DETERMINAR LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LA ARQUITECTURA Y ESTRATEGIAS DE NEGOCIOS DE EMPRENDIMIENTOS PYMES ORIENTADAS A SOLUCIONES TI EN COLOMBIA

.

CRISTIAN CAMILO MEDINA LLANOS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
FUSAGASUGA - CUNDINAMARCA
2025

DETERMINAR LA IMPORTANCIA DE LA CIBERSEGURIDAD EN LA ARQUITECTURA Y ESTRATEGIAS DE NEGOCIOS DE EMPRENDIMIENTOS PYMES ORIENTADAS A SOLUCIONES TI EN COLOMBIA

CRISTIAN CAMILO MEDINA LLANOS

MONOGRAFIA

Proyecto de Grado – Monografía desarrollada y presentada para optar por el titulo
ESPECIALISTA EN SEGURIDAD INFORMATICA

MSc. EDGAR ROBERTO DULCE VILLAREAL
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMATICA
FUSAGASUGA - CUNDINAMARCA
2025

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Fusagasugá, 15 de mayo de 2025

DEDICATORIA

Quiero dedicar el desarrollo de este trabajo monográfico a mi madre Amparo Llanos y mis hermanos Duban Felipe Medina y Juan Carlos Medina, que con su apoyo y cariño he logrado sacar adelante mis objetivos académicos. A mi padre Yesid Medina (Q.E.P.D) que desde niño me indico que para lograr mis objetivos tenía que estudiar y esforzarme para ser alguien en la Vida. Dedicar este logro a mi Novia y futura esposa Natalia Godoy Díaz, que con su apoyo, amor y palabras de aliento ha logrado que termine este ciclo académico de la mejor manera.

Cristian Camilo Medina Llanos

AGRADECIMIENTOS

Inicialmente agradecer a Dios, a mi madre y mis hermanos por el apoyo que he recibido durante el desarrollo de este trabajo monográfico y el desarrollo óptimo de la carrera. Adicionalmente agradecer a las directivas administrativas y grupo de docentes de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su compromiso y entrega brindan la oportunidad de adquirir conocimiento, orientan sobre un proceso de formación y fortalecer mi destreza para el mundo laboral. Realizo un especial agradecimiento al ingeniero especialista Edgar Roberto Dulce Villareal por su acompañamiento y retroalimentación experimentada durante el proceso de diseño y desarrollo de este trabajo.

TABLA DE CONTENIDO

LISTA DE TABLAS **8**

LISTA DE FIGURAS **9**

1. GLOSARIO **10**

2. RESUMEN **13**

3. INTRODUCCIÓN **15**

4. DEFINICIÓN DEL PROBLEMA **16**

4.1. ANTECEDENTES DEL PROBLEMA **16**

4.2. FORMULACIÓN DEL PROBLEMA **16**

5. JUSTIFICACIÓN **17**

6. OBJETIVOS **18**

6.1. OBJETIVO GENERAL **18**

6.2. OBJETIVOS ESPECÍFICOS **18**

7. MARCO REFERENCIAL **19**

7.1. MARCO TEÓRICO **19**

7.1.1. **Bases teóricas:** 19

7.2. MARCO CONCEPTUAL **24**

7.3. MARCO HISTÓRICO **26**

7.4. ANTECeDENTES **28**

7.5. MARCO LEGAL **29**

7.5.1. **Ley 2069 del 31 de diciembre de 2020:** 30

7.5.2. DECRETA:ARTÍCULO 1. 30

7.5.3. Ley 1273 de 2009: "CIBERSEGURIDAD ENTORNO COLOMBIANO" 30

8. DESARROLLO DE LOS OBJETIVOS 32

8.1. RESALTAR el impacto de la ciberseguridad en los procesos de creación y consolidación de pymes en Colombia, con el fin de identificar cómo su integración temprana en el diseño de arquitecturas tecnológicas y estrategias de negocio influye en la viabilidad, sostenibilidad y crecimiento de estas organizaciones en entornos digitales. 32

8.2. EXAMINAR la importancia de la ciberseguridad al momento de seleccionar una idea de negocio pymes en TI. 36

8.3. Evaluar las condiciones de ciberseguridad de proyectos TI en el sector pyme en Colombia, antes y después de la emergencia sanitaria generada por la pandemia 42

8.4. Compilar las características de ciberseguridad que moldean los proyectos pymes enfocados en TI. 46

9. CONCLUSIONES 51

10. RECOMENDACIONES 52

11. BIBLIOGRAFÍA 53

pág.

LISTA DE TABLAS

Tabla 1 Factores de Seguridad del Negocio – lASME Standard v.....47
Tabla 2 controles del ISSA-UK 5173 48

LISTA DE FIGURAS

Gráfica 1 Clasificación de empresas Colombia 2024.....19
Gráfica 2 Diagrama de como ocurren los ataques informáticos o cibernéticos: ...33

1. GLOSARIO

AMENAZA: aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas). [1]

APLICACIÓN: una aplicación es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajo[2]

CIBERSEGURIDAD: la ciberseguridad es la práctica de defender sistemas, redes y programas de ataques digitales. Generalmente, dichos ciberataques apuntan a entrar, cambiar o eliminar la información confidencial; Extorsionar a los usuarios o los usuarios o interrumpir la continuidad del negocio.[3]

CLOUD: red mundial de servidores, cada uno con una funcionalidad exclusiva. La nube no es una entidad física, sino una gran red de servidores remotos de todo el planeta que permanecen conectados para funcionar como un exclusivo ecosistema. Dichos servidores fueron creados para guardar y regir datos, realizar aplicaciones o dar contenido o servicios, como streaming de vídeos, correspondencia web, programa de ofimática o medios sociales.[4]

CONFIDENCIALIDAD: la confidencialidad es la garantía de que la información personal va a ser protegida para que no sea difundida sin consentimiento del individuo. Esa garantía se realiza mediante un conjunto de normas que limitan el acceso a ésta información.[5]

DISPONIBILIDAD: supone que el sistema informático se mantenga trabajando sin sufrir ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los

---

[1] AMBIT TEAM. {en línea} «Tipos de Vulnerabilidades y Amenazas informáticas». Recuperado 21 de abril de 2022 (https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas?hs_amp=true).

[2] ECURED. {en línea} «Aplicación (informática) - EcuRed». Recuperado 21 de abril de 2022 (https://www.ecured.cu/Aplicaci%C3%B3n_(inform%C3%A1tica)).

[3] CISCO. {en línea} «¿Qué es la ciberseguridad? - Cisco». Recuperado 21 de abril de 2022 (https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html).

[4] Microsoft. {en línea} «Qué es la nube: definición | Microsoft Azure». Recuperado 21 de abril de 2022 (https://azure.microsoft.com/es-es/overview/what-is-the-cloud/?cdn=disable).

[5] Morales, Omar Bazan. «Comité de ética en investigación». Sitio Web del Comité de ética en investigación. Recuperado 21 de abril de 2022 (https://www.incmnsz.mx/opencms/contenido/investigacion/).

recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados.[6]

EMPRENDIMIENTO: plan que se inicia para edificar o conseguir un objetivo que en su mayoría tiene alguna iniciativa creativa. Por consiguiente, emprender significa actuar o comenzar actividades para concretar o materializar algo, que en el campo empresarial se traduce en la construcción de organizaciones y negocios.[7]

EMPRESA: organización de personas y recursos que buscan la consecución de un beneficio económico con el desarrollo de una actividad en particular. Esta unidad productiva puede contar con una sola persona y debe buscar el lucro y alcanzar una serie de objetivos marcados en su formación.[8]

INFORMACIÓN: grupo organizado de datos, que constituye un mensaje sobre un cierto fenómeno o ente. La información posibilita solucionar inconvenientes y tomar elecciones, debido a que su uso racional es la base del entendimiento.[9]

INTEGRIDAD: supone que la información se mantenga inalterada ante accidentes o intentos maliciosos. Sólo se podrá modificar la información mediante autorización.

MIPYME: las micro, pequeñas y medianas empresas (Mipymes) son actores estratégicos en el incremento de la economía, la transformación del aparato productivo nacional y el mejoramiento de la postura competitiva de la nación. Además, las Mipymes contribuyen a minimizar la pobreza y la inequidad, al ser alternativas de generación de trabajo, ingresos y activos para un enorme conjunto de individuos.[10]

NEGOCIO: cualquier actividad, ocupación o método que tiene como fin obtener una ganancia.[11]
NORMATIVIDAD: conjunto de normas que regulan un tema o ámbito determinado y que se encuentran vigentes

---

[6] ISOTools, Excellence. {en línea}. 2018. «Confidencialidad, integridad y disponibilidad en los SG-SSI». PMG SSI - ISO 27001. Recuperado 21 de abril de 2022 (https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/).
[7] Gerencie, {en línea}. «Emprendimiento | Gerencie.com». Recuperado 21 de abril de 2022 (https://www.gerencie.com/emprendimiento.html/amp).
[8] Sánchez Galán, Javier. 12-2015 {en línea} «Empresa - Qué es, definición y concepto | 2022 | Economipedia». Recuperado 2 de diciembre de 2015 (https://economipedia.com/definiciones/empresa.html).
[9] EcuRed.{en línea} «Información - EcuRed». Recuperado 21 de abril de 2022 (https://www.ecured.cu/Informaci%C3%B3n).
[10] DNP. {en línea}. «Micro, Pequeña y Mediana Empresa». Recuperado 21 de abril de 2022 (https://www.dnp.gov.co:443/programas/desarrollo-empresarial/micro-pequena-y-mediana-empresa/Paginas/micro-pequena-y-mediana-empresa.aspx).
[11] Roldan, Paula Nicole. 2017. {en línea}. «Negocio - Definición, qué es y concepto». Economipedia. Recuperado 21 de abril de 2022 (https://economipedia.com/definiciones/negocio.html).

PROCESO: es un programa en ejecución el cual está gestionado por el sistema operativo[12]

RIESGO: amenazas que tienen la posibilidad de atentar contra la seguridad de nuestros propios recursos, nuestra información o nuestra organización por medio de ataques digitales.[13]

SEGURIDAD INFORMÁTICA: es el proceso de evitar y ubicar la utilización no autorizado de un sistema informático con el propósito de defender la totalidad y la privacidad de la información almacenada en un sistema informático.[14]

VULNERABILIDAD: fallo o postración de un sistema de información que pone en peligro la estabilidad de la misma. Se trata de un "agujero" que podría ser producido por un error de configuración, una carencia de métodos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para lograr entrar en los mismos y hacer ocupaciones ilegales, hurtar información sensible o interrumpir su funcionamiento.[15]

[12] Academic. {en línea}. «Proceso (informática)». Los diccionarios y las enciclopedias sobre el Académico. Recuperado 21 de abril de 2022 (https://es-academic.com/dic.nsf/eswiki/959703).
[13] Marin, Oscar. 2003. {en línea}. «Definición de Riesgo | TENDENCIAS | ComputerWorld». Recuperado 21 de abril de 2022 (https://www.computerworld.es/tendencias/definicion-de-riesgo).
[14] Netec. {en línea}. «¿Qué es seguridad informática? | Netec Global Knowledge». Netec. Recuperado 21 de abril de 2022 (https://www.netec.com/que-es-seguridad-informatica).
[15] AMBIT TEAM. 2020. {en línea}. «Tipos de Vulnerabilidades y Amenazas informáticas». Recuperado 21 de abril de 2022 (https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-inform%C3%A1ticas?hs_amp=true).

2. RESUMEN

La siguiente monografía buscar determinar mediante una investigación exploratoria, recopilar información que permita validar la relevancia e importancia que le otorgan a la ciberseguridad los emprendedores en Colombia que están enfocados en TI, al momento de estructurar y diseñar una idea o estrategia de negocio principalmente en las pymes. De igual forma, comprender qué papel toma la ciberseguridad, por medio de la aplicación y uso de buenas prácticas que orienta la ISO 27001 y 27002, al momento de estructurar sus ideas de negocio, teniendo en cuenta los riesgos y vulnerabilidades que se encuentran en el contexto digital en una humanidad que está unida por medio de la globalización.

Durante la investigación se ha de explorar la situación actual de los emprendedores TI en Colombia y como su estrategia de negocio está orientada en un marco de seguridad informática. Se busca establecer el nivel de conocimiento y percepción en cuanto al riesgo que se encuentra en la red y estructura tecnológica.

En esta recopilación monográfica se va a resaltar el cómo la era digital está cada día integrándose al estilo de vida de los individuos, empresas y gobiernos, de tal forma, que para el cumplimiento de sus diferentes objetivos se apoyan en la estructura y soluciones que otorga las herramientas tecnológicas a las que se tienen acceso. La ciberseguridad pasa a tomar un papel muy importante para garantizar y potencializar la estructura tecnológica a nivel físico y lógico, y que tiene como objetivo primario salvaguardar y gestionar de forma eficiente los datos.

Palabras Clave: Ciberseguridad, Seguridad Informática, Emprendedores TI, estrategia de negocio.

ABSTRACT

The following monograph seeks to determine, through exploratory research, the collection of information that will allow validating the relevance and importance that IT-focused entrepreneurs in Colombia give to cybersecurity when structuring and designing a business idea or strategy, mainly in SMEs. Likewise, to understand what role cybersecurity plays, through the application and use of good practices guided by ISO 27001 and 27002, when structuring their business ideas, taking into account the risks and vulnerabilities found in the digital context in a humanity that is united through globalization.

During the research, the current situation of IT entrepreneurs in Colombia must be explored and how their business strategy is oriented within a computer security framework. The aim is to establish the level of knowledge and perception regarding the risk found in the network and technological structure.

This monographic compilation will highlight how the digital era is increasingly integrating into the lifestyle of individuals, companies and governments, in such a way that, in order to achieve their different objectives, they rely on the structure and solutions provided by the technological tools to which they have access. Cybersecurity becomes very important in guaranteeing and enhancing the technological structure at a physical and logical level, and whose primary objective is to safeguard and efficiently manage data.

Key words: *Cybersecurity, Information Security, IT Entrepreneurs, business strategy.*

3. INTRODUCCIÓN

La era digital esta cada día integrándose al estilo de vida de las personas, empresas y gobiernos, estableciendo que para el cumplimiento de sus diferentes objetivos se apoyan en la estructura y soluciones que otorga las herramientas tecnológicas a las que se tienen acceso. Aquí entra a jugar un papel importante los pilares de la seguridad informática que trata de los conceptos y fundamentos de la seguridad, la confidencialidad y la integridad de la información, que se considera como uno de los activos más importantes. La ciberseguridad pasa a tomar un papel relevante para garantizar y potencializar la estructura tecnológica a nivel físico y lógico, y que tiene como objetivo primario salvaguardar y gestionar de forma eficiente los datos.

La ciberseguridad se convierte en un pilar fundamental a la hora de diseñar, desarrollar, implementar y mantener una idea de negocio de tipo pymes que tiene por objetivo satisfacer una necesidad o complementar un servicio de TI. La siguiente monografía buscar determinar la relevancia e importancia que le otorgan los emprendedores enfocados en TI a la ciberseguridad, partiendo de la percepción de riesgo y vulnerabilidad de la información en un contexto globalizado y digital.

4. DEFINICIÓN DEL PROBLEMA

4.1. ANTECEDENTES DEL PROBLEMA

Las organizaciones y empresas en Colombia están basando sus procesos operativos, administrativos y logísticos en las tecnologías de la información, lo cual permite que la información esté disponible a todos los niveles. Como el aspecto digital está en su auge, se han identificado sus fortalezas y debilidades. Entre sus debilidades está el omitir el proceso de garantizar la integridad y salvaguardar la información.

Dado lo anterior, los gurús y profesionales de la seguridad informática han desarrollado esfuerzos para integrar el concepto de ciberseguridad a los procesos empresariales, creando normatividades, buenas prácticas y procedimientos que garanticen la seguridad de la información. A partir del concepto que tiene como premisa la seguridad informática, se debe crear y desarrollar la cultura en ciberseguridad, desde las ideas de negocio hasta la implementación de dicha idea. Esto permite que el valor de la información sea respaldado por las diferentes políticas y normatividades de seguridad informática que están vigentes en la actualidad.

Las personas que tienen como iniciativa generar un emprendimiento enfocado en TI, la mayoría de las veces omiten este proceso de inclusión de seguridad cibernética en sus procesos de arquitectura y estrategias de negocio, solo se centran en iniciar y percibir ganancias, no comprenden ni tienen idea del valor de la información para los delincuentes cibernéticos o empresas desleales que quieren salir adelante a cualquier costo. Las iniciativas de negocio van a adquirir información de clientes, socios, proveedores y empleados, para lo cual como requisito indispensable de estas iniciativas debería estar el incluir procesos de ciberseguridad.

La falta de compromiso con la inclusión y creación de la cultura de ciberseguridad esta desde la formación académica, puesto que se tiene un concepto mal interpretado de ciberseguridad. En el contexto colombiano se cree que la seguridad informática es sinónimo de compras de tecnología que son catapultadas por una sociedad consumista que al final no son funcionales o son innecesarias. Es por ello, por lo que los emprendedores no tienen la noción de importancia de la ciberseguridad al momento de desarrollar una estrategia de negocio y por ende una arquitectura basada en la seguridad informática.

4.2. FORMULACIÓN DEL PROBLEMA

¿Cuál es la importancia de la ciberseguridad y el impacto que tiene en la arquitectura y estrategias de negocios de emprendimientos pymes orientadas a soluciones TI en Colombia?

5. JUSTIFICACIÓN

Este estudio monográfico se basa en determinar la importancia que tiene la ciberseguridad y su impacto a la hora de emprender y sacar adelante una idea de negocio en contexto pymes, que satisfaga una necesidad en TI. La tecnología día tras día está apoyando el progreso bajo su premisa de mejorar y transformar los procesos de tal forma que sean eficientes y eficaces a la hora de contribuir con el cumplimiento de los objetivos institucionales. Durante la emergencia sanitaria a causa del surgimiento del COVID 19, las grandes, medianas y pequeñas empresas optaron por realizar sus procesos a través de la figura de trabajo en casa por medio de la virtualidad. Sin embargo, para esta estrategia no se tenía considerado el nivel de riesgo y vulnerabilidad para la información y su estructura tecnológica. A partir de allí las empresas potenciaron sus esfuerzos en acelerar la implementación de la ciberseguridad e incentivar el hábito de seguridad informática en los individuos que hacen parte de la organización.

Con base en lo anterior se hace necesario que todo este proceso de ciberseguridad este presente a la hora diseñar la arquitectura y estrategia de negocios de los diferentes emprendimientos pymes que están orientados a satisfacer o prestar un servicio en Tecnologías de la información. Este proceso se debe realizar para estar alertas a las diferentes situaciones que puedan comprometer la seguridad informática y de esta forma fomentar la cultura en ciberseguridad en todos los niveles. El presente estudio monográfico se concentrará identificar, analizar, estudiar y aprender sobre la situación actual de las estrategias de negocio pyme enfocadas en TI y que estén en proceso de arquitectura y diseños de estrategia de negocios y que tan comprometidas están los aspectos de ciberseguridad.

6. OBJETIVOS

6.1. OBJETIVO GENERAL

Establecer la importancia de la ciberseguridad y su impacto en el momento de estructurar ideas y/o estrategias de negocio pymes enfocadas en brindar soluciones TI en Colombia.

6.2. OBJETIVOS ESPECÍFICOS

- Resaltar el impacto de la ciberseguridad en los procesos de creación y consolidación de pymes en Colombia, con el fin de identificar cómo su integración temprana en el diseño de arquitecturas tecnológicas y estrategias de negocio influye en la viabilidad, sostenibilidad y crecimiento de estas organizaciones en entornos digitales.

- Examinar la importancia de la ciberseguridad al momento de seleccionar una idea de negocio pymes enfocadas en TI

- Evaluar las condiciones de ciberseguridad de proyectos TI en el sector pyme en Colombia, antes y después de la emergencia sanitaria generada por la pandemia

- Compilar las características de ciberseguridad que moldean los proyectos pymes enfocados en TI.

7. MARCO REFERENCIAL

7.1. MARCO TEÓRICO

7.1.1. Bases teóricas:

Durante el desarrollo del presente estudio monográfico se empieza por conocer los inicios del concepto y contexto de pymes en Colombia. El término Pyme hace referencia al grupo de empresas pequeñas y medianas con activos totales superiores a 500 SMMLV y hasta 30.000 SMMLV[16] (Bancoldex, 2018). El gobierno nacional establece que este concepto fue concebido como una política nacional, mediante la ley 590 del año 2000, de acuerdo con la filosofía de generar empleo y riqueza.

Las MiPymes representan más del 99% de las empresas del país, generan aproximadamente 79% del empleo y aportan 40% al Producto Interno Bruto (PIB)[17] (ANIF – Centro de estudios económicos, 2021). De esta forma se ha convertido en el eje fundamental de las políticas económicas que tengan por objetivo el desarrollo productivo y la igualdad social.

En Colombia el segmento empresarial esta clasificado en micro, pequeñas, medianas y grandes empresas, esta clasificación estuvo reglamentada en la Ley 590 de 2000 conocida como la Ley Mipymes y sus modificaciones (Ley 905 de 2004); y posteriormente por el Decreto MinCIT No. 957 del 5 de junio de 2019, que rige actualmente[18]. (Bancoldex, 2021).

Gráfica 1 Clasificación de empresas Colombia 2024

Cuadro clasificación 2024 1 UVT= $47.065 pesos:

Clasificación	Manufactura	Servicios	Comercio
Microempresas	Hasta $1.108.992.595	Hasta $1.552.580.220	Hasta $2.107.052.985
Pequeñas empresas	Superior a $1.108.992.595 y hasta $9.648.089.675	Superior a $1.552.580.220 y hasta $6.210.273.815	Superior a $2.107.052.985 y hasta $20.292.968.985
Medianas empresas	Superior a $9.648.089.675 y hasta $81.731.431.725	Superior a $6.210.273.815 y hasta $22.733.995.210	Superior a $20.292.968.985 y hasta $101.692.968.980
Grandes empresas	Superior a $81.731.431.725	Superior a $22.733.995.210	Superior a $101.692.968.980

Fuente: *Clasificación de Empresas en Colombia*. (2021, julio 29). Bancoldex.

[16] *¿Qué es una pyme?* (2018, julio 30). Bancoldex. https://www.bancoldex.com/es/que-es-una-pyme-1338

[17] *Retos y oportunidades de las Pymes—ANIF*. (s. f.). Recuperado 13 de enero de 2025, de https://www.anif.com.co/comentarios-economicos-del-dia/retos-y-oportunidades-de-las-pymes/

[18] *Clasificación de Empresas en Colombia*. (2021, julio 29). Bancoldex. https://www.bancoldex.com/es/sobre-bancoldex/quienes-somos/clasificacion-de-empresas-en-colombia

Teniendo en cuenta que las pymes son un eje fundamental para la economía del país, el gobierno nacional y la globalización han abierto una puerta bastante amplia hacia la era digital y tecnológica. Dado lo anterior, el gobierno nacional por medio de su Ministerio de Tecnologías de la Información y las Comunicaciones (TIC) ha desarrollado una guía para la comprensión del modelo y su estrategia de implementación para los emprendedores en soluciones orientadas a tecnologías de la información (TI)[19]. Esta guía busca presentar una reflexión sobre el modelo de emprendimiento en Colombia, partiendo de la convergencia de los elementos fundamentales: Los individuos, la destreza o conocimiento y sus intereses.

Partiendo de estos elementos, el Ministerio TIC mediante centros de investigación de las distintas universidades e instituciones educativas y las organizaciones, desarrollan de manera continua y asertiva, estrategias y actividades en las cuales se recrea el ambiente necesario para todas esas personas con espíritu emprendedor, que poseen una iniciativa que se fundamenta en sus conocimientos, actitudes y destrezas, logren diseñar, desarrollar e implementar un producto o servicio innovador con enorme efecto en los múltiples sectores basados en tecnologías de la información.

El Ministerio TIC, define el concepto de emprendedor como:" Persona con unas cualidades constitutivas de su ser: con una capacidad propositiva que lo impulsa a explorar y buscar formas de innovar en su área de conocimiento"[20]. A su vez, de acuerdo con la ley 1014 del 26 de enero de 2006, el concepto de emprendimiento se define como: "una manera de pensar y actuar, orientada hacia la creación de riqueza. Es una forma de pensar, razonar y actuar centrada en las oportunidades, planteada con visión global y lleva a cabo mediante un liderazgo equilibrado y la gestión de un riesgo calculados; su resultado es la creación de valor que beneficia a la empresa, la economía y la sociedad".

Los emprendedores TI tienen un modelo que orienta la eficiencia y eficacia de infraestructura y soporte, innovación, productividad y competitividad. Las ideas de negocio que están orientadas a tecnologías de la información promueven que haya una mejor gente o capacidad humana para la industria, que se diseñen, desarrollen e implementen productos innovadores, competitivos y confiables, así como, que generen una fortaleza financiera que se nutra el desarrollo de negocios, responsabilidad social y empresarial.

[19] *Modelo de emprendimiento TI Colombia*. (s. f.). Recuperado 13 de enero de 2025, de https://colombiatic.mintic.gov.co/679/w3-article-73972.html
[20] *Modelo de emprendimiento TI Colombia*. (s. f.). Recuperado 13 de enero de 2025, de https://colombiatic.mintic.gov.co/679/w3-article-73972.html

Teniendo en cuenta lo anterior los emprendedores en TI tiene una responsabilidad muy grande para fortalecer el ecosistema TI.
De igual forma, las ideas de negocio orientadas a TI tienen el apoyo por medio del modelo que establece el ministerio TIC. A estas ideas de negocio que apoya el modelo en mención, se debe adicionar el aspecto de ciberseguridad, como ese activo de alto valor que busca obtener seguridad, confidencialidad y disponibilidad de los procesos que abarcan su sistema de información, en una era donde lo digital y lo tecnológico no solo son un complemento si no una necesidad.

Desde la ley 527 de 1999 que hace referencia a la ley de comercio electrónico, Colombia entro en el ámbito de la revolución informática. Se tiene presente que así como otorga muchas soluciones y ventajas también tiene sus desventajas reflejadas en riesgos, vulnerabilidades y peligros que dan vida a los ciberdelincuentes.

La ciberseguridad se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas informáticos, las aplicaciones, los dispositivos, los datos, los activos financieros y las personas contra el ransomware y otros malware, las estafas de phishing, el robo de datos y otras ciber amenazas [21].(IBM, 2024). Con respecto a Amazon Web Services (AWS), el concepto de ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales.

Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa.[22] (AWS, 2025). La base de la ciberseguridad se basa en la principal protección de los datos, como activo mas valioso de las compañías en la revolución informática.

Teniendo en cuenta lo anterior, es propicio resaltar que la falta de experiencia al momento de desarrollar una idea de negocio orientada a una solución TI, puede generar vulnerabilidades y peligros a tal punto que afecte drásticamente su sistema de información y este se vea reflejado en altos costos económicos, tecnológicos y físicos.

Es importante mencionar que la ciberseguridad está regida por mejores prácticas que están soportadas mediante diferentes estándares como ITIL (significan *Information Technology Infrastructure Library*, que se traduce

[21] *¿Qué es la ciberseguridad? | IBM*. (2024, agosto 12). https://www.ibm.com/es-es/topics/cybersecurity

[22] *¿Qué es la ciberseguridad? - Explicación de la ciberseguridad* | AWS. (2025, Agosto 26). https://aws.amazon.com/es/what-is/cybersecurity/

literalmente como Biblioteca de Infraestructura de Tecnologías de Información), COBIT 5 como marco que permite comprender el gobierno y la gestión de TI y la familia ISO 27000, siendo la más relevante la ISO 27001, que establecen una guía de buenas prácticas para desarrollar el sistema de gestión de seguridad informática. En este contexto, los marcos ITIL 4, COBIT 5 y la norma ISO/IEC 27001:2022 se posicionan como herramientas clave para fortalecer la ciberseguridad desde diferentes niveles: operación, gobernanza y gestión de riesgos.

La guía que nos proporciona ITIL 4, publicado en 2019, utiliza el Sistema de Valor del Servicio (SVS) para integrar todas las actividades organizacionales en la creación de valor, incorporando la seguridad como componente esencial del ciclo de vida del servicio.[23] Incluye la práctica de gestión de seguridad de la información mediante la definición estructurada de políticas, evaluación de riesgos, aplicación de controles, gestión de incidentes, alineación a las diferentes regulaciones y promover la mejora continua.[24]

Con respecto las prácticas de COBIT 5, proporciona un marco integral de gobernanza y gestión de TI. Bajo los principios esenciales de que abarca toda la empresa y no solo el área TI, se apoya en el marco normativo de la ISO 27001 y las buenas prácticas de ITIL, proporciona un enfoque estructurado para identificación, evaluación y mitigación de riesgos TI en el contexto de la gobernanza empresarial.[25] Su mayor sinergia esta alineada a la ISO 27001, donde se proporcionando visión de alto nivel para gobernanza de TI mientras ISO 27001 aborda implementación de SGSI; juntos, fortalecen la coherencia, auditabilidad y alineación con estrategias de seguridad.

En cuanto a la normativa ISO 27001:2022 publicada en octubre de 2022, establece requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo el ciclo PHVA (Planear, Hacer, Verificar, Actuar).[26] Presenta un enfoque basado en gestión de riesgos y mejora continua, reforzando la integración de ciberseguridad con objetivos empresariales, alineando la gestión de riesgos con estrategia y liderazgo, promoviendo participación de la alta dirección. Exige actividades que permitan identificar, evaluar y tratar riesgos, con monitoreo continuo para adaptarse a amenazas emergentes. [27]

---

[23] *ISEOblue. Strategic Information Security Management within ITIL v4. 2024.*
[24] *EasyVista. Integrating ITIL and Cybersecurity Frameworks to Improve Security Governance. 26 junio 2025.*
[25] *Ciberprisma. Gobierno de las TIC: COBIT. 30 septiembre 2024.*
[26] *ISMS.online. Cómo alinear los riesgos de ciberseguridad con los objetivos de negocio mediante la norma ISO 27001:2022.*
[27] *WeLiveSecurity. ISO 27001:2022: qué cambió con el nuevo estándar de seguridad. 9 febrero 2023*

Como resultado final de combinar las bondades de las prácticas y normativas ya mencionadas, permite abordar la ciberseguridad desde la operación (ITIL), gobernanza (COBIT) y gestión de riesgos/control (ISO 27001:2022) de forma complementaria y robusta.

IBM como un referente de tecnologías de la información han presentado una serie de capas de protección para defenderse de los delitos cibernéticos, los cuales se definen como contramedidas y estas abarcan:

Seguridad de infraestructura fundamental[28]: se define como una serie de prácticas que tienen por objetivo defender los sistemas informáticos, activos TI, redes de información y telecomunicaciones. Estas prácticas tecnológicas contribuyen con la estabilidad nacional, economía y seguridad ciudadana. (IBM, 2024)

Seguridad en la red: estrategias y medidas de seguridad que tienen por objetivo defender la infraestructura de una red informática de los atacantes e intrusos por medio de conexiones inalámbricas o alámbricas. (IBM, 2024)

Seguridad de la aplicación: conjunto de procesos que promueven la defensa de las aplicaciones que operan en modo local o por medio de la nube. Este proceso de seguridad se debe integrar en las aplicaciones en la etapa de diseño e implementación, teniendo presente el proceso de gestión de datos, autenticación del cliente, etc. (IBM, 2024)

Seguridad en la nube: en especial, computación realmente confidencial que cifra los datos en la nube en reposo (almacenados), en desplazamiento (mientras migran hacía, a partir de y en la nube) y en uso (durante el procesamiento) para asegurar la privacidad del cliente y cumplir con los requisitos comerciales y los estándares de conformidad regulatoria. (IBM, 2024)

Seguridad de información: medidas de defensa de datos, como el Reglamento General de Protección de Datos o RGPD, que salvaguardan sus datos más confidenciales contra el acceso no autorizado, la exposición o el hurto. (IBM, 2024)

Educación del usuario final: proceso de enseñanza que tiene el objetivo de concientizar la importancia de la estabilidad al interior de la organización y de esta forma fortalecer la seguridad en los aspectos finales [29]. (IBM, 2024)

[28] Para más información remitirse a la referencia 21.
[29] Para mas información remitirse a la referencia 21.

Las Pymes y los diferentes emprendedores en soluciones orientadas a TI, deben tener en cuenta que hoy en día todo hace parte de una red interconectada y globalizada, donde los sistemas de información, datos de usuarios, clientes y datos financieros están allí de forma vulnerable que se puede aprovechar los ciberdelincuentes y proporcionar mucho daño. De ahí parte la importancia de identificar el nivel de relevancia que toma la ciberseguridad y el uso de las buenas prácticas que se deben seguir al momento de diseñar y estructurar la arquitectura de negocio o estrategia de negocio de un emprendimiento TI en concepto de Pymes.

7.2. MARCO CONCEPTUAL

Para el desarrollo de la presente monografía se debe partir del conocimiento y definición de los conceptos fundamentales que hacen parte del proyecto y como se interrelacionan estos entre sí, para la comprensión de todos los elementos que sustentan el mismo

Ciberseguridad: conjunto de prácticas y acciones que tiene por objetivo proteger la información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos y actividades económicas. (*¿Qué es la ciberseguridad? - Soporte técnico de Microsoft*)

Soluciones TI: son un conjunto de software o aplicaciones informáticas que facilitan la gestión y administración de un negocio. (CISET – Centro de innovación y soluciones empresariales y tecnológicas).

Emprendedores TI: personas con Ideas de negocio que basan su estrategia con enfoque en ofrecer servicios basados en las Tecnologías de la Información. (Ministerio TIC, 2019)

Emprendimiento TI: desarrollo de actividades o productos que establecen impactos en la forma de vida de las personas y el funcionamiento de la sociedad. Está enfocado en el diseño, innovación de soluciones y productos basados en TI. Su campo de acción está en software, hardware, servicios TI, biotecnología, nanotecnología y de más ramas de las tecnologías. (Ministerio TIC, 2019)

Confidencialidad: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. (Conceptos básicos de ciberseguridad que debes conocer | Ciudadanía | INCIBE.).

Seguridad en la Información: medidas y técnicas de seguridad utilizadas para controlar y proteger los datos que se manipulan y se generan dentro de la organización y asegurar que estos datos no salgan del sistema de información que se ha establecido. (Conceptos básicos de ciberseguridad que debes conocer | Ciudadanía | INCIBE.).

Integridad de la Información: Hace referencia a los datos que permanecen intactos y sin cambios a lo largo de todo su ciclo de vida, los cuales no tengan el riesgo de que se corrompan de manera accidental o maliciosa. (Conceptos básicos de ciberseguridad que debes conocer | Ciudadanía | INCIBE.).

Arquitectura y Estrategia de Negocio TI: Diseño, Creación e implementación de una idea basada en Tecnologías de la Información. (Ministerio TIC, 2019)

ITIL: guía de buenas practica que se utilizan para la gestión de servicios de TI. La guía se ha desarrollado para la infraestructura tecnológica en su totalidad, operaciones y servicios TI que tienen como objetivo final la calidad del servicio. (GlobalSuite Solutions, 2020.)

COBIT: estándar que se compone de herramientas orientadas a garantizar el control y seguimiento de gobernabilidad. Se enfoca en garantizar, organizar y compilar un control de calidad preciso en todo el proceso de información de la empresa. (ISACA, 2024).

NIST: Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés) ayuda a los negocios de todo tamaño a entender mejor sus peligros de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. (NIST, 2024).

ISO 27001: estándar internacional que se enfoca en la gestión de la seguridad de la información en la empresa, mediante un marco de trabajo que se establece como sistema de gestión de seguridad de la información. este marco se basa en los pilares de confidencialidad, integridad y disponibilidad continua de la información y su cumplimiento legal. (GlobalSuite Solutions, 2023.)

ISO 38500: Proporciona un marco de seis principios para que los directores de la empresa puedan tomar decisiones basadas en los resultados que obtengan al dirigir, monitorizar y evaluar el uso de las TI en su organización. Su propósito principal es el de promover el uso efectivo, eficiente y aceptable de las TI en todas las organizaciones para asegurarles a los involucrados que pueden tener la confianza en el Gobierno Corporativo de TI de la organización,

así como proporcionar guías a los directivos para el uso adecuado de las TI. (GlobalSuite Solutions, 2023.)

7.3. MARCO HISTÓRICO

Durante los últimos años el término emprendimiento ha tomado mayor relevancia en el ámbito nacional debido, principalmente, a un mayor acceso a la Información por parte de la sociedad en general y al impulso de programas por parte del Gobierno nacional, por lo cual las personas optan por desarrollar sus ideas de negocio surgiendo así muchas nuevas empresas en diversos ámbitos de la economía en Colombia sobre todo para el sector de las PYME. De acuerdo a esto, se enfocan en las ideas para las cuales se tienen las habilidades, conocimiento, creatividad e ingenio, así como la innovación y necesidad que se presente en el mercado.

De igual forma, desde las Instituciones de Educación Superior, Instituciones Educativas, empresas privadas y entidades Gubernamentales crean estrategias y propician alternativas de espacios que permiten la incubación de ideas innovadoras que, finalmente, se convierten en emprendimientos, y es allí donde las Tecnologías de la Información entran a jugar un papel fundamental pues son el puente para que estas se lleven a cabo, proveyendo las herramientas para su ejecución o para ser el eje central u objetivo fundamental del diseño, desarrollo e implementación de la idea.

Para esto, desde el Ministerio de las Tecnologías de la Información y las Comunicaciones se definió y acuñó el Modelo de **Emprendimiento TI** de **Colombia** el cual tiene como principio la generación de confianza, la capacidad de que como instituciones de apoyo se pueda infundir constantemente la oportunidad de generar ilusión en **emprendedores**, este principio es fundamental para continuar un pensamiento vigente hacia la innovación. En este contexto se puede mencionar la ley 1014 de 2006, aprobada en el congreso de Colombia, ley de fomento a la cultura de emprendimiento, donde su objetivo es promover el espíritu emprendedor en todos los estamentos educativos y de desarrollo productivo para las pymes.

Es así como en la última década, desde la articulación planteada que se incluyó en el plan nacional de desarrollo 2014 -2018 (DPN, 2014), en la cual se resalta la importancia que tiene la integración de los sectores productivos del país (gobierno, academia, empresa y sociedad) para crear sinergia a nivel global, la tecnología de la Información asumió el papel de hilo conductor como agente de asociación y convergencia de muchos proyectos de emprendimiento Pyme con iniciativas basadas en TI.

Por su parte, el plan nacional de ciencia, tecnología e innovación (ETIC, 2013), dejó ver la evolución tecnológica a nivel infraestructural del país para ese momento, dándole mayor importancia a la tecnología para mejorar la productividad, eficiencia y eficacia dentro de los procesos que se llevan a cabo a nivel organizacional

Así mismo, el plan vive digital Colombia 2014 – 2018 (MinTIC, s.f.), se convirtió en otro elemento y estrategia fundamental que recalcó la relevancia que tiene la integración tecnológica, como ayuda para potenciar la sostenibilidad y el desarrollo nacional, por medio de la creación de alianzas que permitían un mayor acceso a las tecnologías de la información desde cualquier sector de la sociedad.

De igual forma, en este sentido desde el 2018 se desarrolló la iniciativa **Incuba TI** del Ministerio de TIC, Colciencias y Creame Incubadora de Empresas que apoya la creación de compañías de base tecnológica especializadas en TI, a través de mentorías a empresarios y emprendedores del sector y el acompañamiento especializado bajo el modelo de incubación.

Esta convocatoria se creó para dirigirse especialmente a emprendedores que cuentan con una iniciativa empresarial relacionada con Tecnologías de la Información (TI); egresados o estudiantes de último semestre de carreras TI de instituciones de educación superior (técnica, tecnología o pregrado) y empresarios de compañías TI legalmente constituidas.

https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/66402:MinTIC-financiara-la-incubacion-de-empresas-de-tecnologias-de-la-informacion

Así mismo, cabe mencionar que en la actualidad existen otras iniciativas como apps.co, iNNpulsa, entre otras, las cuales tienen el mismo objetivo, impulsar propuestas e ideas de negocio que permitan ofrecer soluciones o complementar servicios con enfoque TI para emprendedores de Pymes.

De acuerdo a lo anterior, se puede deducir que en Colombia durante los últimos años se ha producido un notable movimiento de emprendimiento el cual ha contado con un creciente apoyo para emprendedores TI, por parte de diferentes entidades de carácter nacional, para que quienes crean sus empresas buscando tener un amplia divulgación y aprovechamiento de sus servicios puedan contar con asesoría, acompañamiento e impulso.

Sin embargo, una vez creadas estas pymes basadas en TI muchas toman un enfoque equívoco, orientándose solamente en lo económico y descuidan la

importancia de la ciberseguridad en un mundo cada vez más digitalizado e hiperconectado, en el cual uno de los mayores retos es poder hacer frente al crecimiento, preparación, magnitud y repercusión de los ciberataques.

De esta manera, nos encontramos con que los recursos que se destinan a la seguridad cibernética no son suficientes para contrarrestar o estar preparados para mantener seguridad en la información que se respalda o se tiene a cargo, es así como solo el 65% de las pymes destina tan solo entre el 1% y el 5% de su presupuesto total a la ciberseguridad. Sin embargo, esta situación presentó un cambio representativo debido a la pandemia del COVID 19 que se inició en el 2020, teniendo un aumento en la inversión que llegó hasta el 27%.

Por otra parte, cabe resaltar que solo el 18% de los emprendimientos en Colombia recurre a una empresa especializada en seguridad informática, mientras que el 59% utiliza personal propio dentro del área de TI.

7.4. ANTECEDENTES

En la actualidad, las empresas colombianas y especialmente las que hacen parte del conjunto de MiPymes están proceso de crecimiento y estabilización en el mercado colombiano. La pandemia generada por el Covid 19 ha impactado en aspectos positivos y negativos. Dentro de los aspectos positivos se ha reflejado la importancia de integrar al modelo de operación las tecnologías de la información. Sin embargo, como aspecto negativo se ha encontrado que las micro, pequeñas y medianas empresas no tienen este aspecto referenciado desde el momento de la arquitectura y estrategia de su *emprendimiento*, por lo que el nivel de riesgos y vulnerabilidades es más latente y atenta al desarrollo de estas empresas.

Hoy en día las MiPymes enfrentan dificultades en todas las direcciones, su limitado presupuesto hace que el objetivo de su operación de prioridad a que están directamente relacionadas con su misión institucional. Sin embargo, en este proceder descuidan áreas importantes que afectan la eficacia y competitividad en el mercado. Una de las áreas que se ven más afectadas es lo relacionado con la ciberseguridad. (Ramírez, B 2016). El área de ciberseguridad está presente como un valor adicional de acuerdo con los diferentes requerimientos de los clientes, con el fin de obtener confidencialidad e integridad de la información que comparten en sus operaciones comerciales.

Las MiPymes en Colombia han encontrado que el diseño, desarrollo e implementación de estándares buenas prácticas y sistemas de gestión informática, representan un alto costo económico para la organización a la cual no le encuentran un beneficio rentable en su adaptación. En la investigación definida como “Medición de madurez de Ciberseguridad en MiPymes colombianas”, Ramírez Benjamín, expresa el nivel de madurez de la

ciberseguridad al momento de operación de sus objetivos. El estudio monográfico en desarrollo, busca establecer qué importancia tiene la ciberseguridad al momento de estructurar y diseñar la arquitectura y estrategia de negocios en soluciones orientadas a soluciones TI.

7.5. MARCO LEGAL

Ley 590 de nivel nacional: La iniciativa de emprendimiento en soluciones TI enfocadas en MiPymes está regulada inicialmente por la ley 590 de nivel nacional conformada con 6 capítulos y 47 artículos que establecen las disposiciones para promover el desarrollo de las micro, pequeñas y mediana empresa. Se establece:[30]

Capítulo I:

Disposiciones generales

Artículo 1°: Este articulo está estructurado por 10 literales que establecen el promover el desarrollo integral de las MiPymes con base en la generación de empleo, desarrollo regional y la integración en los sectores económicos. De esta manera contribuye con el crecimiento económico de país. Estimula a los emprendedores crear y materializar sus ideas de negocio en mayor cantidad. Adicionalmente promover el acceso a los mercados de bienes y servicios, la formación de talento humano, asistencia para el desarrollo tecnológico y finalmente acceso a los mercados financieros institucionales.

Artículo 2°: Este articulo hace referencia a una serie de modificaciones de la ley 905 de 2004, 1151 de 2007, decreto nacional 957 de 2019 donde establece definiciones para todos los efectos de las micro, pequeñas y medianas empresas en el contexto de actividades empresariales, agropecuarias, industriales, comerciales o de servicio, rural o urbano. Para tal efecto se define:

1. Mediana Empresa:

   a) Fuerza de trabajo de entre 51 a 200 personas actas para laborar.
   b) Activos totales de 5001 a 15000 salarios mínimos mensuales legales vigentes.

2. Pequeña Empresa:

[30]. Función Pública. «Ley 590 de 2000 - Gestor Normativo - Función Pública». Recuperado 10 de mayo de 2022 (https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672).

a) Fuerza de trabajo de entre 11 a 50 personas actas para laborar.
b) Activos totales de 501 a 5001 salarios mínimos mensuales legales vigentes.

3. Microempresa:

a) Fuerza de trabajo no superior a 10 personas actas para laborar.
b) Activos totales por valor mínimo de 501 salarios mínimos mensuales legales vigentes.

Capitulo IV

Desarrollo tecnológico y talento humano

Artículo 17: Modificado por el art. 12, Ley 905 de 2004, Modificado por el art. 73, Ley 1151 de 2007, Subrogado por el art. 44, Ley 1450 de 2011, Modificado por el art. 13, Ley 1753 de 2015. En este articulo se crea el fondo colombiano de modernización y desarrollo tecnológico de las MyPymes y se asigna al ministerio de desarrollo económico que tiene por objetivo la financiación de proyectos, programas y actividades para el desarrollo tecnológico de las MyPymes.

7.5.1. **Ley 2069 del 31 de diciembre de 2020:**
"POR MEDIO DEL CUAL SE IMPULSA EL EMPRENDIMIENTO EN COLOMBIA"

7.5.2. DECRETA:ARTÍCULO 1.
Establece un marco regulatorio que propicie el emprendimiento, crecimiento, consolidación y sostenibilidad de las empresas. Por medio de bienestar social y principio de generar equidad. Lo anterior se rige a la realidad de la realidad socioeconómica de cada región.

7.5.3. Ley 1273 de 2009: "CIBERSEGURIDAD ENTORNO COLOMBIANO"
Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

En esta ley está enfocada a la protección de la información y los datos. En el primer capítulo se enfoca en los pilares de la seguridad

informática: confidencialidad, integridad y disponibilidad de los datos y los sistemas informáticos.

Para el presente trabajo monográfico se basará en el artículo 269A que trata sobre la acción de acceso abusivo a un sistema informático autorización de la empresa.
Articulo 269B donde trata sobre la obstaculizar o impedir el funcionamiento o el acceso normal a un sistema informático, datos informáticos o red de telecomunicaciones.

Articulo 269C donde indica las sanciones a la interceptación de datos informáticos en su origen, destino o el interior de un sistema informático.

Articulo 269D: establece las sanciones para las acciones que destruya, dañe, borre, deteriore, altere o suprima datos informáticos o un sistema de tratamiento de información en sus partes o componentes lógicos.

Articulo 269E: Indica las sanciones sobre la producción, trafico, adquisición, distribución, venta, envío o implementación de software malicioso de efectos dañinos hacia sistemas informáticos.

Articulo 269F: establece las sanciones sobre obtener, compilar, sustraer, ofrecer, venta, intercambio, envío, compra, intercepción, divulgación, modificación de forma indebida datos personales.

Articulo 269G: trata sobre la suplantación de sitios web para capturar datos personales para fines ilegales, así mismo establece las sanciones para quien modifique el sistema de resolución de nombre de dominios e ip de una empresa diferente en la creencia de que se acceda a su banco o a otro sitio personal o de confianza.

8. DESARROLLO DE LOS OBJETIVOS

8.1. RESALTAR EL IMPACTO DE LA CIBERSEGURIDAD EN LOS PROCESOS DE CREACIÓN Y CONSOLIDACIÓN DE PYMES EN COLOMBIA, CON EL FIN DE IDENTIFICAR CÓMO SU INTEGRACIÓN TEMPRANA EN EL DISEÑO DE ARQUITECTURAS TECNOLÓGICAS Y ESTRATEGIAS DE NEGOCIO INFLUYE EN LA VIABILIDAD, SOSTENIBILIDAD Y CRECIMIENTO DE ESTAS ORGANIZACIONES EN ENTORNOS DIGITALES.

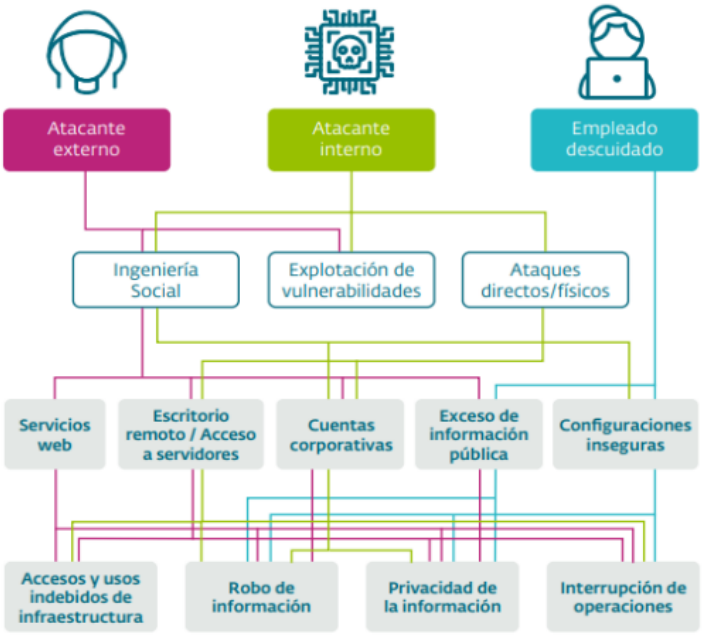
La seguridad de la información pasa a ser un factor relevante que se debe manejar a niveles corporativos y personales, teniendo en cuenta que el nivel de riesgo y vulnerabilidad aumenta cada día desde acciones normales y rutinaria como navegar en la red, abrir un correo electrónico, realizar compras por internet y el uso excesivo de las redes sociales. Esto permite que el porcentaje de ataques y amenazas aumente considerablemente y es debido a que no se toman las medias de ciberseguridad, no se ejecutan guías de buenas prácticas de seguridad informática que tienen por objetivo salvaguardar la integridad y confidencialidad de la información.

Las empresas del sector Pymes en Colombia valoran la ciberseguridad una vez hayan sufrido un ataque o amenaza que ponga en riesgo la seguridad de la información. Los efectos hoy en día son tan críticos que pueden afectar la operación en un 100%, afectación de los activos financieros, puesto que en una infraestructura no segura son fáciles de acceder, ocasionando que se generen pérdidas económicas y de información relevante para la gobernanza corporativa.

Los emprendimientos TI deben considerar el formar y generar conciencia sobre los riesgos que se presentan en el mal uso de los TI, acotar y gestionar la reducción de vulnerabilidades siguiendo buenas prácticas de uso de la información, implementar sistemas y medidas de ciberseguridad que, si bien representa un costo, este será un beneficio para garantizar la integridad, disponibilidad y confidencialidad de la información. A continuación, se

presenta un diagrama desarrollado por el laboratorio de investigación de ESET en el año 2020 y que muestras las acciones o contextos más utilizados para ejecutar ataques informáticos[31]:

Gráfica 2 diagrama de como ocurren los ataques informáticos o cibernéticos:



Fuente: Tomado de laboratorio de investigación ESET (2019)

El emprendimiento en Colombia estaba en una fase de crecimiento exponencial antes de la pandemia, generando empleo y contribuyendo con el crecimiento del producto interno bruto al momento de consolidar y fortalecer su estrategia de negocio orientada en TI. Dentro de este contexto los emprendedores estaban en un proceso de conocimiento y adaptación a la ciberseguridad. Sin embargo, este aspecto no era considerado por algunos emprendedores como necesario y relevante, creando una brecha de seguridad fácilmente vulnerable.

(Gallegos & Valencia, 2023) señalan que los nuevos desarrollos e innovaciones tecnológicas han aumentado la vulnerabilidad de los sistemas, haciendo realidad los ataques informáticos y la ciberseguridad. Las empresas enfrentan una variedad de amenazas, como actores maliciosos, phishing, ataques de malware y ransomware, que son especialmente frecuentes en las pequeñas y medianas empresas debido a la falta de compromiso para implementar medidas de seguridad adecuadas.

[31] Ramírez Mesa, C y González López, J. (2020). Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes. Tecnológico de Antioquia, Institución Universitaria.

Durante el aislamiento obligatorio decretado por el Gobierno Nacional a causa del COVID 19, la actividad maliciosa en internet en Colombia incrementó en más de 150% según reporte de la policía Nacional de nuestro país. Colombia tiene un centro cibernético policial que estudia y realiza seguimiento a este tipo de actividades denunciadas por los diferentes actores que son víctimas de este delito.

No obstante, el 87% de las empresas que han sido afectadas por incidentes digitales no denuncian los ataques, los cuales son realizados por los delincuentes aprovechando que no se tiene presente la ciberseguridad al momento de omitir los programas de prevención, el uso de buenas prácticas y la no integración de una normatividad de seguridad informática en sus sistemas de información.

El diario La República ha publicado en su portal web un artículo denominado: “Ataques cibernéticos ocurren frecuentemente a pequeñas y medianas empresas"[32], donde destaca el crecimiento exponencial de los ciberataques a nivel mundial que superan los 41 billones donde Colombia aporta siete billones de estos ataques. Siendo el ransomware el ataque más común, este actúa secuestrando los datos de la organización y posteriormente pide un rescate en términos económicos. Lo anterior ha generado que empresas dedicadas a la ciberseguridad como FORTINET creen un portafolio accesible para las micro, pequeñas y medianas empresas, esto con el objetivo de implementar la cultura de ciberseguridad y fortalecer la seguridad de la información.

Dado el contexto anterior, Kaspersky un referente de ciberseguridad a nivel global, ha realizado un estudio enfocado a MiPymes titulado: **“El ajuste de las inversiones: cómo alinear los presupuestos de TI con las cambiantes prioridades de seguridad”[33]** en el cual se expone la importancia y crecimiento de la ciberseguridad en las fases de implementación y mejora continua de sus procesos. El estudio muestra que el 70% de las empresas estudiadas, asegura que los dispositivos usados en su emprendimiento tienen software de seguridad instalado y de estos, 96% están protegidos con licencias pagas, cifras que son indicadores de la importancia que las micro, pequeñas y medianas empresas otorgan a la

[32] S.A.S, Editorial La República. s. f. «“Ataques cibernéticos ocurren frecuentemente a pequeñas y medianas empresas"». Diario La República. Recuperado 29 de abril de 2022 (https://www.larepublica.co/empresas/ataques-ciberneticos-ocurren-mas-frecuentemente-a-pequenas-y-medianas-empresas-3228459).

[33] Kaspersky. 2021. «El presupuesto en ciberseguridad aumenta en empresas, pese a los recortes por COVID-19». latam.kaspersky.com. Recuperado 21 de abril de 2022 (https://latam.kaspersky.com/about/press-releases/2021_el-presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-los-recortes-por-covid-19).

ciberseguridad, generando un impacto positivo en cuanto a establecer la ciberseguridad como un requerimiento más al momento de estructurar una idea de negocio orientada a soluciones TI.

Valora Analitik en su artículo: "Día de las MiPymes: ¿cómo avanzan en ciberseguridad?"[34], resalta en el estudio realizado por Kaspersky cómo las micro, pequeñas y medianas empresas han aumentado su presupuesto dedicado a ciberseguridad de 114.000 dólares en el año 2019, tiempo antes de la pandemia a 250.000 dólares en año 2020 durante el tiempo de pandemia. Lo anterior está posiblemente relacionado con el hecho de que el 25% de las empresas consultadas optaron por aumentar el presupuesto de ciber seguridad a causa de ser víctima de incidentes digitales. Lo anterior, genera un impacto positivo en el 22% de las empresas estudiadas, donde expresan que el aumento del presupuesto se da luego de conocer los ataques realizados a diferentes empresas siendo víctimas de brechas de seguridad.

El estudio arroja indicadores sobre la importancia que las micro, pequeñas y medianas empresas le están dando a su infraestructura tecnológica, pues 96% de ellas respondieron que dichos equipos están protegidos con licencias pagas, y solo 4% tienen software gratuito.

Así mismo, el 50% de las empresas indagadas dio a conocer que en sus organizaciones utilizan software diseñado para MiPymes. Quizá el dato más importante es que 70% de las empresas consultadas aseguró que los dispositivos usados en su emprendimiento cuentan con software de seguridad instalado, comprobando el aporte de la ciberseguridad al momento de diseñar la arquitectura de su emprendimiento. Lo anterior, es muy valioso puesto que prepara a los emprendedores para afrontar la era digital y tecnológica con buenas prácticas y responsabilidad digital.

"Afortunadamente, las micro, pequeñas y medianas empresas latinoamericanas están cada vez más conscientes de la importancia de la ciberseguridad y vemos que, a pesar de que muchas compañías han tenido efectos económicos adversos como consecuencia de la pandemia, tienen claro de que la ciberseguridad no es un gasto, sino una inversión", dijo Claudio Martinelli, director general para América Latina en Kaspersky.[35]

---

[34] "Valora. 2021. «Día de las mipymes: ¿cómo avanzan en ciberseguridad?» Valora Analitik. Recuperado 21 de abril de 2022 (https://www.valoraanalitik.com/2021/06/24/dia-de-las-mipymes-como-avanzan-en-ciberseguridad/).

[35] Kaspersky. 2021. «El presupuesto en ciberseguridad aumenta en empresas, pese a los recortes por COVID-19». latam.kaspersky.com. Recuperado 21 de abril de 2022 (https://latam.kaspersky.com/about/press-releases/2021_el-presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-los-recortes-por-covid-19).

En conclusión, la evaluación de las condiciones de ciberseguridad en proyectos TI en el sector PYME en Colombia evidencia una evolución significativa después de la pandemia del COVID-19. Si bien la transformación digital acelerada trajo consigo nuevos riesgos, también permitió un mayor nivel de concienciación y la implementación de mejores prácticas de seguridad. No obstante, para garantizar una protección efectiva y sostenible en el tiempo, es crucial que las PYMEs continúen invirtiendo en estrategias de ciberseguridad y capacitación especializada para mitigar las amenazas digitales en un entorno post-pandemia.

8.2. EXAMINAR LA IMPORTANCIA DE LA CIBERSEGURIDAD AL MOMENTO DE SELECCIONAR UNA IDEA DE NEGOCIO PYMES EN TI.

Las ideas de negocio potencian la reactivación económica de Colombia, donde se tiene registro de que el 95% de las empresas en Colombia corresponden a MiPymes, estas iniciaron como una idea de negocio y posteriormente se consolido mediante el emprendimiento. el portal web CEPYMENEWS ha publicado un artículo denominado: "¿Cómo identificar nuevas oportunidades para emprender un negocio?"[36], en este artículo se plantea una serie de estrategias que son necesarias para tener en cuenta al momento de la selección de una idea de negocio:

1. Identifica clientes que tengan necesidades casi cubiertas.
2. Identifica lo que puede ser mejorado en el mercado.
3. Busca ideas en la frustración de la gente.
4. Piensa en las nuevas tecnologías.
5. Toma en cuenta la aparición o desaparición de leyes.
6. Piensa en como eliminar las barreras tradicionales.
7. Piensa en negocios que funcionen en otros países.

La revolución industrial 4.0 ha creado una puerta para el fortalecimiento de los procesos al interior de una organización, con su enfoque de mejora en el diseño, fabricación y operación de los sistemas productivos a partir de las herramientas y desarrollo tecnológicos donde se incluyen sistemas ciber-físicos, internet de servicios, robótica, internet de las cosas, *big data*, *Cloud*, inteligencia artificial y fabricación aditiva. Este conjunto de herramientas fortalece el proceso productivo y contribuye de forma exponencial con el cumplimiento de los objetivos estratégicos planteados.

En Colombia, el sector empresarial de Pyme está en proceso de análisis y preparación de una hoja de ruta que indique el proceso correcto y seguro de

[36] CepymeNews. 2017. «Identificar oportunidades y emprender un negocio». CepymeNews. Recuperado 29 de abril de 2022 (https://cepymenews.es/identificar-nuevas-oportunidades-para-emprender-negocio/).

implementación de dichas tecnologías y de esta forma romper los esquemas tradicionales y paradigmas que caracterizan este sector. Colombia en los últimos años presenta índices muy bajos en competitividad digital ocupando un puesto de 61 sobre 63 países objeto de estudio de competitividad digital que mide la capacidad y disposición para aprovechar, adoptar y explorar las herramientas TI como un punto clave para el crecimiento económico del país. Además, obtiene un puesto 62 sobre 85 países alrededor del mundo que han sido objetos de estudio de índice de calidad de vida digital, que mide la inclusión de los cinco pilares fundamentales de las herramientas TI: accesibilidad a la red, calidad del internet, infraestructura electrónica y tecnológica, seguridad y gobiernos electrónicos. Lo anterior plasma un panorama crítico para el sector Pyme, puesto que se están omitiendo las bondades, beneficios y fortalezas de la revolución industrial 4.0.

El sector Pyme en Colombia representa en la actualidad el segmento de micro, pequeñas y medianas empresas (MiPymes) más del 95% de las empresas del país, el cual conforma el 65% del empleo y generan más del 35% de la producción nacional. En el artículo de investigación: "Industria 4.0: el reto para las pymes manufactureras de Bogotá, Colombia"[37] realizado por un grupo de investigación en comercio electrónico en Colombia (Giecoecol), muestra el nivel de afectación que sufrió la industria durante la emergencia sanitaria que detuvo el país a causa del virus COVID 19. Se refleja la situación del sector manufacturero como uno de los más afectados durante el suceso sanitario. Este sector lo componen 80.724 empresas registradas en la cámara de comercio de Bogotá donde su promedio de empleados es de 1 a 15 individuos. Sin embargo, el COVID 19 no es el único desafío que presenta este sector, previamente los cambios sociales y tecnológicos hacen que la situación de las pymes sea más complicada, puesto que no se realizan los suficientes esfuerzos en crear estrategias que permitan obtener mejor competitividad en sus respectivos mercados.

Previamente el sector Pyme de la ciudad de Bogotá tenían conocimiento de las herramientas y tecnologías de la información emergentes, pero el conocimiento no se veía reflejado en la acción e implementación de estas. El artículo de investigación determina que la tecnología de mayor apropiación es el *cloud computing* con un porcentaje de 71,8% del sector pyme manufacturero. Adicionalmente el 30,2% del sector requieren implementar estrategias en comercio electrónico y atención al cliente por medio de plataformas y aplicaciones en la web. Claramente se obtiene que las tecnologías de la información asociadas con la industria 4.0 representan un punto positivo hacia el fortalecimiento de las empresas y de esta manera reducir los riesgos económicos que se pueden generar a través de la

[37] Fernández, J. M. L., Barrero, D. L. B., & Rojas, L. A. R. (2022). Industria 4.0: el reto para las pymes manufactureras de Bogotá, Colombia. *Revista Mutis*, *12*(1).

emergencia sanitaria, abriendo la puerta a la posibilidad de implementar herramientas TI en sectores manufactureros que no se tenían contemplados.

El sector pyme manufacturero de la capital de la república, indica que las empresas tienen en mayor proporción utilizan para ofrecer sus productos y servicios son los canales físicos con un 77% de la muestra del estudio, 65% por medio del canal de las redes sociales y 29% por intermedio de aplicaciones y sitios web. Posteriormente 49% las empresas recopilan datos e información por medio de las redes sociales, 35.3% por medios físicos o telefónicos y un alto 29.4% de las empresas de la capital no recopilan datos o información. Este intercambio de información hace que el 85.3% se reúnan de forma presencial, seguido de las reuniones virtuales, el correo electrónico y reportes escritos. Así mismo, el sector pyme utiliza como herramientas de ciberseguridad para prevenir riesgos a el Antivirus en un 60.8%, 24,5% *firewall,* 17.6% filtros web y 36.3% no tienen concebido en sus procesos la aplicación de la ciberseguridad.

Explorando el contexto del desarrollo de software en Colombia, un grupo de especialistas en gestión empresarial liderado por Jessica Piña realiza un análisis denominado: “Análisis prospectivo de la industria de desarrollo de software en Colombia”[38]. Hace énfasis en el crecimiento de la industria de desarrollo de software, siendo esta opción la de mayor crecimiento al momento de emprender y formalizar una idea de negocio, y es que esta industria está relacionada de forma directa con las tecnologías de la información.

En la actualidad hay un numero representativo de empresas dedicadas a la prestación de servicios en la creación, desarrollo, innovación e implementación de sistemas de software que se especializan de acuerdo con la necesidad a satisfacer y el mercado que desean incursionar. La demanda actual ha venido en crecimiento de acuerdo fortalecimiento de la infraestructura relacionada con las TI y cada día los emprendedores ven una oportunidad de concretar sus ideas y estrategias de negocio especialmente en actividades de información y comunicaciones.

Como evidencia de lo anterior, la revista portafolio en su artículo: “Debemos mejorar los índices de rotación de personal en sector TIC”[39], resalta un crecimiento del 19% de la industria de desarrollo de software para el año 2018 lo que se transforma en un movimiento económico de 13.5 billones que son lideradas por emprendimiento y fortalecimiento de las pymes de la industria

[38] Taborda, Jessica Piña, Diana Marcela Castaño Ospina, Leonardo Enrique Hernández Díaz, y Juan David Garro Torres. 2019. «Análisis prospectivo de la industria de desarrollo de software en Colombia». Punto de vista 10(16). doi: 10.15765/pdv.v11i16.1415.

[39] Portafolio. (Mayo de 2019). Obtenido de ‘Debemos mejorar los índices de rotación de personal en sector TIC’: https://www.portafolio.co/economia/empleo/debemos-mejorar-los-indices-de-rotacion-de-personal-en-sector-tic-52999

del software, así mismo este crecimiento se ve reflejado en el producto interno bruto al contribuir con 1.7% sobre este crecimiento. El sector ha crecido un 16.7% durante los últimos 6 años otorgando empleo a 115.000 desarrolladores y analista de software en una plataforma de 7650 empresas de categoría pymes. Este crecimiento está liderado en por los departamentos de Cundinamarca, Antioquia y Valle del Cauca.

Este crecimiento de la industria pyme trae consigo un aspecto negativo, de acuerdo con un informe presentado por Colombia productiva, durante una encuesta realizada a 330 empresas de la industria de calidad de software, el 89.9% no cuentan con un parámetro de calidad que puede otorgar Microsoft, Itil, Oracol, Java, Cisco, etc. Sin embargo, este aspecto se puede controlar y transformar en un evento positivo donde las empresas como estrategia de crecimiento, estabilidad y consolidación en el mercado pueden certificarse y mejorar sus indicadores de cumplimiento de calidad a nivel nacional e internacional.

Ante el fortalecimiento de la industria de software en Colombia, Monster en su artículo: “Amenazas informáticas“[40] expresa que un factor muy importante y de alto impacto que los emprendedores y directivos de Pymes no deben pasar por alto son las vulnerabilidades de software que se crean a partir de los diferentes riesgos de no aplicar procesos de calidad de software y aplicar el uso de las buenas prácticas que ofrece la ciberseguridad, esto implica que el sector presenta falencias y abre la ventana a los ciberdelincuentes para ejecutar ataques y crear amenazas que afectan la integridad y confidencialidad de la información y por ende la sostenibilidad del sector.

En el contexto anterior se evidencia que al establecer las diferentes estrategias o iniciativas de emprendimiento TI no se considera la ciberseguridad como un factor importante. El solo antivirus, firewall o filtros web no es suficiente para detener el accionar de los ciberdelincuentes. Esto hace que la estructura tecnológica de las empresas sea vulnerable y poco solida al momento de actuar frente a peligros en la web, ataques informáticos y emergencias sanitarias que tengan la capacidad de frenar el avance de un país. Colombia entre sus políticas de crecimiento y fortalecimiento empresarial ha direccionado sus esfuerzos hacia el emprendimiento en el sector TIC, estas estrategias son lideradas por el ministerio de las tecnologías de la información y las comunicaciones del gobierno colombiano y de esta forma contribuir con el aumento en productividad y fortalecimiento de la inclusión de las TI que ofrece la era digital.

[40] Monster. (Agosto de 2019). Amenazas Informáticas. Obtenido de https://www.monster.es/orientacion-laboral/articulo/amenazas-informaticas

En una era digital las iniciativas TI transformadas en Pymes están expuestas distintas formas de riesgos digitales, por lo que se hace necesario y muy eficiente el incentivar a los individuos de una organización la cultura de la ciberseguridad. A medida que la era tecnológica avanza los diversos métodos de ciberdelincuencia se están especializando, tanto que los hackers han tomado este contexto para generar rentabilidad económica, a través de la búsqueda y aprovechamiento de vulnerabilidades empresariales.

Tigo Panamá en un artículo denominado “Pymes ¿necesitan herramientas de ciberseguridad?” hace una observación muy asertiva para el interrógate del objetivo estudiado: “frecuentemente, el trabajador siente que los pasos de confirmación y verificación son tediosos y retrasan. Lo cierto, es que dicha imagen negativa se debería a la desinformación. Además, se da una vez que el capacitador no consigue comunicar bien las causas para protegerse de la red. O sea, no transmiten la urgencia del valor del asunto. “[41]. Lo anterior obedece a una falta de cultura de ciberseguridad donde las consecuencias se reflejan al momento de sufrir ciberataques y ver comprometida su infraestructura tecnológica y su sistema de información. Es allí donde los empresarios MiPymes empiezan a considerar el aspecto de ciberseguridad para proteger, potenciar y consolidar su estrategia de negocio.

La dinámica del cibercrimen que se refleja en Colombia durante los últimos años indica que hay un crecimiento gradual en el número de incidentes cibernéticos reportados a las autoridades competentes al contexto de ciberseguridad. Durante un informe realizado por el equipo de investigación de la Policía Nacional denominado “INFORME DE LAS TENDENCIAS DEL CIBERCRIMEN EN COLOMBIA (2019-2020)”, refleja que a través de los canales de atención dispuestos por la policía nacional se registraron 28.827 casos de incidentes relacionados con cibercrimen durante el año 2019, donde 15.948 fueron denunciados como infracciones a la ley 1273 de 2009, siendo un equivalente al 57% de los casos denunciados.

El informe expone que los delitos e incidentes informáticos que afectan a los empresarios colombianos y personas del entorno familiar son los casos de Phishing con un 42%m suplantación de identidad con un 28%, el envió de malware con un 14% y los fraudes en medios de pago en línea con 16%. Lo anterior indica que hay una gran brecha digital que los ciberdelincuentes están aprovechando para fortalecer sus actividades ilegales y maliciosas, donde las principales víctimas son empresarios de micro, pequeña y mediana empresa donde el concepto y cultura de ciberseguridad es pasado por alto. Indicando que los emprendedores al momento de plantear su iniciativa de negocio y

[41] Panama, Tigo. 2021. «Pymes ¿necesitan herramientas de ciberseguridad?» Blog Tigo Panamá. Recuperado 9 de mayo de 2022 (https://blog.tigo.com.pa/tigo-business/pymes-necesitan-herramientas-de-ciberseguridad/).

plasmar su estrategia comercial o de operación pasan por alto el concepto de ciberseguridad.

Según el Análisis del Nivel de Madurez de Ciberseguridad en Colombia, que se basa en datos oficiales, el país experimentó 28.000 millones de ciberataques en 2023. Sin embargo, a junio de 2024, ya se registraron 20.000 millones de ataques, lo que indica una aceleración alarmante en la actividad cibernética maliciosa. [42]A pesar del aumento preocupante en los ataques, las empresas colombianas respondieron con un notable incremento en la inversión en ciberseguridad. De 2023 a 2024, el 85% de las empresas aumentaron sus presupuestos destinados a proteger sus sistemas. Además, se prevé que para 2025 la inversión en ciberseguridad en Colombia crecerá un 19%, lo que posiciona al país entre los cinco primeros en el ámbito de la inversión en seguridad en la región.

La mediana, pequeña y microempresa han sido víctima de ataques y amenazas cibernéticas en los últimos años, en el estudio de la policía nacional indica que hay un nivel de vulnerabilidad mediante las comunicaciones establecidas entre clientes y proveedores. Dado lo anterior la ciberseguridad requiere ser implementada a tal nivel que los emprendedores, alta dirección de pymes ya constituidas permita identificar y plantear los riesgos como parte de la gestión corporativa y administrativa.

En la actualidad se han realizado esfuerzos de educación e incentivación por el adoptar la cultura de ciberseguridad por medio de los estándares que dan una serie de conceptos, recomendaciones, estrategias y buenas prácticas que brindan herramientas y conceptos para que el emprendimiento se haga en el margen de la ciberseguridad. Lastimosamente estas acciones se están llevando a cabo después de haber sucedido los casos, cuando ya ha tenido un efecto negativo que se refleja en daños y perjuicios a nivel económico y actitudinal.

En este aspecto entra a jugar un papel importante la cultura organizacional que hace referencia a un conjunto de hábitos, valores, costumbres y destrezas que adquiere un grupo de personal que hacen parte de una pyme. En este punto se hace fuerte la estrategia de implementar y desarrollar la cultura basada en los estándares de la seguridad de la información y ciberseguridad, para ello los emprendedores y directivos de Pymes deben iniciar el proceso de diseñar, desarrollar e implementar las diferentes medidas necesarias para

[42] Fernández, P. J. E. (2024, agosto 22). *Finanzas de los colombianos podrían tener problemas por ciberataques: Empresas tuvieron que tomar millonaria decisión*. infobae. https://www.infobae.com/colombia/2024/08/22/finanzas-de-los-colombianos-podrian-tener-problemas-por-ciberataques-empresas-tuvieron-que-tomar-millonaria-decision/

adaptar la ciberseguridad y hacer frente a los riesgos y amenazas que se encuentran a diario en el contexto de las TI.

Es importante que los empresarios tomen conciencia y empiecen a invertir y tener presente desde el primero momento la adición de cultura de ciberseguridad y conceptos de seguridad informática para fortalecer sus procesos operacionales y administrativos. Así mismo, el sector pyme y los emprendedores que están fortaleciendo el crecimiento de las TI en Colombia deben integrar el componente de seguridad informática y ciberseguridad, adicionarlo como factor diferencial al promover y garantizar políticas de seguridad de la información, aplicación de buenas prácticas en ciberseguridad de tal forma que permita satisfacer necesidades en productos, bienes y servicios en los diferentes sectores que las TI pueda fortalecer.

8.3. EVALUAR LAS CONDICIONES DE CIBERSEGURIDAD DE PROYECTOS TI EN EL SECTOR PYME EN COLOMBIA, ANTES Y DESPUÉS DE LA EMERGENCIA SANITARIA GENERADA POR LA PANDEMIA

Como se ha expuesto ampliamente a lo largo del desarrollo del presente proyecto, las condiciones de ciberseguridad de proyectos TI en el sector PYME en Colombia cambió drásticamente, por así decirlo, con la llegada de la pandemia a nuestro país, pues revolucionó la forma en la que se venían realizando los procesos al interior de éstas y requirió que dichas acciones se mudaran casi en su totalidad a la virtualidad, permitiendo así que se expusieran a distintos riesgos comprendidos por ataques cibernéticos. Es por esto que se hace necesario tener una visión más amplia de cómo se entendía y aplicaba la ciberseguridad antes y cómo este término resulto teniendo mayor relevancia en las pymes de nuestro país después de la emergencia sanitaria generada por la pandemia.

La ciberseguridad en el sector de las pequeñas y medianas empresas (PYME) en Colombia ha sido históricamente un desafío debido a la limitada inversión en infraestructura tecnológica y la falta de capacitación en seguridad informática (MINTIC, 2019). Antes de la pandemia del COVID-19, muchas PYMEs carecían de estrategias robustas de ciberseguridad, lo que las hacía vulnerables a ataques como el phishing, el ransomware y las violaciones de datos. Con la llegada de la pandemia por Covid-19 se aceleró el proceso de la transformación digital para Pymes, lo cual les ayudó a mantener la disponibilidad y operación de sus servicios, pero incrementó su riesgo cibernético, convirtiéndose en un blanco perfecto para los ciberdelincuentes.

Sin embargo, la emergencia sanitaria aceleró la transformación digital, obligando a las PYMEs a adoptar soluciones tecnológicas a gran velocidad. El

teletrabajo, el comercio electrónico y el uso masivo de servicios en la nube incrementaron significativamente la superficie de ataque para los ciberdelincuentes (Cepal, 2021). Según el Centro Cibernético Policial de Colombia (2022), los incidentes de seguridad aumentaron en un 40% durante la pandemia, afectando principalmente a empresas sin planes de contingencia. A partir de ese momento la ciberseguridad se empezó a entender como un elemento indispensable y prioritario, que podía ayudarles a asegurar su permanencia en el mercado y así mismo les brindaba mayores herramientas para ofrecerles a sus clientes.

De acuerdo con un informe revelado por la revista Latinpyme “En el 2020 en Colombia, el 76% de las organizaciones consultadas por la firma multinacional Sophos, especializada en seguridad cibernética en más de 150 países, confirmaron haber tenido y padecido al menos un incidente en la nube pública poniendo en riesgo la seguridad de su información corporativa. De 2017 a 2020 según el estudio de Tendencias del Cibercrimen en Colombia, liderado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) del Tanque de Análisis y creatividad de las TIC (TicTac), se reportaron 52.901 denuncias de las cuales el mayor número de hurtos se realizaron a través de medios informáticos (31.058), seguido por robo de identidad (8.037), donde Bogotá fue la ciudad con más incidentes reportados (5.308), seguida de Cali (1.190) y Medellín (1.186). Otro dato importante para resaltar es que, durante la temporada de aislamiento obligatorio la actividad maliciosa en internet se incrementó en más de 150%, según informe de la Policía Nacional donde el objetivo de casi todos los ataques siempre fue el mismo: robo de dinero o información que vale dinero.

Continuando con datos y estadísticas de la Policía Nacional en el 2020 cerca del 45% de los ataques fueron a Pymes, es por esto por lo que la seguridad en la nube es un reto importante”.

Según la Cámara Colombiana de Informática y telecomunicaciones “para el cierre del primer trimestre de 2020, el mercado mundial de ciberseguridad creció un 9,7%, cifra que en gran parte se dio por la COVID-19. La inversión total alcanzó los 10.400 millones de dólares. En Colombia la demanda de los servicios de ciberseguridad tuvo un incrementó de 40%”. Todo lo anterior porque según esta misma organización se indicaba que el 60% de las Pymes en Proyectos TI en Colombia para esa fecha no podían sostener sus negocios luego de sufrir un ataque cibernético.

De acuerdo con lo anterior, ya desde hace dos años el concepto de ciberseguridad cobró más relevancia para las Pymes en el desarrollo de su negocio, debido a la gran cantidad de datos que se comparten por medio de las diferentes redes. Por ello, esto se convirtió en un gran reto para las mismas,

porque debían asegurarse de proteger los datos tanto propios, así como de quienes forman parte de éstas ya sean clientes, proveedores o demás miembros de su cadena de valor, partiendo de la base que la información confidencial es el activo más importante con que cuentan y su pérdida significaría un altísimo costo tanto económico como en su reputación. No obstante, aunque la cifra creció notablemente, se ha determinado que es necesario seguir trabajando para generar conciencia y darle mayor importancia al riesgo que se corre al no tener protegida la información que para las empresas es indispensable, ya que para el 2021 el 19% de las empresas en Colombia, de las cuales en su mayoría corresponden a Pymes, se vieron afectadas por al menos un ciberataque de acuerdo con el informe The State of Ransomware 2021 presentados por Sophos.

Para el presente año, las cifras que se reportaron en materia de ciberseguridad al cierre del primer semestre de este 2022, demostraron que “algunas tipologías del cibercrimen han evidenciado una reducción significativa como la Violación de Datos Personales, la Suplantación de Sitios Web para Capturar Datos Personales y el Uso de Software Malicioso que presentaron variaciones del -11%, -13% y -27% respectivamente. Así mismo hay otro tipo de vectores que siguen creciendo, como el acceso abusivo a sistema informático que presentó 6.407 casos, es decir 46% más que en el mismo periodo del año anterior, ubicándolo como el delito con mayor crecimiento, y el hurto por medios informáticos que presentó un incremento del 15% con 11.078 casos denunciados” de acuerdo con la Cámara Colombiana de Informática y Telecomunicaciones

En este sentido se podría mencionar que los cambios más significativos para las Pymes en Colombia en proyectos TI, que tienen que ver con adopción de tecnologías en ciberseguridad, tuvieron que ver con la adquisición de software para video llamadas y colaboración remota (68%) y por otra parte con un 61%, destaca la compra de equipos de cómputo portátil. Por último, pero no menos importante, se encuentra el almacenamiento en la nube, una modalidad de protección en ciberseguridad adoptada por el 54% de las Pymes. Para tal fin es importante destacar que 7 de cada 10 pymes colombianas está capacitando a sus empleados en nuevas tecnologías frente a los ciberataques, ya que en un total del 58% de las pymes se muestran más preocupadas por la ciberseguridad en el nuevo entorno digital.

Así mismo, cabe destacar que gracias a esto diferentes empresas líderes en ciberseguridad a nivel mundial, han incursionado en el mercado de Colombia en época post pandemia, con el fin de ofrecer su portafolio de soluciones contra ciber amenazas, debido a que nuestro país ha demostrado un mercado en constante crecimiento, con un desarrollo empresarial fuerte y con madurez tecnológica, lo cual se dio a conocer según la firma PricewaterhouseCoopers,

la cual realizó una encuesta en la que se evidencio que el 69% de las organizaciones en el país aumentarán sus inversiones en el sector ciberseguridad.

El Gobierno colombiano ha venido desarrollando estrategias que han resultado acertadas en establecer lineamientos que permitan un mayor fortalecimiento de la seguridad digital en Colombia con un enfoque especial en las Pymes. A pesar del aumento en las amenazas, la crisis también incentivó mejoras en la ciberseguridad. Organismos como ColCERT y MINTIC impulsaron programas de concienciación y formación, mientras que algunas empresas adoptaron mejores prácticas, como la autenticación multifactor y la encriptación de datos (MinTIC, 2021). No obstante, las brechas persisten debido a factores como la falta de presupuesto y la resistencia al cambio organizacional (Deloitte, 2022).

Otra de las razones por las que estas empresas han fijado su atención en el segmento de seguridad cibernética colombiano es que, si bien se piensa que las ciber amenazas solo atacan a las grandes empresas o al gobierno, los pequeños negocios también corren riesgo de verse afectadas con el aumento de la digitalización, lo que puede representar un riesgo para las cuentas de las Pymes y los equipos TI.

Lo anterior claramente denota que para el sector de las Pymes en proyectos TI en Colombia se hace necesario que se sigan adoptando mecanismos que faciliten la sensibilización de los usuarios a través de ciber academia, socialización de los riesgos y la participación de todos los niveles de las organizaciones, por pequeñas que estas sean, en los procesos de formación y capacitación en materia de ciberseguridad empresarial que este dirigida sobre todo a estas Pymes. Para ello, se requiere que se integren soluciones seguras, auditadas y en conformidad con las normas que ayuden a proteger la privacidad sin comprometer la seguridad, así como poner en práctica estrategia de defensa en profundidad de seguridad cibernética, para no solo enfrentar si no anticipar las amenazas por lo tanto, su implementación debe ser pensada estratégicamente junto con una colaboración a gran escala, responsabilidad, apertura, accesibilidad y, sobre todo, confianza entre todas las partes involucradas: proveedores, integradores de sistemas, consultores, departamentos de TI y especialistas en ciberseguridad.

En conclusión, si bien la pandemia exacerbó los riesgos de ciberseguridad en las PYMEs colombianas, también promovió una mayor conciencia sobre la importancia de proteger la información. Sin embargo, para consolidar estas mejoras a largo plazo, es fundamental que las PYMEs sigan invirtiendo en seguridad digital, capacitaciones y cumplimiento normativo.

8.4. COMPILAR LAS CARACTERÍSTICAS DE CIBERSEGURIDAD QUE MOLDEAN LOS PROYECTOS PYMES ENFOCADOS EN TI.

En un mundo digital en constante evolución, la ciberseguridad se ha convertido en un pilar fundamental para las pequeñas y medianas empresas (PYMEs) que desarrollan proyectos enfocados en tecnologías de la información (TI). A medida que estas organizaciones adoptan soluciones digitales para optimizar sus operaciones, también se exponen a crecientes amenazas cibernéticas, lo que hace indispensable la implementación de estrategias de protección robustas.

Con el fin de apoyar a las pequeñas y medianas empresas en la identificación de vulnerabilidades y amenazas que se presentan en el medio tecnológico, las diferentes entidades enfocadas en ciberseguridad han definido ciertas características que las Pymes deben considerar para aplicar a su infraestructura tecnológica:

- **Sistema de Gestión de la Seguridad Informática (SGSI):**
  Permite que las pymes puedan implementar de manera organizada y eficiente los objetivos que dan origen a las iniciativas en seguridad de la información. Esta implementación permite que las empresas realicen una apropiada gestión de la seguridad informática.

  El sistema esta definido por la normal internacional ISO/IEC 27001:2022, estructura basada en el ciclo PHVA (Planificar, hacer, verificar y actuar) (Johnson, 2002). Esta norma es certificable por una entidad externa que valida que la organización haya establecido un SGSI conforme a los requerimientos de esta. Esta norma estandariza la seguridad de la información con base en los objetivos estratégicos de la organización con base en la seguridad de la información.

- **Gestión de riesgos:** Se conoce como riesgo a nivel de Ciberseguridad como la posibilidad de sufrir pérdida o daño (Richard a Caralli, Allen, Curtis, White, & Young, 2010). También se define como la probabilidad de que una amenaza explote una vulnerabilidad (International Organization for Standardization, 2008b). La gestión de riesgos tiene como objetivo identificar, analizar y mitigar los riesgos que puedan afectar a los activos de información de la empresa (Richard a Caralli et al., 2010).
  La gestión de riesgos es quizás uno de los temas más complejos al momento de aplicar los conceptos de ciber seguridad, ya sea por la baja inversión, falta de personal especializado en el tema y la falsa sensación de seguridad. Por lo que han surgido metodologías de apoyo que hacen posible el realizar una gestión acertada, adecuada y eficiente, donde las empresas de a poco han integrado en su arquitectura tecnológica:

- IASME: IASME (Information Assurance for Small and Medium Sized Enterprises), es un estándar que ha sido creado por el IASME Consortium. Creado para que las Pymes se apoyaran en sus iniciativas de seguridad de la información a través de la gestión de riesgos. Para ello el IASME ha creado factores de seguridad del negocio el cual cada uno tiene un objetivo, como se observa en la siguiente tabla:

Tabla 1 Factores de Seguridad del Negocio – IASME Standard v.

Factor	Descripción
Organización	Gestionar los recursos de información dentro de la organización y las relaciones de la organización con aliados.
Riesgo	Entender y gestionar el riesgo al que está expuesta la información del negocio
Políticas y cumplimiento	Establecer los requerimientos regulatorios y legales, dirección de la gerencia y las comunicaciones. Conocer qué se requiere y monitorear su cumplimiento.
Activos	Conocer el valor de los activos de información. Adquirir y disponer de manera segura dichos activos.
Planeación	Construir seguridad y privacidad desde el inicio, asegurándose que se tienen los sistemas de información adecuados.
Acceso	Controlar quiénes y a qué pueden acceder de la información del negocio
Personas	Conocer a los empleados y educarlos en seguridad del negocio.
Física y ambiental	Proteger los activos de información de daños físicos y ambientales.
Disrupción	Defender la información de la empresa de ataques hostiles y preparar a la empresa para recuperarse de los efectos de dichos ataques.
Operaciones	Gestionar y monitorear los sistemas de información efectivamente.
Gestión de incidentes	Asegurar que las violaciones de confidencialidad, integridad y disponibilidad de los sistemas de la empresa sean detectados y gestionados, aprendiendo las lecciones en cada caso.
Continuidad	Asegurarse de que la empresa puede recuperarse rápidamente de la pérdida total o parcial de activos clave de información

Fuente: Ramírez Montealegre, B. (2016). *Medición de madurez de ciberseguridad en pymes colombianas.*

Las pymes por medio de esta implementación tienen la capacidad de dar manejo al riesgo y mitigar sus efectos negativos sobre la arquitectura tecnológica y afectar la continuidad del negocio.

- **ISSA-UK 5173:** Estándar creado por la ISSA (Asociación de Seguridad en Sistemas de Información), tiene por objetivo establecer lineamientos de apoyo para que las pymes puedan implementar controles con el fin de lograr el aseguramiento de la información de la empresa a través de los pilares de la seguridad informática (Information Systems Security Association, 2011).

  ISSA-UK 5173 resalta que el dato más relevante desde la perspectiva de seguridad es la cantidad de empleados que hacen parte de la organización (micro, pequeña o mediana empresa). En la siguiente tabla se agrupan los controles de la siguiente manera:

Tabla 2 controles del ISSA-UK 5173

Medidas básicas de seguridad:	Se compone de 4 grupos de controles: • Compromiso del Propietario o Gerente • Entendimiento de las obligaciones Entendimiento de los riesgos de seguridad • Contramedidas esenciales de seguridad
Régimen de seguridad definido	Se compone de los siguientes grupos de controles: • Reglas de seguridad • Responsabilidades de seguridad • Plan de supervivencia a desastres • Vigilancia en seguridad Tiene por objetivo asegurar la efectividad de las medidas de seguridad adoptadas.
Sistema de seguridad gestionado	Se compone de los siguientes grupos de controles: • Políticas y procedimientos • Sistema de gestión • Tecnologías de seguridad

	• Educación en seguridad Tiene por objetivo realizar mediciones de seguimiento y monitoreo y gestión efectivas de las medidas adoptadas.

Fuente: Ramírez Montealegre, B. (2016). *Medición de madurez de ciberseguridad en pymes colombianas.*

Una de las características más relevantes de la ciberseguridad en PYMEs es la seguridad de los puntos de conexión (endpoints), la cual protege los dispositivos que acceden a la red empresarial. De acuerdo con Deloitte (2020), el cifrado de datos y el monitoreo de dispositivos externos son esenciales para prevenir accesos no autorizados y ataques de malware. Además, es crucial contar con un plan de recuperación ante desastres y continuidad del negocio, el cual permite reducir el impacto de incidentes de seguridad. Transparent Edge (2023) destaca que la capacidad de respuesta rápida puede marcar la diferencia entre una interrupción menor y una crisis operativa prolongada.

Otro aspecto clave es la educación y concienciación del personal, ya que los errores humanos siguen siendo una de las principales causas de ciberataques exitosos. Según Euncet Business School (2023), la formación en identificación de correos electrónicos fraudulentos y la adopción de políticas de uso seguro de contraseñas son estrategias eficaces para mitigar riesgos.

Asimismo, la evaluación y gestión de riesgos es fundamental para anticipar y prevenir posibles vulnerabilidades en la infraestructura de TI. Un informe de Transparent Edge (2023) sugiere que las auditorías de seguridad periódicas pueden reducir significativamente la exposición de las PYMEs a ataques informáticos. En este sentido, la implementación de herramientas de seguridad, como firewalls, software antivirus y sistemas de detección de amenazas, refuerza la protección digital. De acuerdo con Nedigital (2023), invertir en estas soluciones es una estrategia rentable para minimizar incidentes de seguridad.

Otra característica esencial es el control de accesos y gestión de contraseñas, que restringe el acceso a información sensible. Deloitte (2020) recomienda adoptar autenticación multifactor y políticas de acceso basadas en roles para mejorar la seguridad. Finalmente, la actualización y mantenimiento de sistemas garantiza que las PYMEs no sean vulnerables a ataques basados en exploits de software obsoleto, mientras que el cumplimiento de normativas y estándares (como ISO/IEC 27000 o

el RGPD) asegura una mejor gestión de la seguridad y la protección de datos.

La ciberseguridad es esencial para las pequeñas y medianas empresas (PYMEs) en Colombia que desarrollan proyectos enfocados en tecnologías de la información (TI). Implementar medidas adecuadas protege los sistemas, redes y datos de amenazas digitales, asegurando la continuidad del negocio y la confianza de los clientes. A continuación, se detallan las características clave de ciberseguridad que deben considerarse:

- **Protección de Datos Sensibles:** Asegurar que solo personal autorizado tenga acceso a información crítica es fundamental para prevenir usos indebidos. Esto incluye realizar copias de seguridad periódicas, controlar y verificar los accesos y cumplir con las regulaciones de protección de datos personales. [43]
- **Implementación de Software de Seguridad:** Contar con soluciones robustas de antivirus, firewalls y sistemas de detección de intrusos actualizados es esencial. El software desactualizado puede dejar vulnerabilidades abiertas que los atacantes pueden explotar fácilmente. [44]
- **Planificación de Recuperación ante Desastres y Continuidad del Negocio:** Desarrollar planes de respuesta permite a las PYMEs reaccionar eficazmente ante incidentes de seguridad, minimizando interrupciones operativas y pérdidas de datos. La ciberseguridad no solo salvaguarda datos confidenciales y activos digitales, sino que también asegura la continuidad operativa de infraestructuras críticas y el cumplimiento normativo. [45]

En conclusión, la ciberseguridad no es un lujo, sino una necesidad para las PYMEs que desean proteger su infraestructura tecnológica y garantizar la continuidad de sus proyectos de TI. La implementación de estas características no solo mitiga riesgos, sino que también fortalece la confianza del cliente y la resiliencia operativa de la empresa en un entorno digital cada vez más hostil.

---

[43] Ciberseguridad para Pymes: Cómo proteger su empresa. (2025, abril 2). *Impacto TIC*. https://impactotic.co/ciber-seguridad/ciberseguridad-para-pymes-de-colombia/

[44] Ciberseguridad para PyMEs: Protege tu Empresa de Amenazas Digitales. (2025). Gestión de Compras Empresariales S.A.S. Recuperado 21 de abril de 2025, de https://lasus.com.co/es/content/ciberseguridad-para-pymes-protege-tu-empresa-de-amenazas-digitales

[45] ¿Qué es la ciberseguridad? Objetivos e importancia. (s. f.). Recuperado 21 de abril de 2025, de https://colombia.unir.net/actualidad-unir/que-es-ciberseguridad

9. CONCLUSIONES

Se comprende la importancia que ha tomado la ciberseguridad en las MiPymes en Colombia, precisando que esta ha sido tenida en cuenta en la estructura y arquitectura de emprendimientos enfocado s en soluciones TI a raíz de casos presentados de ataques cibernéticos. Esto demuestra que los emprendedores están tomando la cultura de la ciberseguridad y la aplican para sus diferentes estrategias empresariales. El impacto obtenido es positivo puesto que prepara de forma eficientes a los emprendedores y disminuye los riesgos y vulnerabilidades.

En Colombia las empresas que hacen parte del sector Pyme no tienen el conocimiento, la destreza y la visión de aplicar los conceptos, fundamentos y herramientas que facilitan las TI para fortalecer la seguridad informática de sus procesos, información e infraestructura tecnológica. Es por ello que se hace supremamente importante el establecer estrategias y aprender de los beneficios que otorga la ciberseguridad para la estabilidad de su operación y poder afrontar de forma asertiva los retos que propone un cambio social, una emergencia sanitaria o un ataque sistemático a escala a los sistemas de información del sector MiPymes.

Una empresa por pequeña que esta sea, también está en riesgo frente a la posibilidad de recibir un ataque cibernético y, por ende, es fundamental que también se le dé importancia a este campo desde el momento en el que se empieza a estructurar, así se fortalecerá desde el principio y evitará consecuencias que puedan afectar su estabilidad económica o su reputación.

Aún queda mucho por aprender sobre ciberseguridad en Colombia y especialmente para las Pymes enfocadas en proyectos de TI, pero se va por buen camino, ya que el despertar ha sido grande el cual se dio principalmente a raíz de la virtualidad como estrategia ante la pandemia por el Covid 19, por lo tanto, los avances hasta el momento han sido sobresalientes y el tema de seguridad informática, hoy más que nunca, ya hace parte de la agenda de muchas organizaciones nacionales.

10. RECOMENDACIONES

Se recomienda a los emprendedores de Colombia y lideres de sectores MiPymes contribuir con la ciberseguridad a través de políticas de ciberseguridad y aprendizaje de forma engranada. Que la ciberseguridad sea adquirida por habito y no por consecuencia de un ataque. Que la ciberseguridad sea el momento preciso para fortalecer sus objetivos estratégicos.

Es importante que el gobierno nacional establezca como una política nacional el uso, sostenimiento y mejora continua de estrategias que fortalezcan la seguridad informática por medio de la Ciber seguridad y sus muchas aplicaciones que fortalecen los procesos operativos y administrativos de las pymes.

Se deben seguir adoptando mecanismos que faciliten la sensibilización y participación en todos los niveles dentro de una organización a través de la ciber academia, así mismo, tener la familiarización con los ataques y socialización de los riesgos, la cual permita crear estrategias que anticipen cualquier anomalía en cuestión de seguridad informática.

Las Pymes deben realizar un constante monitoreo de los sistemas de seguridad informática que poseen y efectuar pruebas de efectividad, puesto que los criminales informáticos siempre están diseñando nuevas formas para un ciberataque, por lo cual no existe la efectividad del 100%. Sin embargo, con una revisión constante se pueden detectar fallas críticas que comprometan la integridad de la empresa.

11. BIBLIOGRAFÍA

ACUMEN IT TRAINING, INC. ITIL® 4 and Cybersecurity: Strengthening IT Service Management Against Threats [en línea]. 2025. Disponible en: https://acumenph.com/itil-and-cybersecurity-strengthening

APLICACIONES INFORMÁTICAS. [en línea]. s. f. Recuperado el 13 de enero de 2025, de https://www.ciset.es/glosario/484-

AVANCE JURÍDICO. Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009] [en línea]. 2022. Recuperado el 21 de abril de 2022, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

ANIF. Retos y oportunidades de las Pymes [en línea]. s. f. Disponible en: https://www.anif.com.co/comentarios-economicos-del-dia/retos-y-oportunidades-de-las-pymes/

BANCOLDEX. ¿Qué es una pyme? [en línea]. 2018, julio 30. Disponible en: https://www.bancoldex.com/es/que-es-una-pyme-1338

BANCÓLDEX. Clasificación de empresas en Colombia [en línea]. 2021, julio 29. Disponible en: https://www.bancoldex.com/es/sobre-bancoldex/quienes-somos/clasificacion-de-empresas-en-colombia

BLOG TIGO PANAMÁ. Pymes: ¿necesitan herramientas de ciberseguridad? [en línea]. 2021. Recuperado el 10 de mayo de 2022, de https://blog.tigo.com.pa/tigo-business/pymes-necesitan-herramientas-de-ciberseguridad/

BULA PÁEZ, A. M.; BAUTISTA GARCÍA, F.; MESA GUZMÁN, L.; ROBLEDO, C.; CRUZ GIRALDO, P. Ciberseguridad en la era de la movilidad digital [en línea]. 2022. Recuperado de: https://www.ccit.org.co/wp-content/uploads/ciberseguridad-en-la-era-de-la-movilidad-digital-version-digital.pdf

CARALLI, R. A.; ALLEN, J. H.; CURTIS, P. D.; WHITE, D. W.; YOUNG, L. R. CERT® Resilience Management Model. Management, 1988(May), 259. 2010.

CARALLI, R.; STEVENS, J.; YOUNG, L.; WILSON, W. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. 2007.

CCIT - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. SAFEPymes [en línea]. 2021. Recuperado el 15 de mayo de 2022, de https://www.ccit.org.co/safepymes/

CCIT - CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del cibercrimen 2021 - 2022: Nuevas amenazas al comercio electrónico [en línea]. 2021. Recuperado el 10 de mayo de 2022, de https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-2021-2022-nuevas-amenazas-al-comercio-electronico/

CEPAL - COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE. Transformación digital en América Latina y el Caribe [en línea]. 2021. Recuperado el 21 de abril de 2025, de https://www.cepal.org/es/publicaciones

CENTRO CIBERNÉTICO POLICIAL. Informe sobre ciberseguridad en Colombia 2020-2022 [en línea]. 2022. Recuperado el 21 de abril de 2025, de https://caivirtual.policia.gov.co/observatorio/analisis-cibercrimen

CIBERPRISMA. Gobierno de las TIC: COBIT [en línea]. 2024. Disponible en: https://ciberprisma.org/2024/09/30/gobierno-de-las-tic-cobit

CIUDADANÍA | INCIBE. Conceptos básicos de ciberseguridad que debes conocer [en línea]. s. f. Recuperado el 13 de enero de 2025, de https://www.incibe.es/ciudadania/blog/conceptos-basicos-de-ciberseguridad-que-debes-conocer

COBIT 5 FRAMEWORK PUBLICATIONS | ISACA. [en línea]. s. f. Recuperado el 13 de enero de 2025, de https://www.isaca.org/resources/cobit/cobit-5

CONSULTORÍA, D. DE. ¿Qué es ITIL y para qué sirve? [en línea]. 2020, noviembre 12. GlobalSuite Solutions. Disponible en: https://www.globalsuitesolutions.com/es/que-es-itil-y-para-que-sirve/

DELOITTE. Tendencias en ciberseguridad para América Latina [en línea]. 2022. Risk Advisory. Recuperado el 21 de abril de 2025, de https://www2.deloitte.com/co/es/pages/risk/articles/ciber-riesgos-y-seguridad-de-la-info-en-america-latina-y-caribe.html

DELGADO, A. M. Lineamientos, tendencias y estrategias sobre ciberseguridad y ciberdefensa en Colombia [en línea]. 2020. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2868/Trabajo%20de%20grado1904.pdf?sequence=1&isAllowed=y

EASYVISTA. Integrating ITIL and Cybersecurity Frameworks to Improve Security Governance [en línea]. 2025. Disponible en: https://www.easyvista.com/blog/integrating-itil-and-cybersecurity-frameworks-to-improve-security-governance

ELNOTARIADO.COM. Ciberseguridad empresarial. Primeras aproximaciones prácticas [en línea]. 2022. Recuperado el 10 de mayo de 2022, de http://www.elnotariado.com/ciberseguridad-empresarial-primeras-aproximaciones-practicas-5594.html

FORBES COLOMBIA. Cinco estrategias para promover la ciberseguridad en los emprendimientos digitales [en línea]. 2021. Recuperado el 21 de abril de 2022, de https://forbes.co/2021/05/28/red-forbes/cinco-estrategias-para-promover-la-ciberseguridad-en-los-emprendimientos-digitales/

FERNÁNDEZ, J. M. L.; BARRERO, D. L. B.; ROJAS, L. A. R. Industria 4.0: el reto para las pymes manufactureras de Bogotá, Colombia [en línea]. Revista Mutis, 12(1), 2022. Recuperado el 10 de mayo de 2025, de https://revistas.utadeo.edu.co/index.php/mutis/article/view/Industria-4.0-reto-para-pymes-manufactureras-Bogota-Colombia

FLORES CCANTO, F.; POZO CURO, C.; FLORES CONISLLA, L. D.; MEDINA, A.; ANDRÉS, W. Desafíos del liderazgo transformacional en asuntos de ciberseguridad organizacional [en línea]. s. f.

FRANCO SUÁREZ, K. A.; ZAMBRANO HERNÁNDEZ, L. F. Análisis documental para la creación de un equipo de respuestas a incidentes informáticos orientado a pequeñas y medianas empresas del sector económico colombiano [en línea]. s. f.

FUNCIÓN PÚBLICA. Ley 590 de 2000 - Gestor Normativo - Función Pública [en línea]. s. f. Recuperado el 10 de mayo de 2022, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=12672

GALLEGOS ALIAGA, M. C.; VALENCIA COLLANTES, A. A. S. Implementación de la norma ISO 27032 para mejorar la gestión de ciberseguridad en RMO Contratistas Generales SAC [en línea]. 2023. Recuperado de: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/8141/M.Gallegos_A.Valencia_Tesis_Titulo_Profesional_2023.pdf?sequence=1&isAllowed=y

IBM – INTERNATIONAL BUSINESS MACHINES. ¿Qué es la ciberseguridad? [en línea]. 2020. Recuperado el 21 de abril de 2022, de https://www.ibm.com/co-es/topics/cybersecurity

ISEOBLUE. Strategic Information Security Management within ITIL v4 [en línea]. s. f. Disponible en: https://www.iseoblue.com/post/information-security-management-in-itil

ISMS.ONLINE. Gestión de riesgos de ciberseguridad según la norma ISO 27001:2022 [en línea]. 2025. Disponible en: https://es.isms.online/iso-27001/risk-management/cybersecurity-risk-management

MINCOMERCIO. Leyes | Mi Pymes [en línea]. s. f. Recuperado el 21 de abril de 2022, de https://www.mipymes.gov.co/normatividad/leyes

MINCOMERCIO. Inicio | Mi Pymes [en línea]. s. f. Recuperado el 21 de abril de 2022, de https://www.mipymes.gov.co/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC. Estrategia Nacional de Ciberseguridad [en línea]. 2019. Recuperado el 21 de abril de 2025, de https://www.mintic.gov.co/portal/715/w3-article-15430.html

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC. Guía de mejores prácticas en ciberseguridad para PYMEs. 2021.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC. Modelo para el emprendimiento TI Colombia [en línea]. 2021. Obtenido de Guía para la comprensión del modelo y su estrategia de implementación: https://colombiatic.mintic.gov.co/679/articles-73972_recurso_1.pdf

MODELO DE EMPRENDIMIENTO TI COLOMBIA. [en línea]. s. f. Recuperado el 13 de enero de 2025, de https://colombiatic.mintic.gov.co/679/w3-article-73972.html

MONTEALEGRE, B. J. R. Medición de madurez de ciberseguridad en MiPymes colombianas [en línea]. 2016. Recuperado de: https://repositorio.unal.edu.co/bitstream/handle/unal/57956/80245271.2016.pdf?sequence=1&isAllowed=y

MORENO LEÓN, A. S.; MORALES BENÍTEZ, C. D.; MARTÍNEZ VARGAS, L. A. Diseño de una propuesta de emprendimiento a partir de un estudio de factibilidad de un outsourcing contable en un escenario de virtualidad en Bogotá, Colombia [Trabajo de grado, Universidad Piloto de Colombia], 2021.

MARTÍNEZ-OSORIO, F. Plan de concienciación sobre la importancia de la seguridad de la información en las entidades de salud del sector público de Bogotá. 2021.

MONSTER. Amenazas informáticas [en línea]. agosto de 2019. Recuperado de: https://www.monster.es/orientacion-laboral/articulo/amenazas-informaticas

NIÑO, Y. A. Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo Pymes [en línea]. 2015. Recuperado de: http://hdl.handle.net/10654/7325

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. [en línea]. 2025, enero 9. Recuperado de: https://www.nist.gov/

OCDE. Seguridad digital y resiliencia en América Latina [en línea]. 2020. Recuperado de: https://www.oecd.org/es/publications/siete-lecciones-aprendidas-sobre-seguridad-digital-durante-la-crisis-de-covid-19_c8fa9059-es.html

PARRADO, V. Cómo implementar un marco de riesgos de TI [en línea]. 2020, junio 18. GlobalSuite Solutions. Recuperado de: https://www.globalsuitesolutions.com/es/implementar-marco-riesgos-ti/

GARCÍA-GONZÁLEZ, J. R.; PEREZ-CORONELL, L.; SÁNCHEZ-SÁNCHEZ, P. A.; TRIANA, A. Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. Información tecnológica, vol. 32, no. 5, pp. 121-128, 2021.

GLOBALSUITE SOLUTIONS. ¿Qué es la norma ISO 27001 y para qué sirve? [en línea]. 2023, marzo 20. Disponible en: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

KASPERSKY. El presupuesto en ciberseguridad aumenta en empresas, pese a los recortes por COVID-19 [en línea]. 2021. Disponible en: https://latam.kaspersky.com/about/press-releases/2021_el-presupuesto-en-ciberseguridad-aumenta-en-empresas-pese-a-los-recortes-por-covid-19

MICROSOFT. ¿Qué es la ciberseguridad? Soporte técnico de Microsoft [en línea]. s. f. Disponible en: https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

MONTEALEGRE, B. J. R. Medición de madurez de ciberseguridad en pymes colombianas. 2016. Departamento de Ingeniería de Sistemas e Industrial.

PACHÓN, C. Ciberseguridad para Pymes: Protección contra amenazas [en línea]. 2021, julio 29. Disponible en: https://www.nsit.com.co/ciberseguridad-para-pymes-proteccion-contra-amenazas/

PÉREZ PÉREZ, Y. Importancia de la ciberseguridad en Colombia. 2017. Trabajo de grado (Pregrado). Universidad Piloto de Colombia.

PORTAFOLIO. Debemos mejorar los índices de rotación de personal en sector TIC [en línea]. 2019, mayo. Disponible en: https://www.portafolio.co/economia/empleo/debemos-mejorar-los-indices-de-rotacion-de-personal-en-sector-tic-52999

RAMÍREZ MESA, C.; GONZÁLEZ LÓPEZ, J. Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes. 2020. Tecnológico de Antioquia, Institución Universitaria.

REVISTA LATIN PYMES. La ciberseguridad, reto de las pymes [en línea]. 2021, febrero 12. Disponible en: https://www.latinpymes.com/la-ciberseguridad-reto-de-las-pymes/

SOPHOS. Estado del ransomware [en línea]. 2022. Disponible en: https://www.sophos.com/en-us/content/state-of-ransomware

TABORDA, J. P.; CASTAÑO OSPINA, D. M.; HERNÁNDEZ DÍAZ, L. E.; GARRO TORRES, J. D. Análisis prospectivo de la industria de desarrollo de software en Colombia. Punto de vista, vol. 10, no. 16, 2019. DOI: 10.15765/pdv.v11i16.1415.

VALORA ANALITIK. Actividad maliciosa en internet aumentó en un 150 % en Colombia durante aislamiento [en línea]. 2021. Disponible en: https://www.valoraanalitik.com/2021/02/27/actividad-maliciosa-en-internet-aumento-un-150-durante-el-aislamiento/

VALORA ANALITIK. Día de las mipymes: ¿cómo avanzan en ciberseguridad? [en línea]. 2021. Disponible en: https://www.valoraanalitik.com/2021/06/24/dia-de-las-mipymes-como-avanzan-en-ciberseguridad/