



República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil

Facultad de Posgrado e Investigación

Tesis en opción al título de Magister en

Sistemas de Información Gerencial

Tema de Tesis:

Factores para la adopción de servicios de Cloud Computing y sus consideraciones de seguridad de la información en las Pymes del Ecuador.

Autor:

Ing. Washington Geovanny Flores Moreno

Director de Tesis:

Ing. Francisco Cedeño Troya, MSc.

Septiembre 2023

Guayaquil – Ecuador

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado me corresponde exclusivamente y el patrimonio intelectual de la misma a la Universidad Tecnológica Empresarial de Guayaquil”

Ing. Washington Geovanny Flores Moreno

CI: 0917624231

DEDICATORIA

El presente trabajo investigativo lo dedico principalmente a Dios, por ser el inspirador y darme fuerza para continuar en este proceso de obtener uno de los metas más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, ya gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que ahora soy. Ha sido el orgullo y el privilegio de ser su hijo, a mi esposa Cristina que me motivo constantemente a alcanzar y terminar mis objetivos.

Geovanny

AGRADECIMIENTO

El actual trabajo de tesis primeramente me gustaría agradecer a Dios por permitirme para llegar hasta esta etapa de mi vida, por hacer realidad este anhelado sueño.

A la UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL por darme la oportunidad de formarme y ser un profesional.

A mi director de tesis MSc. Francisco Cedeño, por su esfuerzo y dedicación, quien, con sus conocimientos, experiencia, paciencia y motivación ha logrado en mí que pueda terminar esta maestría con éxito.

Son muchas personas las que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos, apoyo y compañía en los momentos más difíciles de mi vida. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de vida, por todo lo que me han brindado y por todas sus bendiciones.

Para todos ellos: Muchas gracias y que Dios los bendiga.

RESUMEN

El presente trabajo de titulación se basa en la adopción de la tecnología cloud computing en las pequeñas y medianas empresas (PYMES) correspondientes al cantón Milagro, el objetivo principal se enfoca en analizar la forma en la que incide la aplicabilidad de esta tecnología en la seguridad informática dentro las organizaciones, por lo que se realizó un estudio y análisis a través de un modelo adecuado en el cual la adopción de la computación en la nube sea mucho más adaptable a las necesidades del negocio.

La investigación se establece en base a las normas ISO 27001 y 27002, así como también bajo los mecanismos de seguridad de la información, para lo cual se realizó un análisis mediante la operacionalización de variables y sus respectivas dimensiones, tales como servicio, control de acceso e identificación, despliegue, cumplimiento, gestión de riesgos, y cada una aplicada a la tecnología cloud. Se optó por realizar un estudio de tipo descriptivo, en el cual se aplicaron metodologías documentales, investigación de campo, y tratamiento estadístico para la recolección de datos e información en las PYMES del cantón Milagro.

Como resultado se final se obtuvo que las dimensiones de servicio, disponibilidad, y despliegue dependiendo del tipo de aplicabilidad que se les dé, cuentan con índice de mayor incidencia en la investigación, por lo que deberían ser tomadas en consideración para tratar de mejorar el nivel de aceptación hacia esta tecnología en estudios futuros.

Palabras clave: computación en la nube, seguridad informática, adopción, tecnología, aplicabilidad.

ABSTRACT

This degree work is based on the adoption of cloud computing technology in small and medium enterprises (SMEs) corresponding to the canton Milagro, the main objective focuses on analyzing the way in which the applicability of this technology affects computer security within organizations, so a study and analysis was conducted through an appropriate model in which the adoption of cloud computing is much more adaptable to the needs of the business.

The research is established based on the ISO 27001 and 27002 standards, as well as under the information security mechanisms, for which an analysis was performed through the operationalization of variables and their respective dimensions, such as service, access control and identification, deployment, compliance, risk management, and each one applied to cloud technology. A descriptive study was chosen, in which documentary methodologies, field research, and statistical treatment were applied for the collection of data and information in the SMEs of the Milagro canton.

As a result, it was found that the service, availability, and deployment dimensions, depending on the type of applicability they are given, have a higher incidence index in the research. Therefore, they should be taken into consideration to try to improve the level of acceptance towards this technology in future studies.

Keywords: cloud computing, information security, adoption, technology, applicability.

ÍNDICE GENERAL

INTRODUCCIÓN	1
CAPITULO I	3
1. Marco Teórico Conceptual	3
1.1. Antecedentes de la Investigación.....	3
1.1.1. Análisis de la situación actual	9
1.1.2. Sistemas de información que utilizan las empresas en el sector industrial 14	
1.2. Planteamiento del Problema	14
1.2.1. Formulación del Problema de Investigación	17
1.2.2. Sistematización del Problema de Investigación	17
1.3. Objetivos de la Investigación	17
1.3.1. Objetivo General	17
1.3.2. Objetivos Específicos	17
1.4. Justificación de la Investigación	18
1.5. Marco de Referencia de la Investigación	19
1.5.1. ¿Qué es Cloud Computing o Computación en la Nube?	19
1.5.2. Características del Cloud Computing.....	20
1.6. Modelos de Servicio del Cloud Computing	21
1.6.1. Modelos de aceptación del cloud computing.....	21
1.6.2. Factores para la Adopción de Servicios de Cloud Computing	26
1.7. La Seguridad de la Información.....	27
1.8. La Seguridad Informática	28
1.9. Seguridad de Cloud Computing	29
1.9.1. Gestión del Riesgo de la Seguridad de la Información	30
1.9.2. Riesgos en Entornos Cloud Computing	31
1.9.2.1. Shadow IT	31
1.9.2.2. Riesgos asociados con Shadow IT	32
1.9.2.3. Norma ISO 27000	33
1.9.2.4. Estándar COBIT	35
1.10. Consideraciones de Seguridad de la Información en Cloud Computing	36
CAPÍTULO II	38
2. Marco Metodológico.....	38

2.1.	Tipo de Diseño, Alcance y Enfoque de la Investigación	38
2.2.	Métodos de Investigación.....	39
2.3.	Unidad de Análisis, Población y Muestra	39
2.4.	VARIABLES DE LA INVESTIGACIÓN, OPERACIONALIZACIÓN.....	41
2.5.	Fuentes, Técnicas e Instrumentos para la Recolección de Información	42
2.5.1.	Fuentes de información	42
2.6.	Técnicas e Instrumentos para la Recolección de Información.....	43
2.7.	Tratamiento de la Información	44
CAPÍTULO III		45
3.	Resultados y Discusión	45
3.1.	PRESENTACIÓN DE RESULTADOS Y DISCUSIÓN	45
3.1.1.	Análisis de la variable servicio para el uso de gestión documental aplicado en la tecnología cloud computing.....	48
3.1.2.	Análisis de la variable servicio en base a una dimensión de infraestructura para el uso de gestión documental aplicado en la tecnología cloud computing.....	48
3.1.3.	Análisis de la variable servicio en base al nivel de servicios a los que acude la empresa para el uso de gestión documental aplicada en la tecnología cloud computing.....	50
3.1.4.	Análisis de la variable garantía en base a sus dimensiones de confidencialidad, integridad y disponibilidad para el uso de gestión documental aplicada en la tecnología cloud computing.....	52
3.1.5.	Análisis de la variable gobernanza en base a sus dimensiones de políticas y normas para el uso de gestión documental aplicada en la tecnología cloud computing.....	54
3.1.6.	Análisis de la variable control de acceso e identificación en base a la aplicación de un mecanismo de autenticación y la validación de acceso a usuarios para el uso de gestión documental aplicada en la tecnología cloud computing.....	57
3.1.7.	Análisis de la variable gestión de riesgos en base a la implementación de una estrategia de mitigación de riesgos, empleo de técnicas de seguridad, y aplicación del marco de referencia para la evaluación y auditoría como ISO 27001-27002 para el uso de gestión documental aplicada en la tecnología cloud computing.....	60

3.1.8. Análisis de la variable cumplimiento Normativo en base a requisitos legales y revisiones de seguridad de la información para el uso de gestión documental aplicada en la tecnología cloud computing.....	64
3.1.9. Análisis de la variable despliegue en base al grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada, recursos compartidos en la nube, para el uso de gestión documental aplicada en la tecnología cloud computing.	66
3.3. Conclusiones.....	70
3.4. Recomendaciones.....	73
REFERENCIAS BIBLIOGRÁFICAS	76
Anexos	80

ÍNDICE DE TABLAS

Tabla 1. Datos de la investigación	41
Tabla 2. Elección de contratación del Cloud Computing como modelo de negocio.....	48
Tabla 3. Resultados globales del análisis de variables	45

ÍNDICE DE FIGURAS

Figura 1. Diferencia de escalabilidad tradicional frente a la de Cloud Computing.	16
Figura 2. TRA - Teoría de acción Razonada.....	22
Figura 3. TBP - Teoría del comportamiento planificado	24
Figura 4. TAM – Modelo de Aceptación de Tecnología.....	26
Figura 5. Seguridad TI.....	28
Figura 6. Principios de COBIT 2019.....	36
<i>Figura 7. Escala para medición y tratamiento de variables.....</i>	<i>43</i>
Figura 8. Entrega de apps Cloud por mercado funcional	14
Figura 9. Análisis en base a sistemas operativos.....	48
Figura 10. Análisis en base a Aplicaciones Ofimáticas.....	49
Figura 11. Análisis en base a otras aplicaciones.....	49
Figura 12. Servicio de almacenamiento utilizado por la empresa	50
Figura 13. Servicio de servidores utilizado por la empresa.....	51
Figura 14. Servicio de correo electrónico utilizado por la empresa.....	51
<i>Figura 15. Garantía de la seguridad de la información en dimensión de confidencialidad.....</i>	<i>52</i>
Figura 16. Garantía de la seguridad de la información en dimensión de Integridad.	53
Figura 17. Garantía de la seguridad de la información en dimensión de Disponibilidad	53
Figura 18. Nivel de importancia de políticas y estándares de seguridad en la empresa.	54
Figura 19. Nivel de importancia de políticas y estándares de seguridad en la empresa expresado en gráfico de pastel.	54
Figura 20. Nivel de importancia de las normas ISO 27001, 27002 en la seguridad de la información Empresa.....	55

Figura 21. Nivel de importancia de las normas ISO 27001 y 27002 en la seguridad de la información de la Empresa expresado en gráfico de pastel.	55
Figura 22. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso.	57
Figura 23. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso expresado en gráfico de pastel	57
Figura 24. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso expresado en gráfico de pastel	59
Figura 25. Nivel de valoración de las PYMES en cuanto a la validación de autenticación de usuarios en el acceso a los recursos de la organización expresado en gráfico de pastel	59
Figura 26. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto a la implementación de una estrategia de mitigación.	60
Figura 27. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto a la implementación de una estrategia de mitigación expresado en gráfico de pastel.....	60
Figura 28. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto al empleo de técnicas y procedimientos para el monitoreo y control de la seguridad de la información.....	61
Figura 29. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto al empleo de técnicas y procedimientos para el monitoreo y control de la seguridad de la información expresado en gráfico de pastel.....	62
Figura 30. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos en la aplicación de un marco de referencia para la auditoria y evaluación como ISO 27001-27002 como aporte a la seguridad de la información.	63
Figura 28. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos en la aplicación de un marco de referencia para la auditoria y evaluación como ISO 27001-27002 como aporte a la seguridad de la información expresado en gráfico de pastel..	63
Figura 29. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en los requisitos legales referentes a la adopción de un servicio cloud computing	64
Figura 33. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en los requisitos legales referentes a la adopción de un servicio cloud computing expresado en gráfico de pastel.	64
Figura 34. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en las revisiones de seguridad de la información en la empresa.	65

Figura 35. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en las revisiones de seguridad de la información en la empresa expresado en gráfico de pastel.	66
Figura 33. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada	67
Figura 37. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada expresado en gráfico de pastel.	67
Figura 35. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada expresado en gráfico de pastel	68
Figura 39. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: recursos informativos compartidos en la nube expresado en gráfico de pastel	68

INTRODUCCIÓN

Actualmente las organizaciones se hallan en busca de ventajas competitivas que las lleve a mantenerse y perdurar en el tiempo, este fenómeno se basa en investigar permanentemente y así satisfacer los requerimientos del cliente, ya que el proceso de toma de decisiones posee una gran importancia en la creación de valor para las empresas.

En la era contemporánea de la tecnología de la información, la adopción de servicios de Cloud Computing ha revolucionado la forma en que las organizaciones gestionan y operan sus recursos tecnológicos. Las Pequeñas y Medianas Empresas (Pymes) en el Ecuador, como en muchas otras partes del mundo, se enfrentan al desafío de mantenerse competitivas y eficientes en un entorno empresarial en constante evolución. La adopción de servicios de Cloud Computing ofrece a las Pymes oportunidades sin precedentes para mejorar su agilidad, flexibilidad y escalabilidad en términos de recursos tecnológicos.

Sin embargo, la adopción de Cloud Computing también plantea preocupaciones sustanciales en términos de seguridad de la información. Las Pymes del Ecuador, al igual que en otros países, deben enfrentar cuestiones críticas relacionadas con la protección de sus datos sensibles, la privacidad de los clientes y la integridad de sus sistemas. En este contexto, es esencial comprender los factores que influyen en la adopción de servicios de Cloud Computing por parte de las Pymes y las consideraciones de seguridad de la información que deben tenerse en cuenta para garantizar una transición exitosa y segura hacia esta tecnología.

Diversos profesionales departen sin distinción de la seguridad informática y la seguridad de la información, sin embargo, cada regla tiene sus características aun cuando están estrechamente relacionadas y cuando hablamos de seguridad del cloud computing se deben considerar factores de riesgo y beneficio y de cómo esta herramienta podría ayudar a las empresas a mejorar la seguridad de la información.

En los últimos años las empresas observan con mucha atención el surgimiento y avances en el desarrollo del cloud computing (llamado también computación

en la nube), concepto que se refiere que todos los recursos de la empresa estén alojados en los servidores que pertenecen a terceras personas o proveedores del servicio y a los cuales se puede tener acceso a través de internet, esto está enfocado a brindar un servicio ya sea a clientes finales, empresas o micro empresas ampliando su abanico de posibilidades. Los proveedores ponen a disposición sus centros de datos para otorgar servicios a numerosos usuarios. Este servicio como parte de su atractivo ofrece a sus clientes un soporte flexible a los requerimientos y necesidades que cada empresa requiere.

En esta investigación, trataremos de identificar los factores que influyen en la adopción de Cloud Computing por parte de las Pymes en Ecuador, pero sobre todo nos centraremos en las empresas de la ciudad de Milagro con considerarse un punto estratégico comercial para él Ecuador, así como las estrategias y mejores prácticas para abordar las consideraciones de seguridad de la información asociadas. Al comprender estos aspectos cruciales, espero proporcionar una base sólida para la toma de decisiones informadas y exitosas en la adopción de servicios de Cloud Computing en el contexto de las Pymes ecuatorianas.

CAPITULO I

1. Marco Teórico Conceptual

1.1. Antecedentes de la Investigación

Cloud Computing ha sido una de las grandes novedades para las empresas, solucionando muchos inconvenientes de compatibilidad de gestión de la información, para tener siempre disponible sus datos en cualquier lugar y dispositivo, para realizar tomas de decisiones que ayuden a resolver diferentes inconvenientes en sus planes de negocio sin la necesidad de cambiar su lugar de trabajo.

En una investigación llamada “La importancia del uso de recursos en la nube para el favorecimiento del emprendimiento corporativo en empresas y organizaciones” se abarcan temas como la globalización y con esto la necesidad de quitar la localidad física de una empresa para llegar a más lugares, también se estudian formas de disminuir los costos obteniendo un aumento en el beneficio o rendimiento de la empresa, se analiza la búsqueda de optimización de procesos en las empresas para consumir menos recursos, un punto interesante que se describe en brevedad es la adopción del Cloud Computing según el conocimiento que se tenga sobre sus funcionalidades y por último se mencionan unos casos de éxito aplicando Cloud Computing (Baena-Luna, Palos-Sanchez, Garcia-Rio, & Casablanca Peña, 2018).

En otros estudios basados en la iniciación de una empresa nos muestran la facilidad que brinda el Cloud Computing a la hora de emprender, el cual nos plantea como un nuevo modelo de negocio que presenta un sin número de ventajas tanto en escalabilidad como permanencia del negocio, se enfrentan a temas como la virtualización de recursos y presentándolos como servicios, otro punto que tiene que ver con las empresas es el ahorro de gastos de mantenimientos en la infraestructura en la iniciación de la empresa. (Andrade, Célleri, y Rodríguez, 2018).

El Cloud Computing ofrece como ecosistema empresarial asociarse a un modelo de negocio, donde aporta muchos beneficios a las empresas, dando un mejor rendimiento al desarrollar sus actividades y obteniendo como resultados la implementación de herramientas de TIC. En este ecosistema que está

compuesto por factores de desempeño tanto internos (áreas, departamentos, jerarquía) como externos (proveedores, administradores, etc.) de índole empresarial, estos dan mayor relevancia a los clientes o usuarios finales a los que van destinados los productos o servicios caracterizados por la globalización, donde la interacción con ellos ofrecerá información para el mejoramiento de la empresa en sus metas y objetivos.

Según un informe presentado por (Mosquera Rodríguez, Chilán Regalado, & Soledispa Rodríguez, 2018) se menciona que las empresas que regularmente utilizan este tipo de servicios de alojamiento en la nube han experimentado posibles riesgos o amenazas por ejemplo en el uso de Interfaces o APIs inseguras que pueden dejar vulnerables las tecnologías compartidas, así como también pérdidas o fugas de datos, el secuestro de servicios y credenciales. También se hace mención que para poder utilizar los servicios de cloud computing se requiere de una interfaz y que la seguridad está directamente relacionada de cuán segura es la misma, por lo que al seleccionar un proveedor de servicios se debe analizar su infraestructura y el contrato que protegerá los derechos sobre la información que solo le pertenecen a la empresa.

Las aplicaciones que utilizan la nube como Software Como Servicio (SaaS) es un modelo que tiene aplicaciones de gestión entre otras aplicaciones que se puede acceder en cualquier dispositivo que tenga acceso a internet.

Las empresas tienen que analizar la interoperabilidad que tiene con los sistemas que utilizan actualmente y los que ofrece el Cloud Computing, para evitar posibles problemas con la migración de datos por las diferencias que tienen actualmente, sea un sistema tradicional o con menos prestaciones que los actuales que ofrecen más beneficios, como diferencia entre estos dos modelos son los siguientes:

- En relación al precio los modelos tradicionales tienen un precio fijo, otorgando a la empresa una licencia de uso permanente, en el caso de los modelos SaaS, es un modelo de costo variable esto implica que se paga por lo que se utiliza, con más servicios que vaya utilizar la empresa tendrá que invertir más dinero anualmente.

- El hardware está incluido en la tasa de servicio que uno solicita en las SaaS evitando problemas de mantenimiento para la empresa, en los modelos tradicionales el hardware se encuentra en el ámbito local, en un espacio específico para los servidores.
- La licencia del sistema como la del software que está en el modelo tradicional están a cargo de la misma empresa, del usuario, por otro lado, en el Cloud Computing la primera licencia ya viene incluida en el pago del servicio y la obtención de la licencia del software se realizará a través de la web.
- Los costos de mantenimiento son a cargo de la empresa, estos suelen realizarse periódicamente, esto conlleva gastos adicionales en el modelo tradicional, en el SaaS todo se encarga la empresa que ofrece el servicio sin tener que retribuir la empresa con pagos adicionales.
- La instalación es otro de los factores que se beneficia la empresa al adquirir los servicios del Cloud Computing, esto es debido a que no necesita ser instalado físicamente en la empresa y es posible la personalización e implementación del servicio, en los modelos más tradicionales esto provoca tener un espacio específico para la instalación de infraestructura y equipos necesarios para el funcionamiento de la empresa y su procedimiento de instalación suelen ser de larga duración hasta que la empresa empiece a utilizarlas.
- Las operaciones realizadas por TI todas son a cargo del personal especializado en la empresa, dando una carga de trabajo mayor a los empleados y gastos adicionales a la empresa, todo esto en el modelo tradicional, por el contrario, con el modelo SaaS todo esto lo lleva la propia proveedora del servicio sin que la empresa gaste por esta gestión.
- Cloud Computing tiene la ventaja de introducir nuevas características diarias en los servicios que ofrece a las empresas sin necesidad de pagos adicionales, comparado con los sistemas tradicionales que incluyen actualizaciones menores y si quieres algún añadido o prestaciones nuevas tienes que hacer un pago adicional para obtener esas características y prestaciones de servicio.

De acuerdo con (Molina Montero, 2020) en su tesis de grado menciona que para lograr la conveniente adopción del Cloud Computing se requiere endurecer diferentes aspectos importantes encontrados de acuerdo al modelo propuesto y que se recomienda tomar en cuenta cada una de las variables como la expectativa de desempeño, expectativa de esfuerzo, influencia social, condiciones facilitadoras y la confianza, considerando las dimensiones o aspectos que conforman las misma, con la finalidad de que los resultados sean considerados validos en el campo y ofrezcan los resultados esperados y que de los cuales siempre se espera que sean placenteros.

“Las empresas mejoran su desarrollo estratégico obteniendo beneficios económicos como tener más impacto en colaboración con otras empresas y acelerando los lanzamientos de sus productos y actualizados en todo momento” (Magaña y Enrique, 2015, p. 307).

Existe la incertidumbre en las empresas al momento de contratar o implementar este servicio, estas barreras que se interponen y hacen que se desconfíen son de índole de seguridad, de privacidad de su información o también en el ámbito legal. Mediante encuestas a diferentes empresas para conocer su entorno y la tecnología que utilizan con las ventajas que ofrecen al mejoramiento de la organización, la mayoría de estas usan los servicios de la nube para la gestión de archivos sea hasta por almacenamiento o tareas de ofimáticas, donde los servicios Cloud que han contratado les brindan seguridad y confianza, las ventajas que obtienen es gran flexibilidad para la utilización de recursos tecnológicos, el rendimiento optimizado a la productividad de procesos y el ahorro en el costo de mantenimientos (Palos Sánchez, 2017).

Una empresa ubicada en Murcia enfocada en las tecnologías de la información, se dedica al desarrollo e implementación de soluciones a gestiones empresariales, como el control y la optimización, otorgando a las empresas una tecnología eficaz y dando un valor agregado a la empresa, su producto de más existo que satisface a la sociedad son las aplicaciones SaaS con un 80% de beneficios, ofreciendo a las otras empresas realizar facturaciones electrónicas y gestión a través de una aplicación que se puede acceder desde un móvil, tableta, u ordenador portátil. Los datos son alojados en la nube de Amazon Web Service (AWS).

Se obtiene la información en cualquier lugar o dispositivo electrónico como también actualizada en tiempo real, es una gran ventaja para la toma de decisiones cuando ocurra alguna anomalía, mejora la respuesta de los clientes en términos de tiempo, permite a las empresas que los servicios se vayan adaptando a la evolución sea por crecimiento o por ofrecer otros servicios.

“Los resultados que obtuvo esta empresa en alojar su aplicación SaaS en Google Play, ofrece datos de 5000 a 10000 instalaciones, ganando más clientes y llegando a empresas que puedan utilizar su aplicación y servicios” (Giuseppe, 2017, p. 131).

La empresa utiliza el Cloud Computing para ofrecer correo electrónico, gestión de versiones y proyectos, facturación, etc. Las funcionalidades como la combinación de un CRM (**Customer Relationship Management**) y ERP (**Enterprise Resource Planning**), les permite llegar a más empresas o personas emprendedoras para gestionar, controlar su negocio desde cualquier zona geográfica, independientemente del enfoque de las empresas, sea estas de compra y venta de productos electrónicos mediante una página web, con la capacidad de tener siempre su información disponible y actualizar su stock en cualquier momento ofreciendo un mejor servicio a sus clientes (Giuseppe, 2017, p. 133).

Las empresas de Perú, donde estas representan el 46% de PIB (**Producto Interno Bruto**), donde tiene mucha importancia en la economía del país, uno de sus retos es el tener mejores resultados en su productividad y aumentar la competitividad mediante herramientas que brinden estas ventajas para la toma de decisiones obtenida por el gran volumen de información recopilada. Estas implementan una solución la cual es Business Intelligence (BI) y Business Analytics (BA) que permite tener una visión de la empresa a través de los análisis de los datos y da información precisa para la toma de decisiones, estas técnicas tradicionales están enfocadas a grandes empresas y muchas organizaciones no cuenta con la facilidad de adquirirlas por sus costos elevados en la implementación y mantenimiento, infraestructura y personal capacitado.

Ante estas circunstancias la tecnología de Cloud Computing y su modelo orientado a servicios bajo demanda permitiendo los requisitos necesarios para

el diseño e implementación del Business Intelligence (BI) y Business Analytics (BA) con un menor costo tanto para el mantenimiento como para el personal y reduciendo los tiempos en los diferentes procesos de la organización (Lopez Inga & Guerrero Huaranga, 2018).

En una empresa de Perú su problema recae en los rubros de compra y venta de materiales, los factores que necesita mejorar son: en relación a la sobrecarga del tiempo y los costos de abastecimiento, provocando que la empresa no tenga una salida competitiva en los mercados tecnológicos y comercial. Sin tener un capital para el cambio de infraestructura de la empresa por su alto costo de adquisición de herramientas tecnológicas, la coordinación, gestión y automatización de los procesos de los materiales abastecidos para la reducción de tiempo y recursos.

Adoptan la idea básica de Cloud Computing enfocándola a los sistemas de cadena de suministros otorgando diferentes ofertas en sus servicios y obteniendo las solicitudes de demanda de los servicios de los clientes para conseguir una respuesta a tiempo real y realizar las tomas de decisiones dependiendo del abastecimiento de los productos como la actualización del stock. Este tipo de servicio desarrollado en la cadena de suministro como servicio (Supply Chain as a Service) con una perspectiva a la computación en la nube (SCAAS) (Oblitas y Chávez, 2017, p. 73).

Este trabajo nos proporciona una estructura de funcionamiento e ilustración de componentes del Cloud Computing la cual puede tener múltiples usos dentro de la empresa, también una variedad de definiciones a favor que trae consigo la implementación de estos servicios, no sin antes contrastarlos con sus desventajas mostrando de esta manera que la inversión inicial que se hace en el Cloud Computing es una buena opción a largo plazo si se quiere la estabilidad de la organización. Como último recurso que se puede encontrar es una comparación de precios entre varias empresas que brindan el Cloud Computing como un servicio. Se brinda una guía detallada para su implementación teniendo en cuenta cada uno de los procesos existentes en la empresa.

La relación con el tema planteado de este trabajo está en la implementación en las pequeñas empresas ya que por lo general no se sienten interesados por

usarlo y esto afecto a todas las futuras inversiones que se tendrían en cuestión tecnológica, y aquí se motiva a su uso desde el comienzo aportando todas sus ventajas en cada área y brindando la forma de implementarlo.

1.1.1. Análisis de la situación actual

Para comprender si el Ecuador preparado para adoptar las tecnologías en la nube, primero debemos determinar si los profesionales de TI comprenden la tecnología en cuestión, los mecanismos legales y regulatorios que facilitan o dificultan su adopción, y los beneficios de adoptar las tecnologías. computación en la nube y posibles barreras para su adopción.

En el estudio presentado por (Abad, Villavicencio, Boza, & Ortega, 2017), el 59% de los participantes siente que entiende en detalle qué es la computación en la nube y el 36% sabe algo sobre estas tecnologías, pero siente que no las entiende en detalle. El 1,8% de los encuestados ha oído hablar de estas tecnologías, pero no sabe en qué consisten, y el 3,5% afirma que nunca antes había oído hablar de los servicios en la nube. El alto nivel de comprensión observado puede deberse al hecho de que la encuesta estaba dirigida a profesionales de TI, o los encuestados pueden haberlo hecho porque son entusiastas de la "nube" con el deseo de aprender o adoptar tecnologías informáticas. en una nube.

Según el informe presentado por (Abad, Villavicencio, Boza, & Ortega, 2017), el empleo de la tecnología de la nube está en constante crecimiento a nivel mundial, la cual abarca diversos tipos de servicios como la gestión de hardware que es proporcionada por un proveedor y rentado por los usuarios a través de modelos de pago flexibles, incluyendo la computación, almacenamiento y comunicación de datos.

En Ecuador, aún no se ha adoptado ampliamente esta tecnología, ya que el 42% de las organizaciones encuestadas en el 2017 (Del total de respuestas recibidas, 114 estuvieron completas,) tienen menos del 25% de sus aplicaciones en la nube, y un 22% no la utilizan. Las áreas más comunes de uso en el país son el hosting, almacenamiento de datos y mensajería. La falta de una conexión a Internet adecuada es el principal obstáculo para la adopción de la nube en Ecuador. Las organizaciones en el país perciben la seguridad de la información como el mayor riesgo al utilizar servicios en la nube. Aunque, la reducción de

costos de infraestructura es la razón principal para adoptar la tecnología de la nube. Las entidades públicas pueden optar por servicios en la nube que involucren almacenamiento de datos en el extranjero, siempre y cuando no estén relacionados con la seguridad nacional o sectores estratégicos. Las pequeñas empresas de tecnología, universidades y ONGs son los principales usuarios de los servicios en la nube en Ecuador. Aproximadamente el 81% de las organizaciones que no usan la nube tienen planes de adoptarla en un plazo de uno o dos años. (Abad, Villavicencio, Boza, & Ortega, 2017).

Para (Phun, 2022) en su artículo, el crecimiento de la nube pública y privada en Latinoamérica a nivel mundial y en la región, cada vez son mínimas las barreras para la adopción de la nube. Hasta antes de la pandemia, el tema de seguridad ya era de mucha preocupación, pero la necesidad de las organizaciones por apresurar el crecimiento de su negocio, disminuir los costos en medida del uso de la infraestructura, la falta y luego la demora en los tiempos de entrega de los servidores en muchos de los países de la región, ha tenido un factor importante, pues la resistencia por la aceptación de la nube pasó a un segundo plano. Si hay algo que se puede considerar como una barrera es la falta de conocimiento de lo que se puede hacer con la nube y la falta de definición de una estrategia concreta para utilizarla.

La tendencia hacia la nube es transversal a todo tipo de industria y tamaño de la empresa y la tasa de crecimiento promedio de adopción de soluciones de nube es de 31.2% para finales de este 2022, y crecerá un 30,4% en Latinoamérica para el 2023, con una tasa de crecimiento compuesta hacia 2025 de 31.9%. Por destacar algunos, el sector público y la industria de distribución y servicios son los de mayor crecimiento esperado hacia 2025 de acuerdo con el estudio (IDC, 2021).

Después de la pandemia, el mundo vivió una significativa transformación tecnológica que originó que las personas de todas las regiones a fortalecer sus destrezas digitales. Ecuador también fue parte de este fenómeno y los usuarios se vieron obligados a adaptarse a esta nueva realidad. Principalmente en escenarios como el teletrabajo, que multiplicó su número de empleados, al pasar de 15.292 antes de la pandemia a 340.846 postpandemia, cantidad que sigue en

aumento. En este sentido, se pueden indicar algunas de las tecnologías más innovadoras que se han desarrollado desde el 2022: Automatización, Edge Computing y nubes nativas, Metaverso, Ciberseguridad, Cloud. (Diario El Universo, 2022).

Según el portal (DATTA Business Innivation, 2021), En una encuesta a nivel global de octubre 2020, la consultora McKinsey reveló que las empresas tuvieron que responder al COVID-19 acelerando la decisión y ejecución de cambios profundos en la digitalización de sus negocios con un factor promedio de 20 a 25 veces más rápido de lo planeado antes de la pandemia. El cambio que encabeza la lista es el teletrabajo y colaboración, seguidos por otros, entre los más relevantes, están el uso de tecnología avanzada en las operaciones, migrar los activos a la Nube, aumento de inversión en Seguridad de datos, entre otros.

También se mencionan varias cifras destacadas que hacen referencia al crecimiento del mercado cloud, el cual indica (DATTA Business Innivation, 2021) un crecimiento sostenido anual del 17% hasta el 2027, y se proyecta que China llegará al 22% anual en el mismo periodo, y en Latinoamérica el IDC proyecta un crecimiento del 27% en 2021 y un 43% acumulado en 2024.

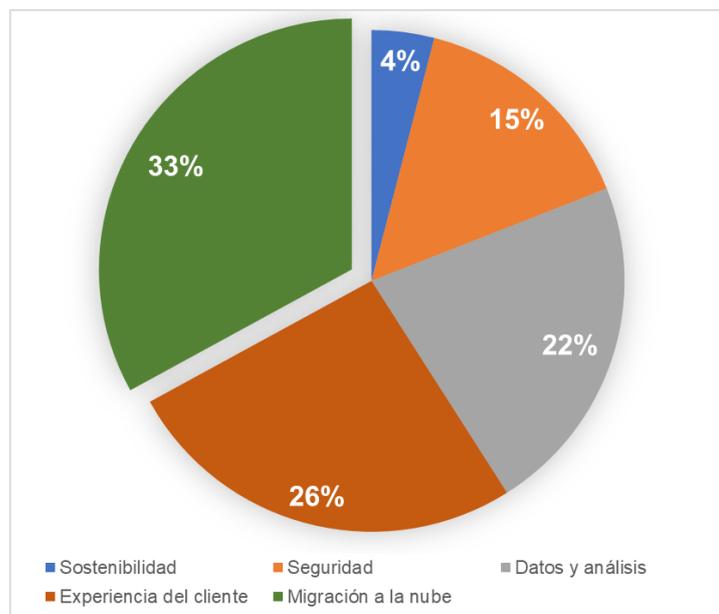
Según el estudio de (IDC, 2022), se estima que para el año 2023, el 80% de las empresas utilizarán servicios vinculados a la nube, este crecimiento es levantado por el interés que las compañías han desarrollado en torno a la ventaja de la nube para el manejo de grandes volúmenes de datos y la gestión de aplicaciones críticas para los negocios.

Según el estudio del (AC3 - Clarity in the Cloud, 2022), casi las tres cuartas partes (72%) de los responsables de la toma de decisiones de TI afirman que su organización está adoptando servicios basados en la nube al actualizar o adquirir nuevas capacidades técnicas. La infraestructura de TI es cada vez más compleja y las empresas deben buscar soluciones de gestión de datos escalables para mantenerse a flote. Llevar a cabo esa gestión en la nube se ha convertido en la solución a la que recurren muchas de ellas. Y es que estas compañías están adoptando ampliamente la nube (pública, privada o mixta) porque ofrece ahorro de costos, disponibilidad de datos, flexibilidad, escalabilidad y otras muchas ventajas. (Vanguardista OnLine, 2023)

La seguridad en la nube ha sido identificada por más del 40% de las empresas encuestadas como el mayor desafío para lograr sus objetivos, convirtiéndose en una preocupación cada vez mayor en numerosas industrias, incluidos los servicios financieros, el sector gubernamental y TI. La migración a la nube, seguida de cerca por la experiencia del cliente, se identificó como la mayor prioridad para las empresas en el mercado actual. Sorprendentemente, la seguridad en la nube clasificó a apenas el 15 % de los encuestados como una prioridad importante para las empresas, a pesar de que se identificó como su mayor desafío para alcanzar los objetivos comerciales. (AC3 - Clarity in the Cloud, 2022)

A continuación, se muestra una gráfica sobre cuál es la máxima prioridad de una Empresa actualmente según el estudio realizado por (AC3 - Clarity in the Cloud, 2022).

Figura 1. Cuál es la máxima prioridad de las empresas actualmente



Fuente: Obtenido de (AC3 - Clarity in the Cloud, 2022)

En base a los resultados obtenidos mediante la investigación realizada, dentro de las razones más importantes que imperan en el mercado, existe cierta relevancia entre ellas, estas nos demostrarán de porque tener un servicio en la nube de la empresa es buena opción.

Por otra parte, los distribuidores que dan servicio en la nube, se someten a auditorias en instancias internacionales de manera constante lo que permite tener confianza, ya que también les permiten obtener certificados que avalúan la calidad del servicio.

La forma en que el mercado va evolucionando está requiriendo un sistema más rápido de respuesta a los mercados, y los consumidores cambiantes están obligando a las empresas a responder más rápidamente a las condiciones cambiantes, pero, lamentablemente, las operaciones de TI tradicionales carecen de la velocidad y la agilidad que se necesitan en la actualidad. Para ser competitivo, es necesario reducir el tiempo de algunos procesos de negocio, y dentro de esto, la computación en la nube tiene que hacer mucho (mejorar el flujo de trabajo, desarrollar la eficiencia, aumentar la velocidad, etc.).

La tecnología de computación en la nube a menudo se puede integrar fácilmente con otras aplicaciones y sistemas comerciales. Los principales proveedores se han comprometido firmemente con el desarrollo de sistemas abiertos, con aplicaciones que se pueden integrar con los sistemas locales, logrando una evolución fluida en la nube híbrida.

Las empresas pueden elegir los servicios en la nube que mejor se adapten a sus circunstancias y necesidades. Además, según el proyecto, se puede actualizar el almacenamiento o la memoria. Los sistemas y aplicaciones de pago por uso han permitido a las empresas reducir costos al pagar solo por lo que usa en cualquier momento.

Las empresas pueden acceder a la información en cualquier momento, en cualquier lugar y en cualquier dispositivo conectado a Internet. Esta movilidad/ubicación/tiempo se convierte en una mejoría competitiva que permite a los empleados trabajar de forma remota, lo que también mejora la flexibilidad laboral.

Gracias a la “independencia” que permite el alojamiento en la nube, no hay necesidad de contratar servidores o expertos en TI para la instalación, mantenimiento, actualización y más, lo que significa más ahorros.

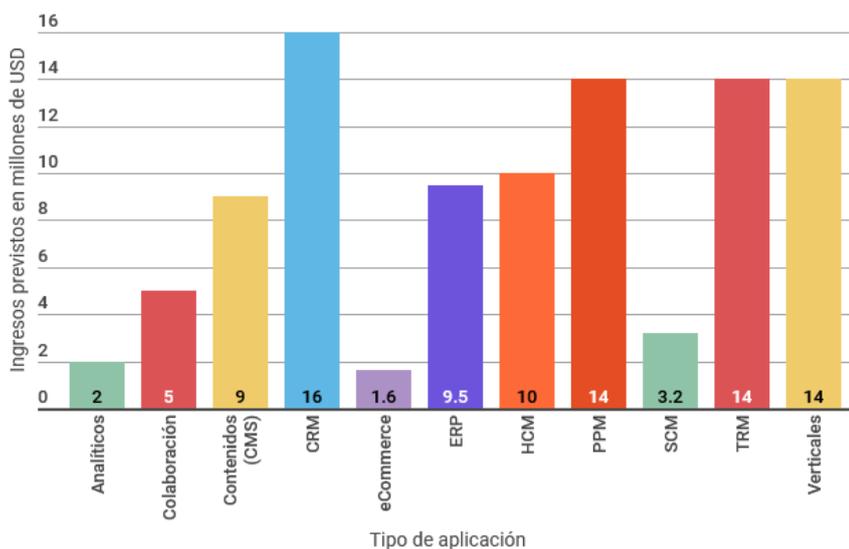
1.1.2. Sistemas de información que utilizan las empresas en el sector industrial

Las empresas cada día acogen distintos sistemas de información para ser gestionados, estos han venido evolucionando con el pasar de los años, permitiendo otorgar la posibilidad a la organización de llevar un mejor control de todo tipo de información de las distintas áreas de trabajo, todo esto mediante tecnología innovadora, que inclusive permite que se integren otros tipos de sistemas.

La finalidad de un sistema de información en una empresa es permitir el cumplimiento de objetivos para lograr a incrementar la productividad en la organización, a la vez se evalúan los distintos niveles de seguridad a través de un análisis de las operaciones y procedimientos de distintas áreas, tales como contabilidad, marketing, finanzas, etc.

A continuación, se muestra una gráfica de los ingresos previstos por entrega de aplicaciones de sistemas de información que son acogidos por las empresas.

Figura 2. Entrega de apps Cloud por mercado funcional



Fuente: Obtenido de (Evaluando Cloud, 2022)

1.2. Planteamiento del Problema

Los gerentes de empresas en Ecuador a menudo sienten un gran desinterés por la inversión en servicios basados en la nube ya sea este de almacenamiento o procesamiento de datos, a veces teniendo la falsa idea de que los procesos no

se pueden mejorar o que ya han alcanzado el punto máximo de optimización, también se suele asociar este pensamiento al hecho de que la empresa es pequeña y por lo tanto no es necesario que se recurran a servicios externos a la organización, aunque la realidad es otra, basta con ver ejemplos de empresas extranjeras donde al implementarse servicios web han disminuido el gasto económico que supone mantenerlos dentro de la organización. Las empresas al contratar servicios web delegan esa responsabilidad a empresas que se dedican al mantenimiento y soporte de esos servicios, es decir están especializados y por lo tanto obtendremos mayor ventaja sobre la competencia que aún manejan todos esos procesos dentro de la institución.

Un error común es pensar que la inversión en la web es innecesaria que ya es suficiente con el alcance que se tiene usando los métodos tradicionales para cada procedimiento, esto causa que no se realice un presupuesto destinado a este tipo de inversiones ni se planifique nada relacionado al tema aumentando de manera exponencial el interés por invertir.

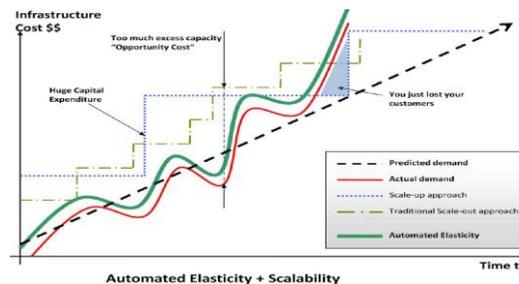
Pero no siempre se trata de la inversión porque en la actualidad hay casos donde empresas están dispuestas a contratar todos los servicios de cualquier tipo existentes con el objetivo de mejorar la productividad de su negocio esto está bien hasta cierto punto, ya que por lo general cuando se trata de una empresa pequeña el gerente que suele ser dueño de la empresa es el encargado de decidir que servicios contratar lo que limita esto a lo que el gerente conoce y no explora otros campos como lo es el Cloud Computing. Esto conlleva a no conocer todos los beneficios que puede generar al negocio ya sea en productividad o disminución de costos operativos y mantenimiento, como consecuencia se tiene el estancamiento del desarrollo empresarial y tecnológico y el riesgo de que la empresa se pierda o quede atrás, como ya ha pasado en muchos casos donde se niegan a innovar y mueren.

Suponiendo que se tiene la inversión y que los gerentes de la empresa conocen sobre el Cloud Computing, aún existe el sacrificio al cambio que acarrea el uso de los servicios en la nube, es en esa parte donde salen las inseguridades y dudas no solo del gerente si no del personal, esto se debe a las pocas ganas del personal en aprender nuevos métodos de realizar un determinado

procedimiento, ya que por lo general cuando se aplica un cambio de esta magnitud se producen ciertos “errores” debido al movimiento después de un largo tiempo de usar lo mismo, y con esto se crea la excusa de que el error es culpa del cambio aplicado y que todo antes del cambio funcionaba de una mejor manera.

Otro de los problemas que adquieren las organizaciones al no trabajar con Cloud Computing es que los empleados suelen recibir demasiada carga de trabajo al momento de necesitar la ejecución de aplicaciones para poder trabajar, lo cual podría ser agilizado y optimizado a través de la computación en la nube. Adicionalmente existen otros tipos de contratiempos al usar sistemas tradicionales, ya que, estos muchas veces no cuentan con los recursos necesarios en cuanto a automatización de reportes o informes que son llevados de manera física por los distintos departamentos de la empresa.

Figura 3. Diferencia de escalabilidad tradicional frente a la de Cloud Computing.



Fuente: Obtenido de (Descom.es, s/f)

Por otro lado, una cuestión que realmente aún sigue siendo algo obsoleto e incensario para varias organizaciones es el que trabajen pagando licencias de programas con los que laboran cada uno de los departamentos, lo cual es un tema bastante importante de analizar en cuanto a la cantidad de presupuesto que se consume; cuando en realidad deberían tratar de optimizar ese consumo e invertirlo en operaciones o procesos que sean mucho más importantes.

Las incidencias de pérdida de información es otro de los problemas presentados en las organizaciones. Existen empleados que usualmente prefieren llevar todo lo realizado de manera física, esto puede ser información financiera, administrativa, entre otras, sin embargo, nadie está libre de que pueda ocurrir incidentes como fallos en los servidores, avería de las máquinas, etc. Por lo

tanto, son temas que realmente podrían ser mejorados con la ayuda de los servicios en la nube.

Mediante una observación minuciosa dirigida a las empresas del cantón Milagro, se pudo constatar como estas tienen un problema acorde a la infraestructura y tecnologías que utilizan: la migración de datos y la rapidez de gestionar los recursos, procesos y mantenimientos.

1.2.1. Formulación del Problema de Investigación

Importante es tener en cuenta que la adopción de tecnologías nuevas en las empresas como el cloud computing no se deberían ejecutar sin antes haber realizado estudios de factibilidad y compatibilidad que son determinantes y que van a permitir tomar una acertada decisión ya que lo que se busca es que esa tecnología permita mejorar la competitividad de la empresa y esto a su vez genere un aumento de la productividad, y por lo tanto contribuir a un mejor bienestar, optimizando cada uno de los recursos, lo que a la empresa le representaría mayores oportunidades de crecimiento. Por esta razón se plantea a continuación la formulación del problema.

¿Cuáles son factores para la adopción de servicio de cloud computing y sus consideraciones de seguridad de la información en las pymes del Ecuador?

1.2.2. Sistematización del Problema de Investigación

- ¿Por qué las empresas no están interesadas en invertir en servicios web?
- ¿Por qué las empresas desconocen o muestran poco interés en los beneficios de la tecnología Cloud Computing?
- ¿Cuánto influye la resistencia al cambio en la implementación de servicios en la nube?
- ¿Qué aspectos en seguridad de la información se consideran en los servicios de Cloud Computing?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Identificar los factores para la adopción del cloud computing y sus consideraciones de seguridad de la información en las Pymes del cantón Milagro.

1.3.2. Objetivos Específicos

- Analizar las causas que originan el poco interés de la inversión en servicios de cloud computing.
- Identificar el impacto que causa en la empresa el no contar con Cloud Computing.
- Identificar el uso y la aceptación de Cloud Computing.
- Identificar los aspectos en la seguridad de la información para el uso de servicios de cloud computing.

1.4. Justificación de la Investigación

En los últimos años las empresas han ido evolucionando a través de diferentes técnicas de negocio como la adaptación de herramientas tecnológicas para mejorar los procesos, la calidad de sus productos o servicios, ampliando su mercado local y global para tener una mayor amplitud dirigida a los clientes y distanciándose de la competencia.

Mediante la presente investigación se analizará como las empresas del cantón Milagro se encuentran actualmente en cuanto al tipo de tecnología o infraestructuras que utilizan, para lo cual es importante conocer el efecto que producen estos servicios conforme al mercado y si estas son satisfactorias para los gerentes.

De acuerdo con (Zabala, Rio, Cilleruela , Garechana, & Gavilanes, 2018) el incremento o reducción de los recursos TI en cloud computing es mucho más barato que en los sistemas tradicionales, donde es necesario realizar grandes inversiones en aquellos momentos donde se hace necesario el empleo de más recursos. Es más, en los momentos en que ya no son necesarios tantos recursos es casi imposible recuperar la inversión realizada (p. 280).

Como indica el autor, se puede justificar que el uso del cloud computing evita que las Pymes inviertan demasiado presupuesto en dar mantenimiento a sistemas tradicionales, o pagando licencias que tarde o temprano llegan a caducar.

Por otra parte, otra ventaja que proporciona la computación en la nube es que, “el acceso a los servicios TI se realiza a través de la red, por lo que diferentes

tipos de dispositivos como teléfonos móviles, PDAs u ordenadores pueden acceder al mismo servicio en la red”

Por esta razón, es necesario que como parte de una idea de innovación sea incluida dentro de los planes de la empresa, esto permitirá que, como tal, otros sistemas heterogéneos tengan la posibilidad de acceder a un solo servicio desde cualquier lugar en donde se encuentren establecidos.

Con los resultados obtenidos de la investigación se determinará qué factores para adopción de los servicios en la nube, que solución o implementación es la adecuada para mejorar la gestión de la información de las empresas del cantón de Milagro para incrementar sus beneficios y tener un mayor alcance para ofrecer sus servicios o productos en el mercado, ya no solo en el cantón si no fuera de sus límites.

1.5. Marco de Referencia de la Investigación

1.5.1. ¿Qué es Cloud Computing o Computación en la Nube?

El termino nube se refiere a una red o al internet, esto implica que la nube está disponible en un área remota, la nube puede ofrecer beneficios sobre los sistemas tradicionales o la web en sistemas abiertos o privados. Aplicaciones como correos electrónicos, video conferencia web, Gestiones de las relaciones con los clientes o CRM, donde todo sigue funcionando normalmente en la nube. La computación en la nube depende del internet donde los servidores virtuales compartidos proporcionan la infraestructura de software a los dispositivos y a otros recursos a los clientes. (Ilyas Malik, Rashid, & Hussain Wani, 2018).

En el artículo (Srivastava & Khan, 2018) se indica que al igual que las nubes reales que son una colección de moléculas de agua, el término "nube" en la computación es la agrupación de redes. El usuario puede utilizar las diferentes modalidades del Cloud Computing. En lugar de implementar su propia infraestructura física, los usuarios contratan un proveedor para que brinde el servicio mediante Internet para acceder a la computación en nube. Los usuarios deben pagar únicamente por los servicios que han utilizado o contratado. La carga de trabajo se puede distribuir para reducir el trabajo en la nube. Una carga de servicio es manejada por las redes que forman la nube, por eso la carga en

las computadoras locales no es pesada cuando se ejecuta una aplicación. Por lo tanto, se reduce la solicitud de hardware y software por parte del usuario. Todo lo que necesitamos es tener un navegador web para usar el Cloud Computing.

(Sunyaev, 2020) menciona en su libro que la computación en la nube es un modelo que permite el acceso a los recursos informáticos que evolucionaron en la tecnología de la información y se ha convertido en un modelo comercial dominante para la entrega de infraestructura, componentes y aplicaciones de TI. Con la computación en la nube que es un modelo centrado en el producto para el aprovisionamiento de TI se transforma en un modelo distribuido global.

Con el pasar del tiempo cada vez el mundo asocia más ámbitos económicos y sociales con la tecnología, el teletrabajo, la educación online y la telemedicina se han convertido en temas de relevancia hoy en día, y en parte se puede decir que es gracias a la llegada de la pandemia Covid-19 a la sociedad. Por lo que, tanto pequeñas como medianas empresas que estaban acostumbradas al trabajo de oficina presencial les costó aprender a trabajar y adaptarse al uso de los medios y herramientas tecnológicas, no obstante, debido a que el problema se vio alargado por mucho tiempo, se vieron obligados a aprender y a remodelar sus métodos y técnicas del manejo de la información.

1.5.2. Características del Cloud Computing

En su libro (Andrade Garda, Célleri Pacheco, & Rodríguez Yáñez, 2018) menciona que las principales características del Cloud Computing son:

- Amplio acceso a la red y a los recursos que están distribuidos a través de la red y que se puede acceder a ellos utilizando los recursos y plataformas heterogéneas como celulares, Computadores de escritorio, Computadoras portátiles, tabletas, entre otros.
- Monitoreo de los recursos, el uso de los recursos puede ser regulado, monitoreado, vigilado y controlado, lo que permite transparencia para el cliente y el proveedor.
- Flexibilidad rápida, ya que los recursos pueden ser proporcionados fácilmente, transmitiendo al cliente la percepción de que la capacidad de operación es ilimitada.

- Autoservicio bajo demanda; Donde el cliente puede solicitar recursos de computación automáticamente y sin necesidad de interactuar con el proveedor de servicios.
- Puesta en común de servicios, las capacidades ofrecidas por el proveedor son asociadas para servir a muchos clientes, son asignados y dirigidos según la demanda y generan sensación de interdependencia de ubicación. El cliente no conoce ni controla la ubicación exacta de los recursos como memoria, almacenamiento, procesamiento y ancho de banda.

1.6. Modelos de Servicio del Cloud Computing

Respecto a los modelos de servicio, el Instituto Nacional de Estándares y Tecnología (NIST) dista entre:

- **Infrastructure as a Service (IaaS).** Al usuario se le ofrece una infraestructura de recursos IT, como procesamiento, energía, almacenamiento y redes entre otros, en un esquema que puede escalarse automáticamente según cada necesidad.
- **Platform as a Service (PaaS).** La capacidad proporcionada al consumidor es el despliegue de todo lo necesario para la construcción y puesta en marcha de aplicaciones y servicios web completamente accesibles en Internet.
- **Software as a Service (SaaS).** Al consumidor se lo habilita para utilizar aplicaciones del proveedor que se ejecutan en una infraestructura de nube, las cuales pueden accederse desde distintos dispositivos e interfaces del cliente, tales como correo, web o VPN.

1.6.1. Modelos de aceptación del cloud computing

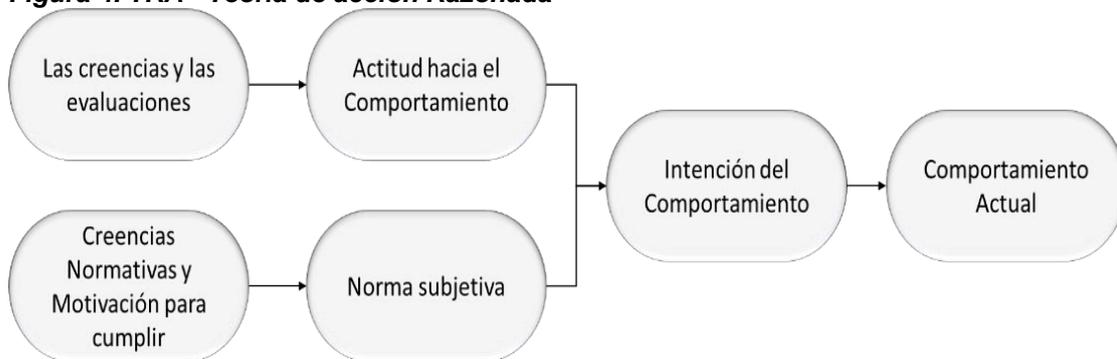
Según (Palos-Sanchez, Reyes-Menendez, & Ramon-Saura, 2019) es posible hallar varios modelos de aceptación de la tecnología que proveen marcos útiles para determinar qué factores críticos influyen en la adopción de las TIC por parte del usuario, así como en el uso y comportamiento del mismo dentro de las organizaciones. Algunos de los marcos teóricos más significativos son: Teoría de la Acción Razonada (TRA) de Fishbein y Ajzen (1975), Teoría del

Comportamiento Planificado (TPB) de Ajzen (1985) y Modelo de Aceptación de la Tecnología (TAM) de Davis (1989).

1.6.1.1. **La Teoría de la Acción Razonada (TRA)**

Ha sido adoptada en muchas disciplinas. Esta teoría explica que las actitudes hacia la realización de una conducta están asociadas positivamente y predicen las intenciones de realizar ese comportamiento. Como puede verse en la Figura, TRA propone una serie de constructos interrelacionados. (Palos-Sanchez, Reyes-Menendez, & Ramon-Saura, 2019)

Figura 4. TRA - Teoría de acción Razonada



Fuente: Adaptado de Fishbein y Ajzen 1975
Elaborado por: El autor

Los factores clave que se consideran en la adopción del Cloud Computing desde el marco de la Teoría de la Acción Razonada se incluyen los siguientes:

Actitudes hacia la adopción de Cloud Computing: Esto se refiere a las percepciones individuales y las actitudes hacia el uso de la tecnología en la nube. Las personas evalúan si creen que la adopción del Cloud Computing será beneficiosa para ellas en términos de ahorro de costos, eficiencia, escalabilidad, etc.

Normas sociales y presión de referencia: Las normas sociales incluyen las expectativas y la influencia de amigos, colegas, superiores y otros miembros de la sociedad o la organización. Si una persona percibe que su entorno social o profesional valora y utiliza el Cloud Computing, es más probable que considere la adopción.

Percepción de control: Este factor se refiere a la percepción de que una persona tiene el control sobre su capacidad para adoptar y utilizar con éxito el Cloud Computing. Esto puede incluir la confianza en las habilidades técnicas necesarias, la percepción de facilidad de uso de los servicios en la nube y la confianza en la capacidad de gestionar los riesgos asociados.

Creencias sobre las consecuencias de la adopción: Las personas evalúan las posibles consecuencias de adoptar el Cloud Computing, tanto positivas como negativas. Esto incluye considerar los beneficios potenciales, como la flexibilidad y la escalabilidad, así como los posibles riesgos, como la seguridad de los datos y la privacidad.

Motivación: La motivación personal desempeña un papel importante en la adopción de la tecnología en la nube. Las personas pueden estar motivadas por la búsqueda de eficiencia, la reducción de costos, la mejora de la productividad o la necesidad de cumplir con requisitos específicos de su trabajo o industria.

Experiencia previa: La experiencia previa con la tecnología en la nube puede influir en la actitud y la disposición a adoptarla. Aquellos que han tenido experiencias positivas previas pueden estar más inclinados a adoptarla nuevamente.

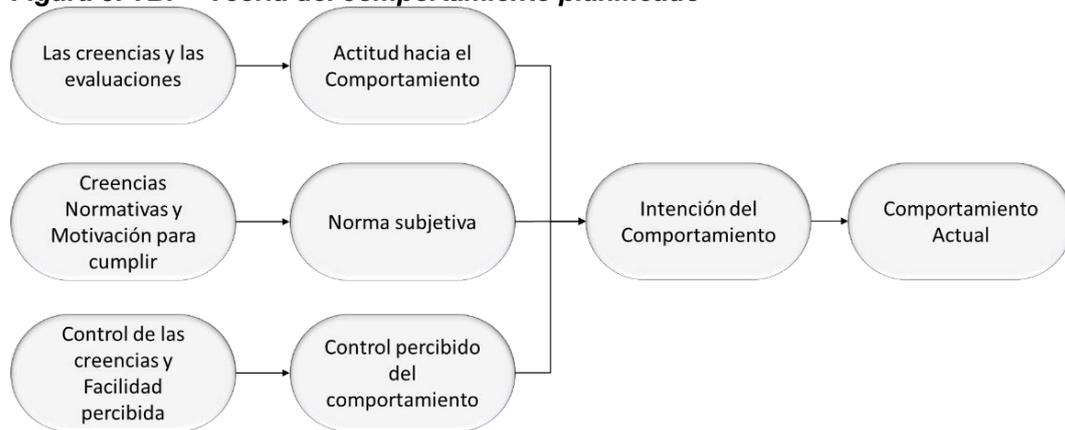
Recursos disponibles: Los recursos disponibles, como el acceso a la infraestructura tecnológica, el presupuesto y el apoyo organizativo, también pueden influir en la adopción. La disponibilidad de recursos puede facilitar o dificultar la adopción del Cloud Computing.

1.6.1.2. Teoría del Comportamiento Planificado (TPB)

Es un modelo teórico utilizado para explicar y predecir el comportamiento humano en relación con una determinada acción. Fue desarrollada por Icek Ajzen en la década de 1980 como una extensión de la Teoría de la Acción Razonada (TRA). Se trata de una teoría aplicada en numerosos campos de estudio, que van desde el marketing hasta la atención sanitaria. La clave de este modelo es la intención de comportamiento. TPB distingue entre tres tipos de creencias: la actitud hacia la acción, la norma subjetiva y el control conductual percibido. La TPB ha sido ampliamente utilizada en diferentes contextos, como

la adopción de tecnología, la elección de productos y servicios, el comportamiento de compra y el comportamiento de salud. Además, ha sido la base de otros modelos teóricos, como el Modelo de Aceptación de Tecnología (TAM, por sus siglas en inglés), que se centra específicamente en la adopción de tecnología. (Palos-Sanchez, Reyes-Menendez, & Ramon-Saura, 2019)

Figura 5. TBP - Teoría del comportamiento planificado



Fuente: Adaptado de Ajzen 1991

Elaborado por: El autor

Este modelo se basa en la idea de que las intenciones de una persona son el predictor más fuerte de su comportamiento y que las intenciones están influenciadas por tres factores principales:

1. **Actitud hacia el comportamiento:** Esta es la evaluación global de una persona sobre si la adopción del Cloud Computing es positiva o negativa.
2. **Norma subjetiva:** Las normas subjetivas reflejan la influencia percibida de las opiniones y expectativas de los demás en relación con la adopción del Cloud Computing.
3. **Control percibido sobre el comportamiento:** Este factor se refiere a la percepción de una persona sobre la facilidad o dificultad de llevar a cabo el comportamiento de adopción del Cloud Computing.

En el contexto de la adopción del Cloud Computing, los factores que se consideran en el modelo de la Teoría del Comportamiento Planificado incluyen:

Actitud hacia el Cloud Computing: Las personas evalúan si creen que la adopción del Cloud Computing les proporcionará beneficios, como la eficiencia,

la escalabilidad, el ahorro de costos y la mejora de la productividad. También consideran si perciben posibles desventajas, como preocupaciones de seguridad o privacidad.

Normas subjetivas: Las normas subjetivas en el contexto del Cloud Computing se refieren a la influencia percibida de colegas, superiores u otros miembros de la organización en relación con la adopción de tecnología en la nube. Las opiniones y expectativas de estos grupos pueden influir en la decisión de adoptar o no el Cloud Computing.

Control percibido sobre el comportamiento: Las personas evalúan si se sienten capaces de adoptar y utilizar el Cloud Computing. Esto incluye la percepción de tener las habilidades técnicas necesarias, el acceso a recursos tecnológicos y la capacidad de superar obstáculos que puedan surgir durante la adopción.

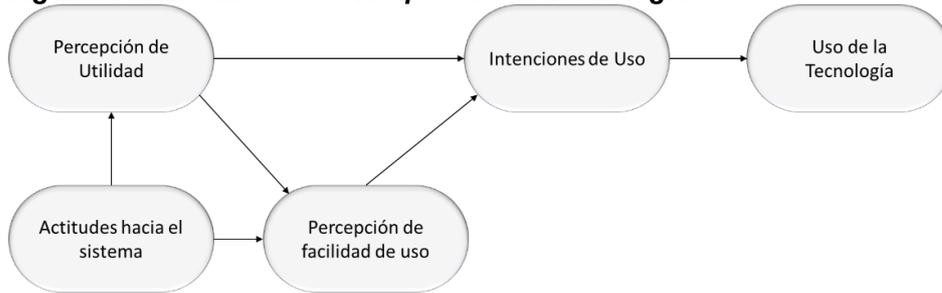
Intenciones de adopción: Las intenciones de una persona para adoptar o utilizar el Cloud Computing se forman en función de la evaluación de sus actitudes, las normas subjetivas y la percepción de control. Las intenciones fuertes suelen ser un indicador de que la adopción es más probable.

Comportamiento real de adopción: Este es el resultado final y se refiere a si una persona efectivamente adopta y utiliza el Cloud Computing.

1.6.1.3. El Modelo de Aceptación de Tecnología (TAM)

Es un modelo teórico que se utiliza para explicar y predecir la aceptación y adopción de tecnología por parte de los usuarios. Fue propuesto por Fred Davis en la década de 1980 y se ha convertido en uno de los modelos más ampliamente utilizados para estudiar la adopción de tecnología. TAM propone y demuestra empíricamente que la Percepción de Utilidad (PU) y la Percepción de Facilidad de Uso (PFU) son los factores más críticos en el proceso de adopción de la tecnología y el uso de los sistemas. TAM se puede considerar como un caso especial de TRA en el que la utilidad percibida y la facilidad de uso percibida se consideran “creencias y evaluación” que llevan a la actitud, que a su vez conduce a la intención de uso, y finalmente al comportamiento real (Palos-Sanchez, Reyes-Menendez, & Ramon-Saura, 2019).

Figura 6. TAM – Modelo de Aceptación de Tecnología



Fuente: Adaptado de Davis 1989

Elaborado por: El autor

TAM tiene sus inicios en el modelo conceptual de Davis en la que sostiene, que el uso actual de la tecnología es directamente influenciado por la motivación del usuario para utilizar el sistema y que a la vez está directamente relacionada por un estímulo externo con características y capacidades del sistema. Los constructos del TAM están formados por la actitud, la utilidad percibida, la facilidad de uso, intención hacia el uso y el uso. La siguiente versión del TAM fue realizada por Davis dos años después, en la que demuestra que la utilidad percibida y la facilidad de uso percibida influyen de manera directa en la intención de uso, eliminándose el constructo actitud hacia el uso, proponiendo la nueva versión del TAM. (Reyes & Castañeda, 2022)

1.6.2. Factores para la Adopción de Servicios de Cloud Computing

En función de los modelos revisados se puede identificar los siguientes factores para la Adopción de Servicios de Cloud Computing:

1. **Costos y Eficiencia:** Evaluación de los beneficios económicos de la adopción de la nube en comparación con la infraestructura local, considerando gastos operativos y de capital, escalabilidad y optimización de recursos.
2. **Escalabilidad y Elasticidad:** Capacidad de aumentar o disminuir recursos de manera ágil según las necesidades, lo que mejora la capacidad de respuesta ante cambios en la demanda.

3. **Flexibilidad y Agilidad:** Posibilidad de implementar rápidamente nuevas aplicaciones y servicios, acelerando el tiempo de comercialización y la innovación.
4. **Acceso Global:** Facilitación del acceso a recursos desde diferentes ubicaciones geográficas, lo que es esencial para empresas con operaciones internacionales.
5. **Actualizaciones y Mantenimiento Simplificado:** Reducción de la carga de administración de TI al encargarse el proveedor de la nube de las actualizaciones y parches.
6. **Colaboración:** Facilitación del trabajo en equipo y la colaboración, ya que los recursos en la nube pueden ser accedidos y editados por varios usuarios de manera simultánea.
7. **Disponibilidad y Tolerancia a Fallos:** Evaluación de la disponibilidad del servicio y los mecanismos de respaldo para garantizar la continuidad del negocio.

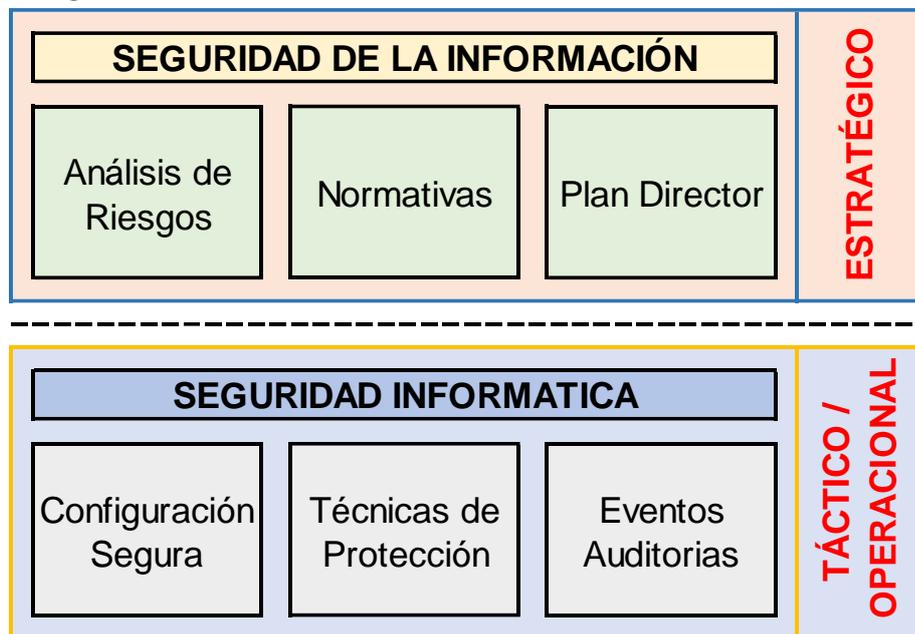
1.7. La Seguridad de la Información

Se ha comprobado que la simple implementación de controles y procedimientos de seguridad de manera frecuente y sin un enfoque claro no es suficiente para preservar la información. Es importante considerar toda la información esencial que necesita protección y establecer un criterio común en torno a la compra de productos técnicos. La Organización Internacional de Estandarización (ISO) ha desarrollado normas como ISO / IEC 27000 para lograr una implementación efectiva de la seguridad de la información empresarial, que incluyen las normas ISO 27001 / ISO 27002 / ISO 27017 / ISO 27018. Estas normas establecen requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI), que se centra en proteger la información en todos sus formatos contra cualquier amenaza, garantizando así la continuidad de las actividades de la empresa en todo momento.

Según (Figuroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018) en su publicación menciona que la seguridad de la información es la norma que se encarga de certificar la confidencialidad, integridad y disponibilidad de la información. Es usual que la seguridad de la información se sostenga en la política de seguridad que se despliegue mediante la aplicación de un plan de

Dirección de Seguridad, en donde la dirección será la delegada para indicar todas las directrices de acción en tema de seguridad, y a través el director para establecer las medidas tanto técnicas como de procesos, que responda por las metas establecidas por la política de seguridad. Las medidas técnicas serán puestas en práctica por el equipo de seguridad informática, administradores de sistemas y seguridad, estas políticas de seguridad que instauran las medidas necesarias para el cumplimiento de la mismas y el análisis de riesgos en el que se debería apoyar la política.

Figura 7. Seguridad TI



Fuente: ISOTools Excellence

1.8. La Seguridad Informática

Según el blog especializado (ISOTools Excellence, 2018), indica que la seguridad informática, también llamada ciberseguridad, se refiere como la distinción táctica y operacional de la seguridad, y es la norma que se encarga de llevar a cabo las soluciones técnicas de protección de la información. La seguridad informática resguarda el sistema informático, intentando asegurar la privacidad e integridad de toda la información que contiene. Consiguientemente, podríamos indicar, que se trata de realizar mediciones técnicas que salvaguardarán las infraestructuras de comunicación que sostienen las operaciones de una empresa, como lo son, el hardware y el software utilizados por las empresas.

(Saltos-Ramírez, 2021) En su artículo hace referencia la seguridad informática en el Cloud Computing o computación en la nube, es un servicio que se ha desarrollado velozmente y promete numerosas formas de ofrecer la seguridad de TI habitual. En esto se encierra el salvaguardar la información crítica frente al robo, la filtración de los datos y la eliminación de los mismos. Así también al escoger los servicios en la nube se puede aplicar a escala y disponer de protección. Actualmente hay una similitud en la forma en que se controla la seguridad, no obstante, existen otras formas adicionales de suministrar soluciones de seguridad para otros aspectos muy importantes.

En su publicación (Figueroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018) menciona que las experiencias en este tipo de seguridad son heterogéneas, y radica por lo general en la restricción del acceso al sistema o parte del sistema. El acceso solo es autorizado a un número limitado de personas que deben encontrarse acreditadas, así como su capacidad de realizar modificaciones dentro de los límites de sus permisos. Las amenazas que se localizan, son debido a que el mismo usuario no tiene en cuenta las vulnerabilidades que existen al hacer un uso del sistema inadecuadamente. Por ejemplo, al descargar archivos comprometidos o infectados, eliminar archivos críticos para el sistema, así también instalar softwares maliciosos como virus o malware.

1.9. Seguridad de Cloud Computing

Se podría considerar al Cloud Computing como un socio de aquellas organizaciones que no disponen de la suficiente capacidad económica para adquirir recursos tecnológicos y estar tecnológicamente a la par con las grandes empresas. Este elemento podría ser la principal causa por la que las empresas están migrando a esta nueva forma de servicio. Los adelantos en la capacidad de procesamiento, acceso a Internet y terminales móviles, conjuntamente con las significativas inversiones realizadas por las grandes organizaciones que dominan el panorama tecnológico mundial, han realizado un vertiginoso progreso en la implementación del Cloud Computing a tal punto que numerosos usuarios ya gozan los servicios en la nube sin percatarse de esto. (Célleri-Pacheco, Andrade-Garda, & Rodríguez-Yáñez, 2018)

Según (Célleri-Pacheco, Andrade-Garda, & Rodríguez-Yáñez, 2018) en su libro indica que se pueden distinguir los siguientes puntos como posibles riesgos del Cloud Computing para las organizaciones:

1. Al elegir un proveedor se debe considerar su reputación, antecedentes y la sostenibilidad. Esta última es muy trascendental ya que avala que los servicios estarán disponibles y que los datos se podrán rastrear.
2. El proveedor del servicio tiene el compromiso y la responsabilidad de manipular la información y si no se actúa de acuerdo con los niveles de servicio pactados afectarán la confidencialidad, la disponibilidad y consiguientemente las operaciones de la empresa.
3. Puede haber desconcierto sobre dónde está almacenada la información lo que puede causar retraso cuando se solicite la recuperación de la información.
4. El ingreso y manipulación de terceros a la información sensible pone en riesgo la privacidad de la información y esto puede simbolizar una amenaza a la protección de la propiedad intelectual.
5. La utilización de las nubes públicas es un aspecto perjudicial en el que es viable combinar los activos de información con los de otros clientes de la nube, incluso de competidores. Es desafiante para las organizaciones cumplir con todas las normas y leyes existentes en los distintos países. Por lo que es totalmente obligatorio que las empresas se asesoren legalmente en la elaboración del contrato en el cual se detalle la responsabilidad legal y financiera del proveedor de servicios
6. Cuando ocurra una desgracia puede acontecer que la información no se halle de manera inmediata en cuyo caso los procedimientos de continuidad del negocio y de recuperación deben estar bien documentados y comprobados. Los lapsos de recuperación que debe de efectuar el proveedor deben estar descritos en el contrato.

1.9.1. Gestión del Riesgo de la Seguridad de la Información

La implementación de una norma de seguridad de la información, al mismo tiempo que ayuda a minimizar el impacto de los riesgos y amenazas, mejora la organización y la gestión de la seguridad de las organizaciones, estableciendo

garantías de prolongación del negocio en caso de contingencia, suministra una imagen de prestigio ante terceros cumpliendo las normativas locales.

Como lo indica (Figuerola-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018) la seguridad de la Información como el método que nos habla de los peligros, de las amenazas, de los estudios de escenarios, de las buenas prácticas y esquemas regulados, que nos piden niveles de fortalecimiento de procesos y tecnologías para realzar el nivel de confianza en la creación, utilización, recuperación, transmisión, disposición y almacenamiento final de la información de la empresa.

(Coello-Yagual & Pico-Versoza, 2018) mencionan en su publicación que la Asociación Española para la calidad describe a la seguridad de la información la cual “tiene como fin la protección de los datos, controlar el acceso, utilización, divulgación, interrupción o destrucción no autorizada”. El término seguridad de información nace por la necesidad de resguardar la información y de todos los sistemas que la gestionan, los cuales pueden ser bienes físicos o informáticos. Así también describen a la seguridad de la información como “un conjunto de normas, procedimientos y acciones que permiten proteger la información manteniendo las propiedades de confidencialidad, integridad y disponibilidad”

1.9.2. Riesgos en Entornos Cloud Computing

La computación en la nube es una tecnología que se ha vuelto cada vez más popular en los últimos años porque puede proporcionar a las empresas y organizaciones infraestructuras de TI escalables y rentables. Sin embargo, como cualquier tecnología, la computación en la nube conlleva algunos riesgos.

1.9.2.1. Shadow IT

Shadow IT se refiere a cualquier tipo de software o hardware utilizado en una organización que no está aprobado o controlado por el departamento de tecnología de la información de la organización. Esta práctica puede tomar muchas formas y puede violar casi cualquier iniciativa de cumplimiento. Hay muchas formas en que Shadow IT se manifiesta en entornos de red. (Cunha Barbosa, 2020)

Shadow IT (Tecnología de la Información en la sombra) se refiere al uso no autorizado de software, hardware u otros sistemas o servicios dentro de una

organización, a menudo sin el conocimiento del departamento de tecnología de la información (TI) de esa organización y a diferencia de la infraestructura de TI estándar, Shadow IT no es administrada internamente por una organización. Puede entrar en una organización de diferentes maneras, pero lo habitual es que se produzca por usar una herramienta no aprobada para acceder, almacenar o compartir datos corporativos, es decir si una empresa ha autorizado usar de forma exclusiva Google Workspace para compartir archivos, un miembro de la organización podría introducir la Shadow IT en la empresa si decide compartir archivos con Microsoft 365. Otra forma es acceder a una herramienta aprobada de una forma no autorizada. (CloudFlare, 2023)

1.9.2.2. Riesgos asociados con Shadow IT

Según el portal (CloudFlare, 2023), la Shadow IT facilita la vida de algunos empleados, pero los inconvenientes superan con creces los beneficios. Si los equipos de TI no pueden rastrear cómo se utilizan las herramientas y los servicios dentro de su organización, es posible que desconozcan hasta qué punto existe la Shadow IT y cómo se accede a ellos, cómo se almacenan y cómo se comprometen los datos corporativos. Siendo transferido. Y con la introducción de Shadow IT, los equipos de TI pierden el control sobre cómo se administran y mueven los datos. Los empleados que brindan servicios no autorizados o usan métodos no autorizados para trabajar en servicios autorizados pueden ver y mover datos confidenciales sin la supervisión de TI adecuada. Como resultado de esta falta de visibilidad y control, la Shadow IT puede crear riesgos adicionales como:

Los datos confidenciales pueden verse comprometidos o ser robados. Los atacantes pueden explotar configuraciones erróneas y vulnerabilidades en los servicios alojados en la nube, lo que abre la puerta a filtraciones de datos y otros ataques cibernéticos. Estos ataques pueden ocurrir sin el conocimiento de su departamento de TI. Especialmente cuando se dirige a aplicaciones y herramientas no autorizadas (y potencialmente inseguras). Además, remediar estos ataques puede ser muy costoso. En un estudio de 2020, IBM estimó que el costo promedio de una violación de datos debido a una configuración incorrecta de la nube es de \$ 4,41 millones.

Las empresas pueden violar las leyes de privacidad sin siquiera darse cuenta. Para las organizaciones que deben cumplir con las regulaciones de protección de datos, es esencial poder rastrear y controlar cómo se procesan y comparten los datos. Cuando los empleados usan herramientas no autorizadas para procesar datos confidenciales, las organizaciones, sin saberlo, corren el riesgo de violar estas leyes, lo que puede resultar en sanciones y multas significativas.

Para el portal (Ciberseguridad, 2022), Los riesgos de seguridad y cumplimiento surgen cuando el departamento de TI no tiene visibilidad de qué aplicaciones SaaS están usando los empleados y departamentos. Hay muchos riesgos de seguridad cibernética asociados con la Shadow IT que no se administran y se ignoran dentro de las organizaciones. Algunos de los más comunes incluyen: Falta de visibilidad, Incumplimiento de leyes, Fugas de datos, Incremento de la superficie de ataque e Ineficiencias en la colaboración.

1.9.2.3. Norma ISO 27000

En el área de la normalización, se cuenta con sistemas de gestión ISO, ISO es la Organización Internacional de Normalización, no gubernamental e independiente que busca la estandarización, la creación de estándares. A nivel mundial existen aproximadamente 22.500 estándares, cubriendo de esta manera casi todas las industrias. (Fustillos-Chimborazo, 2021).

Para el ámbito de la Gestión de la Seguridad de la Información se cuenta con la norma ISO 27000, la cual pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la aplican. (ISOTools Excellence, 2018)

De acuerdo con (Coello-Yagual & Pico-Versoza, 2018) la norma ISO 27000 tiene una serie de recomendaciones clasificadas en varios documentos tales como:

- **ISO 27000:** Visión General de Sistemas de Gestión de Seguridad de la Información (SGSI).
- **ISO 27001:** Requerimientos de los Sistemas de Gestión de Seguridad de la Información (SGSI).

- **ISO 27002:** Directrices y Principios Generales (Code of Practice for Information Security Management).
- **ISO 27005:** Directrices para la Gestión de Riesgos de Seguridad de la Información.
- **ISO 27035:** Mejores prácticas para la Gestión de Incidentes de Seguridad de la Información.
- **ISO 27701:** Propone implementar un Sistema de Gestión de Privacidad de la Información (SGPI) para la aplicación de políticas y controles que protejan los datos personales de la empresa, ya sea desde el punto de vista de Controlador de Datos Personales o de Procesador de Datos Personales.
- **ISO 27017:** (Código de prácticas para la seguridad de la información en la nube) Establece controles de seguridad específicos y mejores prácticas para proteger la información almacenada, procesada o transmitida en la nube. Estos controles se basan en los requisitos de la norma ISO 27002, que es una norma más amplia de seguridad de la información.
- **ISO 27018:** (Código de prácticas para la protección de datos personales en la nube) Se aplica a cualquier tipo de organización que procese datos personales en la nube para garantizar la transparencia en la gestión de los mismos, el control del cliente sobre los datos personales, la responsabilidad del proveedor de servicios en la nube y la seguridad de estos.
- **ISO 27032:** Se aplica a cualquier tipo de organización que maneje información sensible o procese datos en línea estableciendo controles y prácticas recomendadas para gestionar los riesgos de ciberseguridad y proteger la información contra los ciberataques y aborda temas como la evaluación y gestión de riesgos de ciberseguridad, la gestión de incidentes de ciberseguridad, la colaboración entre diferentes partes interesadas, la protección de datos personales, la seguridad de las redes y la gestión de la continuidad del negocio.
- **El Framework CIS (Center for Internet Security Framework):** Es un conjunto de mejores prácticas y recomendaciones de seguridad

cibernética que ayuda a las organizaciones a mejorar su postura de seguridad y reducir el riesgo de ataques cibernéticos.

- **El Framework NIST (National Institute of Standards and Technology Framework):** Es un conjunto de directrices, estándares y mejores prácticas de ciberseguridad desarrollado por el National Institute of Standards and Technology (NIST) de los Estados Unidos y se centra en ayudar a las organizaciones a gestionar y reducir los riesgos de seguridad cibernética.

1.9.2.4. Estándar COBIT

El modelo COBIT es un modelo de evaluación que admite verificar y llevar un control de los sistemas de información de las empresas y la seguridad, por medio de este modelo se enlaza la tecnología, orientado a todos los sectores de una organización, es decir: dirigentes, beneficiarios y los auditores responsables del proceso. Este modelo posee una organización con marco de operación donde se ajustan los razonamientos de exploración, por ejemplo, la seguridad y eficacia, se comprueban los recursos que distinguen la tecnología de información, a través los recursos humanos, infraestructuras técnicas, entre otras y al final una estimación sobre los métodos implicados en la empresa (Figuroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018).

El estándar COBIT (Control Objectives for Information and Related Technology) brinda un conjunto de “mejores prácticas” para la gestión de los Sistemas de Información de las empresas. El objetivo principal de COBIT es brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las acciones de una manera manejable y lógica. Estas prácticas están encaminadas más al control que a la ejecución. (Asociación Española para la Calidad (AEC), 2021).

En su publicación (Figuroa-Suárez, Rodríguez-Andrade, Bone-Obando, & Saltos-Gómez, 2018) indica que la distribución del modelo COBIT plantea un marco de acción donde se valoran los criterios de información, como por ejemplo la seguridad y calidad, se verifican los recursos que involucran la tecnología de información, como es el caso de recurso humano, infraestructuras, sistemas, entre otros, y finalmente se efectúa una valoración sobre los procesos implicados en la empresa.

Según la (Asociación Española para la Calidad (AEC), 2021) El estandar COBIT muestra, asimismo, una guía respecto a métodos de acuerdo a las fases del ciclo de Deming, brindando un enfoque de extremo a extremo de la TI, ayudando a identificar los recursos principales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas. La nueva versión 2019 del COBIT se fundamenta en cinco principios básicos

1. Satisfacer las necesidades de las Partes Interesadas.
2. Cubrir la organización de principio a fin, Integrando el Gobierno corporativo con el Gobierno de las TI. Orientación al negocio.
3. La aplicación de un único marco de trabajo integrado.
4. Habilitación de un enfoque holístico. Para conseguir una Gestión y Gobierno de las TI con eficiencia y eficacia.
5. La separación la Gestión de Gobierno.

Figura 8. Principios de COBIT 2019



Fuente: Elaborado por: El Autor, basado en el modelo COBIT 2019

1.10. Consideraciones de Seguridad de la Información en Cloud Computing

En función de los estándares de seguridad y gestión de los riesgos revisados se puede identificar las siguientes consideraciones de Seguridad de la Información en Cloud Computing:

1. **Privacidad y Cumplimiento Normativo:** Evaluación de la capacidad del proveedor para cumplir con regulaciones y estándares de seguridad, así como la protección de datos personales.
2. **Gestión de Identidad y Acceso:** Implementación de controles para asegurar que solo usuarios autorizados puedan acceder a los recursos en la nube.
3. **Seguridad en la Transmisión de Datos:** Protección de la información durante su transmisión entre los usuarios y los servidores en la nube.
4. **Seguridad en Reposo:** Medidas para proteger los datos almacenados en la nube de accesos no autorizados.
5. **Aislamiento y Multi-Tenancy:** Garantizar que los datos y recursos de un cliente estén aislados de los de otros clientes en entornos de múltiples usuarios.
6. **Resistencia a Ataques y Amenazas:** Implementación de medidas de seguridad para prevenir, detectar y responder a ataques cibernéticos.
7. **Auditoría y Monitoreo:** Establecimiento de mecanismos de registro y seguimiento de actividades para garantizar la trazabilidad y detectar comportamientos anómalos.
8. **Plan de Recuperación ante Desastres:** Desarrollo de estrategias para recuperarse de eventos catastróficos y minimizar el impacto en la operación.
9. **Evaluación del Proveedor de Servicios:** Análisis exhaustivo de la seguridad ofrecida por el proveedor de la nube, incluyendo su historial de seguridad y medidas implementadas.
10. **Educación y Concienciación:** Capacitación de los usuarios y personal de TI sobre las prácticas de seguridad y las responsabilidades en la gestión de datos en la nube.

CAPÍTULO II

2. Marco Metodológico

2.1. Tipo de Diseño, Alcance y Enfoque de la Investigación

En el presente proyecto se trabajará con el tipo de investigación exploratoria, ya que, esta permitirá que se analice un problema que no cuenta con una definición clara y concisa. Con ello se podrá tener una perspectiva o acercamiento mucho más asertivo referente al problema planteado que se será analizado, adicionalmente se podrá conocer más a fondo sobre los factores que impiden la implantación de los Cloud Computing en las PYMES del cantón Milagro.

Este tipo de investigación ayuda al equipo de investigación a familiarizarse con el tema e identificar recursos básicos para comprenderlo. Entre los resultados puede ser que se comprenda mejor la magnitud del problema o necesidad, las características de los actores implicados y cuáles son los puntos de interés más significativos. (Técnicas de Investigación, 2020)

Para el presente estudio se requiere familiarizarse con el tipo de población sobre el que va a realizar la respectiva investigación, esto permitirá que se tenga un criterio mucho más completo, y que el estudio a realizar sea más afín hacia el objetivo al se quiere dirigir.

El contexto de la investigación es de campo, lo cual amerita trabajar mediante la investigación de tipo descriptiva, sobre la cual se realizarán encuestas para un conjunto de empresas escogidas, mismas que residen en el cantón Milagro. Con ello se busca obtener resultados concernientes en cuanto a los factores que afectan a que las PYMES puedan adoptar a la computación en la nube como parte de la seguridad de su información.

Si bien la presente investigación se menciona a las pymes del país, el estudio a realizar contará con un alcance comprendido en una población significativa correspondiente a un conjunto de empresas seleccionadas para la investigación residentes en el cantón Milagro de la provincia del Guayas.

2.2. Métodos de Investigación

El enfoque de la presente investigación será de tipo cuantitativo, esto debido a que se trabajará con datos obtenidos a través de las técnicas de recolección, como tal un enfoque de investigación de carácter cuantitativo, “usa la recolección de datos para probar una hipótesis con base en la medición numérica y el análisis estadístico, y de esta manera establecer patrones de comportamiento y probar teorías” (Dzul, 2019).

Dentro de la presente investigación se hará uso del método teórico el cual, “permite revelar las relaciones esenciales del objeto de investigación, no observables directamente. Participan en la etapa de asimilación de hechos, fenómenos y procesos” (Cobas, Romeu, & Macías, 2018). Con ello se busca asimilar la situación existente basado en los resultados obtenidos en cuanto los factores que inciden en adopción del cloud computing como medio para la seguridad de la información.

Así mismo se hará uso del método empírico dentro del estudio, mediante el cual se empleará la observación como técnica para la obtención de los resultados, manteniendo así una idea acertada del mismo, de esta forma se espera encontrar los factores que interfieren o las causas de alguna u otra manera impiden la aplicación de computación en la nube.

2.3. Unidad de Análisis, Población y Muestra

Como tal la unidad de análisis correspondiente a la presente investigación estará dirigida a un conjunto de PYMES que radican en el cantón Milagro y que trabajan bajo el uso de internet en sus procesos operativos. Para ello se optará por conseguir la data desde fuentes de datos obtenidos de la plataforma “Ecuador en Cifras”, de los cuales se tomará en consideración las pequeñas y medianas empresas, y mediante ello poder realizar el análisis en base a los factores de incidencia.

La población como tal se enfocará en las PYMES del cantón de Milagro que gestionan información a través de servidores u otra infraestructura tecnológica para el mejor rendimiento y optimización de procesos o las que quieren

implementar el Cloud Computing, no obstante, la presente investigación busca demostrar el por qué aún existe un impedimento para poder hacerlo.

Tipo de Muestra

Se obtiene la respectiva muestra para el estudio en base a un muestreo de población finita, es decir que se conoce el tamaño de la población. Para el presente estudio a realizar se conoce que 332 empresas según el INEC (Instituto Nacional de Estadísticas y Censo) (Ver Anexo 1) hacen uso de internet para trabajar en el cantón Milagro; por consiguiente, se obtiene la muestra mediante formula basada en la población determinada.

A continuación, se detalla la formula a utilizar para obtener el cálculo del tamaño de la muestra:

$$n = \frac{k^2 * p * q * N}{(e^2 * (N - 1)) + K^2 * p * q}$$

Descripción de variables de la fórmula:

N = Tamaño de la población

k = 1.96 al cuadrado (nivel de confianza del 95%)

q = proporción no esperada (1-p)

p = proporción esperada (este es un dato desconocido comúnmente, p=q= 0.5)

e = error muestral deseado

n = tamaño de la muestra

Cálculo de la muestra:

$$n = \frac{1,96^2 * 0,5 * 0.5 * 332}{((0.05)^2 * (332 - 1)) + (1.96)^2 * 0.5 * 0.5}$$

$$n = \frac{3.8416 * 0,5 * 0.5 * 332}{(0.0025 * 331) + 3.8416 * 0.5 * 0.5}$$

$$n = \frac{318.8528}{1.7879}$$

$$n = 178$$

Con la formula aplicada se obtuvo que la muestra para ser aplicada a las respectivas encuestas es de 178 empresas PYMES del cantón Milagro. Consiguientemente se procede a detallar mediante el análisis de datos en una tabla donde se muestran el tipo de muestreo, el margen de error, intervalo de confianza, entre otros datos necesarios para la investigación.

Tabla 1. Datos de la investigación

Tipo de muestreo	Pymes que tienen conexión a internet y personal ocupado de utiliza computadoras
Población	332
Tamaño de la población	Aleatorio simple
Intervalo de confianza	95%
Error de muestreo	5%
Tamaño de muestra	178
Recolección de datos	Encuesta vía online

Fuente: Obtenida por investigación propia del autor.

2.4. Variables de la Investigación, Operacionalización

Las variables a ser utilizadas en el presente estudio investigativo se dividirán en dos partes, variables dependientes e independientes, las cuales se basarán en el estado en que se encuentran las PYMES en el cantón Milagro respecto a la seguridad de la información a través de las tecnologías de la información.

Las variables como tal consisten en analizar aspectos afines a la situación de las empresas que buscan adoptar el uso del Cloud computing como parte de su seguridad de la información, pero que, no obstante, se ven afectados de alguna manera.

Variable Dependiente (VD)

Adopción en la nube: Para el presente estudio se adoptará una única variable dependiente, la cual se enfocará en la idea central del proyecto, que como tal se basa en la adopción del Cloud computing como parte de los procesos inmersos en la seguridad de la información de las PYMES.

Variables independientes (VI)

Servicio: Mediante esta variable se tendrá la posibilidad de medir los servicios y apps que hacen uso de la tecnología cloud computing como un sistema estructurado dentro de la empresa.

Garantía: Con esta variable se valida que prevalezca la seguridad de la información, es decir, que se encuentre disponible, sea íntegra y confiable.

Privacidad en el Control del Acceso e Identificación: Mediante esta variable se evalúan todo tipo de funciones de control de accesos de usuarios, permisos y autenticación.

Gestión de riesgos: Se hará uso de esta variable para medir el control de los procesos realizados diariamente en la empresa, el monitoreo de seguridad en base a las falencias e incidentes ocurridos, roles administrativos, etc.

Cumplimiento Normativo: Con esta variable se valida que se sigan los estándares en base a las normas estipuladas mediante chequeos de cumplimiento en la seguridad de la información

Despliegue: Se evalúa la aplicabilidad y desenvolvimiento del cloud computing dentro de escenarios privados, públicos y colaborativos.

2.5. Fuentes, Técnicas e Instrumentos para la Recolección de Información

2.5.1. Fuentes de información

Fuente primaria

Como fuente de información primaria se optó por la información obtenida mediante encuestas vía online dirigidas a las PYMES del cantón Milagro, las cuales se enfocaron en los procesos y métodos utilizados en las empresas para resguardar sus datos.

Fuentes Secundarias

- Tesis relacionadas a la adopción del Cloud Computing como parte de sus procesos operativos.
- Artículos científicos relacionados a los avances en la seguridad de la información respecto al uso del Cloud Computing.
- Portal web del INEC (Instituto Nacional de Estadísticas y Censo).
- Portal web del INIST (Instituto Nacional de Estándares y Tecnología).

2.6. Técnicas e Instrumentos para la Recolección de Información

Encuestas: Se realizaron cuestionarios como instrumento de recolección de información, estas fueron dirigidas al personal administrativo y a los gerentes de cada una de las PYMES del cantón Milagro.

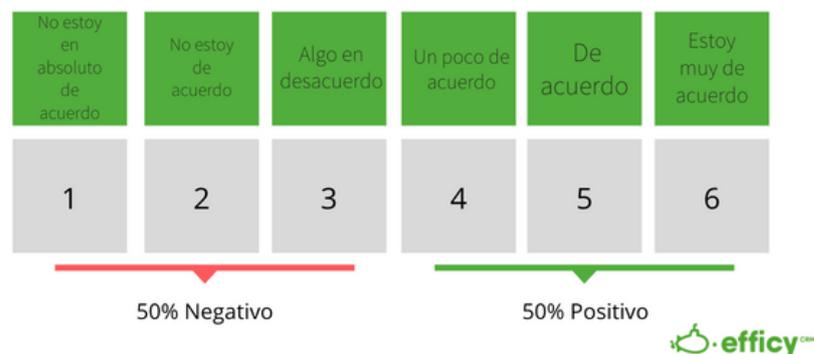
Documental: Mediante el empleo de esta técnica se logró obtener información valiosa como el modelo TOE (Tecnología, Organización, Entorno), que sirvió para definir las variables a utilizar en el presente estudio, esto se logró consultando documentación como tesis y artículos científicos subidos a distintas plataformas.

Estadística: Es una de las técnicas más utilizadas en estudios e investigaciones, para el presente estudio se aplicó esa técnica para recolectar, tratar, organizar, analizar e interpretar los distintos datos obtenidos durante la investigación.

Escala aplicada para la evaluación y tratamiento de variables

Para la evaluación y tratamiento de las variables de la investigación se hará la ponderación mediante escala Fuzzy, la cual da la opción de que las variables tipo lingüísticas sean transformadas a una escala continua, en otras palabras, se asigna un valor porcentual a las categorías existentes en la escala, y de esta forma poder obtener resultados cuantitativos al responder las preguntas.

Figura 9. Escala para medición y tratamiento de variables



Fuente: Obtenida de (Efficacy, 2022)

Encuesta: Se hizo uso de la encuesta como instrumento de recolección de información, en la cual se formularon 21 preguntas, de las cuales 5 de ellas

fueron respondidas mediante el esquema de respuesta de escala Likert. (Ver Anexo 4)

2.7. Tratamiento de la Información

Por naturaleza la investigación se efectuará mediante encuestas realizadas a las 178 PYMES obtenidas en la muestra, antes de realizarla se tiene que recolectar, ordenar tratar y analizar la información del problema para establecer preguntas apropiadas respecto a las Cloud Computing de las PYMES.

Al momento de obtener las respuestas establecidas por parte de las PYMES se hará uso de la información extraída de las encuestas para realizar el respectivo análisis y tratamiento correlacional a la variable dependiente respecto a cada una de sus variables independientes a través del software SPSS, mediante el cual se obtendrán resultados de diferentes tipos tablas y gráficos (barras, pasteles, etc.), mismos que servirán posteriormente para responder a los objetivos específicos de la presente investigación.

Adicionalmente se utilizará la prueba estadística Chi Cuadrado para medir la incidencia de cada una de las variables, para lo cual se tendrá un intervalo de confianza del 95%, y un margen de error del 5% (0.05), todo eso con el fin de poder de obtener las respectivas conclusiones en base a las variables del caso.

CAPÍTULO III

3. Resultados y Discusión

3.1. PRESENTACIÓN DE RESULTADOS Y DISCUSIÓN

En base al análisis y la revisión realizada a las diferentes variables que se presentaron de la encuesta se procede a efectuar un conglomerado de las diferentes variables y sus resultados.

Tabla 2. Resultados globales del análisis de variables

Variables Independientes y sus dimensiones	Aspectos y preguntas	Resultado
Servicio (infraestructura, almacenamiento, servidores, correo electrónico)	Elección del servicio cloud computing como modelo de negocio.	30% en desacuerdo
	Los sistemas operativos como Linux una opción segura para manejar la información.	61% en total desacuerdo
	Las aplicaciones ofimáticas como apoyo a la seguridad de los documentos	56,5% totalmente de acuerdo
	Hacer uso de otros tipos de software como parte de la seguridad de la empresa	80,6% en total desacuerdo
	Servicio de almacenamiento utilizado por la empresa.	50% totalmente de acuerdo
	Servicio de servidores utilizado por la empresa	95,5% totalmente de acuerdo
	Servicio de correo electrónico utilizado por la empresa	35,5% totalmente de acuerdo
Garantía (confidencialidad, integridad, disponibilidad)	Garantía de la seguridad de la información en dimensión de confidencialidad.	55% de acuerdo
	Garantía de la seguridad de la información en dimensión de Integridad	75% totalmente de acuerdo
	Garantía de la seguridad de la información en dimensión de Disponibilidad	40% ni de acuerdo ni en desacuerdo
Gobernanza	Nivel de importancia de políticas y estándares de seguridad en la empresa.	85% totalmente de acuerdo
	Nivel de importancia de las normas ISO 27001 y 27002 en la seguridad de la empresa.	90% totalmente de acuerdo
Control de acceso e identificación	¿Considera importante aplicar un mecanismo de autenticación para validar el uso de Password, validaciones mediante emails u otros como medida de seguridad mediante el uso del cloud computing?	85% totalmente de acuerdo
	¿Considera que se debe validar la autenticación de los usuarios antes de permitir el acceso a un recurso de la organización?	100% totalmente de acuerdo
Gestión de riesgos	¿Cree usted que es importante el que se implemente una estrategia que ayude a mitigar los riesgos para mejorar la seguridad de la información en la empresa?	55% totalmente de acuerdo

	¿Considera que se debería emplear técnicas y procedimientos para el monitoreo y control de la seguridad de la información?	75% totalmente de acuerdo
	¿Cree que sería de aporte a la seguridad de la información el contar con un marco de referencia para la auditoría y evaluación como ISO 27001-27002?	85% totalmente de acuerdo
Cumplimiento Normativo	¿Es importante para su empresa basarse en requisitos legales referentes a la adopción de un servicio cloud computing?	60% totalmente de acuerdo
	¿Considera importante el que se realicen revisiones de seguridad de la información en su empresa?	100% totalmente de acuerdo
Despliegue	¿Hace uso frecuente de varios servicios de forma pública y otros de forma privada?	40% de acuerdo
	¿Hace uso frecuente de recursos informativos compartidos en la nube?	60% en desacuerdo

Fuente: Datos de la investigación Elaborado por: El autor

De acuerdo con lo presentado previamente en la tabla 3, se exponen el total de resultados generales en cuanto al análisis del tratamiento de variables y sus respectivas dimensiones. Donde se ponderan un total de 21 variables, cada una evaluadas a través de preguntas y aspectos relacionados a la adopción del cloud computing como parte de la seguridad de la información.

Se pudo determinar que, de un total de 21 indicadores, 14 de ellos cuentan con un nivel de aceptación respecto a la seguridad de la información de parte de la población evaluada, mientras los 7 restantes que equivalen al 33% necesita que le sea dado una atención mucho más enfocada debido a la falta de cumplimiento de garantizar la seguridad de la información en los sistemas de gestión documental y de datos aplicado a la tecnología cloud computing en las PYMES del cantón Milagro.

Entre los indicadores que necesitan ser evaluados para poder solventar su falta de cumplimiento se encuentran la infraestructura como servicio de despliegue, el almacenamiento, la garantía de la seguridad de la información en dimensión de disponibilidad, hacer uso de otros tipos de software como parte de la seguridad de la empresa y hacer uso frecuente de recursos informativos compartidos en la nube.

Es de suma importancia el que se tome en consideración a las variables que no fueron aceptadas como aplicación en la seguridad de la información durante esta evaluación, es necesario que se trabaje en ellas para poder incrementar la

adopción de los servicios en la nube como parte de los procesos operativos y de seguridad de las organizaciones. El trabajar con la tecnología cloud computing permite que se pueda optimizar el tiempo de trabajo, recursos y sobre todo ahorrar en la economía de la empresa, no obstante, siempre existirá la posibilidad de afrontar riesgos al aplicar cualquier tipo de tecnología de innovación, pero lo importante es que se garantice una mejor forma de trabajo.

Por otro lado, durante el transcurso del análisis llevado a cabo se pudo notar una particularidad en cuanto a la posibilidad de aplicar la tecnología cloud computing como modelo de negocio. En este aspecto se pudo evidenciar que aún la mayoría de la población no considera necesario el que se haga uso de esta tecnología al 100% para que forme parte de los procesos operativos de las organizaciones, en otras palabras, los dueños de las PYMES reconocen la importancia de tenerla como un eje central en la empresa, no obstante, no es considerada necesaria.

Mientras un porcentaje de empresas apoyan el hecho de que la tecnología en la nube ayuda a garantizar un mejor posicionamiento en el mercado debido a sus amplias ventajas competitivas en cuanto a gestión de la información, otras aseguran que este tipo de tecnología aún no cuenta con el suficiente tiempo en el mercado, y que dado a ello la mayoría de las organizaciones prefieren no arriesgarse a poner toda la responsabilidad de su empresa sobre esto.

Por consiguiente, visto desde la perspectiva de un sistema de gestión documental, es necesario el que se puedan respaldar cada uno de los archivos e informes que son manejados en los procesos operativos de la empresa, si bien es cierto el cloud computing no es aceptado por todos, en cierto modo realmente necesitan de los servicios en la nube como respaldo de sus documentos, debido a que la pérdida de los mismos resultaría un tema demasiado agravante y perjudicial para el bienestar de la organización, y mucho más aún si se trata de documentos de índole contable o financieros.

3.1.1. Análisis de la variable servicio para el uso de gestión documental aplicado en la tecnología cloud computing.

En base a la revisión realizada de las diferentes variables de la encuesta presentada se procede a realizar un conglomerado de las diferentes variables y sus resultados en la cual se evalúa si el contratar con cloud computing resulta tan eficiente como para formar parte de un modelo de negocio para las organizaciones.

Tabla 3. Elección de contratación del Cloud Computing como modelo de negocio

Elección del servicio Cloud Computing como modelo de negocio					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En total desacuerdo	3	15,0	15,0	15,0
	En desacuerdo	6	30,0	30,0	45,0
	Ni acuerdo ni en desacuerdo	4	20,0	20,0	65,0
	En acuerdo	3	15,0	15,0	80,0
	En total acuerdo	4	20,0	20,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

Según los datos evaluados mediante la encuesta realizada, se determinó que un 30% de los encuestados respondieron estar en desacuerdo con que el Cloud computing sea considerado como un modelo de negocio dentro del ámbito empresarial, esto se debe a que algunos temen a que pueda suceder algún tipo de fallo en la seguridad de las operaciones realizadas a diario, por lo tanto, en base al análisis realizado se llega a la conclusión de que no es adecuado.

Adicionalmente, también se obtuvieron dos porcentajes de respuesta bastante interesantes, en este caso un 20% considera estar totalmente de acuerdo con la adopción del cloud computing, no obstante, otro 20% considera no estar ni de acuerdo ni en desacuerdo.

3.1.2. Análisis de la variable servicio en base a una dimensión de infraestructura para el uso de gestión documental aplicado en la tecnología cloud computing.

Figura 10. Análisis en base a sistemas operativos

Software Libre - Sistemas Operativos (p.e. LINUX)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	1265	39,0	39,0	39,0
	NO	1980	61,0	61,0	100,0
	Total	3245	100,0	100,0	

Fuente: Datos de la investigación. Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: El autor a través del SPSS

En esta tabla se obtuvo que 61% de las entidades no considera a los sistemas operativos como Linux una opción segura para manejar la información, y por otro lado un 39% afirma que si es conveniente.

Figura 11. Análisis en base a Aplicaciones Ofimáticas

Software Libre - Aplicaciones ofimáticas (p.e. Open Office)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	1834	56,5	56,5	56,5
	NO	1411	43,5	43,5	100,0
	Total	3245	100,0	100,0	

Fuente: Datos de la investigación. Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: El autor a través del SPSS

En el caso de las aplicaciones ofimáticas cambió el escenario, puesto que un 56,5% considera a estas herramientas como apoyo a la seguridad de los documentos, no obstante, un 43,5% no concuerda con lo mismo.

Figura 12. Análisis en base a otras aplicaciones

Software Libre - Otras, como software de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	628	19,4	19,4	19,4
	NO	2617	80,6	80,6	100,0
	Total	3245	100,0	100,0	

Fuente: Datos de la investigación. Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: El autor a través del SPSS

En este análisis se puede constatar que un 80,6% no está de acuerdo con hacer uso de otros tipos de software como parte de la seguridad de la empresa. Sin embargo, el otro 19,4 % cree que si es conveniente.

Los servicios se encargan de hacer uso de las aplicaciones, dispositivos de conexión, servidores, etc. No obstante, no se lleva nada a través de la nube, lo cual, de acuerdo a varias indagaciones, es bastante riesgoso para las empresas.

En el análisis realizado colocando los distintos tipos de software libre, se obtuvo que tan solo las aplicaciones ofimáticas están consideradas como una opción segura para el manejo de gestión documental.

3.1.3. Análisis de la variable servicio en base al nivel de servicios a los que acude la empresa para el uso de gestión documental aplicada en la tecnología cloud computing.

Para este análisis se tomará en consideración todo tipo de medio tecnológico de las empresas, tales como aplicaciones de correo electrónico, páginas a las que se accede a diario, servidores, entre otros. Todos estos servicios serán medidos desde la valoración muy alta hasta la muy baja, la cual se adaptará al modelo de escala de evaluación Likert.

A continuación, se muestran tres de los servicios evaluados:

Figura 13. Servicio de almacenamiento utilizado por la empresa

Almacenamiento					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy baja	1	5,0	5,0	5,0
	Media	1	5,0	5,0	10,0
	Alta	10	50,0	50,0	60,0
	Muy alta	8	40,0	40,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

Para el servicio de almacenamiento un 50% y 40% de los encuestados aseguraron que hacen uso de manera frecuente del almacenamiento, y lo consideran bastante útil dentro de los distintos servicios con los que se trabaja en la empresa. En escala Likert esto corresponde a los valores de 4 y 5, mismos

que valoran como **de acuerdo** y **totalmente de acuerdo** en lo que respecta a la seguridad de la información

Figura 14. Servicio de servidores utilizado por la empresa

Servidores					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Alta	1	5,0	5,0	5,0
	Muy alta	19	95,0	95,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

En cuanto al servicio de servidores las respuestas fueron bastante claras, obteniendo un 95,5% de las respuestas como muy necesario el uso de los servidores, y por otro lado un 5% de que es necesario el servicio. Lo cual en escala Likert corresponde a 4 y 5 como **de acuerdo** y **totalmente de acuerdo** en cuanto a una opción segura para la información.

Figura 15. Servicio de correo electrónico utilizado por la empresa

Correo_electrónico_gmail_outlook					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy baja	1	5,0	5,0	5,0
	Baja	4	20,0	20,0	25,0
	Media	3	15,0	15,0	40,0
	Alta	5	25,0	25,0	65,0
	Muy alta	7	35,0	35,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

Finalmente, el servicio de correo electrónico, para cual se obtuvo que el 35% lo considera como una opción muy importante dentro de los servicios, y por otro lado le sigue un 25% que es considerado como importante dentro de la empresa. En escala Likert estos valores pertenecen a 4 y 5 como **de acuerdo** y **totalmente de acuerdo** en cuanto a una opción segura para la información.

Según los datos obtenidos, a nivel global los servicios más importantes para la seguridad de los datos en las empresas PYMES se basan en lo que son de

mayor peso y cuenten con la capacidad de soportar mayores cantidades de información.

3.1.4. Análisis de la variable garantía en base a sus dimensiones de confidencialidad, integridad y disponibilidad para el uso de gestión documental aplicada en la tecnología cloud computing.

Confidencialidad: Este análisis se lo realiza mediante la siguiente afirmación: “El rol de los usuarios se considera como una medida de confidencialidad para contar con la adecuada seguridad de la información en la empresa”

Figura 16. Garantía de la seguridad de la información en dimensión de confidencialidad.

		Confidencialidad			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni en acuerdo ni en desacuerdo	2	10,0	10,0	10,0
	En acuerdo	11	55,0	55,0	65,0
	Totalmente de acuerdo	7	35,0	35,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

En base a la afirmación propuesta se obtuvo que un 55% de los encuestados afirman estar de acuerdo que el rol sea considerado una medida de confidencialidad para garantizar la seguridad de la información, a lo cual se sigue un 35% que asegura estar totalmente de acuerdo, en este caso tan solo una mínima cantidad es la que no decide por si está correcta o no la afirmación.

En escala Likert los resultados corresponde a la valoración de los números 4 y 5 que corresponden a **de acuerdo** y **totalmente de acuerdo**.

En sí la confidencialidad si está cien por ciento ligada al rol que lleva cada usuario en la organización, ya que, cada uno es responsable de sus credenciales, por lo que, si llegara a ocurrir algún tipo de incidente, será mucho más sencillo que se identifique a la persona responsable.

Integridad: Este análisis se lo realiza mediante la siguiente afirmación: “La integridad es un fundamento utilizado para asegurar que la información se mantenga resguardada mediante el otorgamiento de permisos a los usuarios”.

Figura 17. Garantía de la seguridad de la información en dimensión de Integridad.

		Integridad			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En acuerdo	5	25,0	25,0	25,0
	Totalmente de acuerdo	15	75,0	75,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través del SPSS

Con la afirmación propuesta se logró obtener que un 75% de las personas encuestadas se encuentran totalmente de acuerdo con lo expuesto, y por otra parte el 25% restante simplemente asegura estar de acuerdo. Para este caso se excluye dentro de la escala los valores negativos o de no aceptación en las respuestas evaluadas del caso.

La integridad siempre ha sido considerada un aspecto importante dentro de la información, ya que, el alterar cualquier tipo de dato de algún asunto en específico puede causar que la información que se quiere dar a conocer sea errónea.

Disponibilidad: Este análisis se lo realiza mediante la siguiente afirmación: “La disponibilidad es uno de los aspectos más importantes para afianzar que la información sea más segura”.

Figura 18. Garantía de la seguridad de la información en dimensión de Disponibilidad

		Disponibilidad			
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Total desacuerdo	5	25,0	25,0	25,0
	En desacuerdo	2	10,0	10,0	35,0
	Ni en acuerdo ni en desacuerdo	8	40,0	40,0	75,0
	En acuerdo	2	10,0	10,0	85,0
	Totalmente de acuerdo	3	15,0	15,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Para el análisis de esta afirmación se obtuvo que de entre los datos más relevantes, que el 40% de los encuestados aseguran estar ni en acuerdo ni en

desacuerdo con lo expuesto, consiguientemente el 25 % de los encuestados responde a en total desacuerdo con que la disponibilidad sea importante para la seguridad de la información, y por otro lado tan solo un 15% asegura estar totalmente de acuerdo con la afirmación.

Realmente es un punto para ponerse a analizar, ya que, si bien es cierto el que la información esté disponible es necesario porque puede ocurrir incidentes donde se requiera de suma urgencia los datos, no obstante, el problema en sí, es si todo el personal tiene acceso a esa disponibilidad como tal. He aquí el porqué de las respuestas en desacuerdo de parte de los encuestados.

3.1.5. Análisis de la variable gobernanza en base a sus dimensiones de políticas y normas para el uso de gestión documental aplicada en la tecnología cloud computing.

Para este análisis de la variable gobernanza se realizó una investigación exhaustiva de manera documental y bibliográfica, misma que sirvió para obtener dos dimensiones que se integran para dar a conocer la importancia y eficiencia de aplicar el uso de las políticas y normas de seguridad informática dentro de la organización.

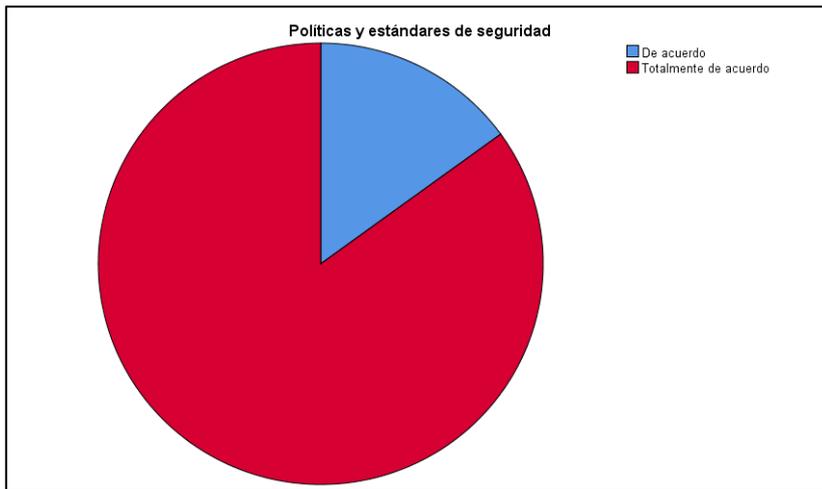
Figura 19. Nivel de importancia de políticas y estándares de seguridad en la empresa.

Políticas y estándares de seguridad					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	De acuerdo	3	15,0	15,0	15,0
	Totalmente de acuerdo	17	85,0	85,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 20. Nivel de importancia de políticas y estándares de seguridad en la empresa expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

De acuerdo con la presente tabla, los resultados obtenidos demuestran que el 85% del total de personas encuestadas responde estar totalmente de acuerdo en que es de suma importancia que se cuente con planificación y control de las políticas de seguridad en la empresa, y por otro lado el 15% restante por lo consiguiente también está de acuerdo. Lo cual en la escala Likert se atribuye a 4 y 5 puntos, **de acuerdo y totalmente de acuerdo**.

Las normas ISO 27001, 27002 son importantes en la seguridad de la empresa, pero el porcentaje de su importancia varía según la naturaleza y el alcance de las actividades de la empresa. A continuación, se presenta una estimación de su importancia basado en la investigación realizada.

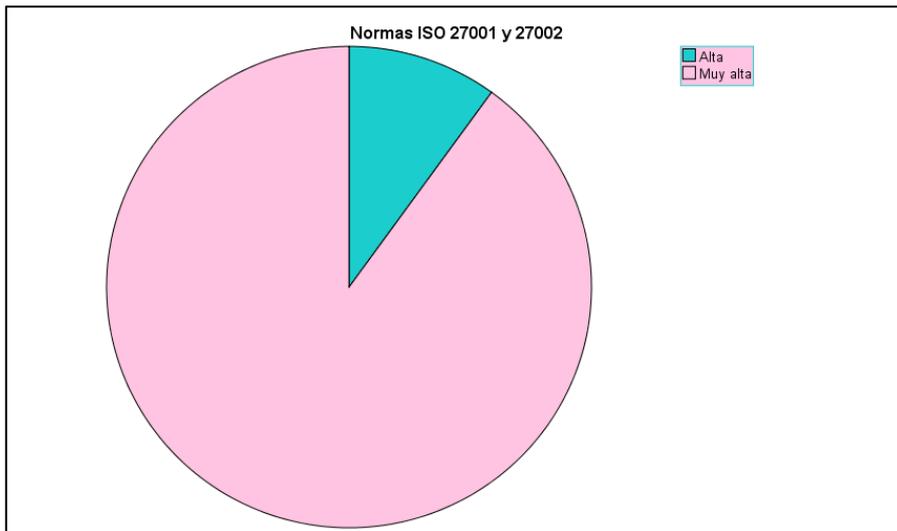
Figura 21. Nivel de importancia de las normas ISO 27001, 27002 en la seguridad de la información Empresa.

Normas ISO 27001 y 27002					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Alta	2	10,0	10,0	10,0
	Muy alta	18	90,0	90,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 22. Nivel de importancia de las normas ISO 27001 y 27002 en la seguridad de la información de la Empresa expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

En cuanto al análisis respecto al nivel de importancia de la aplicación de las normas ISO 27001 y 27002, se obtuvo un 90% de nivel de importancia muy alto, y por otra parte el 10% restante corresponde a un nivel de importancia alto; lo cual atribuye a que realmente este es un punto bastante importante a considerar por las PYMES en el cantón Milagro. En escala Likert los valores obtenidos equivalen a 4 y 5 puntos, **de acuerdo y totalmente de acuerdo**.

Aunque no se menciona dentro de las encuestas las Normas ISO 27017 que trata sobre los Códigos de prácticas para la seguridad de la información en la nube y la Norma ISO 27018 que aplica a los Códigos de prácticas para la protección de datos personales en la nube, se debe hacer énfasis en que estas establecen controles específicos adicionales aplicables en entornos en la nube, donde los clientes, sean estos gerentes de tecnología y las personas del departamento técnico podrán minimizar los riesgos que se encuentren presentes si aplican si aplican él es estándar 27017, o proveedores del servicio ya que con las normas establecidas se proporcionará mayor seguridad y protección de datos lo cual les ayudará a establecer una ventaja competitiva dentro del mercado. Por otro lado, la Norma ISO 27018 se la utiliza en conjunto a los objetivos y controles de seguridad de la Norma ISO/IEC 27002, cuya misión es crear un conjunto común de categorías y controles de seguridad que puedan ser implementados por un proveedor de Cloud Computing para proteger los datos personales de sus clientes en la nube. (Pinargote & Townsend, 2021)

3.1.6. Análisis de la variable control de acceso e identificación en base a la aplicación de un mecanismo de autenticación y la validación de acceso a usuarios para el uso de gestión documental aplicada en la tecnología cloud computing.

Para el análisis de la variable autenticación se analizaron dos aspectos en base a el nivel de valoración que tienen las PYMES en cuanto al uso del control de acceso e identificación como medida de seguridad informática en la adopción de la tecnología cloud computing.

¿Considera importante aplicar un mecanismo de autenticación para validar el uso de password, validaciones mediante emails u otros como medida de seguridad mediante el uso del cloud computing?

Figura 23. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso.

¿Considera importante aplicar un mecanismo de autenticación para validar el uso de passwords, validaciones mediante emails u otros como medida de seguridad mediante el uso del cloud computing?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	= De acuerdo	3	15,0	15,0	15,0
	Totalmente de acuerdo	17	85,0	85,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 24. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso expresado en gráfico de pastel



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Según los resultados obtenidos de acuerdo a la interrogante planteada se pudo obtener respuestas bastante favorables, se obtuvo que el 85% de los encuestados afirman estar **totalmente de acuerdo** con que se debe aplicar un mecanismo de autenticación que ayude a validar el uso de contraseñas, validaciones de emails, entre otros medios como una medida de seguridad a través del uso del cloud computing, y por consiguiente el 15% restante opina casi lo mismo estando **de acuerdo**, lo cual en escala Likert resultan valores de 4 y 5 puntos..

El control de acceso es un tema de suma importancia dentro de las organizaciones, con este se puede validar que usuario tiene acceso a la información de la empresa, así como también quienes irrumpen en datos a los que no están autorizados. Es importante que cada organización otorgue permisos solo al personal autorizado, y mucho más cuando se trata de datos financieros o contables, de esta forma se logra evitar pérdidas, alteraciones o robos de información.

¿Considera que se debe validar la autenticación de los usuarios antes de permitir el acceso a un recurso de la organización?

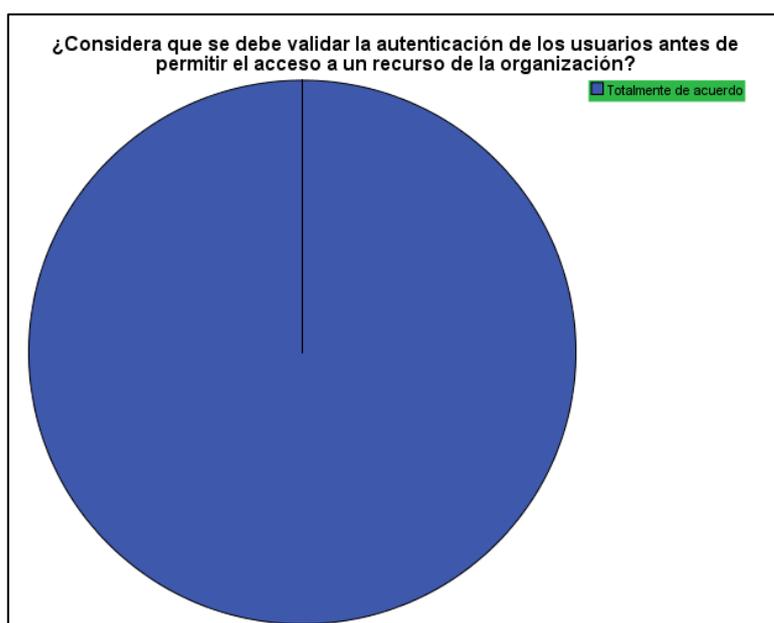
Figura 25. Nivel de valoración de las PYMES en cuanto control de acceso e identificación considerando un mecanismo de acceso expresado en gráfico de pastel

¿Considera que se debe validar la autenticación de los usuarios antes de permitir el acceso a un recurso de la organización?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Totalmente de acuerdo	20	100,0	100,0	100,0

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 26. Nivel de valoración de las PYMES en cuanto a la validación de autenticación de usuarios en el acceso a los recursos de la organización expresado en gráfico de pastel



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Respecto al análisis de la segunda pregunta planteada en base a la variable control de acceso e identificación, se obtuvo que el 100% de los encuestados considera estar **totalmente de acuerdo** en que se debería validar los accesos a cada uno de los recursos que son accedidos por los usuarios, lo que en escala Likert resulta un valor de 5 puntos. Con esto se llega a la conclusión de que en algún momento han existido inconvenientes por el hecho de no validar a los usuarios que acceden a los sistemas.

3.1.7. Análisis de la variable gestión de riesgos en base a la implementación de una estrategia de mitigación de riesgos, empleo de técnicas de seguridad, y aplicación del marco de referencia para la evaluación y auditoría como ISO 27001-27002 para el uso de gestión documental aplicada en la tecnología cloud computing.

Con este análisis se evaluó la importancia sobre la gestión de riesgos que le dan las PYMES en cuanto a la seguridad de la información, se analizarán tres aspectos planteados en tres interrogantes.

¿Cree usted que es importante el que se implemente una estrategia que ayude a mitigar los riesgos para mejorar la seguridad de la información en la empresa?

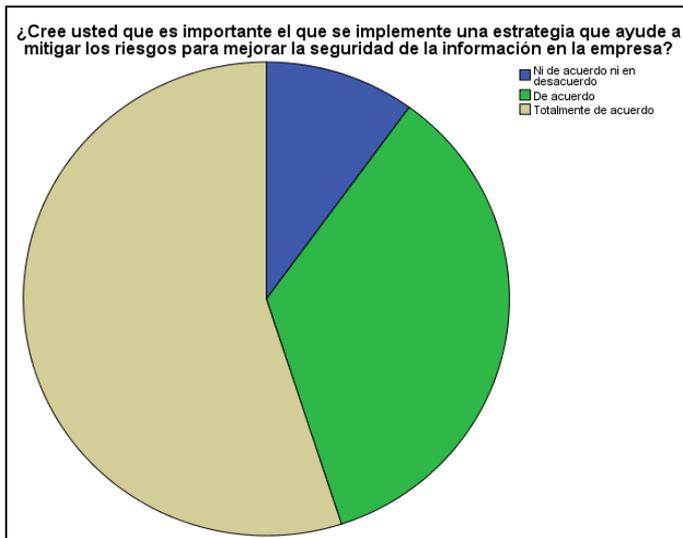
Figura 27. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto a la implementación de una estrategia de mitigación.

¿Cree usted que es importante el que se implemente una estrategia que ayude a mitigar los riesgos para mejorar la seguridad de la información en la empresa?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Ni de acuerdo ni en desacuerdo	2	10,0	10,0	10,0
	De acuerdo	7	35,0	35,0	45,0
	Totalmente de acuerdo	11	55,0	55,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 28. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto a la implementación de una estrategia de mitigación expresado en gráfico de pastel



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Para el análisis de la primera interrogante de la variable gestión de riesgos se obtuvo que el 55% y el 35% de los encuestados afirmaron estar **totalmente de acuerdo** y **de acuerdo** en cuanto a la implementación de una estrategia que ayude a mitigar los riesgos y a mejorar la seguridad de la información en las PYMES, lo cual en escala Likert resulta en valores de 4 y 5 puntos. Por otro lado, hubo un 10% de encuestados que consideraron estar **ni de acuerdo ni en desacuerdo** con que se implemente algún tipo de estrategia para mejorar la seguridad, lo cual en escala Likert equivale a 3 puntos.

De acuerdo con la mayoría de respuestas en acuerdo a la interrogante planteada se llega a la conclusión de que las estrategias son a menudo utilizadas por las organizaciones para mantener segura su información, que en este caso aplicado al sistema de gestión documental mediante la adopción del cloud computing les sería algo beneficioso.

¿Considera que se debería emplear técnicas y procedimientos para el monitoreo y control de la seguridad de la información?

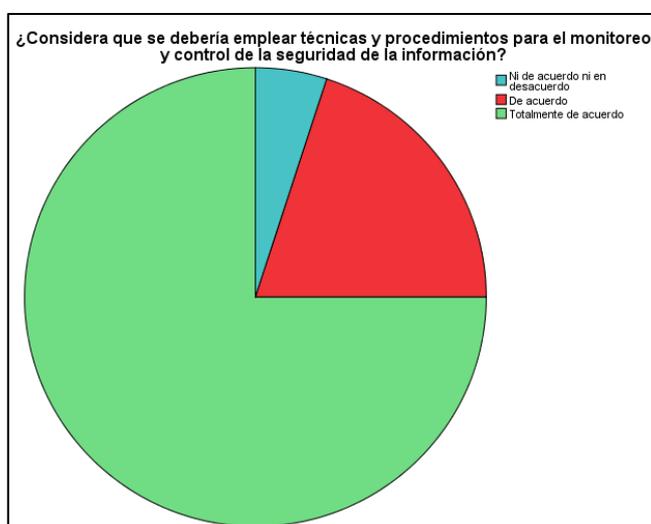
Figura 29. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto al empleo de técnicas y procedimientos para el monitoreo y control de la seguridad de la información.

¿Considera que se debería emplear técnicas y procedimientos para el monitoreo y control de la seguridad de la información?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Ni de acuerdo ni en desacuerdo	1	5,0	5,0	5,0
	De acuerdo	4	20,0	20,0	25,0
	Totalmente de acuerdo	15	75,0	75,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 30. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos respecto al empleo de técnicas y procedimientos para el monitoreo y control de la seguridad de la información expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

En el análisis de la segunda interrogante los resultados estuvieron englobados dentro de la misma valoración de escala Likert que se obtuvo en la primera, se obtuvo que el 75% y 20% de los encuestados afirmaron estar **totalmente de acuerdo** y **de acuerdo** con que se empleen técnicas y procedimientos para el control y monitoreo de la seguridad de la información, lo cual en escala Likert equivale a 4 y 5 puntos. Por otra parte, el 5% restante de los encuestados expresó no estar **ni de acuerdo ni en desacuerdo** con que se emplee algún tipo de técnica, lo cual equivale a 3 puntos dentro de la escala Likert.

Con esto también se determina que la mayor parte de las PYMES si necesita hacer empleo de estas técnicas para mantener segura su información, y mucho

más al tratarse de un sistema de gestión documental en el cual se manejan informes y reportes de suma importancia para la organización.

¿Cree que sería de aporte a la seguridad de la información el contar con un marco de referencia para la auditoria y evaluación como ISO 27001-27002?

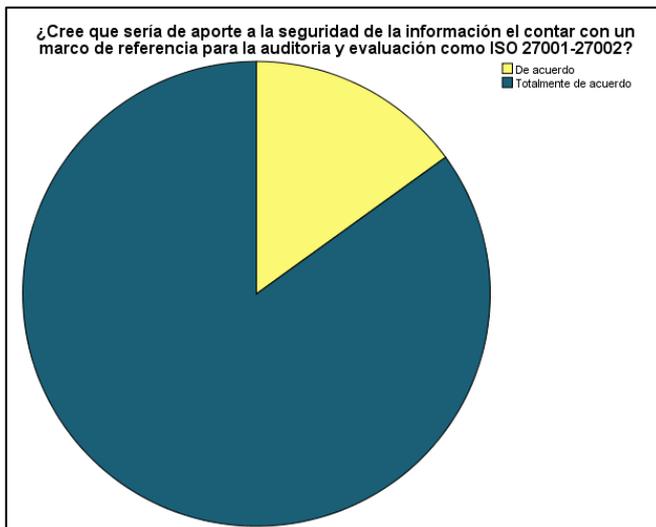
Figura 31. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos en la aplicación de un marco de referencia para la auditoria y evaluación como ISO 27001-27002 como aporte a la seguridad de la información.

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	De acuerdo	3	15,0	15,0	15,0
	Totalmente de acuerdo	17	85,0	85,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 32. Nivel de importancia de las PYMES en cuanto a la gestión de riesgos en la aplicación de un marco de referencia para la auditoria y evaluación como ISO 27001-27002 como aporte a la seguridad de la información expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

De acuerdo con los resultados del análisis en base a la tercera interrogante de la variable gestión de riesgos se obtuvo que el 85% y 15% de los encuestados afirmaron estar totalmente de acuerdo y de acuerdo con aplicar un marco de

referencia para la auditoria y evaluación de la información mediante la ayuda de las normas ISO 27001 y 27002, lo cual en escala Likert equivale a 4 y 5 puntos.

Con ello se puede concluir en que las PYMES también se encuentran dispuestas a adoptar un marco de referencia con las ISO 27001 y 27002, lo cual a su vez permitirá que sea de apoyo en el sistema de gestión documental adoptado a la tecnología cloud computing.

3.1.8. Análisis de la variable cumplimiento Normativo en base a requisitos legales y revisiones de seguridad de la información para el uso de gestión documental aplicada en la tecnología cloud computing.

A través de este análisis se busca obtener la valoración sobre la importancia que le dan las PYMES a las medidas legales para el cumplimiento de las normativas, para analizarán dos aspectos en base a dos interrogantes planteadas.

¿Es importante para su empresa basarse en requisitos legales referentes a la adopción de un servicio cloud computing?

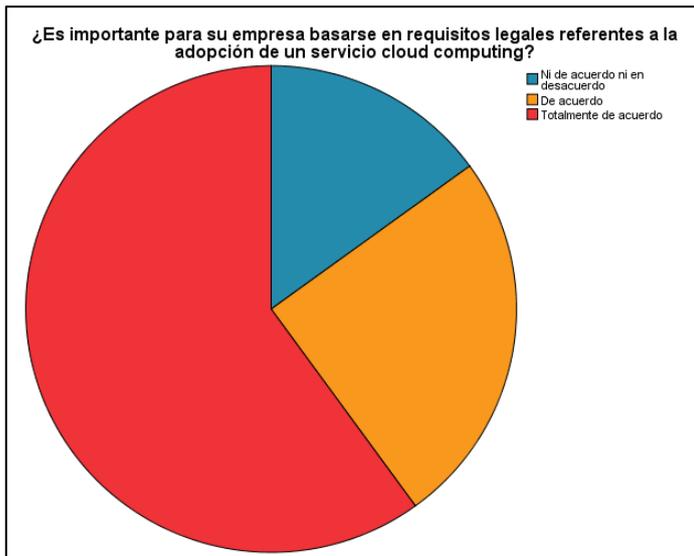
Figura 33. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en los requisitos legales referentes a la adopción de un servicio cloud computing

¿Es importante para su empresa basarse en requisitos legales referentes a la adopción de un servicio cloud computing?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Ni de acuerdo ni en desacuerdo	3	15,0	15,0	15,0
	De acuerdo	5	25,0	25,0	40,0
	Totalmente de acuerdo	12	60,0	60,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 34. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en los requisitos legales referentes a la adopción de un servicio cloud computing expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Como resultados de este análisis de la variable cumplimiento respecto a la primera interrogante planteada se obtuvo que el 60% y 25% de los encuestados asegura estar **totalmente de acuerdo** y **de acuerdo** con que es esencial que se cumpla con los requisitos legales en la adopción de un servicio de cloud computing, lo cual en escala Likert equivale a 4 y 5 puntos. Por otra parte, un 15% de los encuestados asegura **ni de acuerdo ni en desacuerdo** con que se cumpla con estos requisitos.

Con los resultados obtenidos se llega a la conclusión de que la mayoría de las PYMES desean innovar aplicando la tecnología cloud computing como parte de su seguridad de la información, no obstante, la responsabilidad que la adopción de la misma acarrea, así como sus aspectos legales, aún no son compartidos por todas las empresas.

¿Considera importante el que se realicen revisiones de seguridad de la información en su empresa?

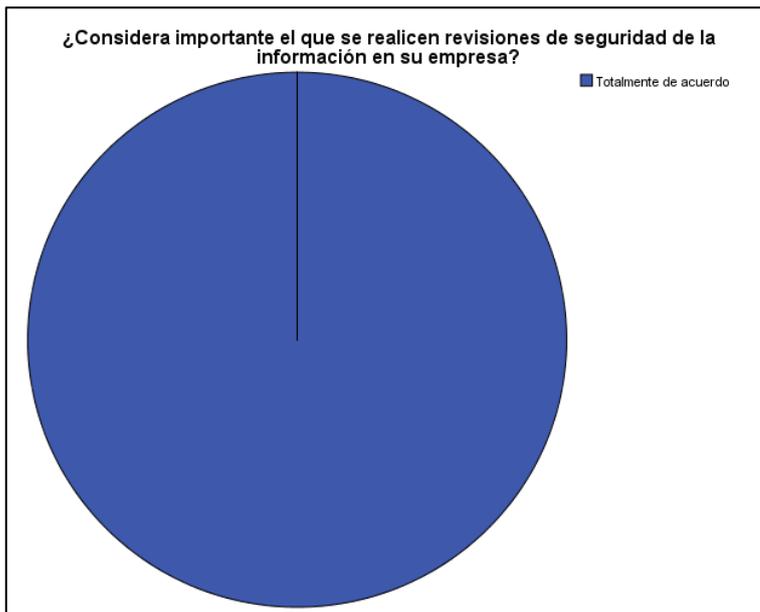
Figura 35. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en las revisiones de seguridad de la información en la empresa.

¿Considera importante el que se realicen revisiones de seguridad de la información en su empresa?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Totalmente de acuerdo	20	100,0	100,0	100,0

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 36. Nivel de importancia de las PYMES en cuanto al cumplimiento basado en las revisiones de seguridad de la información en la empresa expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

En base al análisis de la segunda interrogante de la variable cumplimiento se obtuvo un 100% respuestas de parte de los encuestados afirmando estar totalmente de acuerdo con que se realicen revisiones de seguridad de la información en las PYMES, ya que esto ayuda a garantizar el que se cumplan las políticas de seguridad establecidas.

3.1.9. Análisis de la variable despliegue en base al grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada, recursos compartidos en la nube, para el uso de gestión documental aplicada en la tecnología cloud computing.

¿Hace uso frecuente de varios servicios de forma pública y otros de forma privada?

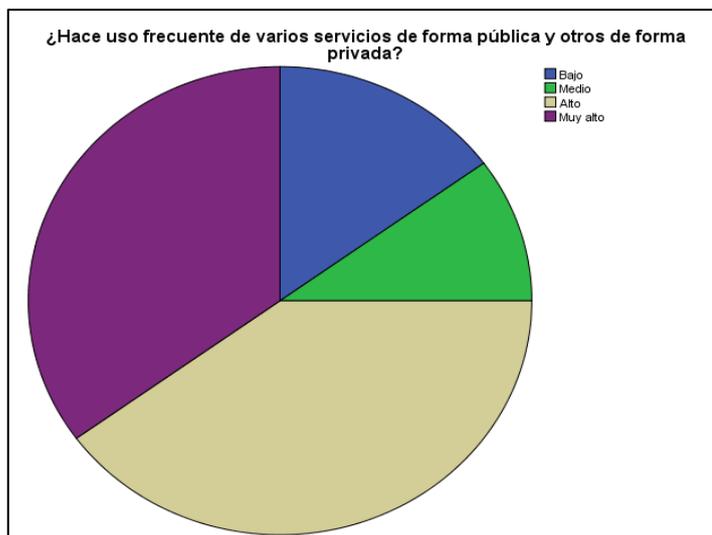
Figura 37. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada

¿Hace uso frecuente de varios servicios de forma pública y otros de forma privada?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Bajo	3	15,0	15,0	15,0
	Medio	2	10,0	10,0	25,0
	Alto	8	40,0	40,0	65,0
	Muy alto	7	35,0	35,0	100,0
	Total	20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 38. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada expresado en gráfico de pastel.



Fuente: Datos de la investigación

Elaborado por: El autor a través de spss

Para el análisis de la última variable despliegue se obtuvo los siguientes resultados en base a la interrogante planteada. Un 75% de los encuestados afirman hacer un uso muy alto y alto de los servicios públicos y privados de la empresa, lo que en escala Likert equivale a un 35% de **totalmente de acuerdo** con 5 puntos, y un 40% **de acuerdo** con 4 puntos. Por otra parte, el 25% de encuestados restantes asegura que le da una usabilidad media y baja, lo que en escala Likert equivale a un 10% de **ni de acuerdo ni en desacuerdo** con 3 puntos y 15% **en desacuerdo** con 2 puntos.

Por consiguiente, en base a los resultados obtenidos se puede determinar que la mayoría de las PYMES hacen uso de servicios de índole pública y privada en su gestión de trabajo.

¿Hace uso frecuente de recursos informativos compartidos en la nube?

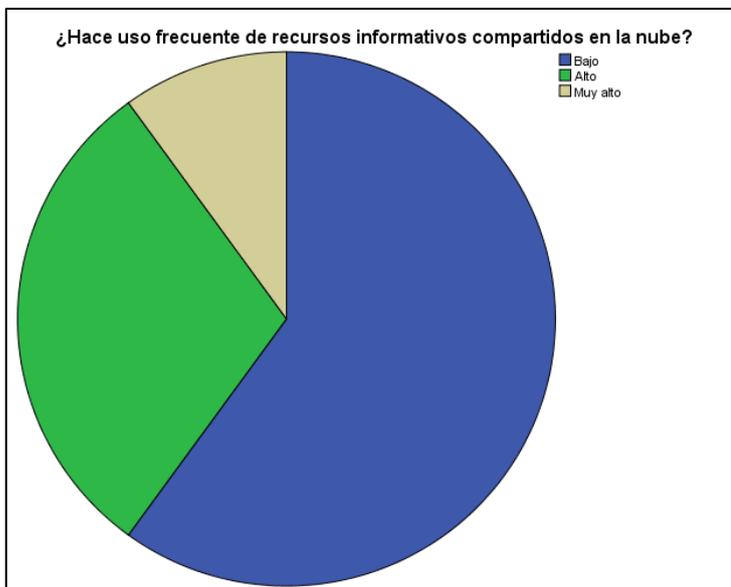
Figura 39. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: servicios de forma pública y privada expresado en gráfico de pastel

¿Hace uso frecuente de recursos informativos compartidos en la nube?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Bajo	12	60,0	60,0	60,0
	Alto	6	30,0	30,0	90,0
	Muy alto	2	10,0	10,0	100,0
Total		20	100,0	100,0	

Fuente: Datos de la investigación

Elaborado por: El autor a través de SPSS

Figura 40. Nivel de importancia de las PYMES en cuanto al despliegue basado en el grado de utilización de la tecnología cloud en la empresa: recursos informativos compartidos en la nube expresado en gráfico de pastel



Fuente: Datos de la investigación

Elaborado por: El autor a través de spss

En la segunda interrogante correspondiente a la variable despliegue se obtuvo que el 60% de los encuestados afirman que hacen un uso bajo de recursos

compartidos en la nube, lo cual en escala Likert equivale a estar **en desacuerdo** con 2 puntos; por consiguiente, un 40% de los encuestados aseguró que hace un uso muy alto y alto de recursos compartidos, que en escala Likert equivale a un 10% de **totalmente de acuerdo** con 5 puntos y un 30% **de acuerdo** con 4 puntos.

Con base en este último análisis se llega a la conclusión de que aún existe un gran porcentaje de PYMES que no trabajan sus recursos a través de compartición en la nube, lo cual realmente ayudaría a evitar pérdidas de información importante para la empresa.

3.3. Conclusiones

De acuerdo con el primer objetivo específico, dentro de esta investigación se analizó las principales causas del que exista poco interés en cuanto a la inversión de servicios de computación en la nube por parte de los gerentes y altos directivos de las distintas organizaciones, de lo cual se pudo determinar que esto se debe a la desconfianza y poca acogida que ha tenido este tipo de tecnología en lo que lleva en el mercado, puesto que para algunos pasa desapercibida gracias a su poca aceptación. Además de que la mayoría afirma que prefieren usarla para temas que no tengan que ver con la seguridad en la organización, puesto que aún el cloud computing se encuentra en una etapa de crecimiento, que sin duda debe ser probada mucho más antes de ser utilizada en procesos de seguridad organizacional.

En cuanto al segundo objetivo específico, en el cual se hace referencia a la medición del impacto y sus causas al no contar con el cloud computing, se pudo obtener que la carencia del mismo podría llegar a ocasionar que en el caso de empresas dedicadas a el manejo de información pura o gestión documental, no cuenten con un respaldo que pueda garantizar la disponibilidad y permanencia de la información en un 100%, no obstante, este comentario difiere de un porcentaje minoritario de empresas, que considera que el hacer uso de los servicios es importante, pero como tal no necesario para que llegue a ocasionar problemas de pérdidas de información.

Por otro lado, respecto al tercer objetivo específico, se pudo identificar también que existe un porcentaje medio que asegura que el hacer uso de la tecnología de la computación es considerado como una oportunidad de crecimiento y competitividad en el mercado actual. Para algunas empresas el que se cuente con este servicio significa querer optimizar recursos físicos y económicos, puesto que gracias a esta tecnología se puede llevar una gran cantidad de información para ser alojada en la nube, donde siempre estará disponible y libre de riesgos de pérdida o alteración de integridad de la misma.

En cuanto al último objetivo específico, al utilizar servicios de cloud computing, hay varios aspectos de seguridad de la información que se deben considerar

para garantizar la protección adecuada de los datos. Aquí hay algunos aspectos importantes que deben ser tomados en cuenta, como:

1. **Transformación Digital Acelerada:** La adopción de servicios de Cloud Computing ofrece a las organizaciones la posibilidad de impulsar su transformación digital al permitirles escalar, innovar y colaborar de manera más eficiente. La flexibilidad y agilidad de la nube son fundamentales para mantenerse competitivos en un entorno empresarial en constante cambio.
2. **Equilibrio entre Beneficios y Riesgos:** Si bien los beneficios económicos, la escalabilidad y la eficiencia operativa son evidentes en la adopción de la nube, es crucial reconocer y abordar los desafíos de seguridad asociados. Las organizaciones deben encontrar un equilibrio adecuado entre aprovechar los beneficios de la nube y mitigar los riesgos de seguridad.
3. **Responsabilidad Compartida:** La seguridad en la nube es una responsabilidad compartida entre el proveedor y el cliente. Si bien los proveedores de servicios de nube implementan medidas de seguridad sólidas, los usuarios también tienen la responsabilidad de aplicar las mejores prácticas de seguridad y comprender cómo proteger adecuadamente sus datos y aplicaciones.
4. **Planificación Estratégica:** La decisión de migrar a la nube debe ser el resultado de una planificación estratégica cuidadosa. Las organizaciones deben evaluar cuidadosamente sus necesidades, objetivos y requisitos de seguridad antes de embarcarse en la adopción de la nube. Una estrategia bien definida asegurará una migración exitosa y reducirá los riesgos potenciales.
5. **Educación y Concienciación Continua:** La educación y la concienciación son elementos esenciales para garantizar la seguridad en la nube. Las organizaciones deben invertir en la formación de su personal, tanto en el uso adecuado de los servicios en la nube como en la comprensión de las consideraciones de seguridad. La formación continua ayudará a prevenir amenazas y a mantener una postura de seguridad sólida.
6. **Evaluación Rigurosa de Proveedores:** Antes de elegir un proveedor de servicios de nube, es fundamental llevar a cabo una evaluación rigurosa de su historial de seguridad, certificaciones y medidas de protección

implementadas. Tomar decisiones informadas sobre proveedores garantizará una asociación segura y confiable.

7. **Enfoque Holístico de Seguridad:** Las consideraciones de seguridad en la nube no deben limitarse solo a la tecnología, sino que deben abarcar procesos, políticas y cultura organizacional. Un enfoque holístico de la seguridad permitirá a las organizaciones abordar de manera efectiva los desafíos de seguridad en un entorno de nube en constante evolución.

Finalmente se llegó a la conclusión de que la tecnología cloud computing, así como los sistemas de información son vistos actualmente por las PYMES como una oportunidad de crecimiento y mejora en su productividad, no obstante, siempre existirán factores como la desconfianza y la poca aceptación debido a ser una tecnología reciente en el mercado, y realmente resulta ser la verdadera razón por la cual muchas organizaciones solo afirman que este tipo de tecnologías son de gran ayuda, pero no demasiado necesarias como para confiar todos los años de operatividad interna y externa de la empresa.

En resumen, la adopción de servicios de Cloud Computing ofrece una serie de beneficios significativos para las organizaciones, pero también implica desafíos de seguridad que deben ser abordados de manera proactiva y estratégica. Al comprender y equilibrar cuidadosamente los factores para la adopción de la nube con las consideraciones de seguridad de la información, las organizaciones pueden aprovechar al máximo las ventajas de la nube mientras protegen sus activos y datos críticos.

3.4. Recomendaciones

El cloud computing al ser tomado como iniciativa de adopción por las empresas debería considerar que se garantice la seguridad de la información, por esta razón se recomienda que sea aplicado en sistemas que estén dispuestos a la optimización de información y que los datos que sean manejados no sean de un nivel de alta criticidad, y de esta forma lograr asociarse de manera más asertiva con la tecnología de computación en la nube.

Algunas recomendaciones clave que podrían derivarse de la investigación sobre la adopción de servicios de Cloud Computing y las consideraciones de seguridad de la información serían las siguientes:

1. **Realizar una Evaluación Integral:** Antes de migrar a la nube, lleva a cabo una evaluación exhaustiva de tus necesidades, objetivos y requisitos de seguridad. Comprende cómo los servicios en la nube pueden beneficiar a tu organización y cómo abordar los riesgos potenciales.
2. **Planificar Estratégicamente:** Desarrolla una estrategia sólida para la adopción de la nube que incluya la selección de proveedores, la planificación de migración, las políticas de seguridad y los procesos de gestión. Un enfoque estratégico minimizará los problemas y optimizará los resultados.
3. **Educación Continua:** Proporciona capacitación y concienciación constante a tu personal sobre las mejores prácticas de seguridad en la nube. Asegúrate de que comprendan las políticas de seguridad, la gestión de identidad y acceso, y los protocolos de respuesta a incidentes.
4. **Establecer Responsabilidades Claras:** Define las responsabilidades tanto del proveedor de la nube como de tu organización en términos de seguridad. Entiende la división de la responsabilidad compartida y asegúrate de que ambas partes cumplan con sus compromisos.
5. **Implementar Controles de Seguridad:** Utiliza medidas de seguridad robustas, como autenticación de múltiples factores, cifrado de datos en tránsito y en reposo, y sistemas de detección de intrusiones. Adapta los controles según las necesidades de tu organización y las regulaciones aplicables.
6. **Auditoría y Monitoreo Constante:** Establece sistemas de auditoría y monitoreo para detectar actividades anómalas y posibles amenazas. Mantén

un registro de eventos y asegúrate de que esté disponible para una revisión en caso de incidentes.

7. **Realizar Pruebas de Resiliencia:** Pon a prueba la resiliencia de tus sistemas en la nube mediante simulaciones de ataques y pruebas de recuperación ante desastres. Esto te permitirá identificar posibles debilidades y fortalecer tu postura de seguridad.
8. **Adoptar un Enfoque Gradual:** Si es posible, considera una migración gradual a la nube, comenzando con cargas de trabajo menos críticas. Esto te permitirá ganar experiencia y abordar problemas de seguridad de manera más manejable.
9. **Actualizar Políticas y Procedimientos:** Revisa y actualiza regularmente las políticas y procedimientos de seguridad para asegurarte de que estén alineados con las últimas amenazas y mejores prácticas.
10. **Colaborar con Expertos:** En caso de dudas o desafíos específicos, busca asesoramiento de expertos en seguridad en la nube. Puedes considerar la contratación de profesionales de seguridad cibernética o consultores especializados.
11. **Mantenerse al Día:** La tecnología de la nube y las amenazas de seguridad evolucionan constantemente. Mantente informado sobre las últimas tendencias y actualizaciones en seguridad en la nube para adaptarte a los cambios.

Al considerar estas recomendaciones, se estará mejor preparado para adoptar servicios de Cloud Computing de manera efectiva y segura, maximizando los beneficios y minimizando los riesgos asociados. Hay que recordar que la seguridad en la nube es un esfuerzo continuo que requiere atención constante y adaptación a medida que evoluciona el panorama de seguridad cibernética.

La seguridad de la información es una consideración importante al utilizar servicios de cloud computing. Las empresas deben tomar medidas para garantizar que sus datos estén protegidos en todo momento, desde la autenticación y encriptación hasta la monitorización de la seguridad y la evaluación del proveedor de servicios.

El presente trabajo de investigación tiene como finalidad servir de aporte en futuros estudios y proyectos, por lo que se recomienda considerar cada uno de los aspectos y variables analizadas para poder proponer estrategias, técnicas y controles de acceso a servicios y aplicaciones relacionados al cloud computing.

REFERENCIAS BIBLIOGRÁFICAS

- Abad, C., Villavicencio, M., Boza, E., & Ortega, G. (2017). *La adopción de computación en la nube en Ecuador*. Guayaquil: ESPOL.
- AC3 - Clarity in the Cloud. (05 de 2022). *Cloud computing survey 2022*. Obtenido de <https://www.ac3.com.au/resources/cloud-computing-survey-2022>
- Andrade Garda, J., Célleri Pacheco, J., & Rodríguez Yáñez, S. (2018). *Cloud Computing para PYMES*. Machala: UTMACH.
- Asociación Española para la Calidad (AEC). (03 de Diciembre de 2021). *AEC - COBIT*. Recuperado el 2021, de <https://www.aec.es/web/guest/centro-conocimiento/cobit>
- ATS Gestión documental. (4 de marzo de 2019). *¿Qué es un software de gestión documental?* Recuperado el 1 de marzo de 2022, de <https://atsgestion.net/que-es-software-gestion-documental/>
- Baena-Luna, P., Palos-Sanchez, P., Garcia-Rio, E., & Casablanca Peña, A. (2018). La importancia del uso de recursos en la nube para el favorecimiento del emprendimiento corporativo en empresas y organizaciones. *International Journal of Information Systems and Software Engineering for Big Companies (IJISEBC)*, 87-98.
- Célleri-Pacheco, J., Andrade-Garda, J., & Rodríguez-Yáñez, S. (2018). *Cloud Computing para PYMES*. Machala: UTMACH.
- Ciberseguridad. (06 de 2022). *ciberseguridad.com*. Obtenido de ¿QUÉ ES SHADOW IT? DEFINICIÓN, RIESGOS Y EJEMPLOS: https://ciberseguridad.com/guias/recursos/shadow-it/#Riesgos_asociados_con_Shadow_IT
- CloudFlare. (03 de 2023). *CloudFlare*. Obtenido de ¿Qué es la Shadow IT?: <https://www.cloudflare.com/es-es/learning/access-management/what-is-shadow-it/>
- Cobas, J., Romeu, A., & Macías, J. (Marzo de 2018). *LA INVESTIGACIÓN CIENTÍFICA COMO COMPONENTE DEL PROCESO FORMATIVO DEL LICENCIADO EN CULTURA FÍSICA*. *Revista eletronica de ciencia e innovacion tecnologica en el deporte*. Recuperado el 24 de febrero de 2022, de <http://dialnet.unirioja.es>
- Coello-Yagual, R. R., & Pico-Versosa, L. M. (15 de Abril de 2018). Análisis de las ventajas y desventajas del sistema de gestión de la seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador. *INNOVA Research Journal*, 181-195.
- Cunha Barbosa, D. (20 de Ago de 2020). *Welivesecurity By ESET*. Obtenido de <https://www.welivesecurity.com/la-es/2020/08/20/shadow-it-que-es-riesgos-puede-causar-empresa/>

- DATTA Business Innivation. (21 de 11 de 2021). *Cloud Computing en la era post Covid-19*. Obtenido de <https://datta.com.ec/noticias/revista/cloud-computing-en-la-era-post-covid-19>
- Descom.es. (s/f). *DIFERENCIA ENTRE HOSTING TRADICIONAL Y CLOUD COMPUTING?* Recuperado el 24 de febrero de 2022, de <https://www.descom.es/blog/cloud/diferencia-entre-hosting-tradicional-y-cloud-computing.html>
- Diario El Universo. (21 de 11 de 2022). *La automatización y la nube marcan el mundo pospandemia*. Obtenido de <https://www.eluniverso.com/larevista/tecnologia/la-automatizacion-y-la-nube-marcan-el-mundo-postpandemia-nota/>
- Dzul, M. (2019). *Aplicación básica de los métodos científicos. Los enfoques en la investigación científica*. Recuperado el 24 de febrero de 2022, de https://www.uaeh.edu.mx/docencia/VI_Presentaciones/licenciatura_en_mercadotecnia/fundamentos_de_metodologia_investigacion/PRES39.pdf
- Efficy. (2022). *Escala likert: Qué es y cómo puedes usarla en tu empresa*. Recuperado el 24 de febrero de 2022, de <https://www.efficy.com/es/escala-likert/>
- Evaluando Cloud. (2022). *Sistemas operacionales o aplicaciones en el Cloud Computing*. Recuperado el 1 de marzo de 2022, de <https://evaluandocloud.com/sistemas-operacionales-aplicaciones-cloud-computing/>
- Figueroa-Morán, G. L., Paladines-Morán, J. P., Paladines-Morán, J. N., Caicedo-Plúa, C. R., & Romero-Castro, M. I. (2018). *Modelo de plan estratégico de sistemas para la gestión y organización a través de una Plataforma Informática*. Manabi: ALICANTE.
- Figueroa-Suárez, J., Rodríguez-Andrade, R., Bone-Obando, C., & Saltos-Gómez, J. (12 de 2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, 145-155.
- Fustillos-Chimborazo, E. G. (2021). *MOOC para formar auditores de seguridad de la información basado en la norma ISO 27000*. Quito: UNIVERSIDAD TECNOLÓGICA ISRAEL.
- IDC. (2021). IDC Latin America Public & Private Cloud Services Tracker .
- IDC. (7 de 12 de 2022). *IDC Latin*. Obtenido de IDC FutureScape 2022: Predicciones e implicaciones en Latinoamérica: https://www.idc.com/latam_es
- Ilyas Malik, M., Rashid, A., & Hussain Wani, S. (2018). *CLOUD COMPUTING-TECHNOLOGIES*. Punjab: International Journal of Advanced Research in Computer Science.
- ISOTools Excellence. (26 de 01 de 2018). *Blog especializado en Sistemas de Gestión*. Recuperado el 03 de 12 de 2021, de ¿Seguridad informática o seguridad de la información?: <https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/>

- León-Acurio, J., Mora-Aristega, J., Huilcapi-Masacón, M., Tamayo-Herrera, A., & Armijos-Maya, C. (Abril de 2018). COBIT como modelo para auditorías y control de los sistemas de información. *Polo del Conocimiento*, 17-36.
- Lopez Inga, M. E., & Guerrero Huaranga, R. M. (2018). Modelo de inteligencia de negocios y analítica en la nube para pymes del sector retail en Perú. *Ingeniería Solidaria*, 17.
- Molina Montero, B. (2020). *Modelo de Aceptación del Cloud Computing para el Despliegue de los Servicios de las Empresas Tecnológicas de la Ciudad de Machala*. Guayaquil: Universidad Tecnológica Empresarial de Guayaquil.
- Mosquera Rodríguez, X., Chilán Regalado, M. L., & Soledispa Rodríguez, X. E. (2018). Análisis de la información en la nube y su impacto en la seguridad y confiabilidad en las PyMES. *Revista Ciencia & Tecnología*, 141-155.
- Palos Sánchez, P. R. (2017). Estudio organizacional del Cloud Computing en empresas emprendedoras. *Congreso Internacional Online Sobre Economía, Empresas y sociedad* (págs. 48-49). Alicante: 3ciencias.
- Palos-Sanchez, P., Reyes-Menendez, A., & Ramon-Saura, J. (2019). Modelos de Adopción de Tecnologías de la Información y Cloud Computing en las Organizaciones. *Información Tecnológica*.
- Phun, E. (06 de 07 de 2022). *iT Ahora*. Obtenido de Crecimiento de la nube pública y privada en Latinoamérica: <https://itahora.com/2022/07/26/crecimiento-de-la-nube-publica-y-privada-en-latinoamerica/>
- Pinargote, B., & Townsend, J. (2021). Incidencias de las Normas ISO en la Seguridad Informática para la protección de datos usada por proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil. *UTEG*, 31-32.
- Reyes, M., & Castañeda, P. (2022). Aplicación del Modelo de Aceptación Tecnológica en Sistemas de Información de la Administración Pública del Perú. *Revista Peruana de Computación y sistemas*, 15-22.
- Salto-Ramírez, E. M. (2021). La seguridad informática en la adopción del cloud computing en la información del sector industrial. *Revista Ciencia & Tecnología*, 57-71.
- Srivastava, P., & Khan, R. (2018). A Review Paper on Cloud Computing. *International Journals of Advanced Research in Computer Science and Software Engineering*, 17-20.
- Sunyaev, A. (2020). *Internet Computing*. Germany: Springer.
- Técnicas de Investigación. (27 de febrero de 2020). *¿Qué es una investigación exploratoria y sus características?* Recuperado el 24 de febrero de 2022, de <https://tecnicasdeinvestigacion.com/investigacion-exploratoria/>
- Vanguardista OnLine. (03 de 2023). *Nube pública, privada o híbrida*. Obtenido de <https://elvanguardistaonline.com/nube-publica-privada-o-hibrida/>

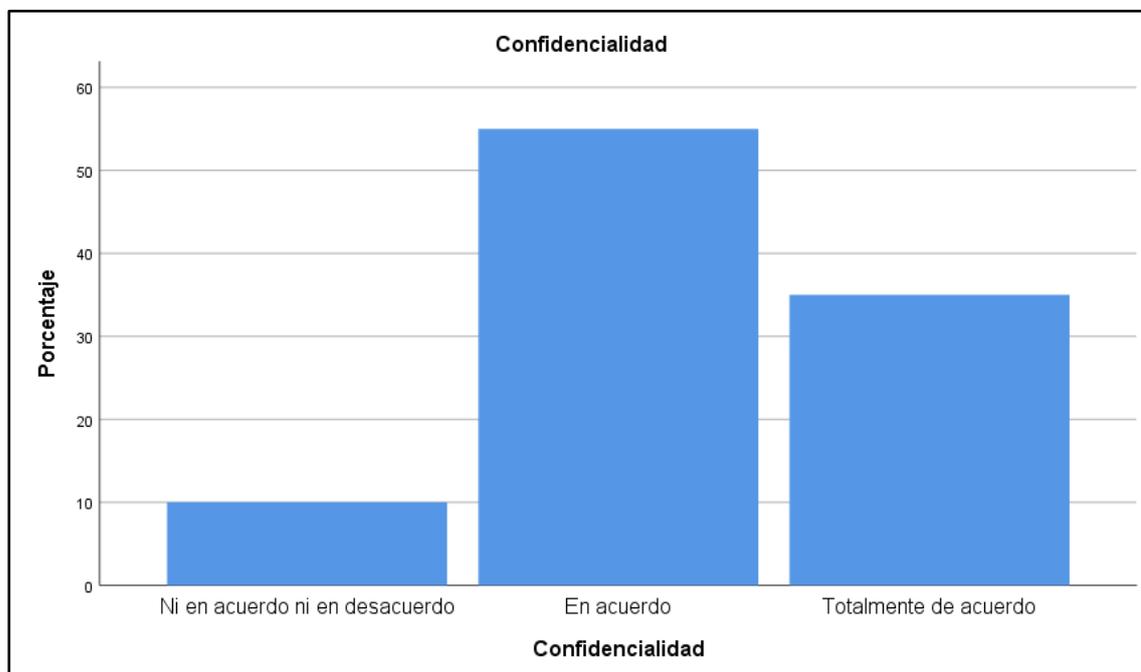
Zabala, J., Rio, R., Cilleruela, E., Garechana, G., & Gavilanes, J. (2018). *Beneficios del Cloud Computing para la Pequeña y Mediana Empresa*. • Vol. 88 nº3. Recuperado el 24 de febrero de 2022, de https://www.researchgate.net/profile/Rosa-Rio-Belver/publication/278376226_Benefits_of_Cloud_Computing_for_Small_and_Medium_Enterprises/links/5abfcf050f7e9bfc045bed45/Benefits-of-Cloud-Computing-for-Small-and-Medium-Enterprises.pdf

Anexos

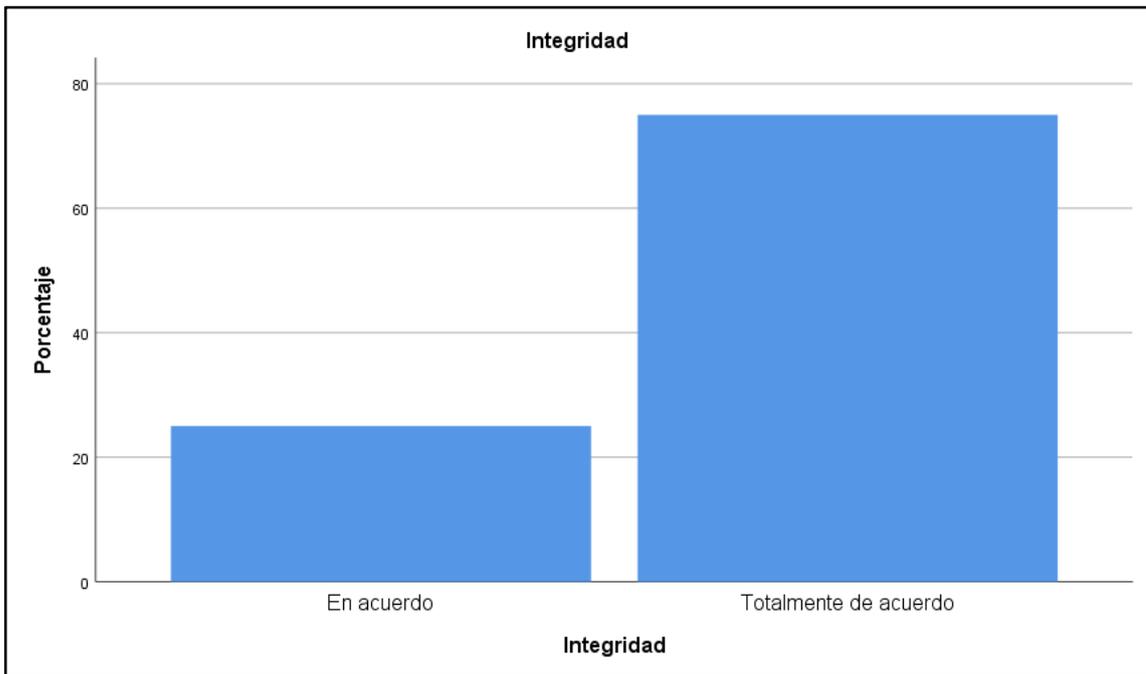
Anexo 1: Data obtenida de la base de datos INEC

Tamaño de Empresa	Número de empresas		
	Total	Realizan transacciones a través de Internet	Porcentaje
TOTAL	3.245	541	17%
MICROEMPRESA	57	6	11%
PEQUEÑA EMPRESA	838	96	11%
MEDIANA EMPRESA A	443	83	19%
MEDIANA EMPRESA B	752	147	20%
GRANDE EMPRESA	1.155	209	18%

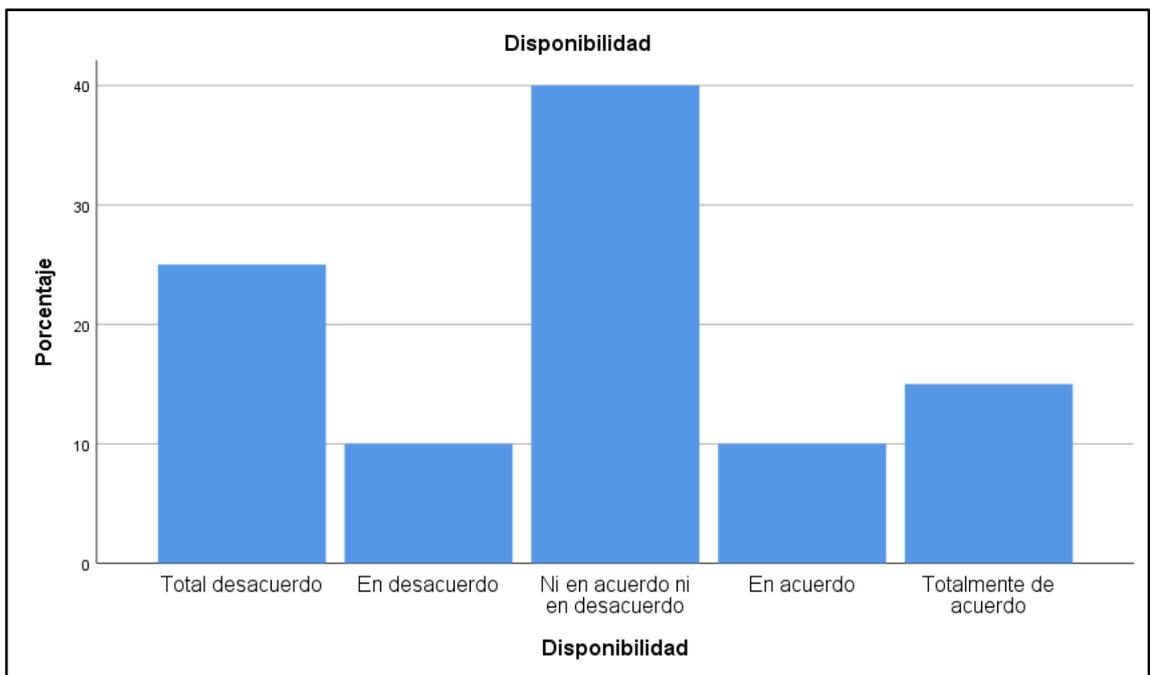
Anexo 2: Análisis gráfico de dimensión confidencialidad



Anexo 3: Análisis gráfico de dimensión Integridad



Anexo 3: Análisis gráfico de dimensión disponibilidad



Anexo 4: Formato de Encuesta

CUESTIONARIO DIRIGIDO A LAS PYMES DEL CANTÓN MILAGRO	
Objetivo de Estudio:	
Identificar los factores para la adopción del cloud computing y sus consideraciones de seguridad de la información en las Pymes del cantón Milagro.	
Sección General	
1	Sexo:
	Edad:
2	Instrucciones
Responda los enunciados según la escala que se presenta en cada ítem	

		ASPECTOS	ESCALA				
SERVICIO	1	¿Esta de acuerdo usted en la elección del servicio de cloud computing como modelo de negocio?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
	2	¿Considera usted que los sistemas operativos como Linux son una opción segura para manejar la información?	Si	No			
	3	¿Considera usted a las aplicaciones ofimáticas como apoyo a la seguridad de los documentos?	Si	No			
	4	¿Considera usted que el uso de otros tipos de software como parte de la seguridad de la empresa?	Si	No			
	5	¿Cómo considera usted el uso de los servicios de almacenamiento utilizado por la empresa?	1	2	3	4	5
	[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto						
GARANTÍA	6	¿Cómo considera usted el uso de los servicios de servidores utilizado por la empresa?	1	2	3	4	5
	[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto						
	7	¿Servicio de correo electrónico utilizado por la empresa?	1	2	3	4	5
		[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto					
GOBERNANZA	8	¿Está de acuerdo usted con la garantía de la seguridad de la información en dimensión de confidencialidad?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
	9	¿Está de acuerdo usted con la Garantía de la seguridad de la información en dimensión de Integridad?	1	2	3	4	5
		[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo					
GOBERNANZA	10	¿Está de acuerdo usted con la Garantía de la seguridad de la información en dimensión de Disponibilidad?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
GOBERNANZA	11	¿Está de acuerdo usted con el nivel de importancia de políticas y estándares de seguridad en la empresa?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
GOBERNANZA	12	¿Cómo considera usted el nivel de importancia de las normas ISO 27001 y 27002 en la seguridad de la empresa?	1	2	3	4	5
	[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto						
ACCESO	13	¿Considera importante aplicar un mecanismo de autenticación para validar el uso de Password, validaciones mediante emails u otros como medida de seguridad mediante el uso del cloud computing?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
ACCESO	14	¿Considera que se debe validar la autenticación de los usuarios antes de permitir el acceso a un recurso de la organización?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
GESTION DE RIESGOS	15	¿Cree usted que es importante el que se implemente una estrategia que ayude a mitigar los riesgos para mejorar la seguridad de la información en la empresa?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
	16	¿Considera que se debería emplear técnicas y procedimientos para el monitoreo y control de la seguridad de la información?	1	2	3	4	5
		[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo					
GESTION DE RIESGOS	17	¿Cree que sería de aporte a la seguridad de la información el contar con un marco de referencia para la auditoría y evaluación como ISO 27001-27002?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
CUMPLIMIENTO	18	¿Es importante para su empresa basarse en requisitos legales referentes a la adopción de un servicio cloud computing?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
CUMPLIMIENTO	19	¿Considera importante el que se realicen revisiones de seguridad de la información en su empresa?	1	2	3	4	5
	[1] - En total desacuerdo [2] - En desacuerdo [3] - Ni desacuerdo Ni en desacuerdo [4] - De acuerdo [5] - Totalmente de acuerdo						
DESPLIEGUE	20	¿Hace uso frecuente de varios servicios de forma pública y otros de forma privada?	1	2	3	4	5
	[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto						
DESPLIEGUE	21	¿Hace uso frecuente de recursos informativos compartidos en la nube?	1	2	3	4	5
	[1] - Muy Baja [2] - Baja [3] - Medio [4] - Alto [5] - Muy alto						