores de comercio, servicios y manufactura.[2]

Para constituir una PYME en Colombia, se debe seguir una serie de pautas legales y administrativas que permitan formalizar el negocio y acceder a los beneficios que el gobierno ofrece a este segmento empresarial. Los pasos básicos son los siguientes, [3]:

- Elegir el nombre o razón social de la empresa y verificar su disponibilidad en la Cámara de Comercio o entidad competente.
- Definir el tipo societario o forma jurídica de la empresa, según la naturaleza y el tamaño del negocio.
- Elaborar los estatutos o documento constitutivo de la empresa, donde se establecen los derechos y obligaciones de los socios o accionistas, el objeto social, el capital social, la duración, la administración y la distribución de utilidades.

- Inscribir la empresa ante la Cámara de Comercio o entidad competente, presentando los documentos requeridos y pagando los derechos correspondientes.
- Obtener el Registro Único Tributario (RUT) ante la Dirección de Impuestos y Aduanas Nacionales (DIAN), donde se identifica a la empresa como contribuyente y se le asigna un número único.
- Abrir una cuenta bancaria a nombre de la empresa, donde se depositará el capital social y se manejarán los recursos financieros del negocio.
- Afiliar a la empresa y a sus trabajadores al sistema de seguridad social integral, que comprende salud, pensión, riesgos laborales y caja de compensación familiar.
- Cumplir con las obligaciones tributarias, laborales, comerciales y ambientales que le correspondan a la empresa según su actividad económica y su tamaño.
- Solicitar los permisos, licencias o registros especiales que se requieran para el funcionamiento del negocio según su sector o actividad.

Partimos del supuesto que la empresa a la que se le va a recomendar implementar un **sistema de gestión de información** ya cumple con todos los requisitos de ley en Colombia y que ella está organizada desde su constitución, es importante recalcar que para que la empresa esté organizada debe tener muy claro dentro de la constitución de sus estatutos o en sus estatutos un organigrama que permita identificar las áreas que hacen parte de ella, una vez cumplido el supuesto avanzamos a revisar qué se necesita para implementar el sistema de gestión de activos.

Sistema de gestión de seguridad de la información

Es un sistema vivo para la gestión de la seguridad de la información que varía en el tiempo y debe ser actualizado, en promedio a un equipo de implementación le podría tardar entre 6 meses a 1 año, dependiendo del tamaño de la organización para llegar a su primera versión. Compuesto de políticas, guías, recursos y actividades gestionados de forma colectiva.

Se debe:

- Evaluar el sistema
- Capacitar

- Implementar normas

Para la implementación de un sistema de seguridad empecemos por seguir la ley que rige el uso y tratamiento de datos en Colombia.

- **Habeas data**

Acerca de la normativa vigente para cuestiones de seguridad de la información también pueden consultarse:

- NIST Cybersecurity Framework
- COBIT 2019
- **ISO/IEC 27001**
- ISO/IEC 27002
- ISO/IEX 27032
- FFIEC
- OWASP
- CIS
- Entre otros

A continuación, se aborda brevemente de qué trata cada uno:

Habeas data es un derecho que tiene toda persona de conocer, actualizar y rectificar la información que se haya recogido sobre ella en archivos y bancos de datos de organismos públicos o privados. Es una garantía constitucional que protege a las personas contra el uso abusivo de información personal, sobre todo cuando esta ha sido obtenida de forma ilícita o fraudulenta. [3]

- NIST Cybersecurity Framework es un marco de referencia para la gestión de la ciberseguridad, que proporciona orientación para identificar, proteger, detectar, responder y recuperarse ante las amenazas cibernéticas. Está basado en las mejores prácticas reconocidas internacionalmente y está dirigido a organizaciones de todos los tamaños y sectores. [4]
- COBIT 2019 es un marco de trabajo para la gobernabilidad y gestión de la información y tecnología empresarial (I&T), que apoya el logro de los objetivos de la organización. Este programa ofrece una guía para establecer, implementar, mantener y mejorar un sistema de

gestión de I&T basado en principios, objetivos, componentes y habilitadores. [5]

- ISO/IEC 27001 es el estándar internacional para los sistemas de gestión de la seguridad de la información (SGSI). Define los requisitos que debe cumplir un SGSI para asegurar la confidencialidad, integridad y disponibilidad de la información. Es consistente con las mejores prácticas descritas en ISO/IEC 27002, que ofrece un conjunto de controles genéricos para la seguridad de la información [6] (27001, 2022)

- ISO/IEC 27002 es una norma internacional que proporciona una referencia para los controles de seguridad de la información, incluyendo orientación para su implementación. Está diseñada para ser utilizada por las organizaciones: a) dentro del contexto de un SGSI basado en ISO/IEC 27001; b) para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente; c) para desarrollar directrices específicas para la gestión de la seguridad de la información [6]

- ISO/IEC 27032 es una norma internacional que ofrece directrices para mejorar el estado de la ciberseguridad, resaltando los aspectos únicos de esa actividad y sus dependencias con otros dominios de seguridad, en particular: seguridad de la información, seguridad de las redes, seguridad en internet y protección de las infraestructuras críticas de información (ICI). Cubre las prácticas básicas de seguridad para los interesados en el ciberespacio [6] (27001, 2022)

  OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web) es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro. Entre sus recursos más destacados se encuentran el OWASP Top 10, que es un documento de concienciación sobre los riesgos más críticos para la seguridad de las aplicaciones web; y el OWASP Testing Guide, que es una metodología para evaluar la seguridad de las aplicaciones web. [7]

- CIS (Center for Internet Security) es una organización sin fines lucrativos que se dedica a salvaguardar a las organizaciones públicas y privadas contra las amenazas cibernéticas. Entre sus recursos más reconocidos se encuentran los CIS Controls, que son un conjunto

de acciones prioritarias para defenderse contra los ataques cibernéticos más comunes; y los CIS Benchmarks, que son unas guías de configuración segura para más de 100 tecnologías diferentes. [8]

El **Habeas Data** es un derecho fundamental que tienen todos los colombianos a conocer, actualizar y rectificar la información personal que hayan recogido los bancos de datos, entidades públicas y privadas. Este derecho está consagrado en la Constitución de 1991 y desarrollado por las leyes 1266 de 2008 y 1581 de 2012. Estas leyes establecen los principios, derechos, deberes y procedimientos para el tratamiento de datos personales, así como las sanciones por su incumplimiento. El Habeas Data es importante porque protege la intimidad, la honra y el buen nombre de las personas, así como el acceso a la información pública. Además, el Habeas Data contribuye a prevenir el fraude, el robo de identidad, el lavado de activos y la financiación del terrorismo. Por lo tanto, revisar la normativa de Habeas Data es fundamental para cumplir con la ley y garantizar la seguridad de la información personal en Colombia

Las **ISO 27001** son normas internacionales que proporcionan un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI). Un SGSI es un conjunto de políticas, procedimientos, controles y medidas que se aplican para proteger la confidencialidad, integridad y disponibilidad de la información. Las ISO 27001 establecen los requisitos para diseñar, implementar, operar y mejorar un SGSI, así como para evaluar su eficacia y conformidad. Las ISO 27001 son beneficiosas porque ayudan a prevenir y mitigar los riesgos de seguridad de la información, tales como ataques cibernéticos, violaciones de datos, pérdidas o daños de información, entre otros. Además, las ISO 27001 mejoran la confianza y la reputación de las organizaciones que las adoptan, ya que demuestran su compromiso con las mejores prácticas de seguridad de la información. Por lo tanto, revisar las ISO 27001 es conveniente para asegurar la calidad y el valor de la información en Colombia. [6]

- Fundamentos
- Implementación
- Auditoría

IV. METODOLOGÍA

Este trabajo se llevó a cabo siguiendo las pautas de la norma ISO 27001 que como cualquier miembro activo de la comunidad de la Universidad de Antioquia puede consultar en el repositorio de la base de datos, antes de generar cualquier ruta a seguir lo primero que se hizo fue hacer una lectura del documento por medio del repositorio de Normas Técnicas Colombianas ICONTEC buscando la norma ISO 27001, cabe resaltar que la norma original en inglés solo da acceso a una sola consulta, por ello se recomienda primero estudiar la normativa en español y cuando se tenga dominio de ella acceder a la consulta de la norma ISO 27001 original en su idioma inglés.

Una vez conocida la estructura y el contenido de la normativa se hizo generó una propuesta en cronograma para abordar la norma con el fin de generar un esquema de ciberseguridad basado en dicha normativa. Para el desarrollo del proyecto que se entrega a Universidad de Antioquia, se aborda este documento de la siguiente manera:

- La primera parte es el contexto del proyecto, donde se definen los objetivos, el alcance, los requisitos y las partes interesadas del esquema de ciberseguridad.
- La segunda parte es el análisis de riesgos, donde se identifican y evalúan los riesgos de seguridad que pueden afectar a las PYMEs, y se determinan los niveles de aceptación y tratamiento de los mismos.
- La tercera parte es el diseño del sistema SGSI, donde se menciona la importancia en crear las políticas, los procesos, los controles y las medidas de seguridad que se aplicarán a las PYMEs para prevenir, detectar y responder a los incidentes de seguridad.
- La cuarta parte es la implementación de un esquema.

Se estableció un cronograma en sus inicios que fue ajustado en el último mes de julio, la siguiente información contiene el cronograma de cómo fueron abordados los temas y revisados con el asesor interno de Universidad de Antioquia:

Viernes 31 de marzo de 2023:

- Revisión de los objetivos del proyecto.
- Revisión de los requisitos del proyecto.
- Definición del plan de trabajo y plazos.

Viernes 8 de abril de 2023:

- Revisión de los procedimientos de gestión de incidentes de seguridad.
- Establecimiento de los procedimientos de auditoría y seguimiento de los procesos de seguridad.

Viernes 14 de abril de 2023:

- Revisión de los procesos de seguridad que se aplicarán a las PYMEs en función de la norma ISO 27001.
- Identificación de los posibles riesgos de seguridad y sus posibles consecuencias.
- Definición de los mecanismos de control de seguridad.

Viernes 21 de abril de 2023:

- Revisión de las políticas de seguridad y procedimientos de seguridad que se aplicarán las PYMEs.
- Definición de las medidas de seguridad física y lógica que se aplicarán para prevenir posibles riesgos.
- Establecimiento de las medidas de seguridad de acceso y autenticación.

Viernes 5 de mayo de 2023:

- Revisión de la documentación necesaria para la implementación del esquema.
- Revisión de la presentación final del proyecto.
- Realización de correcciones y aclaraciones necesarias.

Viernes 26 de mayo de 2023:

- Revisión final del esquema general de ciberseguridad basado en ISO 27001 para PYMEs.
- Preparación de la documentación final y entrega del proyecto.
- Realización de correcciones y aclaraciones necesarias.

Viernes julio 7 de 2023:

- Revisión y corrección final del proyecto.
- Preparación de la presentación final.

Viernes Julio 14 de 2023:

- Presentación final del proyecto.
- Resolución de dudas y preguntas.
- Realización de correcciones y aclaraciones finales.

V. RESULTADOS

Siguiendo la metodología y las pautas establecidas para generar el esquema de ciberseguridad estos son los resultados esperados:

1. Un esquema de ciberseguridad bien definido y documentado que incluya una lista clara de las buenas prácticas y los estándares que se van a utilizar en la protección de los datos.
2. Un análisis detallado de los riesgos asociados a los procesos y las automatizaciones utilizados en las PYMES que podrían aumentar significativamente el volumen de datos, y cómo estos riesgos van a ser mitigados.
3. Una estrategia clara para implementar y escalar el esquema de ciberseguridad en diferentes tipos de empresas, desde las PYMES hasta las grandes empresas.

Siguiendo la guía de los resultados esperados, estos son los resultados obtenidos:
1. Un esquema de ciberseguridad bien definido y documentado debe incluir los siguientes elementos:

- Un **análisis de riesgos** que identifique los activos de información más críticos y sensibles para tu negocio, así como las amenazas y vulnerabilidades que los ponen en peligro.
- Una **política de seguridad** que establezca los objetivos, principios, roles y responsabilidades de la gestión de la seguridad de la información en tu empresa, así como las normas y estándares que se van a seguir.
- Un **conjunto de controles de seguridad** que implementen las medidas técnicas, organizativas y legales necesarias para proteger los activos de información, prevenir los incidentes, detectarlos y responder a ellos, y recuperarse de ellos.
- Un **plan de formación y concienciación** para tus empleados, que les enseñe las buenas prácticas de seguridad y les haga partícipes de la protección de la información.

- Un **plan de auditoría y revisión** que verifique el cumplimiento de la política y los controles de seguridad, así como su eficacia y eficiencia, y que proponga acciones de mejora continua.

2. Para generar un análisis detallado de los riesgos asociados a los procesos y las automatizaciones utilizados en las PYMES, se puede seguir los siguientes pasos basados en la norma ISO/IEC 27001:

- Define una metodología de evaluación de riesgos que se adapte a tu contexto y a tus objetivos, y que especifique los criterios para evaluar las consecuencias y las probabilidades de cada riesgo, así como el nivel de riesgo aceptable.
- **Identifica los activos** de información que son relevantes para tu negocio, como los datos de clientes, proveedores, empleados, productos, servicios, etc., y asigna un responsable para cada uno de ellos.
- **Identifica las amenazas** que pueden afectar a tus activos de información, como los ataques cibernéticos, los errores humanos, los desastres naturales, etc., y las vulnerabilidades que pueden facilitar su ocurrencia, como las debilidades técnicas, organizativas o legales.
- **Evalúa las consecuencias** y las probabilidades de cada combinación de activo/amenaza/vulnerabilidad, utilizando la escala que hayas definido en tu metodología. Puedes hacerlo de forma cualitativa (usando categorías como bajo, medio o alto) o cuantitativa (usando valores numéricos o monetarios).
- **Calcula el nivel de riesgo** para cada combinación, multiplicando las consecuencias por las probabilidades. Puedes usar una matriz de riesgos para visualizar el resultado y comparar los diferentes riesgos**.**
- **Determina cuáles son los riesgos no aceptables**, es decir, aquellos que superan el nivel de riesgo aceptable que hayas establecido en tu metodología, y que requieren una acción de tratamiento.

Para mitigar los riesgos no aceptables, tienes cuatro opciones:

- **Aplicar controles de seguridad** que reduzcan la probabilidad o el impacto del riesgo. Puedes basarte en el anexo A de la norma ISO/IEC 27001, que contiene 114 controles agrupados en 14 dominios, o en otras fuentes de buenas prácticas.

- **Transferir el riesgo a otra parte,** por ejemplo, contratando un seguro o externalizando un servicio.
- Evitar el riesgo, eliminando la actividad o el proceso que lo genera.
- **Aceptar el riesgo,** asumiendo sus posibles consecuencias.

Para cada opción de tratamiento, se debe documentar los recursos necesarios, los responsables asignados y los plazos previstos. También se debe revisar periódicamente la efectividad de los tratamientos aplicados y actualizar el análisis de riesgos según cambien las circunstancias.

3. Para implementar una estrategia clara para implementar y escalar el esquema de ciberseguridad en diferentes tipos de empresas, siguiendo la norma ISO/IEC 27001, se puede seguir los siguientes pasos:

- **Define el alcance y los objetivos de tu sistema** de gestión de seguridad de la información (SGSI), teniendo en cuenta el contexto y las partes interesadas de tu organización, así como los requisitos legales y contractuales que debes cumplir.
- **Establece una política de seguridad de la información** que refleje el compromiso de la dirección con el SGSI y que sea coherente con los objetivos estratégicos de tu organización.
- **Asigna los roles y responsabilidades para la gestión del SGSI**, asegurando que haya una persona o un equipo encargado de liderar, coordinar y supervisar el SGSI, y que todos los empleados estén involucrados y capacitados en materia de seguridad de la información.
- **Realiza un análisis y una evaluación de riesgos,** siguiendo la metodología que hayas definido previamente, para identificar y valorar los riesgos que afectan a tus activos de información y determinar cuáles son los riesgos no aceptables que debes tratar.
- **Selecciona e implementa los controles de seguridad** adecuados para mitigar los riesgos no aceptables, basándote en el anexo A de la norma ISO/IEC 27001 o en otras fuentes de buenas prácticas. Documenta los controles en una declaración de aplicabilidad (SOA) y en otros procedimientos o registros que sean necesarios.
- **Establece un proceso de monitorización, medición, análisis y evaluación del SGSI**, definiendo los indicadores e instrumentos que te permitan verificar el desempeño y la eficacia del SGSI, así como el cumplimiento de los requisitos y objetivos establecidos.

- **Implementa un proceso de auditoría interna del SGSI**, que te permita verificar el grado de conformidad del SGSI con la norma ISO/IEC 27001 y con tu propia política y procedimientos, así como identificar las oportunidades de mejora.
- **Implementa un proceso de revisión por la dirección del SGSI**, que te permita evaluar el estado general del SGSI, así como su alineación con la estrategia y las necesidades de tu organización, y tomar las decisiones pertinentes para mejorar su funcionamiento.
- **Implementa un proceso de mejora continua del SGSI,** que te permita corregir las no conformidades detectadas en las auditorías o revisiones, así como prevenir su recurrencia o su ocurrencia potencial. También debes estar atento a los cambios internos o externos que puedan afectar al SGSI y adaptarlo en consecuencia.

Para hacer tangible el texto anterior y su explicación presentada, se organizó la información del esquema final de este trabajo en un esquema de flujo. A continuación, presentamos el resultado final que es el esquema de ciberseguridad propuesto teniendo en cuenta todas las cuestiones normativas expuestas:

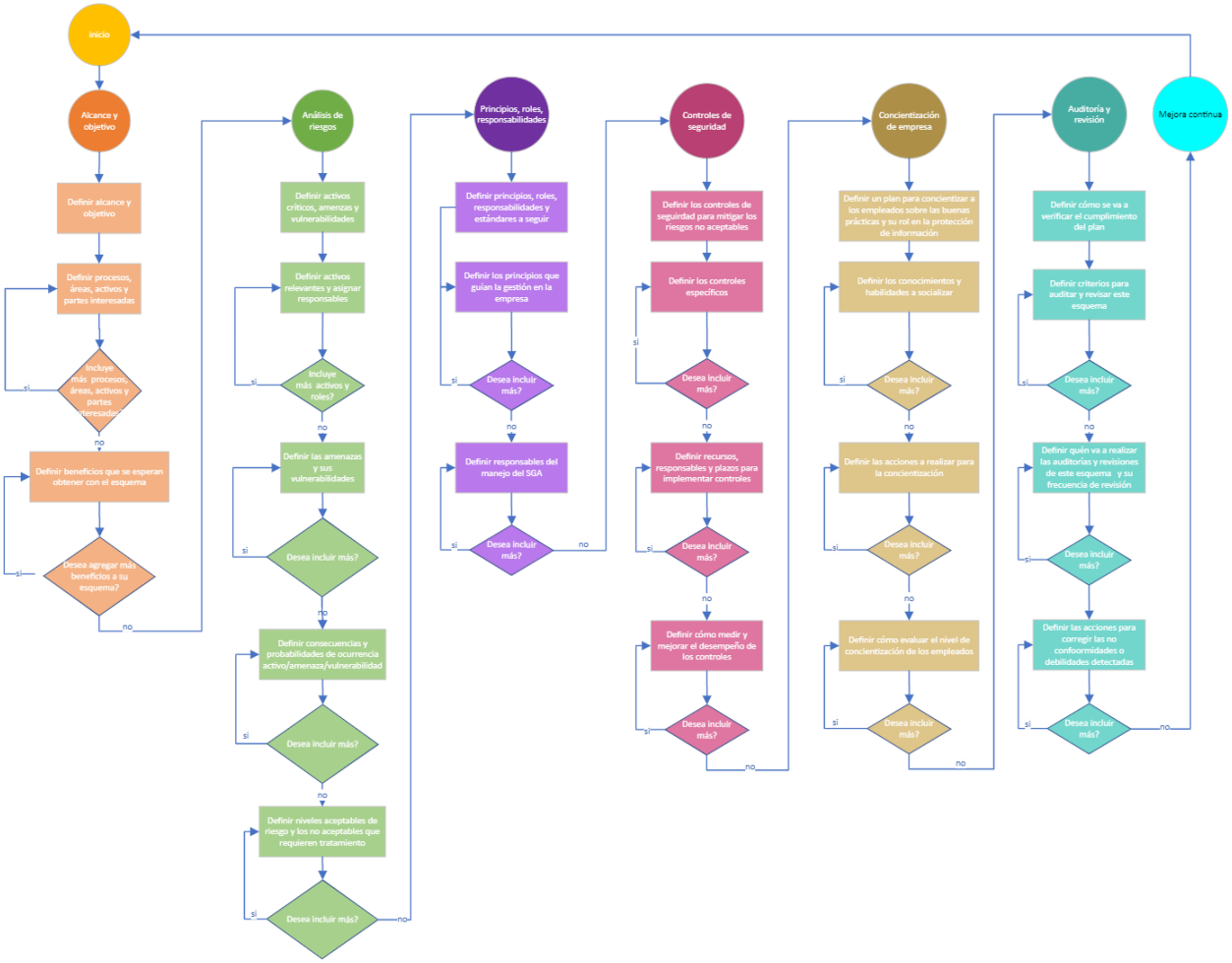

Fig. 1. Esquema de ciberseguridad para PYMES en Colombia

VI. ANÁLISIS

Se recalca la importancia de conocer el dominio de cada uno de los negocios y diferenciar que cada empresa maneja un core diferente en su manejo de información, la normativa es cambiante y se adapta en el tiempo a los cambios y restructuraciones que tenga la vida misma en materia de manejo de información. Se sugiere implementar estos sistemas de gestión de información desde la misma constitución de las compañías pues generar los cambios después de nunca haber tenido estos sistemas de gestión suele tomar tiempo adicional mientras se identifica la información previa y se realiza la migración.

Para hacer un correcto uso del diagrama que se presenta en este trabajo, se recomienda guiarse por las pautas que brinda la normativa ISO 27001, en dicho sentido, es muy importante tener en cuenta que la normativa puede variar en el tiempo y que cada actualización debería actualizar el esquema que en este trabajo se presenta, por otra parte, merece resaltar que estamos viviendo un momento de eclosión tecnológica donde avanzan sus técnicas a pasos agigantados con la aparición de las inteligencias artificiales y el uso comercial que todos le están dando a ellas, de modo que es posible que existan cuestiones normativas en ISO 27001 que aún no se hayan tenido en cuenta y que en el curso de un mes o dos puedan cambiar la forma como se lleva a cabo la seguridad de la información y la ciberseguridad en las empresas por lo que se sugiere al lector, utilizar esta normativa como una de tantas que debe consultar y mantenerse actualizado con las vulnerabilidades, riesgos, técnicas y normas que puedan recomendarse para que pueda proteger, salvaguardar la información y que al mismo tiempo su información esté siempre disponible.

Cabe resaltar que el ciclo de mejora continua va a permitir tener sistemas que puedan escalar en el tiempo y se adapten a las nuevas necesidades de las empresas.

VII. CONCLUSIONES

- La implementación de un esquema de ciberseguridad basado en ISO 27001 y normativa colombiana para pymes es un proceso que requiere planificación, ejecución, seguimiento y mejora continua.
- El esquema de ciberseguridad tiene como objetivo proteger los activos de información más críticos y sensibles para el negocio, así como cumplir con los requisitos legales y normativos vigentes.
- El esquema de ciberseguridad se basa en un análisis de riesgos que identifica las amenazas y vulnerabilidades que pueden afectar a los activos de información, y determina los controles de seguridad adecuados para mitigarlos.
- El esquema de ciberseguridad se rige por una política de seguridad que define los principios, roles y responsabilidades de la gestión de la seguridad de la información en la empresa, así como las normas y estándares que se van a seguir.
- El esquema de ciberseguridad implica la formación y concienciación de los empleados sobre las buenas prácticas de seguridad y su papel en la protección de la información.
- El esquema de ciberseguridad se somete a auditorías y revisiones periódicas para verificar su cumplimiento, eficacia y eficiencia, y proponer acciones de mejora continua.

VIII. RECOMENDACIONES

- Antes de iniciar el proceso de implementación, debes contar con el apoyo y el compromiso de la alta dirección de tu empresa, ya que ellos son los responsables de definir la política de seguridad y asignar los recursos necesarios para el esquema de ciberseguridad.
- Durante el proceso de implementación, debes involucrar a todos los empleados y partes interesadas de tu empresa, ya que ellos son los usuarios y custodios de la información, y deben estar alineados con los objetivos y las buenas prácticas de seguridad.
- Después del proceso de implementación, debes mantener y mejorar el esquema de ciberseguridad, ya que la seguridad es un proceso dinámico y continuo, que debe adaptarse a los cambios internos y externos que afecten a tu empresa.
- En todo momento, debes cumplir con la normativa colombiana vigente en materia de protección de datos personales, ciberseguridad y demás aspectos relacionados con la gestión de la información, ya que esto te evitará sanciones legales y reputacionales.

IX. LECCIONES APRENDIDAS

A continuación presentó algunas de las lecciones aprendidas en el curso de esta práctica tanto de ejecución de labores como las que tienen que ver específicamente con el esquema que se presenta en este documento:

Lección 1. Entrar en contexto. En el curso de la practica lo primero es ponerse en contexto y en línea con las pautas generales que tiene la organización, conocer de qué trata su razón principal ayuda a alinearse con ella. Algunas organizaciones cuentan con un tiempo de capacitación que le permiten al practicante conocer esas primeras pautas que permiten establecer una comunicación certera con los equipos que se va a trabajar.

Lección 2. Estar en contexto. Una vez conocidas las pautas de comunicación con la organización, poner en práctica sus pautas.

Lección 3. Pregunta cualquier cosa que tengas dudas. A veces el temor de creer que te han seleccionado por que ya posees el conocimiento en un área determinada hace que tu creas que ellos dan por sentado que tu conoces como realizar cierto proceso, lo cual se aleja de la realidad, tu equipo siempre estará dispuesto a apoyarte, a resolverte dudas y guiarte en el proceso, es probable que en muchas ocasiones los encuentres ocupados, pero siempre va existir un tiempo para ti de modo que recuerda preguntar siempre que existan dudas.

Lección 4. Sigue las pautas de tu mentor. A veces la confianza que empiezas a tomar en el camino suele hacer que tengas un exceso de confianza recuerda que tu mentor conocer los tiempos, los modos, el ambiente de trabajo mejor que tú, guíate por lo que él diga.

Lección 5. Recuerda el conocimiento de tus talleres. Bastante del conocimiento de lecciones aprendidas es probable que haya sido recopilado por los talleres impartidos por Universidad de Antioquia, así que también recuerda seguir sus consejos y aportar a su actualización.

Lección 6. Tiempo para todo. Tendrás tiempo para todo, sigue una actividad a la vez, cuando trabajas en un equipo es probable que tengas varias asignaciones, organiza tu tiempo, revisa que exista tiempo para todo lo asignado, cuando en la medida de lo posible en tu calendario no exista tiempo también puedes decidir no aceptar nuevas asignaciones mostrando que te han pedido dar prioridad a otras, por lo cual, hay tiempo para todo pero todo lo posible, de modo que si algo no

es posible también debes darlo a conocer de ese modo puedes negociar realizar esa asignación en otro momento o pedir colaboración a tu equipo.

Lección 7. Trazabilidad a las tareas iniciadas. Puedes llevar una trazabilidad a las tareas que has realizado de ese modo contribuir con aportar a las metas del equipo de manera más eficaz.

Lección 8. En el contexto del esquema de ciberseguridad. Mantenerse actualizado es lo más importante, leer, consultar muchas normas, seguir las pautas de aquellos que son autoridad en el mundo para esos fines y además de eso ser muy curioso en buscar nueva información y además entenderla.

REFERENCIAS

[1] Bancolombia. (2023). *Todo sobre las PYMES en Colombia*. Obtenido de https://www.bancolombia.com/negocios/actualizate/legal-y-tributario/todo-sobre-las-pymes-en-colombia.

[2] Forbes. (2022). *Información sobre PYMES*. Obtenido de https://forbes.co/2022/07/13/actualidad/listado-25-pymes-exitosas-de-colombia.

[3] Colombia, S. d. (2023). *Manejo de información personal*. Obtenido de https://www.sic.gov.co/manejo-de-informacion-personal.

[4] NIST. (2023). *Cyberframework*. Obtenido de https://www.nist.gov/cyberframework.

[5] IASACA. (2023). *COBIT*. Obtenido de https://www.isaca.org/resources/cobit.

[6] 27001, I. (2022). *Certificación ISO*. Obtenido de https://www.nqa.com/es-co/certification/standards/iso-27001-2022.

[7] OWASP. (2022). *PRÁCTICAS OWASP*. Obtenido de https://owasp.org/.

[8] CIS. (2023). *CIS SECURITY*. Obtenido de https://www.cisecurity.org/.