Institución Universitaria

Diseño y sistematización de un modelo de madurez de seguridad de la información basado en ISM3, adaptable a las micro y pequeñas empresas.

John Eriberto Gaviria

Jhon Mauricio Poveda Vergara

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Antioquia, Colombia

2023

Diseño y sistematización de un modelo de madurez de seguridad de la información basado en ISM3, adaptable a las micro y pequeñas empresas.

John Eriberto Gaviria

Jhon Mauricio Poveda Vergara

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

Título (Ph.D.,) Paula Andrea Rodríguez Marín

Codirector (a):

Título (Mg.,) Miguel Mariano Manosalva Pinedo

Grupo de Investigación:

Máquinas inteligentes y reconocimiento de patrones

Instituto Tecnológico Metropolitano

Facultad

Antioquia, Colombia

2023

(Dedicatoria o lema)

Dedicamos el presente trabajo de investigación a nuestras familias por su regocijo, amor, paciencia e impulso constante. A nuestros amigos y compañeros en quienes pudimos encontrar guía, aprendizaje y lealtad y finalmente a nuestros profesores y directores de grado quienes nos suministraron su toque final de confianza, amistad y conocimiento constante.

Resumen

Dado la creciente evolución de las tecnologías de la información y la aplicación de estas en el sector empresarial como soporte de sus procesos; las amenazas y explotación de vulnerabilidades tecnológicas actúan como una constante intrínseca a este crecimiento o evolución, generando ataques informáticos, acceso y uso no autorizado de activos, entre otros. No obstante, existen diversos marcos, normas y estándares que proponen estrategias para gestionar la seguridad de la información en las empresas, con el fin de mitigar el impacto de estas amenazas y vulnerabilidades presentes.

Sin embargo, la incorporación de estándares y modelos de gestión tecnológica no son de común aplicación en las empresas del país, en donde las pequeñas y microempresas constituyen un porcentaje mayor dentro del sector productivo, las cuales por su propia característica y estructura pueden requerir aplicaciones normativas y modelos de gestión de seguridad adaptados a su realidad.

Por tal motivo se pretende diseñar e implementar un modelo de seguridad de la información con base en ISM3 (Information Security Management Maturity Model), apoyado en el desarrollo de una herramienta informática que permita generar el nivel de madurez y recomendaciones de seguridad a las micro y pequeñas empresas MYPE.

Lo anterior, basado en una metodología donde se define y plantea una matriz de riesgo para los activos de información estándares aplicables a las micro y pequeñas empresas, y definiendo métricas ajustadas a este sector. Posteriormente se diseña e implementa el modelo de gestión de seguridad de la información adaptado a los niveles de madurez que propone ISM3. Finalmente, se valida y analiza el mismo a través de un caso de estudio, en donde se analizarán los resultados, generando conclusiones acerca de esta iniciativa.

Palabras clave: Activos de información, Ataques informáticos, Implementación ISM3, Seguridad en pequeñas empresas, SGSI en Colombia, vulnerabilidades informáticas.

Abstract

Given the increasing evolution of information technologies and their application in the business sector as support for their processes, threats and the exploitation of technological vulnerabilities act as an inherent constant to this growth or evolution, generating computer attacks, unauthorized access and use of assets, among others. However, there are various frameworks, norms, and standards that propose strategies for managing information security in companies, in order to mitigate the impact of these present threats and vulnerabilities.

However, the incorporation of technological management standards and models is not commonly applied in the country's businesses, where small and microenterprises constitute a larger percentage within the productive sector. These enterprises, due to their own characteristics and structure, may require regulatory applications and security management models adapted to their reality.

For this reason, the aim is to design and implement an information security model based on ISM3 (Information Security Management Maturity Model), supported by the development of a computer tool that enables the generation of maturity levels and security recommendations for micro and small enterprises.

The above is based on a methodology that aims to define and propose a risk matrix for information assets applicable to micro and small enterprises, and define metrics tailored to this sector. Subsequently, the information security management model will be designed and implemented, adapted to the maturity levels proposed by ISM3. Finally, it will be validated through a case study, where the results will be analyzed, generating conclusions about this initiative.

Keywords: Cyber-attacks, Information assets, ISM3 implementation, ISMS in Colombia, Security in small businesses, Informatics vulnerabilities

Contenido

Lista de ilustraciones

Pág.

Lista de tablas

Listado de símbolos y abreviaturas

- **COBIT:** Marco de gestión y gobierno de tecnologías de la información, por sus siglas en inglés.
- **IEEE:** Instituto de Ingenieros Eléctricos y Electrónicos, por sus siglas en inglés. Organización profesional que desarrolla estándares en áreas técnicas.
- **ESET:** Compañía de software de ciberseguridad, con alto impacto en todo el mundo por sus aportes en el área.
- **ITIL:** Information Technology Infrastructure Library. Conjunto de prácticas para la gestión de servicios de tecnologías de la información.
- **ISO:** Organización Internacional de Normalización, por sus siglas en inglés. Desarrolla estándares internacionales.
- **MYPE:** Esta sigla se deriva de las palabras "Micro" y "Pequeña" se emplea para englobar a ambos tipos de empresas en un solo término.
- **O-ISM3:** Modelo abierto de madurez para la gestión de la seguridad de la información, por sus siglas en inglés "Open Information Security Management Maturity Model", el cual proporciona un marco para la gestión de la seguridad de la información que puede adaptarse y personalizarse según las necesidades específicas de una organización.
- **PYMES:** Se refiere a las "Pequeñas y Medianas Empresas". Estas empresas son unidades económicas que se caracterizan por tener un tamaño y una capacidad productiva limitada
- **RA:** Análisis de Riesgos, por sus siglas en inglés.
- **RRHH:** Recursos humanos.
- **RUES:** Registro único empresarial y social
- **TI:** Tecnologías de la Información.
- **UML:** Lenguaje Unificado de Modelado, por sus siglas en inglés “Unified Modeling Lenguage”, es un estándar de la industria utilizado en ingeniería de software para visualizar, diseñar, construir y documentar sistemas software complejos.
- **WEB:** Red de alcance mundial, por sus siglas en inglés “World Wide Web”, es un sistema de información en el que documentos, imágenes, videos y otros recursos multimedia están vinculados entre sí y son accesibles a través de Internet.

Introducción

Con la implementación y evolución de nuevas tecnologías de la información, se identifican nuevas aplicaciones de estas como el desarrollo de comercio electrónico, cumplimientos legales y regulatorios que demande las organizaciones gubernamentales y de control en Colombia, entre otras, generando una adopción acelerada de estas, tanto en las actividades cotidianas como en el sector Productivo. Sin embargo, a esta evolución tecnológica se suma la existencia de amenazas tecnológicas, las cuales pueden ser explotadas por los ciberdelincuentes, teniendo como principal objetivo, atacar la infraestructura tecnológica y sistemas de información, para generar dinero o dañar la reputación. [1]. Dichos ataques se realizan buscando vulnerabilidades de los sistemas de información y así aprovechar para causar el mayor daño posible. Estos ataques, influyen negativamente en las compañías, afectando su economía, imagen y operación, en Colombia en el 2022 según un artículo publicado por la revista dinero las redes criminales realizan hurtos a diario que superan los $100 millones [2].

De acuerdo con las cifras de creación de empresa en Colombia según el tamaño, las microempresa y pequeñas empresas, representan más del 99%, tan sólo un 1% son de tamaño medianas y grandes empresas, por tal razón, es indispensable fomentar el apoyo y regulación que se debe atender para este nicho empresarial en términos de prevención y gestión de la seguridad de la información.

Tabla 1. Unidades productivas por tamaño Ene-Dic 2022/21

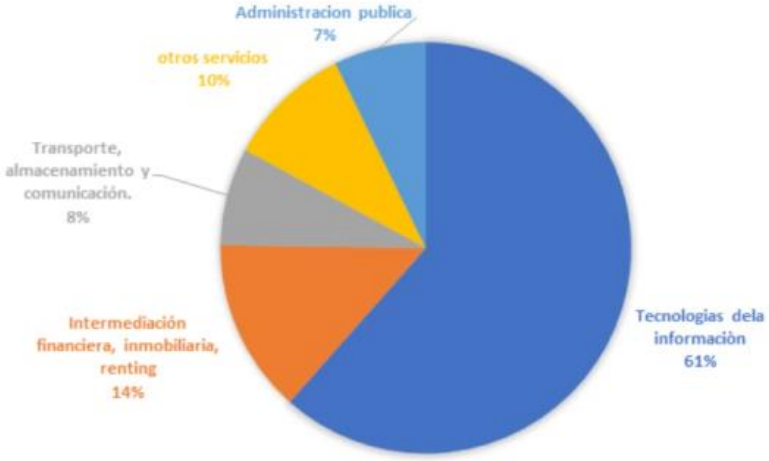
Tamaño	2021	2022	Variación, %	Contribución
Microempresa	306.140	309.488	1,1%	1,1%
Pequeña	1.449	1.147	-20,8%	-0,1%
Mediana	69	69	0,0%	0,0%
Grande	21	27	28,6%	0,0%
Total	**307.679**	**310.731**	**1,0%**	**1,0%**

Fuente: RUES – Registro Único Empresarial y Social

No obstante, las certificaciones y adopción de normas, políticas y procedimientos centralizados en la gestión de seguridad de la información son aplicadas por un pequeño porcentaje. Según la Organización Internacional de Normalización (ISO, por sus siglas en inglés) [3], en el año 2021 en Colombia se certificaron en la norma ISO 27001 únicamente 269, principalmente empresas del

sector de tecnologías de información con un 61%, empresas de intermediación financiera con un 14%, del sector transporte con un 8% y de otros servicios con un 10%.

Ilustración 1 Porcentaje de certificaciones por sector económico ISO 27001



Fuente: https://www.implementandosgi.com/sistemas-de-gestion/certificacion-iso-para-colombia/

Lo anterior, evidencia que la comparación de empresas certificadas en la norma ISO 27001 en el año 2021 y la cantidad de empresas establecidas en Colombia en el año 2020 y año 2021 define una brecha significativa. Según el Directorio Estadístico de Empresas [4] Colombia contaba con un total de 5.044.633 empresas establecidas en el año 2020 y para el año 2021 con un total de 5.704.308. Si se compara el número de empresas certificadas en la norma ISO 27001 en el año 2021, cuya cifra es 269, con el total de empresas consolidadas en Colombia, se concreta que sólo el 0.0047% de las empresas implementan un Sistema de Gestión de Seguridad de Información.

Adicional a ello, según un estudio de la firma de auditoría Ernst & Young, realizado a 1200 medianas y grandes empresas del país, se puede evidenciar la falta de adopción de políticas, normas o estrategias, enfocadas en gestionar la seguridad de la información, en donde existía una carencia del 58% de la población total, [5] cuyo objetivo sería, mitigar la explotación de vulnerabilidades tecnológicas y la ejecución de ataques informáticos, protegiendo así la confidencialidad, integridad y disponibilidad de la información de las compañías.

El anterior panorama demuestra las falencias en la adopción de estrategias de gestión de seguridad de la información, de la mediana y grande empresa, sin embargo, no son tan representativos los estudios, estadísticas y diagnósticos realizados para las micro y pequeñas empresas. A pesar de ello, por ser este sector empresarial (Micro y pequeña empresa), un porcentaje diferenciador en la economía de países en vía de desarrollo como Colombia, se evidencia la necesidad de fortalecer, apoyar y proponer estrategias y diagnósticos de gestión de seguridad de la información que ayuden a obtener un nivel de seguridad aceptable, según modelos, normas o marcos de referencia especializados.

A continuación, se detallan porcentaje de empresas con incidentes de códigos maliciosos por tamaño de empresa, según información recopilada por el laboratorio de investigación de ESET Latinoamérica y publicada en el "ESET Security Report 2018", informe que analiza el estado de la seguridad informática en Latinoamérica, donde se identifica que el 40% de las pequeñas empresas reportaron haber tenido incidentes de seguridad. Por lo anterior, si bien las empresas más grandes presentan valores porcentuales similares, se debe tener en consideración que la población de pequeñas empresas es mayor, en consecuencia, el valor neto de número de pequeñas empresas afectadas es superior a las demás, lo que puede llevar a concluir que las empresas más grandes estén mejor preparadas no sólo para detectar incidentes de seguridad, sino también para poder corregirlos.

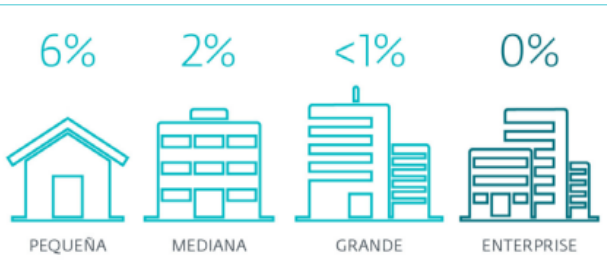
Como conclusión

Ilustración 2 Porcentaje de empresas con incidentes de códigos maliciosos por tamaño de empresa

Fuente: Clasificación de los incidentes de seguridad. Tomado de "Eset Security Report Latinoamérica 2018"

Así mismo, se puede observar según este mismo reporte, el análisis de porcentaje de empresas sin ningún control de seguridad, el cual cataloga a las pequeñas empresas con el más alto porcentaje, evidenciando algunas falencias en gestión de seguridad este sector:

Ilustración 3 Porcentaje de empresas que no tienen ningún control de seguridad



Fuente: Clasificación de los incidentes de seguridad. Tomado de "Eset Security Report Latinoamérica 2018".

Finalmente, se identifica según el siguiente gráfico que el porcentaje de pequeñas y microempresas en el país es significativamente más alto, que el porcentaje de medianas y grandes empresas, por ende, un 6% de pequeñas empresas que no cuentan con controles de seguridad, acoge un número representativamente más alto vs el 1% de las grandes empresas que no poseen controles de seguridad. Por otro lado, se debe tener en cuenta que el porcentaje de microempresas que no cuentan con controles de seguridad, no se detalla en el reporte anteriormente referenciado:

Tabla 2. Número de empresas por sectores económicos y tamaño año 2018

	Gran Empresa	Mediana empresa	Pequeña empresa	PYME (Pequeña + Mediana)	Microempresa	TOTAL
A : Agricultura, ganadería, caza, silvicultura y pesca	343	1.341	3.261	4.602	21.038	25.983
B : Explotación de minas y canteras	249	393	953	1.346	10.011	11.606
C : Industrias manufactureras	1.072	2.499	9.926	12.425	122.111	135.607
D : Suministro de electricidad, gas, vapor y aire	119	71	177	248	2.690	3.057
E : Distribución de agua, saneamiento ambiental	70	159	490	648	6.490	7.208
F : Construcción	772	2.585	8.170	10.755	82.418	93.945
G : Comercio al por mayor y al por menor;vehículos	1.146	4.476	18.824	23.300	261.295	285.741
H : Transporte y almacenamiento	313	1.030	4.363	5.393	38.408	44.113
I : Alojamiento y servicios de comida	105	341	1.829	2.170	24.301	26.576
J : Información y comunicaciones	165	482	2.410	2.892	44.119	47.176
K : Actividades financieras y de seguros	621	861	2.068	2.930	29.463	33.013
L : Actividades inmobiliarias	541	2.261	6.828	9.088	48.468	58.098
M : Actividades profesionales, científicas y técnicas	333	1.491	8.380	9.871	141.863	152.067
N : Actividades de servicios administrativos y de apoyo	247	1.042	4.124	5.166	63.478	68.891
O : Administración pública y defensa;seguridad social	18	11	37	48	1.590	1.656
P : Educación	16	98	675	773	13.239	14.028
Q : Actividades de salud humana y asistencia social	169	565	2.432	2.997	29.830	32.997
R : Actividades artísticas, de entretenimiento	33	121	690	811	11.315	12.160
S : Otras actividades de servicios	130	82	507	589	13.779	14.497
T : Actividades hogares en calidad de empleadores	-	-	1	1	153	154
Z : Actividad no Homologada a CIIU V4	332	1.550	11.617	13.167	538.271	551.769
Total	**6.793**	**21.459**	**87.761**	**109.220**	**1.504.329**	**1.620.342**

Fuente: Estimación con base en Cifras Cámaras de Comercio y Confecámaras

Existen diversos marcos, normas y estándares especializados, en gestionar la seguridad de la información en las compañías. Cada una de ellas con metodologías y focos de atención diferentes. Un ejemplo, es el modelo ISM3, modelo que actúa con base a los activos de información y estructura de cada empresa. Adicionalmente, se identifican las pequeñas y microempresas MYPE como unidades productivas, organizadas para el desarrollo y prestación de un bien o servicio [6], y las cuales pueden ser clasificadas de la siguiente manera:

Microempresa: 2 a 10 empleados.
Pequeña empresa: 11 a 50 empleados.
Por consiguiente, al ser la micro y pequeña empresa, una unidad empresarial estructurada en función a sus objetivos productivos, se puede considerar los activos de información, como uno de los insumos para definir el flujo estratégico de la empresa y por ende definir su esquema o estructura principal.

Por lo anterior, se pretende proponer una iniciativa enfocada en articular la funcionalidad y buenas prácticas presentadas por el modelo ISM3 y acoplarlo a los activos de información reales que se puedan identificar en las micro y pequeñas empresas MYPE. En otras palabras, se espera presentar un modelo adaptable a la estructura de estas, apoyado en una herramienta informática que permitirá generar el nivel de madurez y recomendaciones de seguridad.

Estas recomendaciones o estrategias de seguridad serían presentadas por la herramienta informática desarrollada, cuya parametrización o variables de entrada serían los activos de información más comunes en las micro y pequeña empresa, aportando así a la implementación de gestión de la seguridad.

Dado que el resultado esperado es un modelo estándar para la micro y pequeña empresa sin importar el sector, el modelo se apoyará en los procesos generales, estratégicos y tácticos del modelo ISM3 y enfocados al nivel técnico de las empresas.

Así mismo, dado que ISM3 utiliza las métricas de clasificación solo en su último nivel de madurez, se pretende incorporar algunas de estas métricas desde el primer nivel de análisis, con el fin de obtener un modelo transversal y que sea aplicable en su totalidad a las MYPE, ya que por su tipología las pequeñas y microempresas no siempre serán aplicables a todos los niveles de madurez que establece ISM3.

Se puede evidenciar que el número de empresas que carecen de medidas de seguridad, en las micro y pequeñas empresas es representativamente más alto frente al número de grandes empresas, por esta razón se pretende desarrollar un modelo de gestión de seguridad de la información adaptable a este sector, facilitando la implementación de medidas de seguridad.

Por lo anterior, se propone realizar un trabajo de investigación en donde se diseñe un modelo de madurez de seguridad de la información con base en ISM3 que, a través del desarrollo de una herramienta informática, permita generar el nivel de madurez y recomendaciones de seguridad a las micro y pequeña empresa MYPE.
Por lo anterior, en el presente trabajo de investigación se alcanzaron los siguientes objetivos específicos:

- Caracterizar de los activos de información y los procesos aplicables a las micros y pequeñas empresas con base en la metodología planteada por ISM3.
- Documentar matriz de riesgo para los activos de información estándares aplicables, que soportan la operación del sector de Micro y Pequeñas empresas.
- Clasificar y seleccionar las métricas adecuadas para cada nivel de madurez de ISM3, que se acoplen a las micro y pequeñas empresas.
- Desarrollar una herramienta informática, que permita la sistematización del modelo diseñado, para generar recomendaciones y planes de acción de Seguridad de la información, así como el nivel de madurez en que se encuentra la empresa.
- Validar el modelo propuesto, a través del uso de la herramienta desarrollada aplicada a un caso de estudio, de micro y pequeña empresa en el sector del Valle de Aburrá.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

1.1.1. Políticas de seguridad de la información:

Las políticas de Seguridad son muy importantes cuando una organización está en busca de gestionar adecuadamente la seguridad de la información, teniendo en cuenta lo anterior, se encuentra que este tipo de políticas puede ser definida conceptualmente como "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos" [7]. Para este trabajo, la primera política abarca aquellos datos informativos que se le entregan a los usuarios finales; la segunda es aquella que sólo puede ser visualizada por personal interno de la empresa [8].

Las políticas de seguridad se desarrollan con el fin de preservar la información y los sistemas de una Empresa, garantizando la integridad, confidencialidad y disponibilidad de la información. A continuación, se describe la definición de estos tres pilares, según la norma internacional ISO 27001. [9].

La confidencialidad se puede definir como un atributo donde la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Para la integridad, es importante el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Así mismo, en la disponibilidad es clave la definición del 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.

1.1.2. Modelo O-ISM3 (Information Security Management Maturity Model)

ISM3 es un estándar de madurez de gestión de seguridad de la información publicado por The Open Group, líder en el desarrollo de certificaciones y estándares de TI abiertos y neutrales para el proveedor. El estándar ISM3 define los procesos de seguridad para administrar el Sistema de Gestión de Seguridad de la Información (SGSI) de una empresa. El estándar ISM3 coloca la responsabilidad

en el negocio para definir sus objetivos de seguridad empresarial requeridos en su Política de seguridad, y luego ofrece un conjunto de procesos de gestión de seguridad desde los cuales el negocio selecciona cuáles implementar en un ISMS coherente. Cada proceso de control de seguridad en el SGSI, devuelve métricas para indicar qué tan bien ese proceso está contribuyendo al logro de los objetivos de seguridad de la empresa. La retroalimentación de métricas estándar ISM3 es una característica diferenciadora importante en comparación con otros sistemas ISMS:

- ¿Qué procesos de control de seguridad revelan áreas operativas de TI que no alcanzan los objetivos de seguridad?
- ¿Qué procesos deben ajustarse para mejorar el rendimiento para alcanzar o superar los objetivos críticos?
- ¿Qué procesos no contribuyen lo suficiente como para justificar la continuación de su uso?

Además, los SGSI basados en ISM3 pueden certificarse bajo ISO 9001 o ISO 27001, lo que quiere decir que se puede usar ISM3 para implementar un SGSI basado en ISO 27001. Esto también puede ser atractivo para organizaciones que ya están certificadas en ISO 9001 y que tienen experiencia e infraestructura [10].

Dentro del modelo de ISM3, se puede identificar los objetivos de negocio e incidentes, cuya función es fijar las metas u objetivos estratégicos bajo los cuales se deben soportar los procesos.

Así mismo, ISM3 define los objetivos de seguridad e incidentes, los cuales se pueden definir como una lista de objetivos de seguridad como base para el diseño, implementación y monitoreo del sistema de gestión de seguridad de la información.

1.1.3. Dimensiones principales del modelo O-ISM3:

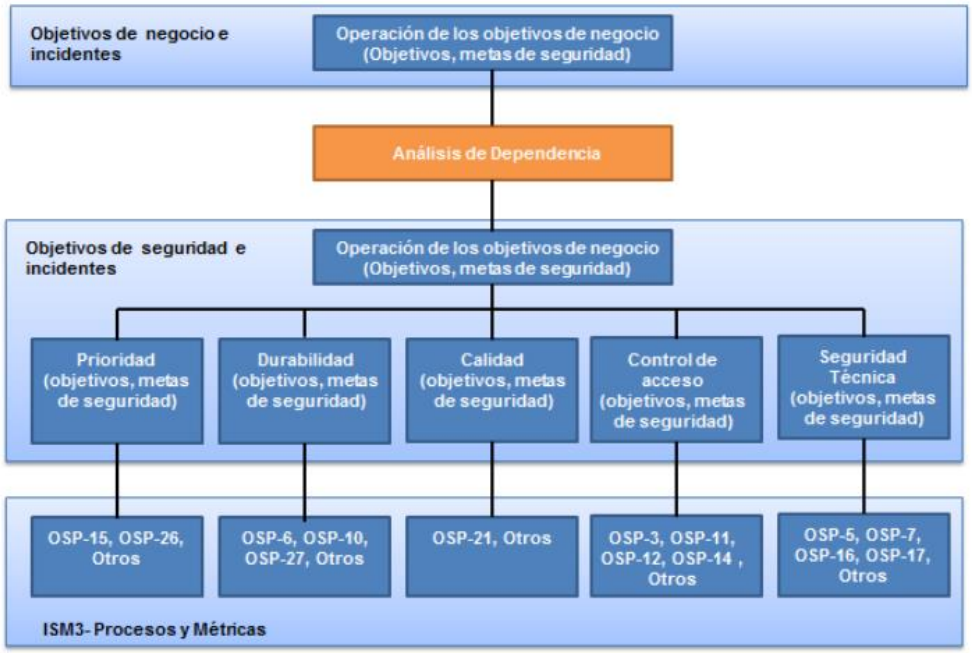
Corresponde a los 3 componentes estratégicos que describe el modelo para implementar la estrategia de Gestión de seguridad de la información en las compañías. Estas dimensiones son: Gobierno, Gestión y Control de las cuales se describen a continuación [10]:

- **Gobierno:** Es el conjunto de estrategias y procedimientos implementados para definir las líneas base de direccionamiento de la compañía respecto a la estrategia tecnológica. Las principales estrategias en esta dimensión contienen:

  - **Política y Estrategia:** Desarrollar y mantener políticas y estrategias de seguridad de la información.
  - **Organización y Estructura de Gobierno:** Establecer y mantener una estructura organizativa para la gestión de la seguridad de la información.
  - **Cultura y Concienciación:** Fomentar una cultura de seguridad y conciencia en toda la organización.
- **Gestión:** Corresponde a las estrategias que las compañías deben implementar como segunda línea de defensa para tener un monitoreo y planeación estratégica sobre la gestión de riesgos, la administración de recursos humanos, entrenamientos y capacitación y la gestión con los terceros y proveedores críticos:
  - **Gestión de Riesgos y Cumplimiento:** Identificar, evaluar y gestionar los riesgos de seguridad de la información y garantizar el cumplimiento normativo.
  - **Recursos Humanos y Formación:** Gestionar el personal, la capacitación y las competencias necesarias para la seguridad de la información.
  - **Relaciones con Terceros:** Gestionar la seguridad de la información en las relaciones con proveedores y otras partes externas.
- **Control:** Estas funciones o procesos representan áreas clave que una organización debe abordar para lograr una gestión efectiva de la seguridad de la información. La norma O-ISM3 proporciona un enfoque detallado para evaluar la madurez de estos procesos y brinda orientación sobre cómo mejorarlos.
  - **Seguridad en Activos:** Esta función se ocupa de la protección de los activos de información de la organización. Incluye la identificación de los activos críticos, la evaluación de los riesgos asociados y la implementación de medidas de seguridad adecuadas para garantizar su integridad, confidencialidad y disponibilidad.
  - **Seguridad en Procesos y Procedimientos:** En esta función, se aborda la implementación y gestión de procesos y procedimientos de seguridad de la información. Esto implica establecer directrices claras y prácticas para que los empleados sigan en relación con la seguridad, como la gestión de accesos, la clasificación de la información y la respuesta a incidentes.
  - **Seguridad Técnica:** La función de seguridad técnica se enfoca en la implementación y gestión de controles técnicos para proteger la infraestructura tecnológica y los sistemas de información. Esto puede incluir medidas como

firewalls, sistemas de detección de intrusiones, cifrado, antivirus, entre otros, que se utilizan para mitigar y prevenir amenazas de seguridad.

Ilustración 4 Objetivos de seguridad e incidentes



Fuente: https://www.ism3.com/node/42

1.1.4. Auditoría:

Existen diversas definiciones a cerca de la auditoria. William Thomas Porter y John C. Burton definen “la Auditoría como el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario” [11]. Donde además se define que la persona quien realiza esta evaluación debe ser diferente de quien elaboró, aprobó o manipuló.

Por otro lado, según una visión más moderna, definen la auditoría como "el examen crítico y sistemático de la actuación y los documentos financieros y jurídicos en que se refleja, con la finalidad de averiguar la exactitud, integridad y autenticidad de estos." [12]. Por consiguiente, tomando estas dos definiciones, se puede identificar la auditoría como una evaluación independiente, de procesos e información construida, con el fin de determinar su veracidad, integridad y exactitud.

1.1.5. Gestión de Gobierno de TI:

El gobierno de TI se puede definir como "una estructura de relaciones y procesos para dirigir y controlar la función de dichas tecnologías de una organización con el fin de alcanzar sus objetivos mediante la agregación de valor y el equilibrio del riesgo y la consideración del retorno sobre TI y sus procesos" [13]. Para su gestión y operatividad se definen 5 áreas de enfoque: Alineamiento estratégico, entrega de valor, gestión de riesgos, gestión de recursos, medición del desempeño. [14].

Finalmente, se identifica la definición de la gobernanza de TI como "una práctica o un conjunto de actividades institucionalizadas que permite reducir la incertidumbre y lograr un mejor desempeño en la relación de subcontratación entre proveedores de servicios de TI y subcontratistas" [15].

1.1.6. Micro y pequeña empresa:

La pequeña empresa se puede definir como "una entidad independiente, creada para ser rentable, que no predomina en la industria a la que pertenece, cuya venta anual en valores no excede un determinado tope y el número de personas que la conforma no excede un determinado límite, y como toda empresa, tiene aspiraciones, realizaciones, bienes materiales y capacidades técnicas y financieras, todo lo cual, le permite dedicarse a la producción, transformación y/o prestación de servicios para satisfacer determinadas necesidades y deseos existentes en la sociedad" [16]. Adicional a ello, se presenta la siguiente clasificación de pequeña y microempresa según la cantidad de empleados [6].

Microempresa: 2 a 10 empleados

Pequeña Empresa: 11 a 50 empleados

1.1.7. Activo de información:

Según la norma ISO 27001, se define los activos de información, desde la dinámica de las empresas en donde "toda organización posee información importante que desea proteger frente a cualquier situación que suponga un riesgo o amenaza. Esta información que resulta fundamental para la organización es lo que se denomina activo". [17]. Así mismo, define la importancia de preservar la integridad, disponibilidad y confidencialidad de estos activos de información.

1.1.8. ISO 27001:

Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan, El estándar 27001:2013 para los SGSI permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. [17].

1.1.9. Cyberdelincuentes:

Son personas o grupos que se apoyan en herramientas informáticas como del desarrollo de script, malware, troyanos y virus informáticos para explotar las vulnerabilidades de los sistemas de información y causar algún tipo de inestabilidad en los sistemas, intrusión o robo de información con algún tipo de beneficio bien sea económico o de reputación; existen cuatro tipos de cyberdelincuentes [18]:

- Estudiantes cualificados, a los que les gusta presumir
- Jóvenes sin experiencia, ayudados por Internet
- Desarrolladores profesionales
- Investigadores

1.1.10. Vulnerabilidades tecnológicas:

Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos [19].

1.1.11. Ataques informáticos:

Son actos en los cuales se cometen agravios, daños o perjuicios en dirigidos a los equipos y sistemas de computación que se encuentran operando en la red a nivel mundial, o puede ser orientado hacia la información y los datos que son almacenados en bases de datos. Al dirigirse a los equipos y sistemas, pueden buscar la anulación del servicio que éstos prestan, en forma temporal o permanente,

introduciendo algún tipo malware o dispositivos electrónicos de captura de información en dichos sistemas que dificulten su operación normal. Los ataques contra los datos, por su parte, pueden ir desde el robo de estos con propósitos militares o comerciales [20].

1.1.12. Sistema de Gestión de Seguridad de la Información SGSI:

Es un enfoque integral para administrar y proteger la seguridad de la información en una organización. Este sistema se basa en estándares y mejores prácticas reconocidos internacionalmente y tiene como objetivo establecer un marco estructurado para identificar, evaluar y gestionar los riesgos de seguridad de la información [21].

Algunos puntos clave sobre un SGSI incluyen:

- **Estándares y Normativas:** Se basa en estándares como ISO/IEC 27001, que proporciona un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.
- **Políticas y Procedimientos:** Incluye el desarrollo e implementación de políticas, procedimientos y controles de seguridad de la información para proteger los activos de información de la organización contra amenazas y vulnerabilidades.
- **Gestión de Riesgos:** Incorpora procesos para identificar, evaluar y gestionar los riesgos de seguridad de la información, con el objetivo de minimizar la probabilidad de incidentes de seguridad y mitigar su impacto en caso de que ocurran.
- **Concientización y Capacitación:** Incluye programas de concientización y capacitación para educar al personal sobre la importancia de la seguridad de la información y proporcionarles las habilidades necesarias para proteger los activos de información de la organización.
- **Auditoría y Revisión:** Incorpora procesos de auditoría interna y externa para evaluar la eficacia del SGSI y garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales relacionados con la seguridad de la información.

1.2. Estado del arte

Para el desarrollo del estado del arte, se realizó una búsqueda en las bases de datos SciELO, IEEE, y Google scholar, con estas palabras clave: SGSI en Colombia, Seguridad de la información en PYMES, Gestión de seguridad en pequeñas empresas, implementación ISM3 y encontrando un total

de 27 resultados. Entre los criterios de inclusión y exclusión, se seleccionaron los artículos que hacían referencia a: “Seguridad en PYMES, SGSI para pequeñas empresas, ISO 27001 para PYMES” y se excluyeron los artículos que estaban relacionados con temas de: “Salud, estrategias militares”. Se seleccionaron entonces 19 artículos relevantes.

- [21], exponen la implementación de gobierno corporativo de TI, utilizando modelos COBIT Y CMMI, detalla la importancia de tener un buen gobierno corporativo, para el eficaz análisis del nivel de maduración en seguridad de la información empresarial y el desarrollo del modelo de gobierno de TI. Dado que para el presente artículo se tiene como referencia el modelo ISM3 el cual está ligado con los modelos utilizados en este documento, el mismo es un referente respecto al modelo que se sea desarrollar, y el análisis de maduración respecto a la seguridad de la información.

- [22], realizan una investigación del nivel de madurez en la PYMES españolas para la implementación de un SGSI, y la utilización de una herramienta para automatizar la metodología, se puede comparar el modelo de esta herramienta, su funcionamiento y aplicabilidad y como se puede adaptar a las micro y pequeñas empresas de Colombia. No obstante, el modelo y herramienta propuesta no se adapta a la infraestructura, ni a los activos de información de las empresas.

- [23], presenta un estudio sobre los problemas que tienen las PYMES en cuanto a la implementación de la seguridad de la información y se apoyan la ISO/IEC 17799, el cual es un estándar adaptable a las PYMES, y sería un referente respecto a la metodología aplicada y el enfoque estratégico que aplica la norma ISO/IEC 17799.

- [24], propone un trabajo de investigación cuyo enfoque se fundamenta en la norma ISO 27001 acopladas a las PYMES, este trabajo también puede servir como guía para la creación de la herramienta que se pretende en el trabajo de grado.

- [25], propone una metodología articulada por cuatro normas fundamentales de la familia ISO, que ayude a la implementación de un SGSI, cuyo valor agregado no es solamente ayudar en qué se debe hacer, sino cómo lograrlo. Este trabajo de investigación es útil, para

la incorporación de procedimientos específicos y para tomar como referencia, los módulos del SGSI propuestos que puedan servir como herramientas de apoyo para el modelo a desarrollar. Sin embargo, esta investigación no plantea una aplicación de dicha metodología, ni presenta sesgos para un sector o industria en específico.

- [26], propone un marco de referencia que permita brindar a las organizaciones planes de contingencia y de continuidad del negocio, para los riesgos de factores externos como los desastres naturales, en donde se pueda implementar medidas de recuperación. Dicho proceso investigativo puede ser muy útil para el tema propuesto, ya que brinda una mirada sobre los planes de continuidad del negocio y sobre los riesgos externos, factores claves y que se deben tener en cuenta para el modelo de referencia o metodología propuesta.

- [27] Este trabajo de profundización de Maestría busca resolver la siguiente pregunta de investigación ¿qué modelo de gestión de TI debería ser implementado por un CIO en una PYME? Esta investigación se apoya en algunos marcos existentes como ITIL, COBIT, TOGAF, CMMI, ISO/IEC 27000, ISO/IEC 20000, PMBOK, PRINCE2. Aunque se enfoca en las PYMES de servicios, Es interesante e innovador el planteamiento del gobierno de TI, el cual se debe tener en cuenta para implementar un SGSI, alineado con las políticas de la alta gerencia.

- [28]. Este trabajo de investigación tiene como objetivo Diseñar un framework que proporcione estrategias de gobierno, gestión de TI y seguridad de la información que sirva como referencia para las contralorías territoriales, basado en el mapeo de los procesos de las mejores prácticas COBIT 5, ISO/IEC 27001: 2013 e ISO/IEC 31000. El valor agregado de esta investigación es la estructuración de un marco de referencia propio, mapeando los principales aspectos de control de las normas y estándares citados, basado en las necesidades y estructura de un ente de control específico (Contraloría Departamental de la Guajira).

- [29] Tiene como objetivo examinar la seguridad de la información empresarial en las pequeñas y medianas empresas (PYME) en Bursa, Turquía, comparando los resultados con estudios de otros países, con el fin de llegar a conclusiones de la gestión adelantada. Uno de los resultados es la conclusión que cuando las comunicaciones y la gestión de operaciones

y la política de seguridad mejoran, también mejoran otros parámetros de seguridad en las empresas, como los valores organizacionales, de personal y físicos y ambientales, lo cual ayuda a justificar uno de los principales objetivos de la presente propuesta de investigación.

- [30] Este trabajo de investigación realiza una revisión de los problemas que enfrentan las pequeñas y medianas empresas (PYME) al tratar de garantizar su alineación con las pautas de la Biblioteca de infraestructura de tecnología de la información (ITIL), que ayuden dentro de muchos aspectos a incorporar estándares para gestionar la seguridad de la información. Como resultado se recopilaron treinta y nueve artículos de relevancia. Dicha investigación se constituye como un mapa de referencia de conceptos y prácticas llevadas a cabo en el sector de las pequeñas y medianas empresas.

De acuerdo al análisis de los anteriores trabajos de investigación, se consolida el siguiente resumen respecto al aporte de estos estudios para el proyecto actual y los aspectos no incluidos y que no soluciona ni concluye con lo propuesto en el presente trabajo de investigación:

Título o Investigación	Aspectos Aportados	Aspectos No Incluidos
[21] Implementación de Gobierno Corporativo de TI.	Proporciona un análisis del nivel de maduración en seguridad de la información empresarial.	No aborda la implementación específica de un SGSI basado en ISM3 ni la adaptación a micro y pequeñas empresas.
[22] Investigación del Nivel de Madurez en PYMES españolas.	Proporciona una metodología y herramienta para la implementación de un SGSI en PYMES.	No se adapta a la infraestructura ni a los activos de información de las empresas colombianas.
[23] Problemas en la Implementación de Seguridad de la Información en PYMES.	Se apoya en la norma ISO/IEC 17799, que es adaptable a PYMES, y proporciona un enfoque estratégico que podría aplicarse en la metodología.	No presenta una aplicación específica ni un enfoque para micro y pequeñas empresas en Colombia.
[24] Implementación de ISO 27001 en PYMES.	Propone una metodología basada en la norma ISO 27001 que podría servir como referencia para la creación de la herramienta.	No se enfoca en la adaptación de la metodología a la realidad de las PYMES colombianas ni en la implementación específica de un SGSI.
[25] Metodología basada en Normas ISO para Implementar SGSI	Proporciona una metodología articulada por cuatro normas ISO que podría adaptarse a PYMES, y presenta	No presenta una aplicación específica ni un enfoque para micro y pequeñas empresas en Colombia.

Título o Investigación	Aspectos Aportados	Aspectos No Incluidos
	módulos de SGSI que podrían servir como herramientas de apoyo.	
[26] Planes de Continuidad del Negocio para Riesgos Externos	Brinda una mirada sobre los planes de continuidad del negocio y los riesgos externos, lo cual es relevante para el modelo de referencia propuesto.	No se centra en la implementación de un SGSI ni en la adaptación a las PYMES colombianas.
[27] Modelo de Gestión de TI para PYMES	Proporciona una visión sobre el gobierno de TI que podría ser relevante para implementar un SGSI alineado con las políticas de la alta gerencia en PYMES.	Se enfoca en el gobierno de TI y no en la implementación específica de un SGSI ni en la adaptación a las PYMES colombianas.
[28] Framework para Gobierno, Gestión de TI y Seguridad de la Información	Estructura un marco de referencia propio basado en normas como COBIT 5 e ISO/IEC 27001, que podría ser relevante para el diseño de un SGSI adaptado a las necesidades de control específicas de una entidad.	No se enfoca en la implementación de un SGSI ni en la adaptación a las PYMES colombianas.
[29] Seguridad de la Información en PYMES en Bursa, Turquía	Examina la seguridad de la información en PYMES y encuentra relaciones entre la mejora de la comunicación, la gestión de operaciones y la política de seguridad.	Los resultados pueden ser relevantes, pero no se enfocan en la implementación de un SGSI ni en la adaptación a las PYMES colombianas.
[30] Problemas al Garantizar la Alineación de PYMES con ITIL	Proporciona una revisión de problemas en PYMES relacionados con ITIL, lo cual puede ser relevante para la incorporación de estándares de gestión de la seguridad de la información.	No se enfoca en la implementación de un SGSI ni en la adaptación a las PYMES colombianas.

2. Metodología

Para cumplir con el objetivo general de este proyecto de investigación, se definió una metodología basada en 5 hitos que permite construir un sistema de gestión de seguridad de la información para micros y pequeñas empresas MYPE en sus frentes principales y teniendo en consideración el ciclo PHVA (Planear, hacer, verificar, actuar). A continuación, se describe el detalle de cada fase:

2.1. Caracterización de Activos de información e identificación de procesos de negocio según ISM3:

Con el objetivo de realizar la caracterización de los activos de información aplicables al público objetivo (Micros y pequeñas empresas MYPE), se consolidó un universo de activos de información, tomando como referencia los aspectos definidos en 4 marcos de referencia (ISO 27001:2013; COBIT 5:2019; ITIL V4:2019; O-ISM3) y con la ejecución de las siguientes actividades:

- **Comparación de tipos de activos de información:**
  Para cada uno de los marcos de referencia analizados, se realizó un comparativo respecto a los tipos de activos de información considerados, con el objetivo de identificar aquellos comunes en los 4 marcos de referencia y definir un inventario de tipos de activos de información.
- **Comparativo de valoración de activos de información:**
  Para cada uno de los marcos de referencia analizados, se realizó un comparativo respecto a los criterios utilizados para definir la valoración o criticidad de los activos de información, y así identificar cual metodología de los marcos de referencia analizados utilizar para la valoración de activos de información
- **Caracterización y clasificación de los activos:**
  Se utilizó la metodología de clasificación de activos de información propuesto por la norma ISO 27001:2013 y se realizó una conciliación frente a los tipos de activos de información definido anteriormente. Esto con el objetivo de tener un inventario clasificado de los activos de información aplicables al modelo propuesto.

Finalmente, para la identificación de las funciones de Negocio aplicables al modelo propuesto y de acuerdo a lo definido en el modelo ISM3 en su enfoque de planeación, se tomará como referencia las 16 funciones de negocio, para referenciarlas al modelo propuesto y relacionarlas con el universo y caracterización de activos de información propuesto.

2.2. Diseño e implementación de metodología de análisis de riesgos para los activos de información.

Se realizó un análisis de riesgo por cada activo de información definido anteriormente en el "Universo y caracterización de Activos de información", analizando su causa y amenaza, con el objetivo de consolidar una matriz de riesgos para cada uno de los activos. Para lo anterior se utilizó la siguiente tabla:

Activo de información	Riesgo	Causa	Amenaza

Así mismo, tomando como referencia la escala de valoración utilizada por O-ISM3, para la definición de criticidad en sus niveles cualitativos y cuantitativos (Bajo, Medio, Alto), se utilizó esta

escala para el cálculo de criticidad de los activos de información y las funciones de negocio dentro del modelo propuesto.

2.3. Tratamiento de riesgos e implementación de métricas de nivel de madurez.

De acuerdo a las fases anteriores, donde se definió el universo de activos de información aplicables al modelo propuesto, la clasificación de los tipos de activos de información y la definición de las funciones de negocio, se definió una arquitectura cuyo objetivo es definir el tratamiento o la implementación de controles que se debe realizar para los activos de información críticos que soportan una función de negocio crítica. Esta arquitectura consta de 3 fases, requiere las siguientes entradas, y arroja las siguientes salidas:

Entradas:

- Funciones de negocio de cada MYPE
- Calificación de criticidad de cada función de negocio
- Activos de información de cada MYPE
- Calificación de criticidad de cada activo de información

Salidas

- Recomendación de controles de seguridad que se deben implementar, de acuerdo a los activos de información críticos que soporta una función de negocio crítica. (Tomando como referencia los controles Anexos de la norma ISO 27001:2013).

2.4. Desarrollo de herramienta informática para sistematización del modelo propuesto.

Una vez consolidado el universo de activos de información aplicable al público objetivo, las funciones de negocio y el tratamiento de a los riesgos identificados por cada activo de información, se procedió a desarrollar una herramienta web, teniendo como modelo la arquitectura propuesta anteriormente.

2.5. Validación del modelo a través de caso de estudio.

Con el objetivo de validar el modelo propuesto se realizó una verificación del modelo a través de un caso de estudio, donde se tuvo en cuenta las siguientes variables:

- Funciones de negocio
- Activos de Información
- Calificación del nivel de madurez de cada función de negocio
- Calificación de la criticidad de activos de información para cada función de negocio

El resultado de esta herramienta web, es proporcionar recomendaciones sobre la implementación de controles de seguridad específicos que puedan mitigar la materialización de riesgos, de acuerdo a la infraestructura tecnológica implementada y a las funciones de negocio críticas de cada MYPE analizada.

3. Resultados y validación

Con el fin de plasmar el cumplimiento del objetivo general del presente trabajo de investigación a través de los objetivos específicos definidos, y de acuerdo a la metodología anterior, se procede a documentar la implementación y desarrollo de cada fase de la Metodología:

3.1. Caracterización de Activos de información e identificación de procesos de negocio según ISM3.

3.1.1. Universo de activos:

Con el objetivo de realizar un universo o consolidación de tipos de activos de información aplicables a procesos corporativos de las empresas, se realizó un comparativo entre los tipos de activos de información y la valoración de estos, considerados por 4 marcos de referencia:

Los marcos de referencia comparados son los siguientes:

- **ISO 27001: 2013:** La norma ISO 27001 es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. [31].

Para el comparativo de los tipos de activos de información, se tomó como referencia los 6 tipos de activos definidos en la norma ISO 27002:

- Información
- Activos de Software
- Activos físicos
- Servicios
- Personas
- Intangibles

Para el comparativo de la valoración de activos, se tomó como referencia los 3 atributos definidos por la norma ISO 27001:

- Confidencialidad
- Integridad
- Disponibilidad

- **COBIT 5:2019:** Según el marco de referencia, su misión es Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento [32].

  Para el comparativo de los tipos de activos de información, se tomó como referencia los 4 tipos de recursos de TI definidos por COBIT:

  - Aplicaciones
  - Información
  - Infraestructura
  - Personas

  Para el comparativo de la valoración de activos, se tomó como referencia los 7 criterios de información definidos por la norma:

  - Efectividad
  - Eficiencia
  - Confidencialidad
  - Integridad

- Disponibilidad
- Cumplimiento
- Confiabilidad

- **ITIL V4: 2019:** (Information Technology Infraestructure Library) es un compendio de publicaciones, o librería, que describen de manera sistemática un conjunto de "buenas prácticas" para la gestión de los servicios de Tecnología Informática [33].

  Para el comparativo de los tipos de activos de información, se tomó como referencia los 9 tipos de activos definidos por ITIL:
  - Gestión
  - Organización
  - Procesos
  - Conocimiento
  - Personas
  - Información
  - Aplicaciones
  - Infraestructura
  - Capital Financiero

  Para el comparativo de la valoración de activos, se tomó como referencia los dos conceptos para valorar un servicio (Utilidad y Garantía), establecidos de la siguiente manera:
  - Utilidad
  - Garantía de Disponibilidad
  - Garantía de Confiabilidad
  - Garantía de Continuidad
  - Garantía de Seguridad

- **O-ISM3:** Es un estándar de madurez de gestión de la seguridad de la información publicado por The Open Group, líder en el desarrollo de estándares y certificaciones de TI abiertos y neutrales para el proveedor. El estándar O-ISM3 define los procesos de seguridad para administrar el sistema de gestión de seguridad de la información (ISMS) de una empresa. El estándar O-ISM3 pone la responsabilidad en la empresa para definir sus objetivos de

seguridad empresarial requeridos en su política de seguridad, y luego ofrece un conjunto de procesos de gestión de seguridad desde los que la empresa selecciona cuáles implementar en un ISMS coherente. Se toma como referencia [4].

Para el comparativo de los tipos de activos de información, se tomó como referencia las características estructurales definidas para un sistema según ISM3:

- Repositorios
- Interfaces
- Canales
- Fronteras
- Dispositivos físicos

Y las características transaccionales dadas por los diversos recursos que utiliza un sistema de información:

- Servicios
- Sesiones
- Mensajes

Para el comparativo de la valoración de activos, ISM3 define objetivos de seguridad alineados con la estrategia y soportando los procesos operativos, es decir el objetivo de valoración se centra en tener una cobertura de los procesos y activos críticos del negocio.

3.1.1.1. Comparación de tipos de activos de información:

Dado los anteriores aspectos y atributos de los 4 marcos de referencia, se realizó el comparativo respecto a los tipos de activos de información considerados por cada uno de ellos, con el fin de identificar aquellos en común y que son destacados por los 4 marcos de referencia seleccionados.

Tabla 3. Comparativo de Marcos de Referencia para el modelo propuesto (Grupo de Activos)

PONDERACIÓN TIPO DE ACTIVOS				
Marco de Referencia / **Activo**	**ISO 27001 (25%)**	**COBIT (25%)**	**ITIL (25%)**	**ISM3 (25%)**
Información	X	X	X	

PONDERACIÓN TIPO DE ACTIVOS				
Aplicaciones, Activos de Software (Repositorios, Interfaces, fronteras, servicios, sesiones, mensajes)	X	X	X	X
Activos físicos, Infraestructura (Dispositivos físicos, canales)	X	X	X	X
Servicios	X			
Personas	X	X	X	
Intangibles	X			
Gestión			X	
Organización			X	
Procesos			X	
Conocimiento			X	
Capital Financiero			X	

Fuente: Elaboración propia

Como resultado se observa los siguientes tipos de activos de información, con una participación del 100% en los 4 marcos de referencia comparados, de todo el universo de activos tomamos los activos físicos.

Tabla 4. Tipo de Activo de información

TIPO DE ACTIVO	DEFINICIÓN
INFORMACIÓN	Toda fuente o repositorio de información física o electrónica (bases de datos, documentos, manuales, diagramas)
APLICACIONES	Todos los componentes de software de los sistemas de información
INFRAESTRUCTURA	Todos las instalaciones y dispositivos físicos requeridos para la ejecución de un proceso (instalaciones, servidores, equipos de telecomunicaciones, dispositivos especiales)
PERSONAS	Personas naturales con el conocimiento, habilidades o destrezas
SERVICIOS	Todo servicio propio o suministrado por terceros (Agua, Energía Eléctrica, Telecomunicaciones, Aire Acondicionado, Sistemas de extinción de incendio, monitoreo, mantenimiento, etc.)

Fuente: Elaboración propia

3.1.1.2. Comparativo de valoración de activos:

Así mismo, de acuerdo a la valoración y aspectos a tener en cuenta para la valoración de activos en cada marco de referencia, se realiza el siguiente comparativo:

Tabla 5. Cuadro comparativo marcos de referencia con el modelo propuesto valoración de activos

COMPARATIVO DE MARCOS DE REFERENCIA, PARA EL MODELO PROPUESTO (VALORACIÓN DE ACTIVOS)				
Marco de Referencia / **Aspecto de valoración**	**ISO 27001**	**COBIT**	**ITIL**	**ISM3 (OBJETIVOS DE SEGURIDAD)**
Efectividad		X		X
Eficiencia		X		X
Confidencialidad	X	X		X
Integridad	X	X		X
Disponibilidad, Garantía de disponibilidad	X	X	X	X
Cumplimiento		X		X
Confiabilidad, Garantía de confiabilidad		X	X	X
Garantía de continuidad			X	X
Garantía de seguridad			X	X
Utilidad			X	X

Fuente: Elaboración propia

Como conclusión se puede observar, que la metodología de valoración adoptada por ISM3, presenta una cobertura de todos los principios de seguridad abarcados por los demás marcos de referencia, ya

que no se centra en custodiar un principio en específico, sino en custodiar los procesos y activos críticos de las organizaciones, los cuales pueden abarcar diferentes principios de seguridad. En este caso se selecciona el marco de referencia que contenga todos los principios de seguridad, ya que el objetivo del modelo propuesto tiene como objetivo brindar el mayor nivel de seguridad posible.

3.1.1.3. Caracterización y clasificación de los activos:

Como O-ISM3 no tiene descripción de activos de información se apoyará en la norma ISO 27001:2013 para la realización de un inventario de activos. Si no se tiene conocimiento de los recursos que soporta la operación del negocio, será muy difícil gestionarlo o controlarlo correctamente. Este inventario se deberá actualizar cada que haya una modificación en los activos de información empresariales o corporativos.

Tabla 6. Entornos de Información

	ENTORNOS DE INFORMACIÓN						
ID	**IDENTIFICACIÓN**	**TIPO**					**DESCRIPCIÓN**
	NOMBRE ENTORNOS	**Información**	**Aplicaciones**	**Infraestructura**	**Personas**	**Servicios**	
1	Equipos Informáticos			X			**Dispositivos tecnológicos que no contienen información, pero sí tienen acceso a servidores y redes.**
2	Servidores físicos			X			**Cualquier equipo de cómputo donde se centralizan documentos de la organización o donde se encuentran las aplicaciones corporativas (ERP, CRM, entre otras).**
3	Equipos red local			X			**Equipos informáticos que permiten la conexión por medios inalámbricos o cableados.**
4	Periféricos y pendrives			X			**Dispositivos extraíbles de almacenamiento.**
5	Portátiles, tabletas y móviles			X			**Dispositivos electrónicos que se retiran de las instalaciones, sea por visitas comerciales, teletrabajo, se llevan a casa después del trabajo, o se ceden temporalmente a terceros.**

	ENTORNOS DE INFORMACIÓN						
6	Oficinas e instalaciones			X			**Espacios físicos donde se encuentran los computadores, los servidores físicos, los archivadores, la documentación en papel entre otros.**
7	Personas				X		**Personas que poseen conocimiento corporativo y de procesos claves del negocio.**
8	Otros contenedores			X			**Activos informáticos que resguardan información de la empresa.**
9	Documentación física	X					**Información corporativa, que se encuentra impresa.**
10	Aplicaciones informáticas		X				**software que contenga o gestione información del negocio.**
11	Sistemas operativos		X				**Software de control para equipos informáticos.**
12	Comunicaciones	X					**Servicios de telecomunicaciones que la empresa posee.**
13	Gestores de bases de datos		X				**Aplicaciones de almacenamiento de información en bases de datos.**
14	Suministro eléctrico			X			**Sistemas de suministro eléctrico**

Fuente: Elaboración propia

3.1.2. Identificación de procesos aplicables a las MYPE:

De acuerdo a O-ISM3, en una de sus recomendaciones de implementación de Análisis de Riesgos [34], propone las siguientes 16 funciones de negocio, que ayudan a cumplir los objetivos de negocio en una compañía.

O-ISM3 Propone una granularidad avanzada en la identificación de estas funciones, ya que de acuerdo al objetivo y procesos core de cada empresa, estas funciones tienen más protagonismo. Para el caso del modelo propuesto, esta granularidad es adecuada ya que si bien las MYPE difiere de las medianas y grandes empresas en su número de empleados y número de áreas funcionales, su razón comercial o su objetivo de negocio puede ser tan diverso y variado como el de este tipo de empresas, por tal motivo es importante definir una variedad de funciones de negocio que se puedan adaptar al tipo de MYPE analizada, ya que el objetivo principal del modelo es presentar recomendaciones de seguridad que permita mitigar la materialización de riesgos en las funciones claves o core de cada MYPE:

Tabla 7. Procesos aplicables a las Mype

	Función	Descripción
1	Gobierno	Definición de los objetivos de la organización, dirección de la organización por reglas, reglas e instrucciones de instrucción y desafío
2	Investigación	Creación de nuevos conocimientos en todas las áreas de interés de la organización
3	Publicidad	Promoción de los servicios y productos de la organización a potenciales clientes, proveedores e inversores
4	Inteligencia de negocios	Mantenimiento y entrega de conocimiento
5	Recursos humanos	Búsqueda, selección y contratación, promoción y cese de personal
6	Tecnologías de la información	Búsqueda, filtrado y adquisición de sistemas de información y comunicación
7	Legal	Reclamar obligaciones legalmente vinculantes a terceros y cumplir con las propias de la organización
8	Relaciones	Generar y mantener confianza, asociación y familiaridad con clientes, proveedores e inversores
9	Administración	Gestión de trámites asociados a todas las funciones comerciales
10	Financiamiento / Contabilidad	Encontrar, seleccionar y adquirir instrumentos financieros como, por ejemplo, dinero, bonos, etc.
11	Infraestructura	Gestión de inmuebles, aire acondicionado, calefacción, suministro de agua, suministro de energía, mobiliario, suministro de alimentos, residuos, reciclaje, control de acceso físico, etc
12	Logística	Entrega de productos o servicios físicos
13	Mantenimiento	Prevención y reparación de averías y deterioro general de infraestructura, herramientas, etc.
14	Obtención	Encontrar, comparar, elegir, seleccionar y obtener información, herramientas, suministros, activos y servicios profesionales
15	Producción	Producción de productos y servicios
16	Ventas	Venta de productos o servicios

Fuente: Elaboración propia

3.2. Diseño e implementación de metodología de análisis de riesgos para los activos de información:

3.2.1. Análisis de Riesgos

Para el análisis de riesgos se toma como alance, el inventario de activos de información aplicables a micro y pequeñas empresas que se definió en el capítulo anterior. Este inventario de activos de información puede ser susceptible a diferentes amenazas y vulnerabilidades a través de los cuales se

podría materializar un riesgo que genere un impacto negativo en las micro o pequeñas empresas. Por tal motivo es a este grupo de activos de información a quien se le realizará el análisis de riesgos inicial y posteriormente realizarle un proceso de tratamiento con base a lo establecido por O-ISM3.

Para definir los posibles riesgos a los cuales pueden estar expuestos los activos de información definidos para las micro y pequeñas empresas, se realizó un análisis teniendo en cuenta las principales causas de ataques para entornos donde no existen controles o medidas de seguridad implementadas, estas serían:

- Ausencia de controles de acceso
- Malas prácticas de configuración de hardware y equipos de cómputo
- Ausencia de políticas de seguridad en configuraciones de equipos
- Ausencia de manuales o procedimientos de operación
- Ausencia de monitoreo a la infraestructura tecnológica

A continuación, se define un escenario de posibles riesgos tecnológicos que podrían materializarse sobre los activos de información definidos, en un entorno para las micro y pequeñas empresas, teniendo en cuenta sus posibles causas y amenazas:

Tabla 8. **Riesgos de seguridad de información**

Activo de Información	Riesgo	Causa	Amenaza
Equipos Informáticos	Interrupción del servicio debido a fallas técnicas.	Falta de mantenimiento preventivo de los equipos.	Daño físico a los equipos por condiciones ambientales desfavorables.
Equipos Informáticos	Pérdida o robo de equipos informáticos.	Falta de medidas de seguridad física, como cerraduras, sistemas de vigilancia o controles físicos.	Acceso no autorizado a los datos almacenados en los equipos.
Equipos Informáticos	Pérdida de la integridad de los datos almacenados en los equipos.	Falta de políticas y controles de seguridad adecuados.	Acceso no autorizado o modificación de los datos por parte de usuarios internos o externos.
Servidores físicos	Interrupción o indisponibilidad del servicio debido a fallos en el servidor.	Sobrecarga de la capacidad del servidor o falta de mantenimiento.	Pérdida de datos o tiempo de inactividad del sistema.
Servidores físicos	Acceso no autorizado a los servidores.	Debilidades en las medidas de seguridad de acceso.	Fuga o robo de información sensible almacenada en los servidores.
Servidores físicos	Falta de respaldo adecuado de los datos almacenados en los servidores.	Ausencia de políticas o procedimientos de respaldo regulares.	Pérdida irreversible de datos en caso de fallo del servidor o incidente de seguridad.
Equipos de red local	Interrupción de la red local debido a fallos en los equipos.	Configuración incorrecta u obsoleta de los dispositivos de red.	Pérdida de conectividad y acceso a recursos compartidos.
Equipos de red local	Acceso no autorizado a la red local.	Falta de controles de seguridad, como contraseñas débiles o no actualizadas.	Ataques de intrusos o robo de información confidencial.
Equipos de red local	Deterioro del rendimiento de la red local debido a problemas de congestión.	Uso intensivo de ancho de banda o mal diseño de la red.	Retrasos en la transferencia de datos y disminución de la productividad.
Periféricos y pendrives	Pérdida o robo de periféricos y pendrives.	Descuido por parte de los usuarios o falta de medidas de seguridad física.	Acceso no autorizado a la información almacenada en los dispositivos.
Periféricos y pendrives	Infección de malware al conectar periféricos o pendrives infectados.	Descarga de archivos o programas maliciosos desde dispositivos externos.	Compromiso de la seguridad y la integridad de los sistemas.
Periféricos y pendrives	Acceso no autorizado a datos almacenados en periféricos o pendrives extraviados.	Pérdida accidental de dispositivos o descuido en su manejo.	Divulgación no autorizada de información confidencial.
Portátiles, tabletas y móviles	Pérdida o robo de dispositivos móviles que contienen datos sensibles	Descuido por parte de los usuarios o falta de medidas de seguridad física.	Acceso no autorizado a la información almacenada en los dispositivos.

Tabla 8. **Riesgos de seguridad de información**

Activo de Información	Riesgo	Causa	Amenaza
Portátiles, tabletas y móviles	Acceso no autorizado a dispositivos móviles perdidos o robados.	Falta de medidas de seguridad, como el cifrado de datos o la autenticación robusta.	Divulgación o uso indebido de información confidencial.
Portátiles, tabletas y móviles	Uso indebido de dispositivos móviles que compromete la seguridad de los datos.	Descarga de aplicaciones no seguras o acceso a redes Wifi no confiables.	Infección de malware, filtración de datos o acceso no autorizado a sistemas.
Oficinas e instalaciones	Acceso no autorizado a áreas restringidas dentro de las oficinas e instalaciones.	Falta de medidas de seguridad física, como sistemas de control de acceso o vigilancia.	Pérdida, robo o daño de activos físicos o información confidencial.
Oficinas e instalaciones	Daños o destrucción de equipos o documentos físicos debido a desastres naturales o incidentes.	Falta de medidas de protección contra incendios, inundaciones u otros eventos adversos.	Pérdida irrecuperable de información o interrupción de las operaciones.
Oficinas e instalaciones	Acceso no autorizado a información sensible dejada sin protección en las instalaciones.	Descuido por parte de los empleados o falta de políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
Personas	Acceso no autorizado o uso indebido de los sistemas por parte de empleados internos.	Falta de políticas claras de seguridad, conciencia o capacitación insuficiente.	Divulgación de información confidencial o daños a los sistemas.
Personas	Ingeniería social y suplantación de identidad por parte de personas externas.	Falta de conciencia y capacitación en seguridad por parte de los empleados.	Divulgación de información confidencial o acceso no autorizado a sistemas.
Personas	Pérdida o robo de dispositivos o credenciales de empleados que dan acceso a los sistemas.	Descuido o falta de medidas de seguridad para proteger los dispositivos y credenciales.	Acceso no autorizado a la información y a los sistemas de la organización.
Otros contenedores	Pérdida o robo de contenedores físicos (por ejemplo, discos duros externos, cintas de back-up).	Descuido por parte de los usuarios o falta de medidas de seguridad física.	Acceso no autorizado a la información almacenada en los contenedores.
Otros contenedores	Acceso no autorizado a los datos almacenados en contenedores perdidos o robados.	Falta de medidas de seguridad, como el cifrado de datos o la autenticación robusta.	Divulgación o uso indebido de información confidencial.

Tabla 8. **Riesgos de seguridad de información**

Activo de Información	Riesgo	Causa	Amenaza
Otros contenedores	Daño o destrucción de contenedores físicos debido a incidentes o desastres.	Falta de medidas de protección contra incendios, inundaciones u otros eventos adversos.	Pérdida irrecuperable de información o interrupción de las operaciones.
Documentación Física	Pérdida, robo o acceso no autorizado a documentos físicos sensibles.	Descuido por parte de los empleados o falta de medidas de seguridad física.	Divulgación de información confidencial o uso indebido de los documentos.
Documentación Física	Daño o destrucción de documentos físicos debido a incidentes o desastres.	Falta de medidas de protección contra incendios, inundaciones u otros eventos adversos.	Pérdida irrecuperable de información o interrupción de las operaciones.
Documentación Física	Acceso no autorizado a información confidencial dejada sin protección.	Descuido por parte de los empleados o falta de políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
Aplicaciones informáticas	Vulnerabilidades en las aplicaciones que pueden ser explotadas por atacantes.	Desarrollo o implementación inadecuada de las aplicaciones.	Compromiso de la confidencialidad, integridad o disponibilidad de los datos.
Aplicaciones informáticas	Acceso no autorizado a las aplicaciones o a los datos que manejan.	Fallas en los controles de autenticación y autorización.	Fallas en los controles de autenticación y autorización.
Aplicaciones informáticas	Interrupción del servicio de las aplicaciones debido a fallos técnicos.	Errores de programación, falta de mantenimiento o infraestructura inadecuada.	Pérdida de productividad, interrupción de las operaciones o pérdida de datos.
Sistemas operativos	Explotación de vulnerabilidades del sistema operativo por parte de atacantes.	Falta de actualizaciones de seguridad o configuraciones inseguras.	Acceso no autorizado, interrupción del servicio o robo de información.
Sistemas operativos	Mal funcionamiento del sistema operativo debido a fallas o errores.	Problemas de compatibilidad, configuraciones incorrectas o fallos en actualizaciones.	Pérdida de datos, tiempo de inactividad o disminución del rendimiento.
Sistemas operativos	Uso indebido de privilegios del sistema operativo por parte de usuarios internos.	Políticas de seguridad inadecuadas o falta de controles de acceso.	Acceso no autorizado, manipulación de datos o compromiso de la integridad del sistema.
Comunicaciones	Interrupción de la red de comunicaciones debido a fallos técnicos.	Problemas en la infraestructura de red o interferencias externas.	Pérdida de conectividad, interrupción de servicios o inaccesibilidad de datos.

Tabla 8. **Riesgos de seguridad de información**

Activo de Información	Riesgo	Causa	Amenaza
Comunicaciones	Interceptación o manipulación de datos en tránsito durante las comunicaciones.	Falta de cifrado o controles de seguridad en las comunicaciones.	Divulgación de información confidencial, robo de datos o suplantación de identidad.
Comunicaciones	Acceso no autorizado a las comunicaciones internas de la organización.	Falta de medidas de seguridad, como autenticación o cifrado de extremo a extremo.	Fugas de información, espionaje industrial o manipulación de datos.
Gestores de Bases de Datos	Explotación de vulnerabilidades del gestor de base de datos por parte de atacantes.	Falta de actualizaciones de seguridad o configuraciones inseguras.	Acceso no autorizado, robo de datos o manipulación de la base de datos.
Gestores de Bases de Datos	Errores de configuración o mala gestión de la base de datos.	Falta de conocimiento o falta de controles adecuados en la administración de la base de datos.	Pérdida de datos, pérdida de integridad en la base de datos o fallos en las operaciones.
Gestores de Bases de Datos	Acceso no autorizado a la base de datos por parte de usuarios internos.	Falta de políticas y controles de acceso adecuados.	Divulgación o manipulación no autorizada de datos sensibles.
Suministro Eléctrico	Interrupciones en el suministro eléctrico que afectan la disponibilidad de los sistemas.	Fallas en la infraestructura eléctrica o cortes de energía.	Pérdida de datos, tiempo de inactividad o daños a los equipos.
Suministro Eléctrico	Variaciones en el suministro eléctrico que pueden dañar los equipos.	Fluctuaciones de voltaje, picos o caídas de tensión.	Daños físicos a los equipos, pérdida de datos o pérdida de integridad de la información.
Suministro Eléctrico	Falta de medidas de respaldo de energía en caso de cortes prolongados.	Ausencia de sistemas de respaldo, como generadores o baterías UPS.	Pérdida de datos, tiempo de inactividad prolongado o interrupción de las operaciones.

Fuente: Elaboración propia

3.2.2. Valoración de criticidad:

Para el análisis del impacto que pueda generar la materialización de algún riesgo sobre los activos de información críticos para cada empresa, O-ISM3 RA utiliza una metodología en donde se debe realizar una evaluación de criticidad de cada uno de los activos de información y una valoración de los procesos de negocio que son soportados por estos activos de información. La guía recomienda una valoración de criticidad de tres niveles (bajo, medio alto), a continuación, se define la escala de valoración para los activos de información y para los procesos de negocio de acuerdo al contexto de las micro y pequeñas empresas y que sea un referente para los empresarios para saber cómo realizar dicha calificación:

Criterio de calificación para los procesos de negocio:

Bajo: El proceso tiene un impacto limitado en el logro de los objetivos empresariales.

Medio: El proceso contribuye de manera significativa al logro de los objetivos empresariales, pero su interrupción no genera un impacto crítico.

Alto: El proceso es fundamental para alcanzar los objetivos empresariales y su interrupción tendría un impacto significativo en el funcionamiento de la empresa.

Criterio de calificación para los activos de información:

Bajo: El activo de información tiene un valor limitado para el negocio y su pérdida o compromiso no tendría un impacto significativo.

Medio: El activo de información tiene un valor sustancial para el negocio y su pérdida o compromiso podría causar un impacto moderado en las operaciones o la reputación de la empresa.

Alto: El activo de información es crítico para el negocio y su pérdida o compromiso tendría un impacto significativo en las operaciones, la reputación o el cumplimiento normativo de la empresa.

Así con esta metodología obtenemos los siguientes resultados:

- Utiliza una profundidad a nivel de gestión**,** es decir que para cada caso definen cuales son los objetivos o metas de negocio los cuales se desean analizar (En el modelo propuestos, estas metas son los procesos aplicables a las micro y pequeñas empresas, identificados en el capítulo anterior).
- Se evalúan los activos de información
- Está enfocado en los procesos de negocio.
- Para la evaluación del riesgo se utilizan solo tres niveles cualitativos Alto, Medio, Bajo. Para el nivel cuantitativo se adoptará de la siguiente manera:

Tabla 9. Valores cualitativos y cuantitativos activo de información

Nivel Cualitativo	Nivel cuantitativo
Alto	30
Medio	20
Bajo	10
No existente	0

Fuente: Elaboración propia

3.3. Tratamiento de riesgos e implementación de métricas de nivel de madurez:

3.3.1. Arquitectura de tratamiento de riesgos y recomendación de controles:

En el subcapítulo anterior se definieron las condiciones y el alcance tanto de los procesos o funciones de negocio y los activos de información, los cuales son los insumos para realizar el análisis de riesgos. Dado que esta metodología de riesgos propone un proceso relacional y dinámico el cual depende de los propios activos de información y procesos de negocio que posea cada empresa, su resultado depende de cada necesidad de negocio. Por lo anterior, para mayor entendimiento se definió la siguiente arquitectura (Compuesta por 3 fases) como se ve en la figura 5, acerca del procesamiento y operaciones que se deben realizar para realizar la gestión de riesgos según O-ISM3, teniendo como insumo los activos de información y los tipos de activos de información que se definieron para el modelo en los capítulos anteriores y se pueda consolidar una matriz de riesgo que permita darle tratamiento a los aspectos críticos.

Ilustración 4 Arquitectura modelo de tratamiento de riesgos y recomendaciones

Fuente: elaboración propia

3.3.1.1. Ingreso de parámetros e Información (Fase 1):

En esta fase, el empresario debe relacionar de acuerdo con los procesos de negocio definidos por O-ISM3, cuáles aplican a su empresa y relacionar la criticidad de cada uno basado en la escala o criterio de calificación definido para los procesos de negocio. Así mismo, debe ingresar los activos de información disponibles en su empresa e igualmente relacionar la criticidad de cada uno con base en los criterios de calificación definidos para los activos de información. Como resultado de esta fase, se consolida la información de procesos de negocio y activos de información de cada empresa con su respectiva criticidad.

3.3.1.2. Declaración de activos de información críticos por cada empresa (Fase 2):

En esta fase, se presenta al empresario los procesos de negocio que él seleccionó para su empresa en la fase anterior, con el objetivo de relacionar para cada uno, qué activos de información lo soporta. Con esta información, el modelo hace un procesamiento y basado en el siguiente mapa de calor, le asigna una criticidad a cada relación de "Proceso de negocio" vs "Activos de información":

Tabla 10. Valoración criticidad de activo de información

	Activo de Información				
Proceso de negocio	NIVELES		Bajo	Medio	Alto
			10	20	30
	Bajo	10	20	30	40
	Medio	20	30	40	50
	Alto	30	40	50	60

Fuente: Elaboración propia

Como resultado de esta fase se consolida los activos de información que según el procedimiento aplicado son críticos por cada empresa y por consiguiente se deben aplican controles de seguridad.

3.3.1.3. Recomendación de controles (Fase 3):

Una vez el modelo define qué activos de información son críticos, de acuerdo a su criticidad y al proceso de negocio que soporta, realiza un comparativo y basado en el "*Cuadro de recomendaciones*" consolidado de controles de ISO 27002, procede a recomendar al empresario cuáles controles y medidas de seguridad debe implementar para tener un nivel de seguridad aceptable y que cubra y soporte su infraestructura y procesos críticos.

Cuadro de recomendaciones:

Tabla 11. Recomendaciones de acuerdo a los activos de información críticos

Activo de Información	Recomendación de controles ISO 27002
Equipos informáticos	**A9.1.1 Política de control de acceso:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la Seguridad de la Información.
	A9.1.2 Acceso a redes y a servicios en red: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A9.2.2 Suministro de acceso de usuarios: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	A9.2.3 Gestión de derechos de acceso privilegiado: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
	A9.2.6 Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A8.1.1 Inventario de activos: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	A8.1.4 Devolución de activos: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
	A10.1.1 Política sobre el uso de controles de cifrado: Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A11.1.4 Protección contra amenazas externas y ambientales: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
Servidores físicos	**A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas:** La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
	A.14.2.6 Ambiente de desarrollo seguro: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
	A10.1.1 Política sobre el uso de controles de cifrado: Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A16.1.2 Reporte de eventos de Seguridad de la Información: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

Activo de Información	Recomendación de controles ISO 27002
	A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de Seguridad de la Información.
	A13.1.1 Controles de redes: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A13.1.2 Seguridad de los servicios de red: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
	A13.1.3 Separación en las redes: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
Equipos red local	**A10.1.1 Política sobre el uso de controles de cifrado:** Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A13.1.1 Controles de redes: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A13.1.2 Seguridad de los servicios de red: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
	A13.1.3 Separación en las redes: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
Periféricos y pendrives	**A10.1.1 Política sobre el uso de controles de cifrado:** Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A13.2.1 Políticas y procedimientos de transferencia de información: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
	A13.2.2 Acuerdos sobre transferencia de información: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
Portátiles, tabletas y móviles	**A9.1.1 Política de control de acceso:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la Seguridad de la Información.
	A9.1.2 Acceso a redes y a servicios en red: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A9.2.6 Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A10.1.1 Política sobre el uso de controles de cifrado: Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Activo de Información	Recomendación de controles ISO 27002
	A11.2.1 Ubicación y protección de los equipos tecnológicos: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
	A11.2.4 Mantenimiento de los equipos: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A11.2.6 Seguridad de equipos y activos fuera de las instalaciones: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
	A11.2.7 Disposición segura o reutilización de equipos: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.
	A8.1.1 Inventario de activos: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	A8.1.2 Propiedad de los activos: Los activos mantenidos en el inventario deben tener un propietario.
	A8.1.3 Uso aceptable de los activos: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
Oficinas e instalaciones	**A11.1.1 Perímetro de seguridad física:** Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.
	A11.1.2 Controles de acceso físicos: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.
	A11.1.3 Seguridad de oficinas, recintos e instalaciones: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones.
Personas	**A7.1.1 Selección:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso y a los riesgos percibidos.
	A7.2.2 Toma de conciencia, educación y formación en la Seguridad de la Información: Todos los colaboradores y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la Institución pertinentes para su cargo.
	A7.3.1 Terminación o cambio de responsabilidades de empleo: Las responsabilidades y los deberes de Seguridad de la Información que permanecen validos después de la terminación o cambio de empleo de deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
	A11.1.2 Controles de acceso físicos: Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.

Activo de Información	Recomendación de controles ISO 27002
Otros contenedores	**A10.1.1 Política sobre el uso de controles de cifrado:** Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A13.2.1 Políticas y procedimientos de transferencia de información: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones
	A13.2.2 Acuerdos sobre transferencia de información: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
	A13.2.4 Acuerdos de confidencialidad o de no divulgación: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
	A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de Seguridad de la Información.
	A16.1.5 Respuesta a incidentes de Seguridad de la Información: Se debe dar respuesta a los incidentes de Seguridad de la Información de acuerdo con procedimientos documentados.
Documentación física	**A8.2.1 Clasificación de la información:** La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	A8.2.2 Etiquetado de la información: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A8.2.3 Manejo de activos: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
Aplicaciones informáticas	**A9.1.1 Política de control de acceso:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la Seguridad de la Información.
	A9.2.2 Suministro de acceso de usuarios: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	A9.2.3 Gestión de derechos de acceso privilegiado: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
	A9.2.6 Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A10.1.1 Política sobre el uso de controles de cifrado: Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Activo de Información	Recomendación de controles ISO 27002
	A16.1.3 Reporte de debilidades de Seguridad de la Información: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de Seguridad de la Información observada o sospechada en los sistemas o servicios.
	A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de Seguridad de la Información.
	A16.1.5 Respuesta a incidentes de Seguridad de la Información: Se debe dar respuesta a los incidentes de Seguridad de la Información de acuerdo con procedimientos documentados.
Sistemas operativos	**A9.1.1 Política de control de acceso:** Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la Seguridad de la Información.
	A9.1.2 Acceso a redes y a servicios en red: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A9.2.2 Suministro de acceso de usuarios: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
	A9.2.3 Gestión de derechos de acceso privilegiado: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
	A9.2.6 Retiro o ajuste de los derechos de acceso: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A10.1.1 Política sobre el uso de controles de cifrado: Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de Seguridad de la Información.
	A16.1.5 Respuesta a incidentes de Seguridad de la Información: Se debe dar respuesta a los incidentes de Seguridad de la Información de acuerdo con procedimientos documentados.
Comunicaciones	**A10.1.1 Política sobre el uso de controles de cifrado:** Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A13.1.1 Controles de redes: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A13.1.2 Seguridad de los servicios de red: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se
	A13.1.3 Separación en las redes: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

Activo de Información	Recomendación de controles ISO 27002
	A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
	A.14.1.3 Protección de transacciones de los servicios de las aplicaciones: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
Gestores de bases de datos	**A10.1.1 Política sobre el uso de controles de cifrado:** Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
	A8.3.2 Disposición de los medios: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
	A8.3.3 Transferencia de medios físicos: Los medios que contienen información de deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
	A9.4.1 Restricción de acceso a la información: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	A9.4.3 Sistema de gestión de contraseñas: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.
	A9.4.4 Uso de programas utilitarios privilegiados: Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
Suministro eléctrico	**A11.2.2 Seguridad en el suministro de electricidad y servicios:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
	A11.2.3 Seguridad en el cableado: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.

Fuente: Elaboración propia

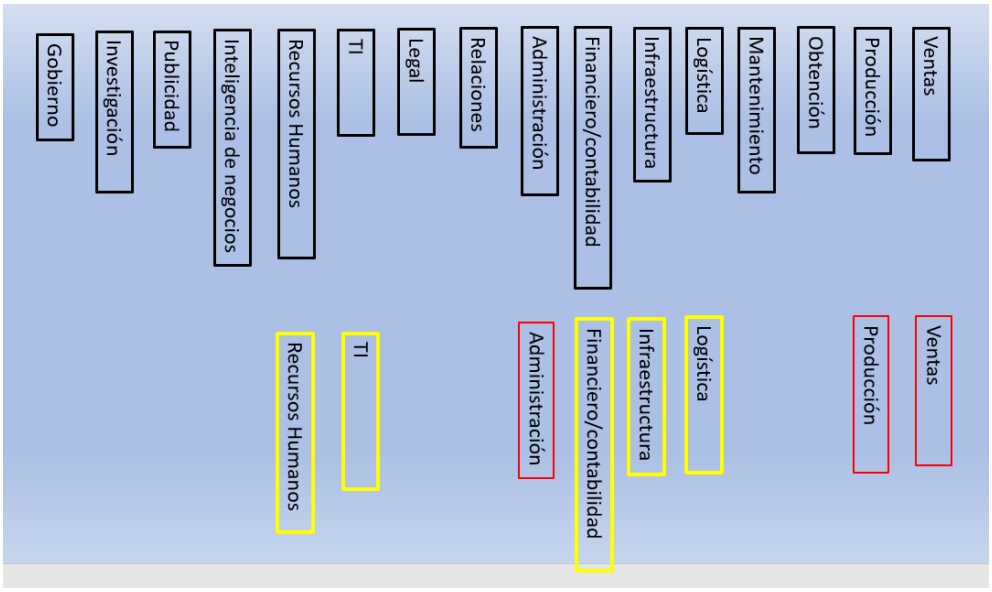
3.3.2. Ejemplo aplicado del modelo de tratamiento de riesgos y recomendación de controles:

Con el objetivo de explicar el funcionamiento de la arquitectura anterior en el modelo, se presenta el siguiente ejemplo de interacción para una empresa con las siguientes condiciones:

- **Razón social:** Microempresa de artículos de madera para el hogar.
- **Procesos de negocio implementados:** Ventas, recursos humanos, logística, infraestructura, financiera y contabilidad, TI, administración, producción.
- **Activos de información disponibles:** Servidores, redes wifi, red local, personas, móviles.

a). Del universo de procesos de negocio (Funciones), se selecciona aquellos que son aplicables al negocio y se asigna una calificación de criticidad. Los procesos de negocio con los que cuenta la empresa son: Ventas, producción, logística, infraestructura, financiero/contable, administración, TI, recursos humanos.

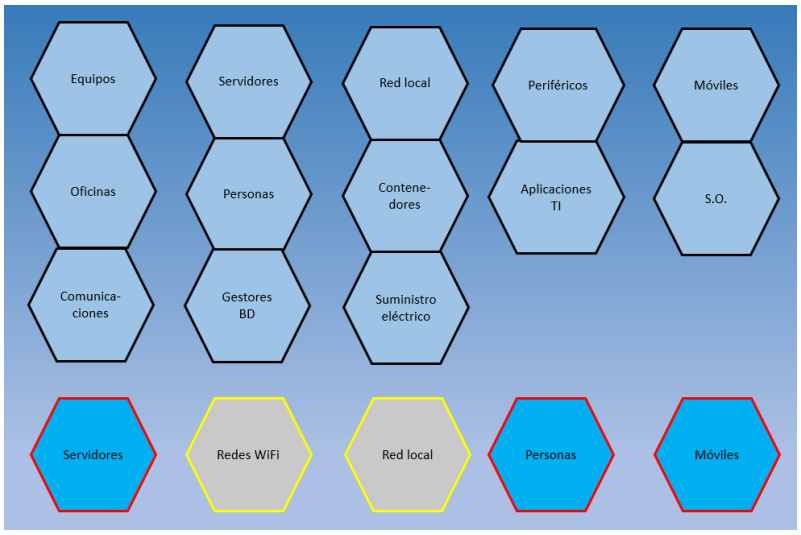
Ilustración 5 Selección de procesos de negocio y su nivel de criticidad (Ejemplo aplicado)



Fuente: Elaboración propia

b). Del universo de Activos de Información definido, se selecciona aquellos que soportan la operación del negocio y se asigna una calificación de criticidad:

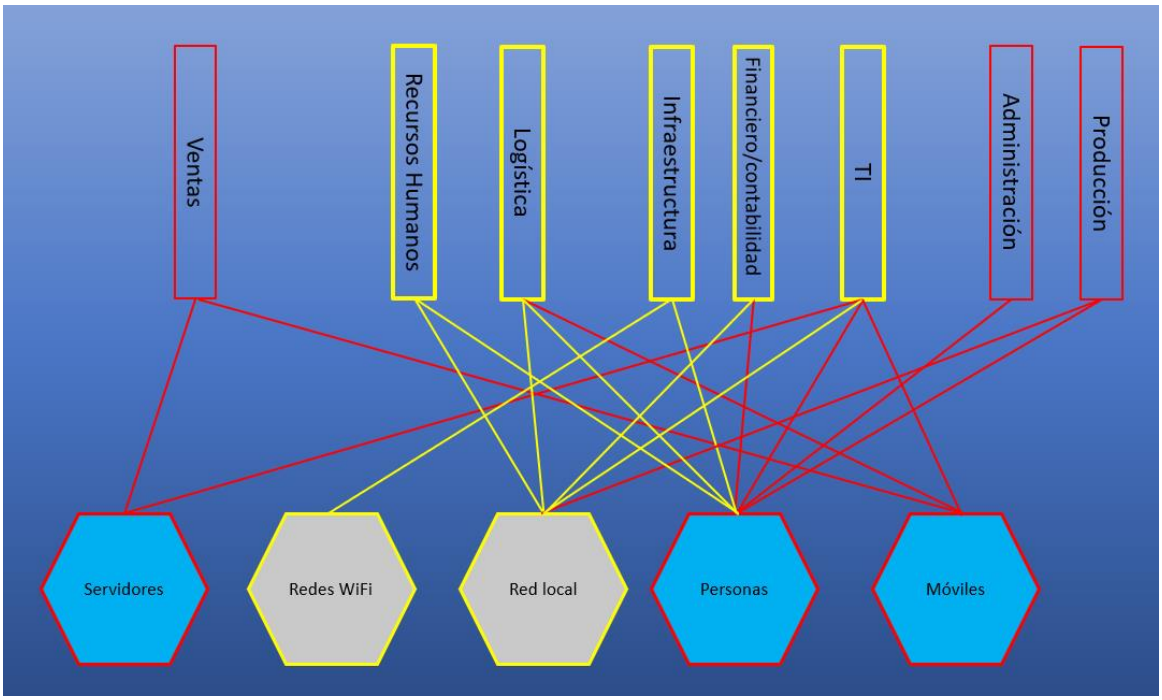
Ilustración 6 Selección de activos de información y su nivel de criticidad (Ejemplo aplicado)



Fuente: Elaboración propia

c). Se relaciona cada uno de los procesos con los activos que soportan su operación:

Ilustración 7 Relación activos de información que soporta cada uno de los procesos de negocio (Ejemplo aplicado)



Fuente: Elaboración propia

d). Una vez se asigna la relación de procesos y activos que soportan su operación, se asigna una calificación a cada relación de acuerdo a la siguiente escala:

Tabla 12. Valoración criticidad de activo de información (Ejemplo aplicado)

	Activos				
Procesos	NIVELES		Bajo	Medio	Alto
			10	20	30
	Bajo	10	20	30	40
	Medio	20	30	40	50
	Alto	30	40	50	60

Fuente: Elaboración propia

e). Como resultado del paso anterior, se establece la matriz de riesgos, ponderando la calificación realizada de cada relación proceso de negocio vs. Activo de información, concluyendo cuáles son aquellos activos de información críticos:

Tabla 13. Valoración criticidad de activo de información (Ejemplo aplicado)

	Producción	Administración	TI	Financiera y Contabilidad	Infra-estructura	Logística	Recursos Humanos	Ventas	Total
Servidores			50					60	55
Redes WIFI					20				20
Red local	50		40	40		40	30		40
Personas	60	60	50	50	40		40		50
Móviles			50			50		60	53

Fuente: Elaboración propia

f). De acuerdo a los activos de información críticos, se define cuáles son los controles y medidas de seguridad que se deben implementar tomando como referencia la norma ISO 27001, Anexo A:

Tabla 14. Recomendaciones de acuerdo a los activos de información críticos

Activos de Información	Controles ISO 27002 a implementar
Servidores físicos	A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas A.14.1.3 Protección de transacciones de los servicios de las aplicaciones A.14.2.6 Ambiente de desarrollo seguro A10.1.1 Política sobre el uso de controles de cifrado A16.1.2 Reporte de eventos de Seguridad de la Información A16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos A13.1.1 Controles de redes A13.1.2 Seguridad de los servicios de red A13.1.3 Separación en las redes
Equipos red local	A10.1.1 Política sobre el uso de controles de cifrado A13.1.1 Controles de redes A13.1.2 Seguridad de los servicios de red A13.1.3 Separación en las redes
Portátiles, tabletas y móviles	A9.1.1 Política de control de acceso A9.1.2 Acceso a redes y a servicios en red A9.2.6 Retiro o ajuste de los derechos de acceso A10.1.1 Política sobre el uso de controles de cifrado A11.2.1 Ubicación y protección de los equipos tecnológicos A11.2.4 Mantenimiento de los equipos A11.2.6 Seguridad de equipos y activos fuera de las instalaciones A11.2.7 Disposición segura o reutilización de equipos A8.1.1 Inventario de activos

	A8.1.2 Propiedad de los activos A8.1.3 Uso aceptable de los activos
Personas	A7.1.1 Selección A7.2.2 Toma de conciencia, educación y formación en la Seguridad de la Información A7.3.1 Terminación o cambio de responsabilidades de empleo A11.1.2 Controles de acceso físicos

3.3.3. Identificación y cálculo de nivel de madurez:

Con base en la guía de ISM3, en su proceso de tratamiento e identificación de niveles de madurez, define los siguientes 6 niveles que puede alcanzar una empresa dependiendo de la capacidad de gestión de seguridad de la información y seguridad informática que posea, así como los procedimientos y frentes que se hayan implementado con el fin de gestionar desde una visión de gobierno corporativo, los retos cibernéticos crecientes en el entorno. Estos niveles son los siguientes:

Tabla 15. Definición de niveles de madurez de acuerdo a la gestión realizada

Niveles	Descripción
Nivel 1: **Ad-hoc**	En este nivel, la gestión de la seguridad de la información es informal y no se basa en ningún marco o estándar establecido. La seguridad de la información es vista como una tarea técnica y no es una prioridad para la organización.
Nivel 2: **En desarrollo**	En este nivel, la organización comienza a establecer una estrategia de seguridad de la información y a definir políticas y procedimientos básicos de seguridad. La seguridad de la información sigue siendo principalmente una tarea técnica.
Nivel 3: **Establecido**	En este nivel, la organización ha establecido una estrategia y un marco de seguridad de la información y ha implementado políticas y procedimientos de seguridad. La gestión de la seguridad de la información es vista como una responsabilidad de toda la organización y no sólo de los expertos técnicos.
Nivel 4: **Controlado**	En este nivel, la organización tiene un enfoque sistemático para la gestión de la seguridad de la información y ha implementado controles de seguridad más sofisticados y efectivos. La gestión de la seguridad de la información está completamente integrada en los procesos y actividades de la organización.
Nivel 5: **Optimizado**	En este nivel, la organización tiene un enfoque continuo de mejora de la seguridad de la información y utiliza métricas para medir y mejorar el rendimiento de la seguridad de la información. La gestión de la seguridad de la información se ve como una parte esencial de la estrategia general de la organización.
Nivel 6: **Innovador**	En este nivel, la organización está a la vanguardia en la gestión de la seguridad de la información y está continuamente explorando nuevas formas de mejorar la seguridad de la información. La gestión de la seguridad de la información es vista como un factor clave para la innovación y el éxito empresarial.

Por consiguiente, y para adoptar la anterior clasificación de madurez en términos de gestión de seguridad de la información en el modelo propuesto, se propone la siguiente lista de chequeo que tendrá como objetivo ubicar o definir el nivel de madurez de cada uno de los procesos aplicables o definidos en la empresa evaluada. El empresario deberá responder a cada una de las peguntas las cuales son secuenciales y definirá el nivel de madurez alcanzado respecto a los procedimientos, controles y gestión realizada en el proceso de negocio en aspectos de seguridad de la información.

3.3.3.1. Lista de chequeo nivel de madurez:

- ¿Cuenta con una estrategia de seguridad de la información o definición de políticas o procedimientos?
  No: *Nivel Ad-hoc*
  Sí: *En Desarrollo*

- Adicional al punto anterior, ¿Esta estrategia ha sido socializada alrededor de la empresa y ha asignado funciones a las áreas funcionales?
  Sí: *Establecido*

- Adicional al punto anterior, ¿Se ha establecido controles de seguridad de la información, enfocados en alguna normatividad o guía de buenas prácticas?
  Sí: *Controlado*

- Adicional al punto anterior ¿Realiza métricas o indicadores de gestión de los controles implementados y son actualizados periódicamente para validar su alcance de ejecución?
  Sí: *Optimizado*

- Adicional al punto anterior ¿Invierte presupuesto para identificar nuevas tendencias e implementar soluciones innovadoras en temas y frentes de seguridad de la información?
  Sí: *Innovador*

3.4. Desarrollo de herramienta informática para sistematización del modelo propuesto

Con el objetivo de aplicar el modelo propuesto, se desarrolló una herramienta informática web, a través de la cual se sistematizó las fases de la arquitectura propuesta para generar recomendaciones de seguridad de manera automática. El objetivo principal de esta herramienta es que pueda ser utilizada por empresarios de pequeñas y microempresas que no tengan mucho conocimiento de seguridad informática y seguridad de la información y sea una ayuda inicial para empezar con una gestión de seguridad en su empresa en los pilares fundamentales.

3.4.1. Módulos de la herramienta informática propuesta

Tomando como referencia la arquitectura definida en los subcapítulos anteriores (Figura 6), la herramienta presenta los siguientes módulos:

- Ingreso de parámetros e información:
  - Ingreso de los procesos de negocio presentes en la empresa.
  - Ingreso de los activos de información que soportan los procesos de negocio.
  - Ingreso del nivel madurez de seguridad en cada proceso de negocio, de acuerdo con la lista de chequeo "Nivel de Madurez".

- Cálculo de Activos de información críticos:
  - Definición de criticidad de cada proceso de negocio de la empresa.
  - Relación de los activos de información que soportan cada proceso de negocio.
  - Calificación de la criticidad del activo de información que soporta cada proceso de negocio según lo establecido en las escalas de "valoración de criticidad".

- Recomendación de controles:
  - Visualización por proceso de los controles de seguridad que se recomiendan implementar, para mitigar riesgos que puedan vulnerar los activos de información que soporta el proceso de negocio específico. Esta visualización incluye los siguientes atributos:

    - Proceso
    - Nivel de madurez
    - Activo
    - Control
    - Tratamiento
    - Riesgo

3.4.2. Estructura y base de datos

Para la realización de la herramienta informática y para el correcto procesamiento de los datos que permita generar las respectivas condiciones de seguridad, se diseñó la siguiente estructura de base de datos:

3.4.2.1. Estructuras de datos:

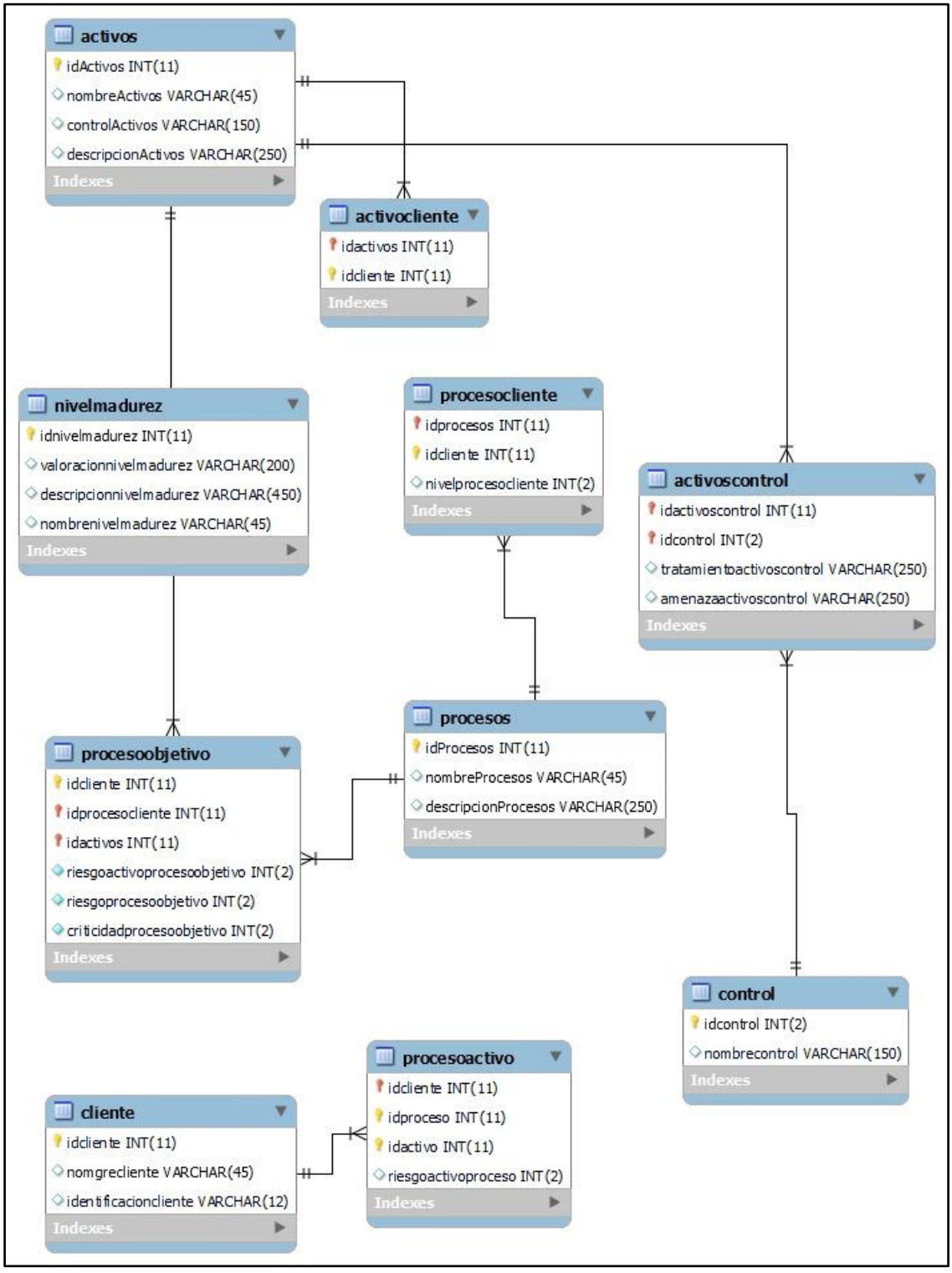
La base de datos diseñada contiene las siguientes estructuras de datos:

- **Activocliente:** Tabla que soporta la conexión y la sesión del empresario que está utilizando la herramienta.
- **Activos:** Tabla que almacena la información de los activos de información definidos en cada empresa.
- **Activoscontrol:** Tabla que gestiona la relación de muchos a muchos que existe entre los activos de información y los controles implementados.
- **Cliente:** Tabla que almacena la información de cada empresario que usa la herramienta.
- **Control:** Tabla que almacena la información de cada uno de los controles definidos en el modelo y que fueron extraídos de la norma ISO 27002, los cuales son recomendados al usuario una vez ejecutado el modelo.
- **Nivelmadurez:** Tabla que almacena la información de cada uno de los 6 niveles de madurez que puede tener un proceso de negocio.
- **Procesoactivo:** Tabla que gestiona la relación existe entre cada proceso de negocio y los activos de información que lo soporta.
- **Procesocliente:** Tabla que gestiona la relación existente entre cada empresa y los procesos de negocio que tiene su empresa
- **Procesoobjetivo:** Tabla que gestiona la relación de muchos a muchos existentes entre procesos de negocio y los activos de información que soportan estos procesos.
- **Procesos:** Tabla que almacena la información de los procesos de negocio que puede tener una pequeña o microempresa de acuerdo al modelo ISM3.

3.4.2.2. Diagrama entidad relación

Basado en las estructuras de datos definidas anteriormente, se diseñó el siguiente diagrama entidad relación, el cual gestiona la relación entre las tablas que permite la correcta funcionalidad de la base de datos que soporta la herramienta informática propuesta:

Ilustración 8 Diagrama entidad relación, base de datos herramienta informática propuesta



Fuente: Generada por herramienta MySql de acuerdo con el diseño de la herramienta informática propuesta.

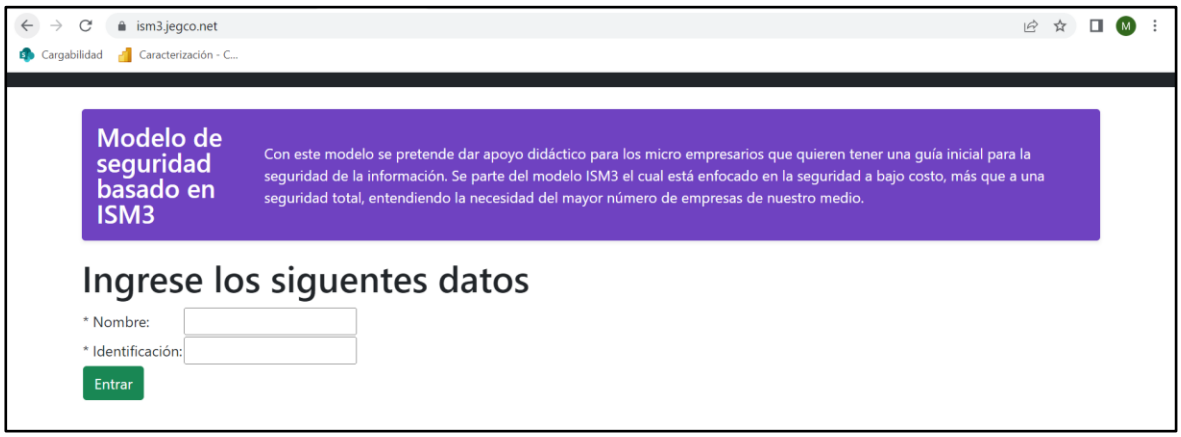
3.4.3. Aspectos técnicos de la herramienta informática desarrollada

Para el desarrollo de la herramienta informática que soporta el modelo propuesto, se desarrolló un software web en lenguaje HTML5 y php 7.3 con estilos CCS. Se utilizó un dominio público propio, con servidor apache y gestor de base de datos MySql.

Para ingresar a la herramienta se puede hacer a través del siguiente link:

https://ism3.jegco.net/

Ilustración 9 Acceso a la herramienta informática propuesta



Fuente: Captura de pantalla a la herramienta desarrollada

Una vez se ingresa a la página web de la herramienta, se debe relacionar el nombre del empresario y su documento de identificación, con el fin de personalizar las recomendaciones de seguridad generadas. Posterior a esto, la herramienta solicita los parámetros de inicio, tales como procesos de negocio y activos de información de la empresa y demás parámetros según las fases definidas en la arquitectura del modelo propuesto.

3.5. Validación del modelo

Después de desarrollada la herramienta, se realizó validación de esta, con un caso de estudio de una "pequeña" empresa de la región Antioqueña de Colombia cuya razón social radica en "*Comercio al por menor de artículos de ferretería pinturas y productos de vidrio en establecimientos especializados*". A continuación, se detalla los resultados arrojados en cada uno de los módulos establecidos en la herramienta informática desarrollada:

3.5.1. Validación módulo "Ingreso de parámetros e información"

Una vez se ingresó la información de la empresa, se procedió a listar los procesos de negocio que posee y sus activos de información:

Procesos de negocio:

- Ventas
- Obtención
- Logística
- Financiamiento/Contabilidad
- Administración

Activos de Información:

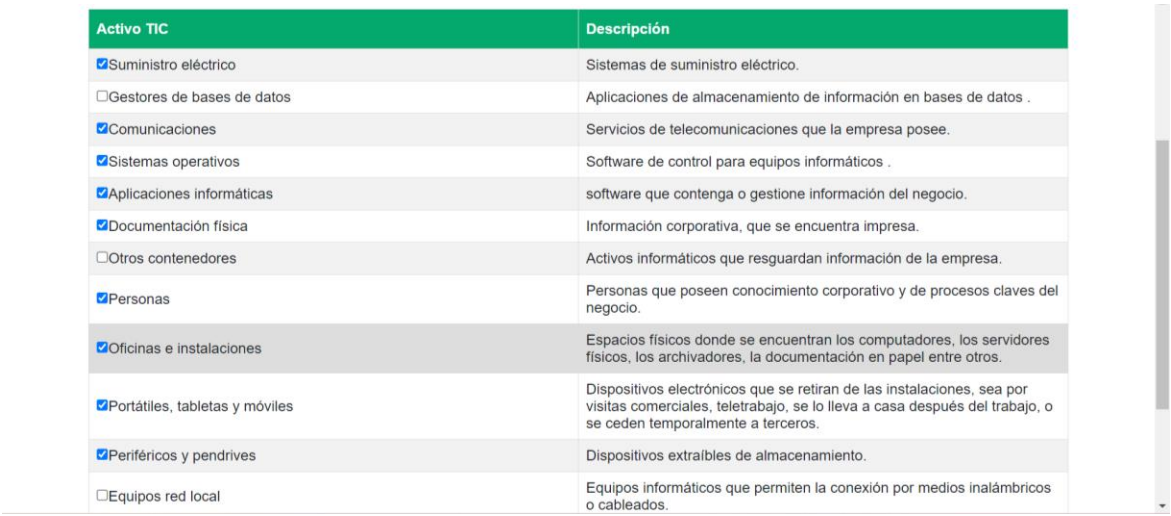
- Suministro eléctrico
- Comunicaciones
- Sistemas Operativos
- Aplicaciones Informáticas
- Documentación Física
- Personas
- Oficinas e instalaciones
- Portátiles, tabletas y móviles
- Periféricos y pendrivers

Ilustración 10 Procesos de negocio caso de estudio

Proceso	Descripcion
☑ Ventas	Venta de productos o servicios
☐ Producción	Producción de productos y servicios
☑ Obtención	Encontrar, comparar, elegir, seleccionar y obtener información, herramientas, suministros, activos y servicios profesionales
☐ Mantenimiento	Prevención y reparación de averías y deterioro general de infraestructura, herramientas, etc
☑ Logística	Entrega de productos o servicios físicos
☐ Infraestructura	Gestión de inmuebles, aire acondicionado, calefacción, suministro de agua, suministro de energía, mobiliario, suministro de alimentos, residuos, reciclaje, control de acceso físico, etc
☑ Financiamiento / Contabilidad	Encontrar, seleccionar y adquirir instrumentos financieros como, por ejemplo, dinero, bonos, etc
☑ Administración	Gestión de trámites asociados a todas las funciones comerciales
☐ Relaciones	Generar y mantener confianza, asociación y familiaridad con clientes, proveedores e inversores
☐ Legal	Reclamar obligaciones legalmente vinculantes a terceros y cumplir con las propias de la organización

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 11 Activos de información Caso de estudio



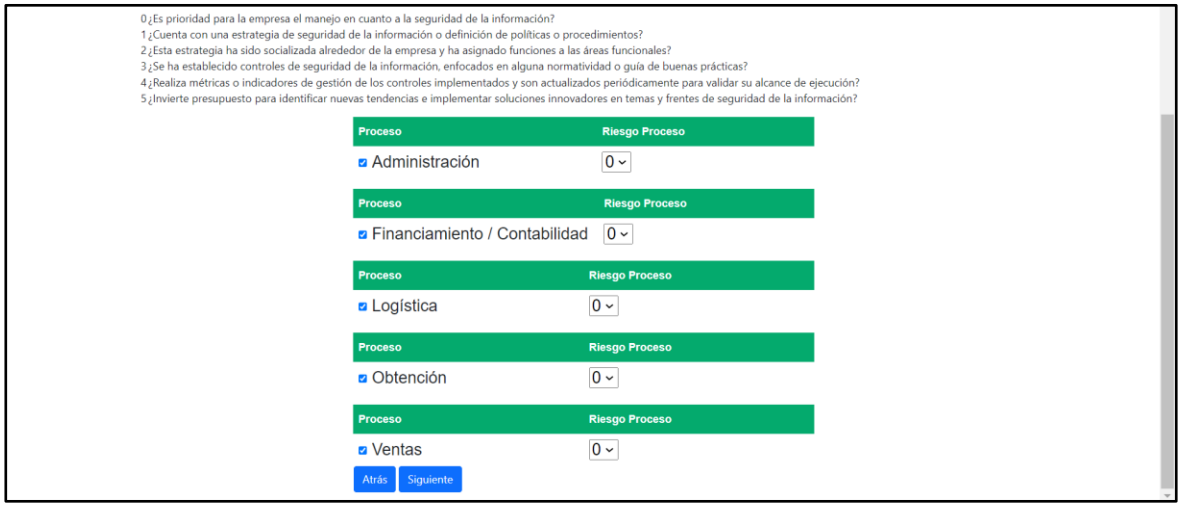
Activo TIC	Descripción
☑ Suministro eléctrico	Sistemas de suministro eléctrico.
☐ Gestores de bases de datos	Aplicaciones de almacenamiento de información en bases de datos .
☑ Comunicaciones	Servicios de telecomunicaciones que la empresa posee.
☑ Sistemas operativos	Software de control para equipos informáticos .
☑ Aplicaciones informáticas	software que contenga o gestione información del negocio.
☑ Documentación física	Información corporativa, que se encuentra impresa.
☐ Otros contenedores	Activos informáticos que resguardan información de la empresa.
☑ Personas	Personas que poseen conocimiento corporativo y de procesos claves del negocio.
☑ Oficinas e instalaciones	Espacios físicos donde se encuentran los computadores, los servidores físicos, los archivadores, la documentación en papel entre otros.
☑ Portátiles, tabletas y móviles	Dispositivos electrónicos que se retiran de las instalaciones, sea por visitas comerciales, teletrabajo, se lo lleva a casa después del trabajo, o se ceden temporalmente a terceros.
☑ Periféricos y pendrives	Dispositivos extraíbles de almacenamiento.
☐ Equipos red local	Equipos informáticos que permiten la conexión por medios inalámbricos o cableados.

Fuente: Captura de pantalla a la herramienta desarrollada

3.5.2. Definición nivel de madurez por proceso de negocio

A continuación, se definió para cada uno de los procesos de negocio presentes en la empresa del caso de estudio, los niveles de madurez teniendo como referencia la lista de chequeo definida. En este caso se identificó que el nivel de madurez es “ad-hoc”, dado que aún no se tienen implementadas políticas de seguridad de la información ni procedimientos mitigantes o definición de controles en términos de seguridad para las áreas funcionales:

Ilustración 12 Definición de nivel de madurez por proceso de negocio

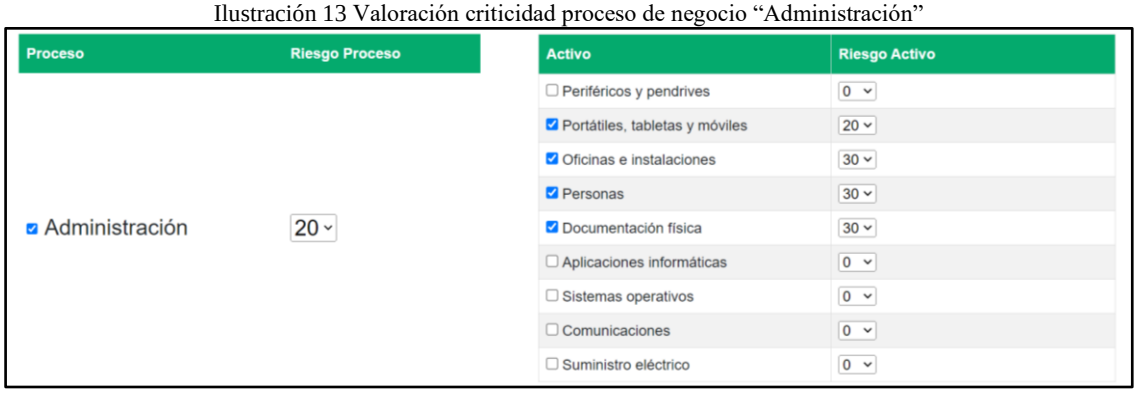


Fuente: Captura de pantalla a la herramienta desarrollada

3.5.3. Validación módulo “Cálculo de Activos de información críticos”

Una vez ingresados los procesos de negocio y activos de información propios del caso de estudio, se definió la criticidad de cada proceso de negocio y la criticidad de cada activo de información que soporta cada proceso de acuerdo a las escalas de valoración definidas en el modelo:

Ilustración 13 Valoración criticidad proceso de negocio “Administración”



Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 14 Valoración criticidad proceso de negocio “Financiamiento/Contabilidad”

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 15 Valoración criticidad proceso de negocio “Logística”

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 16 Valoración criticidad proceso de negocio “Obtención”

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 17 Valoración criticidad proceso de negocio “Ventas”

Fuente: Captura de pantalla a la herramienta desarrollada

3.5.4. Reporte de recomendaciones de seguridad generadas

Finalmente, después de relacionar la criticidad de los activos de información respecto al proceso de negocio que soporta, la herramienta generó las recomendaciones de implementación de los respectivos controles de seguridad:

Ilustración 18 Recomendación de implementación de controles para el proceso "Administración"

Proceso	nivel	Acitvo	Control	Tratamiento	Riesgo
Administración	Ad-hoc	Documentación física	Criptografía-Cifrado y gestión de claves	Acuerdo de confidenicalidad con los empleados, políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
		Oficinas e instalaciones	Seguridad física y Ambiental	Medidas de seguridad física, como sistemas de control de acceso o vigilancia. políticas claras de seguridad, conciencia o capacitación insuficiente. conciencia y capacitación en seguridad por parte de los empleados.	Divulgación de información confidencial o acceso no autorizado a sistemas.
		Personas	Seguridad física y Ambiental	Medidas de seguridad para proteger los dispositivos y	Acceso no autorizado a la información y a los sistemas de

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 19 Recomendación de implementación de controles para el proceso "Financiamiento/Contabilidad"

Financiamiento / Contabilidad	Ad-hoc	Documentación física	Controles de acceso	medidas de seguridad física.	Divulgación de información confidencial o uso indebido de los documentos.
		Aplicaciones informáticas	Gestión de incidentes de seguridad de la Información	Mantenimiento o infraestructura inadecuada.	Pérdida de productividad, interrupción de las operaciones o pérdida de datos.
		Portátiles, tabletas y móviles	Controles de acceso	medidas de seguridad, autenticación robusta.	Acceso no autorizado a la información almacenada en los dispositivos.
		Documentación física	Criptografía-Cifrado y gestión de claves	Acuerdo de confidenicalidad con los empleados, políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
		Personas	Seguridad física y Ambiental	Medidas de seguridad para proteger los dispositivos y credenciales.	Acceso no autorizado a la información y a los sistemas de la organización.

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 20 Recomendación de implementación de controles para el proceso "Logística"

Logística	Ad-hoc	Personas	Seguridad física y Ambiental	Medidas de seguridad para proteger los dispositivos y credenciales.	Acceso no autorizado a la información y a los sistemas de la organización.
			Seguridad de los recursos humanos	Políticas claras de seguridad, conciencia y capacitación periodicas.	Divulgación de información confidencial, daños o acceso no autorizado a sistemas.
		Documentación física	Controles de acceso	medidas de seguridad física.	Divulgación de información confidencial o uso indebido de los documentos.
			Criptografía-Cifrado y gestión de claves	Acuerdo de confidenicalidad con los empleados, políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
			Gestión de activos	medidas de protección contra incendios, inundaciones u otros eventos adversos.	Pérdida irrecuperable de información o interrupción de las operaciones.

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 21 Recomendación de implementación de controles para el proceso “Obtención”

Obtención	Ad-hoc	Personas	Seguridad de los recursos humanos	Políticas claras de seguridad, conciencia y capacitación periodicas.	Divulgación de información confidencial, daños o acceso no autorizado a sistemas.
		Comunicaciones	Criptografía-Cifrado y gestión de claves	Cifrado y controles de seguridad en las comunicaciones	Divulgación de información confidencial, robo de datos o suplantación de identidad.
			Adquisición, desarrollo y mantenimiento del sistema	Problemas en la infraestructura de red o interferencias externas.	Pérdida de conectividad, interrupción de servicios o inaccesibilidad de datos.
		Documentación física	Gestión de activos	medidas de protección contra incendios, inundaciones u otros eventos adversos.	Pérdida irrecuperable de información o interrupción de las operaciones.
		Comunicaciones	Seguridad en	Medidas de seguridad, como autenticación y	Fugas de información, espionaje

Fuente: Captura de pantalla a la herramienta desarrollada

Ilustración 22 Recomendación de implementación de controles para el proceso “Ventas”

Ventas	Ad-hoc	Aplicaciones informáticas	Gestión de incidentes de seguridad de la Información	Mantenimiento o infraestructura inadecuada.	Pérdida de productividad, interrupción de las operaciones o pérdida de datos.
		Documentación física	Controles de acceso	medidas de seguridad física.	Divulgación de información confidencial o uso indebido de los documentos.
			Criptografía-Cifrado y gestión de claves	Acuerdo de confidenicalidad con los empleados, políticas y controles de seguridad adecuados.	Divulgación o uso indebido de información confidencial.
		Aplicaciones informáticas	Controles de acceso	controles de autenticación y autorización.	Divulgación, manipulacion o perdida de información
		Personas	Seguridad física y Ambiental	Medidas de seguridad para proteger los dispositivos y credenciales.	Acceso no autorizado a la información y a los sistemas de la organización.

Fuente: Captura de pantalla a la herramienta desarrollada

4. Conclusiones y recomendaciones

4.1. Conclusiones

- Referenciando el trabajo de investigación realizado se pudo demostrar que la incorporación de estándares y modelos de gestión de seguridad de la información en las micro y pequeñas empresas es fundamental para mitigar los riesgos asociados a las amenazas y desafíos tecnológicos actuales. La adaptabilidad de un modelo de madurez, como el propuesto basado en O-ISM3, permite abordar las particularidades y limitaciones propias de estas empresas, brindando recomendaciones y estrategias adecuadas a su realidad.

  Por lo anterior, la investigación realizada ha demostrado que la adopción de estándares y modelos de gestión de seguridad de la información es esencial para las micro y pequeñas empresas (MYPEs) con el fin de hacer frente a los riesgos asociados a las amenazas y desafíos tecnológicos actuales. La adaptabilidad de un modelo de madurez, como el propuesto basado en O-ISM3, se ha revelado como una solución viable y efectiva que permite abordar las particularidades y limitaciones inherentes a estas empresas. Al brindar recomendaciones y estrategias adecuadas a su realidad, este enfoque soporta que las MYPEs puedan fortalecer su postura de seguridad de la información de manera proactiva y sostenible, sin verse abrumadas por la complejidad de los estándares diseñados para empresas más grandes.

- La implementación de un modelo de gestión de seguridad de la información, respaldado por una herramienta informática, facilita la evaluación de la madurez de seguridad y ofrece recomendaciones específicas para mejorarla. A través de la metodología y la matriz de riesgo definidas en esta investigación, las micro y pequeñas empresas pueden comprender mejor las amenazas y vulnerabilidades a las que están expuestas, lo que contribuye a una mayor concienciación y prevención en materia de seguridad de la información.

  Igualmente, la adopción de esta herramienta informática proporciona un enfoque sistemático y eficaz para realizar un diagnóstico sobre la gestión de riesgos transversal realizada a la compañía y la madurez del Gobierno Corporativo implementado. Este diagnóstico puede ofrecer una estructura sólida que permite a las MYPEs comprender mejor las amenazas y vulnerabilidades a las que están expuestas y realizar estrategias de mejora continúa apoyadas

en estructuras de control corporativas. Al ofrecer recomendaciones específicas para mejorar la seguridad de la información, estas herramientas no solo aumentan la conciencia sobre la importancia de la seguridad cibernética, sino que también contribuyen significativamente a la prevención de incidentes y a la protección de los activos de información críticos para el negocio.

- La validación del modelo propuesto a través del caso de estudio definido proporcionó evidencia concreta de su efectividad y aplicabilidad en situaciones reales. Los resultados obtenidos ofrecieron una perspectiva práctica de cómo el modelo puede mejorar la seguridad de la información en una empresa específica, proporcionando recomendaciones puntuales que pueden ser aplicadas al interior de sus procesos de negocio cubriendo sus activos de información base.

  Igualmente, al proporcionar recomendaciones puntuales que pueden ser implementadas dentro de las funciones de negocio existentes, el modelo demuestra su capacidad para abordar las necesidades y desafíos únicos de las MYPEs independiente de su sector de operación, tamaño o estructura, cubriendo sus activos de información críticos y por ende fortaleciendo su postura de seguridad en un entorno cada vez más complejo y dinámico. Al identificar que este sector empresarial corresponde a un porcentaje alto del total de Compañías que compone el empresariado del país, iniciativas como estas estaría protegiendo la integridad y disponibilidad del servicio de un sector representativo.

4.2. Recomendaciones

- Es importante visibilizar las brechas y falencias en gestión de Seguridad de la información y Seguridad informática presente en los sectores empresariales del país, en aras de crear consciencia e implementación de posibles soluciones.
- Se recomienda una constante capacitación e instrucción por parte de los líderes empresariales de las pequeñas y microempresas del país en términos de ciberseguridad y evaluar el impacto que estás podrían tener al interior.
- Desde el sector académico e investigativo es importante concientizar y resaltar la responsabilidad del Gobierno y los entes del control para la gestión de la tecnología, riesgos, desafíos y mitigación de ciberataques.

- Para la maduración del modelo propuesto, se recomendaría una aplicación a escala de casos de estudio que permita identificar mejoras y variables importantes que permitiera identificar casuísticas nuevas que permita mejora el modelo.

Bibliografía

[1] P. security, «https://www.pandasecurity.com/,» 2020. [En línea]. Available: https://www.pandasecurity.com/spain/mediacenter/seguridad/en-la-cabeza-del-cibercriminal-que-busca-y-por-que-quiere-atacar-tu-empresa/.

[2] Digiware, «dinero.com,» 2022. [En línea]. Available: https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321.

[3] ISO, «implementandosgi.com,» 2021. [En línea]. Available: https://www.implementandosgi.com/sistemas-de-gestion/certificacion-iso-para-colombia/.

[4] DEE, «Directorio Estadístico de Empresas,» 2021. [En línea]. Available: https://www.dane.gov.co/files/investigaciones/boletines/registro-estadistico/boletin-directorio-estadistico-empresas-2019-2021.pdf.

[5] EY, «Colombia digital,» 2017. [En línea].

[6] F. Villarán, El mundo de la pequeña empresa, Lima, 2007.

[7] W. Vega, «POLITICAS Y SEGURIDAD DE LA INFORMACION,» *Fides et ratio*, 2008.

[8] ARCHIVO, «ARCHIVO GENERAL DE LA NACIÓN,» 2015. [En línea]. Available: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/3_Transparencia/3.3%20Procesos%20y%20Procedimientos/GIT-G-01_GUIA_PARA_LA_CALIFICACI%C3%93N_DE_LA_INFORMACI%C3%93N_AGN.pdf.

[9] ISO, «ISO 27001,» 2012. [En línea]. Available: http://www.iso27000.es/sgsi.html.

[10] O-ISM3, «https://www.ism3.com/node/42,» 2017. [En línea].

[11] W. Porter y J. Burton, Auditoría un enfoque conceptual, México: Limusa, 1983.

[12] A. Holmes, Principio básicos de auditoría, México: C.E.C.S.A, 1984.

[13] Verhoef, Quantifying the effects of IT-governance rules, Science of Computer Programming, 2007.

[14] «HEFLO,» 2019. [En línea]. Available: https://www.heflo.com/es/blog/gobernanza/gobierno-ti/.

[15] Y. Kim, J. Lee, C. Koo y K. Nam, The role of governance effectiveness in explaining IT, International Journal of Information Management, 2013.

[16] Promonegocio, «Promonegocio,» 2019. [En línea]. Available: https://www.promonegocios.net/empresa/pequena-empresa.html#que-es.

[17] ISO Tools, «ISO Tools,» [En línea]. Available: https://www.isotools.org/2014/08/19/iso-27001-activos-informacion-empresa-3/ .

[18] kaspersky, «kaspersky.es,» [En línea]. Available: https://www.kaspersky.es/resource-center/threats/computer-vandalism.

[19] incibe, «https://www.incibe.es,» 2019. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian.

[20] N. Frett, «https://www.auditool.org/,» [En línea]. Available: https://www.auditool.org/blog/auditoria-de-ti/3423-que-es-un-ciberataque.

[21] T. Valásquez, A. Puentes y Y. Pérez, «Un enfoque de buenas prácticas de gobierno corporativo de TI,» *Tecnura,* 2015.

[22] L. Sánchez, A. Santos, E. Fernández y M. Piattini, «Características deseables para un SGSI orientado a PYMES,» *SICAMAN,* 2015.

[23] D. Villafranca, L. Sánchez, F. Eduardo y M. Piattini, «La norma ISO/IEC 17799 como base para Gestionar la Seguridad de la Información,» *SICAMAN,* 2014.

[24] A. Parra, «ISO 27001 para PYMES,» *Universidad Internacional de la Rioja,* 2014.

[25] F. Valencia y M. Orozco, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *Risti,* 2017.

[26] J. Romero y J. Ramírez, «Diseño e implementación de un prototipo que permita el despliegue de un plan de recuperación de desastres aplicable a empresas MIPYMES Colombianas,» *Universidad Católica de Colombia,* 2013.

[27] A. M. MAYA, «repository.eafit.edu.co,» 2016. [En línea]. Available: 1. https://repository.eafit.edu.co/bitstream/handle/10784/9521/Andr%C3%A9s_MadridMaya_2016.pdf?sequence=2&isAllowed=y.

[28] K. J. J. González, «repositorio.cuc.edu.co,» 2016. [En línea]. Available: 5. http://repositorio.cuc.edu.co/bitstream/handle/11323/213/1143121379.pdf?sequence=1&isAllowed=y.

[29] Y. Ebru, A. Gizem, A. Serpil y B. Nuran, «Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey,» *International Journal of Information Management,* 2011.

[30] N. Cruz y J. Gutierrez, «Literature review of the situation research faces in the application of ITIL in Small and Medium Enterprises,» *Computer Standards & Interfaces,* 2016.

[31] ISO, *Norma ISO 27001:2013,* 2013.

[32] EAFIT, «EAFIT,» [En línea]. Available: https://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/A%20COBIT.pdf. [Último acceso: 2021].

[33] IBM, «IBM,» [En línea]. Available: https://www.ibm.com/es-es/topics/it-infrastructure-library.

[34] confecamaras, «http://www.confecamaras.org.co,» [En línea]. Available: http://www.confecamaras.org.co/phocadownload/2018/Cuadernos_An%C3%A1lisis_Econ%C3%B3mico/Cuaderno_demografia_empresarial/Cartilla17.pdf.

[35] ISO, «(ISO/IEC 27001:2013),» 2013.