República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil - UTEG
Facultad de Estudios de Postgrado

Tesis en Opción al título de Magister en:
Sistemas de Información Gerencial

Tema de Tesis:

Factores que Inciden en la Seguridad Informática y Aplicabilidad en el Cloud Computing de las Empresas del Sector Industrial en la Ciudad de Manta, Provincia de Manabí

Autor:
Ing. Evelin María Saltos Ramírez

Director de Tesis:
PHD. José EnriqueTownsend Valencia, Msc.

Septiembre 2018

Guayaquil - Ecuador

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Graduación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la **"UNIVERSIDAD TECNOLÓGICA EMPRESARIAL DE GUAYAQUIL".**

(Reglamento de Graduación de la UTEG)

_____

Ing. Evelin María Saltos Ramírez

CI. 1311998957

DEDICATORIA

A Dios que derrama sobre mi bendiciones y me permite despertar día a día para luchar y cumplir mis objetivos.

A mi Madre, por ser mi luz y mejor amiga que me ha ayudado a crecer como persona y que ha estado en todo momento conmigo siempre apoyándome en las decisiones que he tomado. Doy gracias infinitas por todo tu amor incondicional, por la paciencia que tienes para hacerme ver las cosas diferentes, por tus cuidados, por las lecciones de vida. Gracias Mamá por estar ahí siempre.

A mi hermana, mi amiga, mi confidente que con su amor y sus consejos me han enseñado a no detenerme y ser firme en mis convicciones. Gracias por estar en otro momento tan importante en mi vida.

A mi padre, por enseñarme a ser una gran persona que siempre he podido salir adelante y conseguir lo que me he propuesto.

A mis amigos y compañeros, Nohelia y Luis, por permanecer juntos en este camino, ayudándonos mutuamente en todo el proceso.

A Eduardo, mi compañero, mi amigo, que ha sabido acompañarme en este camino, siendo paciente y también por estar presente en todo el proceso.

Con esfuerzo y dedicación para todos los que creyeron en mí.

Evelin María Saltos Ramírez

AGRADECIMIENTO

Este trabajo de tesis es el resultado de un gran esfuerzo en el cual participaron distintas personas mediante opiniones y colaboración en el desarrollo de la misma, siempre inyectándome ánimo y acompañando en los momentos difíciles.

Mi agradecimiento a la Universidad Tecnológica Empresarial de Guayaquil, alma máter donde tuve la oportunidad de adquirir nuevos conocimientos para ser aplicados en mi entorno laboral y profesional.

Al Doctor José Townsend Director y Tutor de tesis, Docente universitario por su ayuda, consejos, conocimientos y experiencia; sobre todo por su valioso tiempo dedicado a este trabajo de tesis.

En general agradezco a todas las empresas que de alguna manera apoyaron con el acceso a la información requerida para cumplir los objetivos planteados en esta tesis.

Finalmente, un agradecimiento especial a mi madre y hermana por recibir siempre su apoyo incondicional.

Evelin María Saltos Ramírez

RESUMEN

El presente trabajo de investigación abarca temas sobre la aplicabilidad del cloud computing, la manera en la que incide en la seguridad informática del sector industrial de la ciudad de Manta, se estudia la incidencia de dichos factores, aportando a la aplicabilidad de cloud computing mediante el modelo adecuado para el sector industrial de la ciudad de Manta Provincia de Manabí.

La investigación se fundamenta en las normas, estándares y mecanismos de seguridad de la información e informática, tomando características específicas de las normas técnicas ISO, Estándar Cloud Security Alliance Cloud Controls Matrix, y demás autores; se analizó las variables intervinientes como la garantía, gobernanza, identidad y control de acceso, gestión de riesgos, servicio, despliegue, cumplimiento, producto del modelo definido para la seguridad informática y aplicabilidad de cloud computing.

Se basa en un tipo de estudio descriptivo – correlacional; se aplica los métodos inductivo, analítico, sintético; se utiliza además las técnicas estadísticas, documental y de campo para la recolección de información en las industrias de la ciudad de Manta Provincia de Manabí.

Los resultados finales indicaron que las dimensiones integridad, confidencialidad, plataforma e infraestructura como servicio en un despliegue público, privado y comunitario según las diferentes aplicaciones que se utilicen, tienen mayor impacto en la investigación por lo que las industrias de la ciudad de Manta deben considerar su atención ante la disponibilidad, confidencialidad e integridad de la información aplicando tecnologías como el Cloud Computing.

Palabras claves: cloud computing, seguridad informática, normas, Matriz de controles en la nube, seguridad de la información.

ABSTRACT

The present research work covers topics about the applicability of cloud computing, the way in which affects the security of the industrial sector of the city of Manta, we study the impact of these factors, contributing to the applicability of cloud computing using the model suitable for the industrial sector of the city of Manta in Manabi province.

The research is based on the norms, standards and security mechanisms of information and computer science, taking the specific characteristics of the ISO standards, standard Cloud Security Alliance Cloud Controls Matrix, and other authors; discussed the intervening variables such as the warranty, governance, identity and access control, risk management, service, deployment, compliance, product of the model defined for computer security and applicability of cloud computing

Is based on a type of descriptive - correlational study; applies the methods of inductive, analytic, synthetic; in addition the statistical techniques used, documentary and field for the collection of information on the industries of the city of Manta, Manabí province.

The final results indicated that dimensions integrity, confidentiality, platform and infrastructure as a service in a public, private, and community deployment depending on the different applications used, have greater impact in research so that the city of Manta industries should consider your attention to availability, confidentiality and integrity of information by applying technologies such as Cloud Computing.

Key words: cloud computing, information security, standards, control array in the cloud, information security standards.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

La seguridad informática y aplicabilidad en el cloud computing tiene un gran impacto en todos los ámbitos de una organización, debido al uso de tecnologías de la información y comunicaciones con nuevas tendencias e innovación en la adquisición de tecnologías virtualizadas como lo es el servicio del cloud computing. Los problemas de seguridad en el cloud computing pueden acarrear grandes complicaciones, ya que la información es vital hoy día, sobre todo a nivel corporativo, la incongruencia o poca fiabilidad de esta puede generar grandes pérdidas, también se pueden presentar situaciones como el robo de información privada, caída o falla de los servicios en momentos críticos, pérdida de recursos, tanto a corto como a largo plazo y pérdida de control de las aplicaciones. (Joyanes 2009)

La seguridad informática en el cloud es un servicio que ha crecido rápidamente y promete numerosas funciones que ofrece la seguridad de TI tradicional. En esto se incluye la protección de la información crítica frente al robo, la filtración de los datos y la eliminación de los mismos. Asimismo al optar por los servicios en la nube se puede operar a escala y tener protección. En la actualidad existe una similitud en el modo que se administra la seguridad, aunque existen formas adicionales de proporcionar soluciones de seguridad para otros aspectos preocupantes. El concepto que encierra la seguridad de la tecnología cloud computing no modifica el punto de vista de la administración de seguridad relacionado a la prevención, detección y resolución, sin embargo permite realizar actividades más ágiles.

El almacenamiento de datos exige seguridad y la garantía de la protección de la información, mediante la incorporación de normas, estándares y buenas prácticas de TI en la gestión de la seguridad de la información que permitiría identificar, gestionar, minimizar y asumir los riesgos potenciales que pueden atentar contra las organizaciones de forma documentada, sistemática estructurada, eficiente para adaptarse a nuevos cambios.

CAPÍTULO I. MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes de la investigación

A nivel mundial han ocurrido muchos eventos relevantes en la historia de la informática y el Internet, paralelo a ese avance, fueron surgiendo los primeros ataques informáticos, siendo en la actualidad más sofisticados y difíciles de detectar. Conforme continúa el avance tecnológico y a medida se perfeccionen los dispositivos de comunicación, surge la necesidad a las empresas de mantener un mayor nivel de seguridad con base en los principios fundamentales de la seguridad informática (integridad, confidencialidad y disponibilidad).

Desde que surgió el Internet de forma globalizado a nivel empresarial, la Seguridad Informática adoptó la seguridad en la conectividad de redes, la protección de servidores de aplicaciones a través de Internet, controlando la seguridad a nivel física y lógica a través de diferentes dispositivos. Asimismo con el desarrollo tecnológico, la información ha tenido consecuencias debido a la existencia de usuarios que intentan la manera de vulnerar la información, con fines impropios; por esta misma razón las empresas han ido desarrollando y adoptando políticas de seguridad informática garantizando la continuidad de las operaciones.

En los años sesenta, las empresas y el gobierno utilizaban sistemas centralizados, los mainframe, las cuales eran grandes, costosas y pesadas. A finales de los años setenta, surgen en el mercado las microcomputadoras, lo que permitió tener otra visión de la tecnología informática. Para los años ochenta y noventa el concepto de seguridad informática se basaba en la protección de los equipos ante los usuarios. Se entendía como una seguridad lógica en la que intentaba evitar que los sistemas dejaran de funcionar, además se centraba en la protección contra los virus informáticos existentes (Ponniah, 2002).

Para los años noventa se popularizó el uso de los cajeros automáticos, dando origen a la computación en la nube, este servicio permitía al usuario acceder al

dinero y a otros servicios desde cualquier terminal, el uso de información en la red hace crecer dudas sobre los mecanismos de seguridad cayendo en manos equivocadas.

Actualmente, las buenas prácticas en seguridad de la información y el cumplimiento de normativas y además de estándares en seguridad, demandan una inversión considerable y necesaria en áreas funcionales como las tecnologías de información, con la finalidad de proveer de protección el activo de toda empresa, la información. De no hacerlo puede verse afectada por la presencia de vulnerabilidades dentro de sistemas informáticos junto a las redes de telecomunicaciones.

Se precisa la integración de Seguridad Informática basados en medidas técnicas y la Seguridad de la Información basada en medidas organizativas en momentos de intensa transformación al aplicar tecnologías actuales como el Cloud Computing, que sirvan para proteger los datos y el desarrollo eficiente de todos los procesos de la empresa.

Por ser tecnologías actuales se evidencia la poca información y desconocimiento por parte de algunos de los sectores que utilizan éstas tecnologías en donde pueden quedar expuestos a amenazas y ataques informáticos. No obstante, en Ecuador poco se conoce sobre los riesgos concernientes a la privacidad, causados por el continuo intercambio de información en la red. Menos todavía se ha investigado acerca de la percepción que existe sobre estos temas, y muy superficialmente se ha discutido acerca de la necesidad de legislación orientada a la protección de los datos.

En esta era tecnológica es necesario estar al tanto del estado de la seguridad a través de diferentes procedimientos como el análisis de riesgos que permitan identificar las principales amenazas y cuantificar los riesgos adjudicados, teniendo presente algunos factores importantes como el valor de la información, la probabilidad que una amenaza se presente, y el impacto que tendría sobre la empresa que se materialice.

1.2. Planteamiento del problema de investigación

El ser humano puede atentar contra la seguridad en cualquier entorno, debido a la presencia de vulnerabilidades en los entornos de TI, puede verse materializada en una amenaza; la creciente rentabilidad de los ataques han provocado en los últimos años un 70% el aumento de amenazas intencionales. De acuerdo a estudios de mercado el 63% de las empresas públicas y privadas pierden anualmente archivos de información valiosa, pero solo un 23% es por robo de datos. De la pérdida de información, un 75% se debe al extravío de equipos portátiles (Mieres, 2009).

Gonzáles (2016), por otro lado, menciona que las causas de falla de seguridad en la nube son de diversas causas, las principales por omisión y ataques directos, para el primer grupo se relaciona una mala conectividad, falta de tecnología o en estado obsoleto y pocos e inadecuados controles de mantenimiento, en el segundo grupo están los ocasionados de forma intencionada, como las medidas de seguridad y accesos vulnerados, ataques a la seguridad, insuficientes e inadecuado controles en seguridad. Por ello una de las principales amenazas que enfrenta toda organización a nivel mundial para proteger su información radica en la desconfianza de los sistemas ya que son muchas las causas y mecanismos que pueden incrementar con gran facilidad el daño o pérdida de la información Cloud Security Alliance (CSA, 2011).

Los problemas de seguridad en la nube pueden llevar a grandes complicaciones, la incongruencia o poca fiabilidad de esta puede generar pérdidas, presentar situaciones como el robo de información privada, caída o falla de los servicios en momentos críticos, pérdida de recursos, tanto a corto como a largo plazo y pérdida de control de aplicaciones (Joyanes, 2009).

El control de la seguridad en la nube es aplicable a diversos niveles y es recomendado llevarlo a cabo de forma personalizada para los servicios que allí se ejecuten, definiendo claros protocolos de seguridad, controles y auditorias periódicas, capacitación adecuada al personal a cargo e innovación en tecnología, es el aporte de Robles, Ramírez, Rodríguez, González y Gayo

(2014), quienes consideran la protección de datos personales, privacidad y seguridad, alineados a estándares y normas que regulen las nuevas tecnologías.

Hoy en día las empresas tienen varias alternativas para proteger la información de toda la organización, como es el caso del Cloud Computing, existen riesgos de que tanto su información como sus servicios se vean comprometidos, dentro de estos riesgos se puede encontrar en los más comunes: pérdida de información, pérdida de control directo de los servicios, no disponibilidad a la información en momentos críticos y extracción de información no autorizada (Gonzales, 2016).

SÍNTOMAS

- Falta de control en accesos a servicios y aplicaciones (CSA, 2011).
- Falta de seguridad y privacidad (Gonzales, 2016).
- Falla de los servicios y aplicaciones en línea (Joyanes, 2009).
- Divulgación de información confidencial (Mieres, 2009).

CAUSAS

- Presencia de ataques informáticos.
- Existencia de vulnerabilidades, tecnología obsoleta.
- No contar con soporte en los modelos de servicios.
- Ingeniería social.

PRONÓSTICO

- Pérdida de información.
- Medidas de seguridad y accesos vulnerados.
- Dependencia en el control de aplicaciones y servicios en línea.
- Reclamos de usuarios.

1.2.1. Formulación del problema

¿De qué manera incide la aplicabilidad de la tecnología cloud computing en la seguridad informática de las empresas del sector industrial en la ciudad de Manta de la provincia de Manabí?

1.2.2. Sistematización del problema

- ¿Es necesario que exista control de acceso a servicios y aplicaciones en el cloud computing?
- ¿Es indispensable para una organización la seguridad y privacidad de la información en todo momento?
- ¿Puede existir falla de los servicios y aplicaciones en el cloud computing?
- ¿Es posible ser víctimas de ataques informáticos debido a la divulgación de información confidencial?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

- Determinar los factores que inciden en la seguridad informática y su aplicabilidad en el cloud computing, para las empresas del sector industrial de la ciudad de Manta en la Provincia de Manabí.

1.3.2. Objetivos específicos

- Identificar los modelos de seguridad informática y analizar su aplicabilidad en el cloud computing.
- Establecer a partir del modelo seleccionado los riesgos informáticos, amenazas y vulnerabilidades.
- Evaluar los servicios que ofrece la tecnología del cloud computing para las empresas del sector industrial de la ciudad de Manta en la provincia de Manabí.

1.4. Justificación de la investigación

A través de la historia el hombre ha resguardado y protegido los conocimientos debido a la ventaja y poder que éste le producía sobre otros hombres o sociedades. En épocas pasadas aparecieron las bibliotecas, lugares donde se podía resguardar la información para trasmitirla y evitar que otros la obtuvieran, dando así algunas de las primeras muestras de protección de la información. Sun Tzu en el arte de la guerra y Nicolás Maquiavelo en el Príncipe, marcan el valor de la información sobre los enemigos y el íntegro conocimiento de sus propósitos para la toma de decisiones (Tescari, 2011).

Actualmente se vive la era tecnológica y de la información accediendo a la información en cualquier momento y lugar, sin embargo se expone a ataques y amenazas como los ataques informáticos en sistemas financieros, defensa nacional, el robo de datos, el fraude informático, entre otros. La seguridad ha sido uno de los primordiales problemas en el ambiente de transferencia de datos. Desde que está vigente la tecnología del Cloud Computing la seguridad es un punto focal, por la ubicación de los datos al ser diferente a la tradicional y que son gestionados por proveedores que suelen no otorgar garantías de confiabilidad (Gradiante, 2010).

Por lo tanto esa investigación sobre los factores que inciden en la seguridad informática ayudará a identificar el modelo apropiado identificando las teorías científicas sobre la seguridad informática y aplicabilidad en la tecnología cloud computing, y de esta manera responder a la pregunta de investigación planteada.

Es importante destacar los beneficios que se tiene con la implementación de seguridad en la nube para el desarrollo eficiente de las empresas, ya que la inversión en TI actualmente está tomando mayor importancia para el logro de objetivos dentro de la misma, además del mejoramiento de procesos, productos y servicios, teniendo ventaja competitiva, escalabilidad, reducción de costos en infraestructura y equipamiento tecnológico, y optimización.

1.5. Marco de referencia de la investigación.

1.5.1. Seguridad Informática.

1.5.1.1. Seguridad.

La seguridad se basa de tres principios fundamentales que forman parte de los objetivos que intentan comprometer los atacantes. Estos principios son la confidencialidad, la integridad y la disponibilidad de los recursos (Mieres, 2009).

Para Aguilera (2010) existen dos tipos de seguridad: activa que comprende el conjunto de medidas para evitar o mitigar riesgos que amenaza al sistema y pasiva que facilita la recuperación o restauración del sistema.

Se pueden encontrar diferentes definiciones sobre seguridad; en el cuadro 1.1 se hace referencia de algunas definiciones con los respectivos autores.

Cuadro No. 1.1 CONCEPTOS DE SEGURIDAD POR DIFERENTES AUTORES

Año	Autores	Conceptos definidos por el autor
2001	DRAE, 22 edición	Cualidad de seguro. (Mecanismo).- Que asegura un buen funcionamiento, precaviendo que éste falle, se frustre o se violente.
2009	Jorge Mieres	La seguridad consta de tres elementos que forman parte de los objetivos que intentan comprometer los atacantes. Estos elementos son confidencialidad, integridad y disponibilidad de los recursos.
2011	Daniel Benchimol	Un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, la integridad y la disponibilidad de los recursos informáticos.
2012	Anna Fielder	Se refiere a la seguridad de la información, en el sentido de proteger la información y los sistemas de información del acceso, uso, revelación, interrupción, modificación o destrucción no autorizados a fin de ofrecer: A) Integridad; B) Confidencialidad y C) Disponibilidad

Fuente: Fielder, A. (2012) Computación en Nube. Bruselas: Unión Europea. Editorial Departamento Temático de Política Económica y Científica, Parlamento Europeo.
Elaborado por: Autor

1.5.1.2. Informática.

De Pablos, Hernández, Romo y Medina (2004) indican que la informática es la ciencia que estudia y se ocupa del tratamiento automático y racional de la información o también como la ciencia de los ordenadores.

Para Echenique (1990), el concepto de la informática es más amplio, ya que considera el total del sistema y el manejo de la información, la cual puede usar los equipos electrónicos como una de sus herramientas. Se puede encontrar una variedad de conceptos sobre informática, en el cuadro 1.2 se hace referencia de algunos conceptos de informática con sus respectivos autores.

Cuadro No. 1.2 CONCEPTOS DE INFORMÁTICA POR DIFERENTES AUTORES

Año	Autores	Conceptos definidos por el autor
1983	Centro de Informática Facultad de Contaduría y administración (CIFCA)	No existe una sola concepción acerca de qué es informática: etimológicamente se deriva del francés informatique. Este neologismo proviene de la conjunción de information (información). Su creación fue estimulada por la intención de dar una alternativa menos tecnocrática y menos mecanicista al concepto de "proceso de datos".
1966	Academia Francesa	Ciencia del tratamiento sistemático y eficaz, realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación en los ámbitos técnico, económico y social.
1975	Oficina Intergubernamental de Informática (IBI)	Aplicación racional, sistemática de la información para el desarrollo económico, social y político.
1977	Academia Mexicana de Informática	Ciencia de los sistemas inteligentes de información

Fuente: Echenique, J. (1990). Auditoría Informática, México DF: México. Editorial McGraw-Hill Interamericana
Elaborado por: Autor

1.5.2. Modelos de seguridad informática.

1.5.2.1. Principales modelos de seguridad informática.

Un modelo de seguridad proporciona una representación científica acerca de las propiedades funcionales y estructurales de seguridad de un sistema de información. El concepto de seguridad informática se ha extendido a nivel mundial a través de las Normas ISO, utilizadas por las empresas. Para Aguilera (2010) define la seguridad informática como la disciplina que diseña normas, procedimientos, métodos y técnicas que están destinados a conseguir un sistema de información seguro y confiable.

Consecuentemente un sistema de información siendo un conjunto de elementos los cuales estando de forma organizada, relacionada y coordinada, preserva los principios de la seguridad informática, por la confidencialidad, integridad y disponibilidad de la información. La seguridad informática abarca la protección de sistemas de información, ordenadores, redes e infraestructura. Además

contenido menor sobre ataques informáticos, virus, spam, análisis de vulnerabilidades, entre otros aspectos.

Según Gómez (2014), en el Glossary (2000) la *"Seguridad informática son las medidas y controles que aseguran la confidencialidad, integridad y disponibilidad de los activos de los sistemas de información, incluyendo hardware, software, firmware y aquella información que procesan, almacenan y comunican."* (p. 39).

Laudon y Laundon (2012) identifica seis tipos de sistemas de información, como:

Sistemas para el Procesamiento de Transacciones, TPS: Procesos automatizados; apoyan al nivel operativo, reducen tiempo de operaciones y actividades diarias.
Sistemas del Trabajo del Conocimiento, KWS: Apoya a los usuarios que manejan información para la creación e integración de nuevos conocimientos.
Sistemas de Automatización de Oficinas, OAS: Ayudan en el procesamiento de información, con el llamado paquete de oficina.
Sistemas de Información Gerencial, MIS: Apoya el nivel administrativo desde el proceso de planificación, control y toma de decisiones.
Sistemas de apoyo a la toma de decisiones, DSS: Interactivos y analíticos, apoya las partes implicadas en la toma de decisiones.
Sistemas de apoyo a Ejecutivos, ESS: Se sitúan en el nivel estratégico de la organización, lo utiliza la alta dirección para trazar estrategias generales a seguir.

Asimismo existen autores como De Pablos, López, Romo, Medina, Montero y Nájera (2006) agregan dos tipos de sistemas de información:

Sistemas de Planificación de Recursos Empresariales, ERP: Son integrales, permiten la ejecución y automatización de procesos de negocio de las áreas funcionales, a través de una plataforma común de tecnología de la información.
Sistemas Expertos (SE): Con base en la inteligencia artificial, capaces de solucionar problemas aplicando la base de conocimientos.
Para CSA (2011) y Grance y Mell, (2011) los controles de seguridad en un entorno tradicional no son diferentes a los controles en el Cloud Computing, pese

a que los modelos de servicios, operativos y las tecnologías utilizados, suelen ocasionar algún riesgo a la empresa.

En el cuadro 1.3 se detalla los autores más desatacados en los modelos teóricos de la seguridad informática.

Cuadro No. 1.3 PRINCIPALES MODELOS CONCEPTUALES DE LA SEGURIDAD INFORMÁTICA

Año	1981	1992	2011	2011	2013
Autor	Carl E. Landwehr	Comité de Sistemas de Seguridad Nacional (CNSS) basado en el modelo McCumber Cube	Cloud Security Alliance (CSA)	Wayne Jansen y Timothy Grance (National Institute of Standars and Technology, NIST)	Normas ISO / IEC
Consideraciones	Modelos formales de seguridad informática.	Propone un análisis de características de información crítica basado en tres dimensiones	Modelo planteado para cada servicio Gestión a través de matriz de controles de referencia para la seguridad.	Modelo basado en argumentos clave de seguridad y privacidad	Modelo establecido por Normas: ISO/IEC 27001, ISO/IEC 27002 ISO/IEC 27017, ISO/IEC 27018

Fuente: Landwher (1981). A survey of formal model for computer security. Washington. Editorial CSUR / Whitman, M., Mattord, H. (2014). Management of Information Security Forth Edition. Estados Unidos: Standford. Editorial Cengage Learnig basado en la teoría de John MacCumber (1991). Assessing and Managing Security Risk in IT Systems a Structured Methodology / Cloud Security Alliance, CSA (2011). Security guidance for critical areas of focus in clod V3.0. Estados Unidos. / (Liu *et al.,* 2011) NIST Cloud Computing Reference Architecture. Gaitherburg. NIST Especial Publications 500-292 / ISO/IEC, (2013) Normas Técnicas ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional).
Elaborado por: Autor

1.5.2.2. Modelos formales para la seguridad informática de Landwher

Como indica Landwher (1981), los modelos imponen controles para cualquier operación en un sistema o aplicación que obedezca a las estructuras de un modelo, y algunas operaciones no permitidas son consideradas fuera del modelo formal. Este autor recopila varios modelos orientados a la seguridad como la protección contra observación, modificación no autorizada o inapropiada de la información procesada y la denegación de un servicio.

Modelo matriz de acceso: Una de las primeras descripciones de este modelo fue provisto por Lampson (1971), Denning (1971) y Graham (1972). Permite una variedad de técnicas de implementación. Tiene tres elementos principales: un

conjunto de objetos pasivos, sujetos activos que pueden manipular los objetos, y un conjunto de reglas que rigen la manipulación de objetos por sujetos. Los objetos son típicamente archivos, terminales, dispositivos y otras entidades implementadas por un sistema operativo. Un sujeto es un proceso y un dominio (un conjunto de restricciones donde un proceso puede acceder a ciertos objetos).

Cuadro No. 1.4 MATRIZ DE ACCESO

r= autorización de lectura
w= autorización de escritura
x= autorización de ejecución

		Objetos				
		Objeto1	Objeto2	Objeto3	…	Objeto n
Sujeto	Sujeto1	rwx	rw	rwx	…	rw
	Sujeto2	x	r	x	…	rw
	Sujeto3	x	rw	rwx	…	r
	…	…	…	…	…	…
	Sujeto n	x	rw	x	…	w

Fuente: Landwher (1981). A survey of formal model for computer security. ACM Computing Surveys. Washington DC: Washington (CSUR). Report (247-278).
Elaborado por: Autor

Control de acceso basado en roles: Representan el comportamiento de una capacidad basada en la operación de los sistemas, controlando tanto la confidencialidad como la integridad. Incluye operaciones de administración utilizadas por el administrador de seguridad. Facilita el diseño y la administración. Un rol corresponde a funciones dentro de un grupo de trabajo.

Modelo formal de confidencialidad Bell LaPadula: Maneja la confidencialidad a través del acceso permitido por una política de seguridad, con reglas y modos de sólo lectura, escritura y lectura y escritura. Controla el flujo de información en un sistema mediante reglas de control de acceso.

Modelo formal de integridad Biba: Controla el flujo de información en un sistema para salvaguardar la integridad de los datos, estableciendo reglas de control de acceso.

Modelo Clark-Wilson: Controla la integridad, evita la modificación de personas no autorizadas.

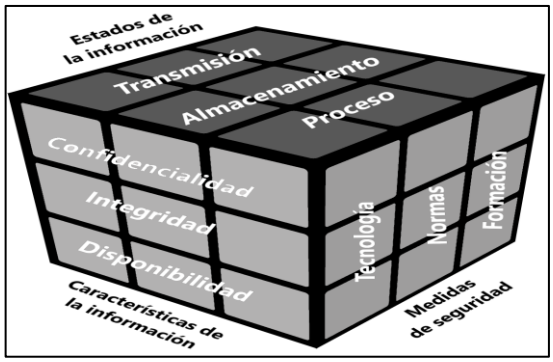
Modelo flujo de Información: Controla el flujo de datos entre objetos según el nivel de seguridad del objeto; flexible para implementar políticas de seguridad.

1.5.2.3. Modelo propuesto por el Comité de Sistemas de Seguridad Nacional (CNSS) basado en el modelo McCumber Cube.

Según Whitman y Mattord (2014) fundamentan el modelo basado en la teoría diseñada por John McCumber (1992), conocido como Cubo de McCumber, o también se conoce como CNSS (Committe on National Security System) Security Model o NSTISSC (National Security Telecommunications and Information Systems Security Committee) Security Model No. 4011.

Para Whitman y Mattord (2014) define las dimensiones encontradas en el modelo apoyado en el análisis de Johnston (2004) que describe las principales características en tres dimensiones con sus atributos aplicables a cualquier entorno. Propone un análisis de características de información crítica para los diferentes estados de información con la finalidad de identificar vulnerabilidades que puedan ser afrontadas por medidas de seguridad, técnicas u organizativas.

Cuadro No. 1.5 MODELO MCCUMBER CUBE.



Fuente: Whitman, M., Mattord, H. (2014). Management of Information Security Forth Edition. Standford: Estados Unidos. Editorial Cengage Learnig basado en la teoría de John MacCumber (1991). Assessing and Managing Security Risk in IT Systems a Structured Methodology
Elaborado por: Autor

Según Whitman y Mattord (2014) considera además como características de información críticas:

Identificación y autenticación: Identificar a los actores intervinientes, donde se platea la interrogante ¿quién es? para el reconocimiento de los usuarios.
Autorización: Establece restricciones de los actores intervinientes, otorgando funciones a los usuarios, plantea la interrogante ¿qué puede hacer?.

Confidencialidad y privacidad: Define los recursos a utilizar, se plantea la interrogante ¿qué puede ver?.

Integridad: Conocer la información que ha sido manipulada.

Auditoría: Establece la aplicación de medidas después de ocurrido una investigación de posible vulnerabilidad en la seguridad.

No repudio: Este aspecto considera la identificación de usuarios que niegan una identidad o autenticación.

1.5.2.4. Modelo propuesto con base en el Estándar Cloud Security Alliance Cloud Controls Matrix (CSA CCM) (Matriz de controles en la nube)

Está diseñado para proporcionar los principios de seguridad, guiar a proveedores y ayudar a clientes potenciales en la nube a evaluar el riesgo general de seguridad de un proveedor. Fortalece entornos mediante requisitos de control de seguridad, reduce e identifica las amenazas y vulnerabilidades en la nube, proporciona seguridad estandarizada y gestión del riesgo, busca normalizar las expectativas de seguridad, terminología, y las medidas implementadas; CSA (2011) indica que tiene relación a otras normas de seguridad, reglamentos, y controla los marcos tales como la ISO 27001/27002, ISACA COBIT, PCI, NIST, entre otras. Se basa en 14 dominios de control según Cloud Security Alliance (2017) presentados en dos categorías como son gobierno y operaciones. En el cuadro 1.6 se presenta los dominios de gobierno, que abordan estrategias y política, para controlar y medir los riesgos.

Cuadro No. 1.6 DOMINIOS DE GOBIERNO EN UN ENTORNO DE CLOUD COMPUTING

GOBIERNO EN EL CLOUD	
Gobierno y Gestión de Riesgos en la empresa	Capacidad para controlar y medir el riesgo empresarial. Aspectos legales por incumplimiento de acuerdos, responsabilidad de proteger datos sensibles cuando tanto usuario como proveedor pueden ser responsables y cómo en lo internacional puede afectar.
Aspectos legales: Contratos y Descubrimiento electrónico	Posibles problemas legales. Requisitos de protección y de los sistemas de computación, leyes sobre violaciones de seguridad por divulgación, requisitos regulatorios y de privacidad, leyes internacionales, etc
Cumplimiento y Auditoría	Mantenimiento y comprobación del cumplimiento legal en el uso Cloud. Evaluación de cómo afecta al cumplimiento legal con políticas de seguridad internas y diversos requisitos de cumplimiento. Este dominio incluye indicaciones para demostrar el cumplimiento legal durante una auditoría.
Gobierno de Información	Trata de los datos que se encuentran en la nube, identificación y controles de datos, y controles para combatir la pérdida de datos en una migración. Responsabilidades de confidencialidad, integridad y disponibilidad de datos.

Fuente: Cloud Security Alliance (2017). The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 “Guidance v4.0”. Recuperado de https://cloudsecurityalliance.org/download/securityguidance-v4/.
Elaborado por: Autor

En el cuadro 1.7 se presenta los dominios operacionales, se centran en la seguridad de la información e implementación dentro de una arquitectura.

Cuadro No. 1.7 DOMINIOS OPERACIONALES EN UN ENTORNO DE CLOUD COMPUTING

OPERACIONES EN EL CLOUD	
Plan de recuperación y continuidad de negocio	Sobre la forma en que la nube afecta a procesos operativos y procedimientos utilizados para implementar seguridad, continuidad de negocio y recuperación ante desastres. El objetivo es discutir y analizar posibles riesgos de Cloud computing, identificar dónde los servicios pueden disminuir riesgos o pueden acarrear aumentos en otras áreas.
Seguridad de infraestructura	Trata de Seguridad de la infraestructura de la nube central, incluidas las redes, la seguridad de la carga de trabajo y consideraciones de nube híbrida. Incluye fundamentos de seguridad para nubes privadas.
Contenedores y Virtualización	Aborda temas sobre seguridad para hipervisores, contenedores y redes definidas por software. Este dominio se centra en los problemas de seguridad que rodean la virtualización del sistema / hardware
Respuesta, Notificación y Remediación ante incidentes,	Correcta detección, respuesta, notificación y remediación ante incidentes, a nivel de proveedor y usuario, permite manejo de incidentes y análisis forense. Ayuda a entender complejidades que los servicios Cloud traen a un programa de gestión de incidentes.
Seguridad de aplicaciones	Asegurar el software de aplicación que se ejecuta o está siendo desarrollado en Cloud. Referente si es apropiado migrar o diseñar aplicación para que se ejecute en Cloud y el tipo de plataforma más apropiada (SaaS, PaaS o IaaS).
Seguridad de datos y Encriptación	Abarca temas sobre la implementación de seguridad y cifrado de datos, uso correcto del cifrado y de una gestión de claves escalable.
Gestión de identidad y de accesos	Gestión de identidades y aprovechamiento de servicios de directorio para proporcionar control de acceso. Centrado en problemas encontrados cuando se extiende la identidad de una empresa en Cloud. Proporciona conocimiento para evaluar el grado de preparación de una organización para llevar a cabo Identity, Entitlement, and Access Management (IdEA) basado en Cloud.
Seguridad como servicio	Garantía de seguridad por terceros, gestión de incidentes, certificación de cumplimiento legal y supervisión de identidad y control de acceso.
Tecnologías relacionadas	Tecnologías establecidas y emergentes con una estrecha relación con la nube, incluidos Big Data, Internet de las cosas y la informática móvil.

Fuente: Cloud Security Alliance (2017). The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 "Guidance v4.0". Recuperado de https://cloudsecurityalliance.org/download/securityguidance-v4/.
Elaborado por: Autor

1.5.2.5. Modelo propuesto por el Instituto Nacional de Normas y Tecnología, NIST

Presenta elementos para obtener medidas más rigurosas en la privacidad y seguridad en la nube de parte de los proveedores (Jansen y Grance, 2011). Estos autores presentan las recomendaciones a considerar dentro del modelo propuesto:

Gobernanza: Control y supervisión de políticas, procedimientos y estándares para el desarrollo de aplicaciones, diseño, implementación, pruebas y monitorización de servicios distribuidos. Jansen y Grance (2011) inndican es necesidad una buena gobernanza, políticas y estándares en la provisión de servicios del cloud computing.

Cumplimiento: Exige la conformidad con especificaciones, estándares, normas o leyes establecidas. Además Jansen y Grance (2011) mencionan que además aborda la ubicación de los datos y la investigación electrónica.

Confianza: Ceder el control de varios elementos de la seguridad otorgando un nivel de confianza sin antecedentes al proveedor de la tecnología cloud; para Jansen y Grance (2011) se debe considerar el acceso desde dentro, la propiedad de los datos, servicios complejos, visibilidad y la gestión de riesgos.

Arquitectura: Jansen y Grance (2011) indican que comprende tanto el hardware como el software. Las máquinas virtuales se utilizan como unidades de distribución de software asociadas a dispositivos de almacenamiento. Las aplicaciones son creadas mediante las interfaces de programación.

Identidad y control de acceso: Jansen y Grance (2011) proponen usar métodos de autenticación, para la organización interna y otro para los clientes.

Aislamiento de Software: Los proveedores deben asegurar una provisión dinámica del servicio y el aislamiento de suscriptores. Mediante la multiplexación; ejecución de las máquinas virtuales para diferentes usuarios en un mismo servidor físico, complejidad del hipervisor y vectores de ataque.

Protección de datos: Datos almacenados en entornos de tecnología cloud suelen permanecer en equipamiento compartido por múltiples clientes. Por ello, Jansen y Grance (2011) sugieren el control de acceso a los datos y garantizar el almacenamiento seguro, considerando el aislamiento y saneamiento de datos.

Disponibilidad: Factor que puede ser interrumpido temporal o permanente, así lo indican Jansen y Grance (2011). Se debe considerar fallos temporales, prolongados y permanentes, denegación de servicio, valor concentrado.

Respuesta a incidentes: Para Jansen y Grance (2011) es necesario realizar la verificación, análisis del ataque, contención, recolección de las evidencias, aplicación de soluciones y restablecimiento del servicio.

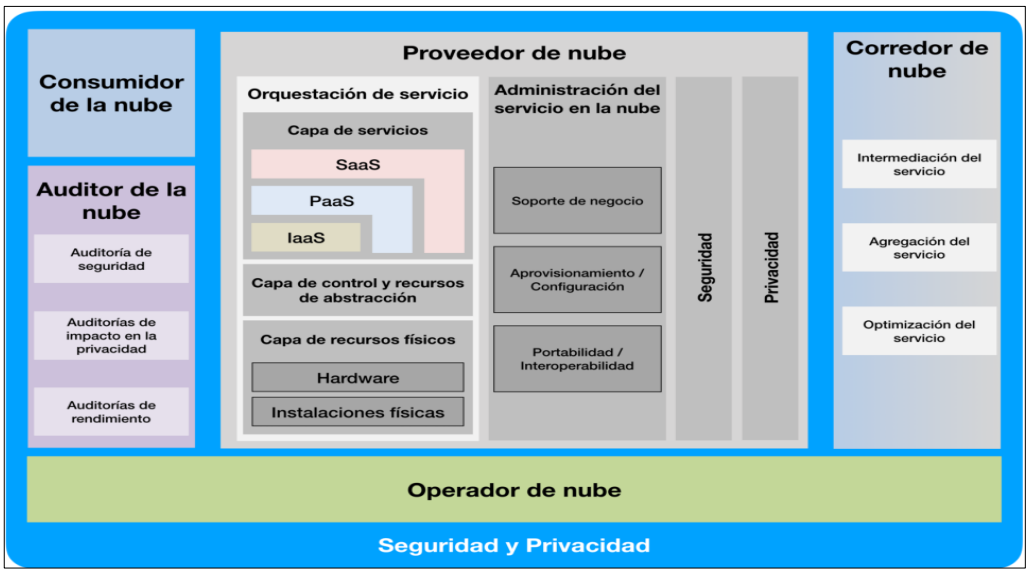
Cuadro No. 1.8 RECOMENDACIONES MODELO PROPUESTO NIST 800-144

ELEMENTO	CARACTERÍSTICA
Gobernanza	Implantar políticas y estándares de servicios cloud. Establecer mecanismos de auditoría y herramientas para el cumplimiento durante el ciclo de vida.
Cumplimiento	Entender leyes y regulaciones y su impacto en entornos cloud. Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.
Confianza	Incorporar mecanismos en el contrato que permitan controlar los procesos y controles de privacidad empleados por el proveedor
Gestión de riesgo	Proceso de identificación y evaluación del riesgo para operaciones de activos o individuos. Incluye realizar evaluación de riesgos, implementación de una estrategia de mitigación, y el empleo de técnicas y procedimientos para el monitoreo continuo del estado de seguridad de la información sistema.
Arquitectura	Comprender las tecnologías que sustentan la infraestructura del proveedor para comprender implicaciones de privacidad y seguridad de los controles técnicos
Identidad y control de acceso	Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso
Aislamiento de Software	Entender la virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados
Disponibilidad	Asegurarse que durante una interrupción prolongada del servicio, las operaciones críticas se pueden reanudar inmediatamente y todo el resto de operaciones, en un tiempo prudente.
Respuesta a incidentes	Entender y negociar los contratos de los proveedores así como los procedimientos para la respuesta a incidentes requeridos por la organización

Fuente: Instituto Nacional de Tecnología de la Comunicación (INTECO), Marzo 2011, Riesgos y amenazas en Cloud Computing Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf
Elaborado por: Autor

En el cuadro 1.9 se presenta el marco de referencia conceptual propuesto por NIST 500-292 para el manejo de seguridades en el cloud computnig:

Cuadro No. 1.9 MODELO CONCEPTUAL DE REFERENCIA CLOUD COMPUTING NIST 500-292



Fuente: Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. y Leaf, D. (2011). NIST Cloud Computing Reference Architecture. Gaithersburg: Estados Unidos. Editorial NIST
Elaborado por: NIST Special Publication 500-292

1.5.2.5.1. Modelos de servicio

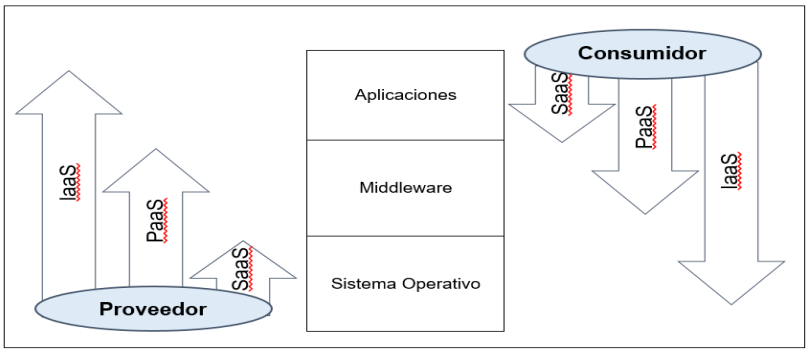
Software como servicio (SaaS): Para Liu, Tong, Mao, Bohn, Messina, Badger, y Leaf (2011) el consumidor utiliza pero no administra ni controla la infraestructura. Proporciona un entorno de trabajo independiente.

Platforma como sevicio (PaaS): El consumidor despliega en la infraestructura del proveedor aplicaciones creadas o adquiridas, usando lenguajes de programación, bibliotecas y herramientas del proveedor; tiene control sobre aplicaciones y de ser posible de configuraciones. (Liu *et al.,* 2011)

Infraestructura como servicio (IaaS): El consumidor aprovisiona recursos de almacenamiento, procesamiento, redes y otros, puede desplegar y correr software, suele incluir sistemas operacionales y aplicaciones. (Liu *et al.,* 2011)

De acuerdo al cuadro 1.10 dependiendo del modelo de servicio, el nivel de administración o responsabilidad se incrementa inversamente proporcional desde el punto de vista del cliente respecto al del proveedor, y viceversa:

Cuadro No. 1.10 ALCANCE DE LOS CONTROLES ENTRE EL CONSUMIDOR Y PROVEEDOR



Fuente: Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. y Leaf, D. (2011). NIST Cloud Computing Reference Architecture. Gaithersburg: Estados Unidos. Editorial NIST
Elaborado por: Autor

1.5.2.5.2. Modelos de despliegue

Nube privada: Administrada por una organización o por un tercero y puede existir dentro o fuera de la misma. (Liu *et al.,* 2011)

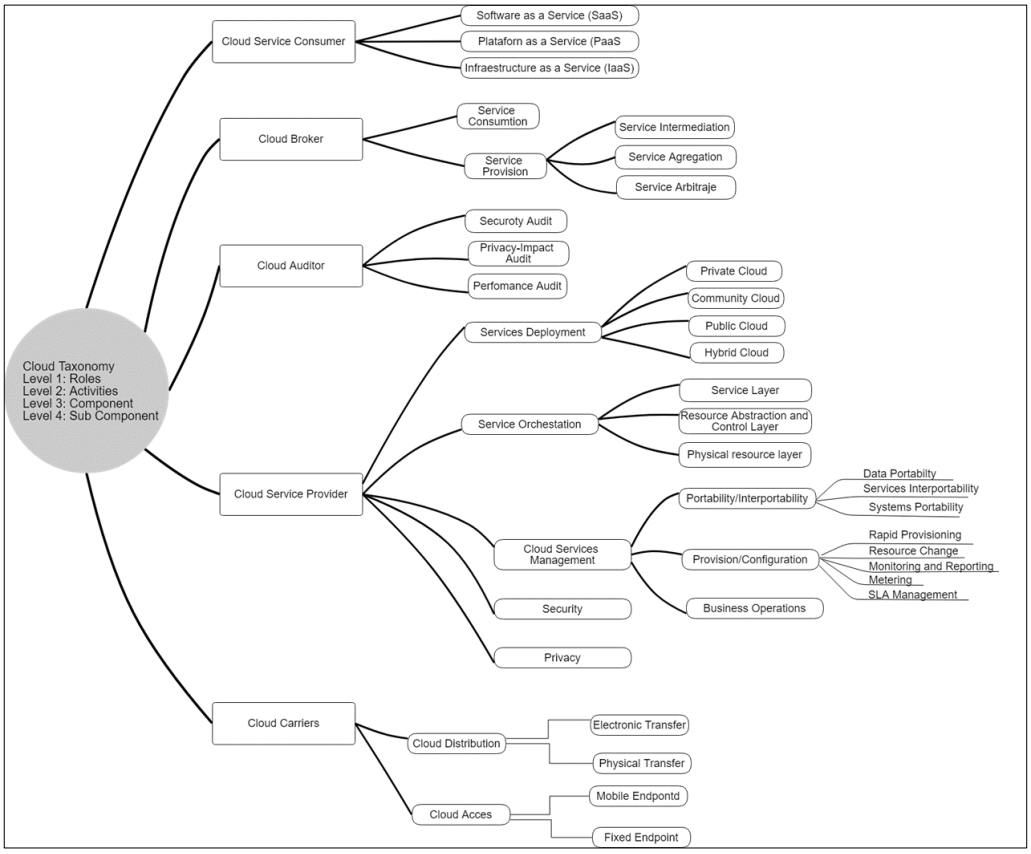
Nube comunitaria: Compartida por varias organizaciones y apoya las preocupaciones de una comunidad particular sobre un tema específico. (Liu *et al.,* 2011) aseguran que puede ser administrada por una organización o por un tercero y puede existir dentro o fuera de la misma.

Nube pública: Para el público o grupos de industrias, la infraestructura la provee una organización dedicada a vender servicios en la nube (Liu *et al.,* 2011)

Nube híbrida: Se compone de dos o más nubes, como privada y pública, para (Liu *et al.,* 2011) indican que se encuentran como entidades únicas pero coexisten debido a la tecnología que les permite compartir datos o aplicaciones.

Según (Liu *et al.,* 2011) presentan una taxonomía compuesta por atributos que definen el servicio del cloud computing, tal como se muestra en el cuadro 1.11.

Cuadro No. 1.11 CLASIFICACIÓN DE DOMINIOS DEL CLOUD COMPUTING SEGÚN EL NIST 500-292



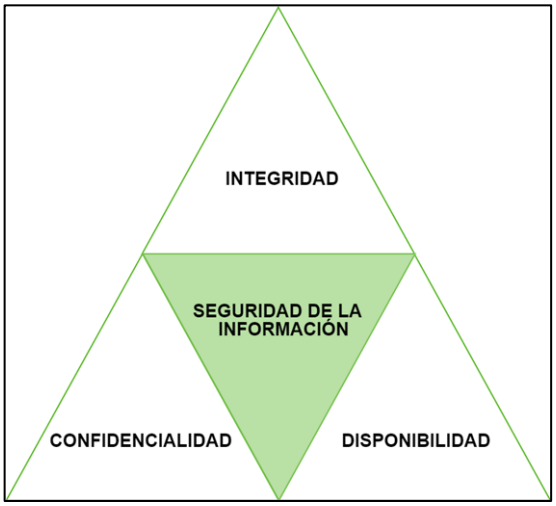
Fuente: Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. y Leaf, D. (2011). NIST Cloud Computing Reference Architecture. Gaithersburg: Estados Unidos. Editorial NIST
Elaborado por: Autor

1.5.2.6. Modelo basado en las Normas Técnicas ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional)

Las normas ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización a nivel mundial. (ISO, 2013)**.**

A través del uso de las normas las organizaciones pueden desarrollar e implementar un marco para la gestión de la seguridad de sus activos de información incluyendo la información financiera, la propiedad intelectual, y detalles de los empleados, o la información confiada a ellos por los clientes o terceros. Cabe mencionar que la seguridad de la información basada en las normas 27000 se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad (medidas conocidas como CIA), originalmente norma ISO 17799, además abarca términos que forman la base para un Sistema de Gestión de Seguridad de la Información.

Cuadro No. 1.12 SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 17799



Fuente: Gómez, A. (2014). Enciclopedia de la Seguridad Informática, 2da Edición. Madrid: España. Editorial RA-MA.
Elaborado por: Autor

Para efectos del desarrollo de la investigación se define a breves rasgos las normas relacionadas a la seguridad de la información en el cloud computing.

1.5.2.6.1. NORMA ISO / IEC 27001:2013

Según la Norma ISO 27001 (2013) específica los requisitos para establecer, implementar, mantener y mejorar consecutivamente un sistema de gestión de seguridad de la información. Contiene requisitos de evaluación y tratamiento de los riesgos de seguridad según necesidades de una organización, una certificación ISO demuestra que cumple con todos los requisitos de la norma ISO 27001 (2013) o con un subconjunto específico de los controles, y el estado de esos controles revisado por un auditor independiente. La compatibilidad ISO declara que sigue los requisitos de la norma, pero no certificados oficialmente.

1.5.2.6.2. NORMA ISO / IEC 27002:2013

Para la Norma ISO 27002 (2013) especifica directrices para los estándares y prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el medio ambiente. Está diseñado para ser utilizado por las organizaciones que pretenden seleccionar controles para proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO, IEC 27001; implementar controles, desarrollar sus propias directrices de gestión de seguridad de la información. Además consta de un anexo que incluye una guía con 14 dominios y 37 controles mapeados y enfocados a estos entornos:

Cuadro No. 1.13 LISTA DE DOMINIOS SEGÚN LA NORMA ISO 27002:2013

ID	Dominio
5	Políticas de seguridad
6	Aspectos Organizativos de la seguridad de la información
7	Seguridad Ligada a los recursos humanos
8	Gestión de activos
9	Control de acceso
10	Cifrado
11	Seguridad física y ambiental
12	Seguridad de las operaciones
13	Seguridad de las telecomunicaciones
14	Adquisición, desarrollo y mantenimiento de sistemas de información
15	Relaciones con los proveedores
16	Gestión de incidentes de seguridad de la información
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio
18	Cumplimiento

Fuente: Organización Internacional para la Estandarización (2013). Controles de Seguridad Norma 27002. Recuperado de: http://iso27000.es/download/ControlesISO27002-2013.pdf
Elaborado por: Autor

Cabe mencionar que esta norma inicialmente se denominaba ISO 17799 revisada en el año 2000 pasando a denominarse después ISO 27002:2005 a partir de julio del 2007, según lo indica (ISO 27000, 2009).

1.5.2.6.3. NORMA ISO / IEC 27017:2015

Según la Norma ISO 27017 (2015) proporciona directrices que fomentan la aplicación de los controles de seguridad para clientes y proveedores de servicios en la nube. La selección de los controles apropiados y la aplicación de la guía, dependen de una evaluación de riesgos y todos los requisitos de seguridad de información, legal, contractual, regulatorias u otras del sector nube.

1.5.2.6.4. NORMA ISO / IEC 27018:2014

Según Norma ISO 27018 (2014) define controles y directrices para la implementación de las medidas de protección de información de identificación personal (PII), según los principios de privacidad. También incluye directrices basadas en la norma ISO 27002, considerando requisitos de PII.

1.5.3. Comparación de otras teorías de seguridad informática en la tecnología cloud computing

La seguridad informática está destinada a la seguridad de los sistemas de información, al entorno de información automatizada; la seguridad de la información abarca la información en todas sus formas, según el ciclo de vida tiene como objetivo proteger de cualquier que ocasione pérdida o disminución del valor. La seguridad informática por lo tanto consiste en la implantación de medidas de confidencialidad, integridad y disponibilidad; y otros principios como son: autenticación, autorización, auditoría, responsabilidad y privacidad. En cada uno de los modelos se destaca dimensiones propuestas en el modelo de (Liu *et al.,* 2011) presentado por el Instituto Nacional de Normas y Tecnología, NIST, incluyendo variables los modelos de la norma ISO 27000 y la guía de seguridad para áreas críticas enfocadas a la seguridad en el cloud computing, publicada por el Cloud Security Alliance (CSA, 2017).

Cuadro No. 1.14 DIMENSIONES RELEVANTES DE OTROS MODELOS SOBRE SEGURIDAD INFORMÁTICA EN TECNOLOGÍA CLOUD COMPUTING

Autores	Año	Descripción y dimensiones de la evaluación
Lamia Youseff, Maria Butrico, Dilma Da Silva	2008	Clasifica en cinco etapas las dimensiones del cloud: • Aplicación cloud • Entorno del software cloud • Infraestructura de software cloud • Núcleo del software y hardware
Prurificación Aguilera	2010	Presenta grupos en relación a funciones y operaciones donde se ejerce mayor control: • Matriz de acceso. • Acceso basado en funciones de control (RBAC). • Multinivel: El modelo de La Bell-Padula, de Biba, Celosía y Clark y Wilson.
ISACA	2012	Principios rectores para la adopción y el uso de la nube para ayudar a las empresas a identificar claramente el camino que debe tomar • Capacitación (eablement) • Relación costo-beneficio • Riesgo para la empresa • Capacidad • Responsabilización (accountability) • Confianza
Cloud Special Interest Group PCI Security Standards Council	2013	Establece un conjunto de normas para asegurar que las empresas que procesan, almacenan o transmiten información de tarjetas de crédito mantengan un entorno seguro. • Verificación y validación de servicios y componentes • Verificación PCI DSS Gestión de control por el proveedor de cloud • Gobierno, riesgo y cumplimiento • Facilidades y seguridad física • Soberanía de datos y consideraciones legales • Seguridad de datos • Seguridad técnica
SMI (Service Measuremente index)	2014	Evalúa y mide servicios cloud en base a los requerimientos técnicos y necesidades específicas, definiendo un conjunto de características, métricas y KPIs para evaluar las características de los proveedores de servicios cloud: • Responsabilidad (accountability) • Agilidad (agility) • Garantía (assurance) • Finanzas (financial) • Seguridad y privacidad (security and privacy) • Usabilidad (usability)
Blacio, K.	2015	La seguridad informática se resume, por lo general, en cinco objetivos principales. • Integridad • Confidencialidad • Disponibilidad • Evitar el rechazo • Autenticación

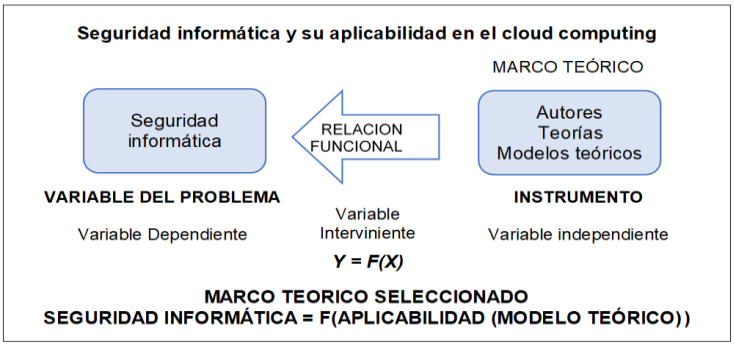
Fuente: Datos recopilados de la investigación
Elaborado por: Autor

En el cuadro 1.14 se presenta un resumen de los diferentes modelos relacionados a la seguridad informática y su aplicabilidad en la tecnología del cloud computing, por tipos de variables junto con el año de publicación.

1.5.4. Selección del modelo de evaluación.

1.5.4.1. Definición de la problemática de seguridad informática a partir de la utilización de un instrumento.

Cuadro No. 1.15 RELACION VARIABLE DEPENDIENTE Y VARIABLE INDEPENDIENTE



Fuente: Problemática planteada en el trabajo de investigación
Elaborado por: Autor

Para determinar si existen factores que inciden en la seguridad informática en la tecnología cloud computing es necesario determinar dichos factores siendo importante emplear un instrumento de estudio de investigación científica. El instrumento de estudio fue necesario sustentarlo mediante las teorías, modelos, investigaciones similares o conceptos desarrollados por autores a partir del objetivo y la formulación del problema (Hernández, Fernández, y Baptista, 2010).

1.5.4.2. Definición de la variable independiente basado en un modelo de atributos de seguridad informática desde las propiedades y elementos

Se consideró lo definido en Normas ISO 27000 (2009) que contiene principios básicos de la seguridad para sistemas de información aplicados a cualquier entorno, rescatando las dimensiones que se refiere a disponibilidad, integridad y confidencialidad según Norma ISO 27002 (2013) en cuanto al cumplimiento de requisitos legales y contractuales y revisiones de seguridad de la información.

Adicionalmente se ha tomado el modelo de Jansen y Grance (2011), presentan a través del NIST 800-144 donde definen el cloud computing como modelo para permitir acceso desde cualquier lugar, forma cómoda y bajo demanda a recursos compartidos, se rescatan las políticas, normas/estándar; el marco de referencia; la autenticación, el control de acceso.

Del modelo propuesto por Whitman y Mattord (2014), basado en la teoría de John MacCumber (1991), se selecciona la Tecnología, considerando las medidas se seguridad a aplicar.

Del modelo propuesto por ISACA (2012) se consideró las responsabilidades que sirve en la comprensión de los riesgos de una empresa, monitoreando el rendimiento y recursos disponibles en la resolución de problemas.

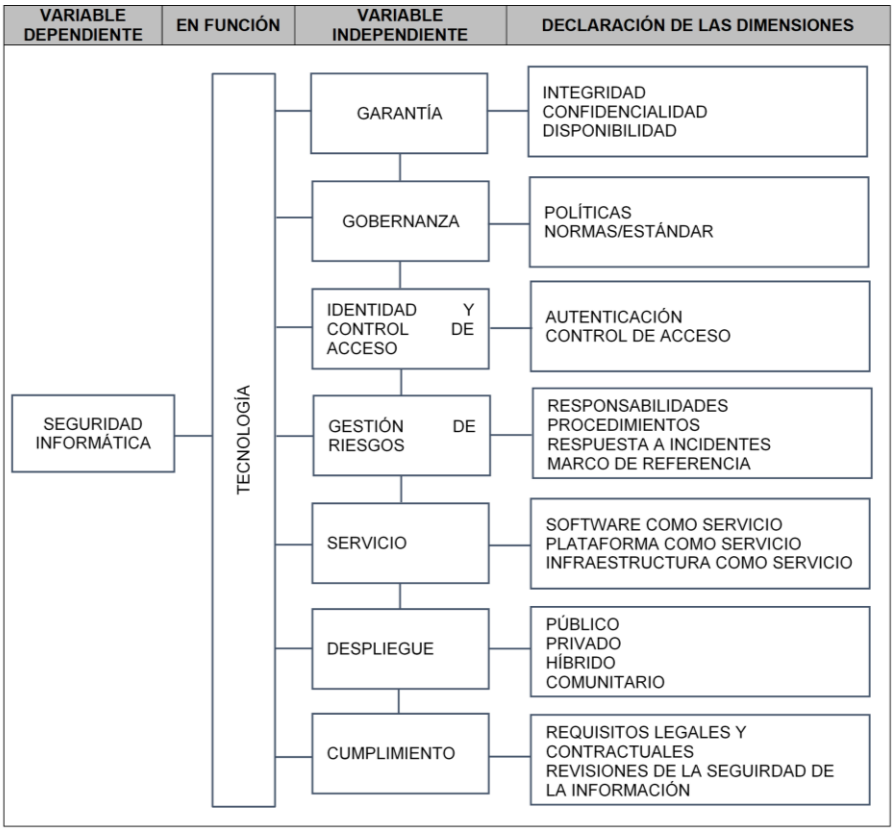
Se consideró los principios básicos de modelo de referencia de (Liu *et al.,* 2011) presentado por el Instituto Nacional de Normas y Tecnología, NIST, además se tomó información de la guía de seguridad para áreas críticas enfocadas a la seguridad en el cloud computing, publicada por el Cloud Security Alliance (2017)

en el que a través de la matriz de controles de referencia ofrece una guía de recomendaciones para la gestión de riesgos.

1.5.4.3. Diagrama del modelo de evaluación propuesto

El cuadro No. 1.16 presenta el modelo conceptual de seguridad informática basado en diferentes teorías, normas y modelos investigados, considerando como instrumento científico al modelo del Instituto Nacional de Normas y Tecnología, NIST junto con el marco de referencia del Cloud Security Alliance que destaca las dimensiones del modelo del cloud computing.

Cuadro No. 1.16 MODELO DE LA SEGURIDAD INFORMÁTICA Y SU APLICABILIDAD TECNOLOGÍA CLOUD COMPUTING



Fuente: Datos recopilados de la investigación a partir del modelo NIST500-592 (2017), Cloud Security Alliance (2011) y otros modelos teóricos para determinar factores que inciden en la seguridad informática y su aplicabilidad en la tecnología del cloud computing.
Elaborado por: Autor

Garantía: Todo proceso dentro de los servicios del cloud computing se mantengan protegidos, mediante la medición de atributos:

- Integridad: garantizar que la información no sea alterada en el contenido.

- Confidencialidad: asegurar control de accesos a la información.
- Disponibilidad: garantizar el alcance de forma oportuna y precisa, Se debe considerar fallos temporales, prolongados y permanentes, denegación de servicio, valor concentrado.

Gobernanza: Se refiere al control y supervisión de políticas de seguridad, incluidos procedimientos y estándares para desarrollar aplicaciones, además del diseño, implementación, pruebas y monitorización de servicios distribuidos.

Identidad y control de acceso: Métodos de autenticación para la identificación de usuarios y mecanismos para el control de accesos.

Gestión de riesgos: Medir y valorar los riesgos en la empresa, procedimientos para el monitoreo continuo del estado de seguridad de la información, Responsabilidades, Procedimientos, Respuesta a incidentes según las actividades de respuesta ante la ocurrencia de algún incidente de seguridad y Marco de referencia.

Servicio: Hace referencia al software, plataforma e infraestructura entregadas al consumidor como un servicio, en donde el software como servicio proporciona al usuario aplicaciones sin tener que ser gestionadas ni controladas. La plataforma como servicio proporciona al usuario la capacidad de crear o adquirir aplicaciones que puede gestionar y controlar pero no puede gestionar ni controlar la infraestructura subyacente (red, servidores, sistemas operativos y almacenamiento). La infraestructura como servicio proporciona al usuario control sobre el procesamiento, almacenamiento, interconexión de red limitada y otros recursos, instalar y ejecutar software; pero no tiene control para gestionar la infraestructura subyacente.

Despliegue: Modelo de implementación para la ejecución de un servicio, nube pública a disposición general o industria en que una organización es propietaria de la venta de servicios. Nube privada tiene un servicio de propiedad o de alquiler por una empresa. Nube híbrida combina las características de las nubes públicas y privadas, manejando las responsabilidades de gestión. Nube comunitaria es

compartida por organizaciones sobre requisitos de seguridad, políticas y cumplimiento legales.

Cumplimiento: Medir el grado de cumplimiento de estándares, normas o leyes a través de Requisitos legales y contractuales y Revisiones de la seguridad de la información.

1.5.5. Tecnología Cloud Computing

1.5.5.1. Características esenciales

Para el Instituto Nacional de Estándares y Tecnología y el laboratorio de tecnología información, define la tecnología Cloud Computing de la siguiente manera:

Cloud Computing es un modelo que permite obtener, desde cualquier lugar y bajo demanda, un cómodo acceso a través de una red a un conjunto (pool) compartido de recursos informáticos configurables, el cual se puede conformar y suministrar rápidamente con un esfuerzo de gestión mínimo o con una interacción mínima con el proveedor de los servicios (Grance y Mell, 2011, p. 2).

Dentro de las características esenciales tecnología cloud computing están:

Auto servicio por demanda: El consumidor puede acumular de manera unilateral capacidades de cómputo, Grance y Mell (2011) indican el tiempo de servidor y almacenamiento en red, en la medida en que las requiera sin necesidad de interacción humana por parte del proveedor del servicio.

Acceso amplio desde la red: Grance y Mell (2011) aseguran que las capacidades se encuentran disponibles en la red y para acceder se hace a través de mecanismos estándares para el uso desde plataformas clientes heterogéneas, pesadas o livianas, como el PC, un teléfono móvil o un navegador Internet.

Conjunto de recursos: El proveedor habilita recursos a múltiples consumidores mediante un modelo “arrendatario”, tanto físicos como virtuales asignados y reasignados de acuerdo con los requerimientos del consumidor. Grance y Mell (2011) definen que existe independencia de ubicación, es decir que el consumidor no tiene control de la ubicación correcta de los recursos.

Rápida elasticidad: Las capacidades pueden ser rápidamente y elásticamente provistas, para escalar hacia fuera y dentro de forma rápida.

Servicio medido: Para Grance y Mell (2011) los sistemas en la nube controlan de forma automática y óptima el uso de recursos mediante una capacidad de medición a un nivel de abstracción según al tipo de servicio.

Para ISACA (2012), considera que el cloud computing ofrece la posibilidad de obtener beneficios de negocios como son de agilidad, contención de costos, arquitectura común multiempresa, confiabilidad y escalabilidad, pero pueden traer consigo riesgos altos sino se cumplen con las normativas vigentes.

Agilidad: Capacidad de implementar tecnologías, desarrollar soluciones innovadoras y satisfacer necesidades de los clientes de manera rápida al momento de adaptar innovaciones eficaces logrando maximizar inversiones.

Contención de costos: Disponer de los fondos financieros para oportunidades operacionales e inversiones de alto retorno al adquirir y utilizar los servicios que brinda el cloud computing, reduciendo la inversión en otras tecnologías.

Arquitectura común multiempresa: Uso compartido de aplicaciones e infraestructuras técnicas y conocimientos. Se comparte costos y capacidades.

Confiabilidad: A partir de la entrada de proveedores internacionales de tecnología en el mercado de la computación en la nube y la virtualización de sus infraestructuras, ha permitido el uso compartido de recursos.

Escalabilidad: Cada empresa puede determinar sus propias necesidades y encontrar una solución que le aporte valor, desde el abastecimiento de infraestructura y plataformas de desarrollo a través de la nube hasta el suministro de software como servicio. Las empresas más grandes, podrían sólo complementar capacidades en materia de sistemas de información, aprovechando las infraestructuras en la nube para cubrir necesidades especiales o incorporar aplicaciones móviles. La facilidad con que se pueden expandir/reducir los niveles de servicio y la lógica de pago en función del uso hacen que la computación en la nube sea particularmente escalable.

1.5.6. Factores que inciden en la seguridad informática y su aplicabilidad en la tecnología cloud computing

Para Casasola, Maqueo, Molina, Moreno, y Recio (2014) consideran la privacidad, protección de los datos y seguridad como factores en el desarrollo tecnológico, además del estado de la tecnología y los riesgos; y finalmente la elasticidad, factor económico y el factor humano por la manipulación de diferentes elementos que puedan comprometer la información.

Según Solórzano, Rezabala y Aranda (2013) indica que la información es un activo valioso en la empresa y se puede ver afectada por robos, incendios, fallas de disco, virus u otros, además del bajo presupuesto en tecnología puede no permitir se implementen correctas medidas de seguridad informática.

ISACA (2012) considera junto a Jansen y Grance (2011) los factores que inciden en la seguridad informática se centran es las diferentes dimensiones o principios rectores que lo componen, como:

Transparencia: Controles de seguridad efectivos y robustos, para asegurar y proteger la información contra acceso no autorizado, cambio o destrucción.

Privacidad: Garantizar los controles de privacidad, capacidad para prevenir, detectar y reaccionar oportunamente ante violaciones de privacidad. Implementar líneas de comunicación antes de la prestación de los servicios.

Flujo de información transfronterizo: Debido a que la información se almacena en cualquier lugar del cloud, la ubicación física determina la jurisdicción y la obligación legal.

Certificación: Proveedores de servicios con certificaciones oficiales. Las auditorías de terceros y/o los informes de auditores de servicios, proveen el aseguramiento independiente.

Gobernanza: Se refiere al control y supervisión de políticas de seguridad, incluidos procedimientos y estándares para desarrollar aplicaciones, además del diseño, implementación, pruebas y monitorización de servicios distribuidos.

Cumplimiento: Consentimiento legal mediante especificaciones estándares, normas o leyes establecidas.

Confianza: Consentimiento de control de muchos aspectos de seguridad.

Arquitectura: Comprende tanto hardware como software. Las máquinas virtuales, las aplicaciones son creadas mediante las interfaces de programación.

Identidad y control de acceso: Métodos de autenticación y control.

Aislamiento de Software: Asegurar la provisión dinámica del servicio y aislamiento de suscriptores por parte de proveedores.

Protección de datos: Gestión de datos confidenciales y garantías que estén almacenados de forma segura, debido al entorno compartido en el cloud.

Disponibilidad: Se debe considerar fallos temporales, fallos prolongados y permanentes, denegación de servicio, valor concentrado.

Respuesta a incidentes: Actividades de respuesta ante la ocurrencia de algún incidente de seguridad por parte de la labor del proveedor.

CAPÍTULO II. MARCO METODOLÓGICO

2.1. Tipo de diseño, alcance y enfoque de la investigación

2.1.1. Tipo de estudio

El proceso de esta investigación es cualitativo y también cuantitativo por lo que se orienta a un tipo de estudio descriptivo y correlacional.

Estudio descriptivo: Esta investigación recogió información independiente de conceptos o variables a las que se refieren el presente trabajo de investigación, permitiendo reflejar la situación real midiendo conceptos con sus componentes.
Estudio correlacional: Permitió conocer la relación o grado de asociación entre dos o más conceptos, categorías o variables en un contexto en particular.

2.1.2. Metodología de investigación

2.1.2.1. Enfoque de la investigación

El enfoque de la investigación es de tipo cualitativo, se procedió a la recolección y análisis de los datos utilizando métodos estadísticos aplicados a la investigación científica para el procesamiento y presentación de los resultados, el análisis consistió en interpretar información y desarrollar temas.

2.2. Métodos de investigación

Método deductivo: Esta investigación aplicó el método deductivo ya que inició de una realidad problemática en la seguridad informática a partir de la aplicación de un modelo teórico donde se pueda identificar la existencia de los factores que determinan la aplicabilidad de la tecnología del cloud computing a partir de la medición cualitativa y cuantitativa de la seguridad informática.

Método histórico: Esta investigación empleó hechos registrados en el 2015, 2016 y 2017 en la seguridad informática de las grandes y medianas empresas del sector industrial de la ciudad de Manta. También se empleó el método de la medición debido a que se obtuvo información numérica y estadística del objeto de estudio de bases de datos de organismos gubernamentales y no gubernamentales, para obtener conclusiones con un sustento más concreto.

2.3. Unidad de análisis, población y muestra

El propósito de esta investigación conllevó a realizar un análisis de datos referente a 15 grandes y medianas empresas del sector industrial manufacturero de actividad económica elaboración de productos alimenticios de la ciudad de Manta, provincia de Manabí. Según la Superintendencia de Compañías, Valores y Seguros (2018), en el Directorio de Compañías existen 153 empresas del sector manufactura, de las cuales 56 registros corresponde a empresas dedicadas a la elaboración de productos alimenticios CIIU C10, código CIIU basado en la clasificación Nacional de Actividades Económicas revisión 4.0 así lo indica el Instituto Nacional de Estadística y Censos INEC (2012); sin embargo la información entregada en ejercicio económico 2017 del Ranking Empresarial de Empresas Sujetas al Control de la Superintendencia de Compañías, Valores y Seguros (2017) indica que existen 39 Compañías activas según tamaño de la empresa grande, mediana, micro y pequeña. En esta investigación se determinó 15 empresas comprendidas en grande y mediana dedicadas a la actividad económica CIIU C10 y afiliadas a la Cámara de Industrias y Cámara de Comercio de Manta, con el fin de identificar factores determinantes de la seguridad informática y su aplicabilidad en la tecnología cloud computing.

Según Instituto Nacional de Estadística y Censos INEC (2015) basado en el Directorio de Empresas de la Superintendencia de Compañías, Valores y Seguros, el 8% de las empresas nacionales residen en la provincia de Manabí, mediante una recopilación e identificación de varias variables intervinientes en la investigación durante el período 2015 y 2016, en el que según las estadísticas del Ministerio de Telecomunicaciones y Sociedad de la información (2015) indica que el 45% de empresas utilizan el servicio de internet, el 23,6%

correspondientes al sector de manufactura CIIU 10 ha realizado inversión en Tecnología, éstos datos son importantes ya que conllevan a interrogantes sobre el manejo de seguridad informática debido a la inversión y aydan a determinar los factores del objeto de estudio identificando el software de facturación como sistema de información aplicable a la tecnología cloud computing, utilizado en empresas del sector industrial manufacturero grande y mediana empresa, actividad económica C10 de la ciudad de Manta. Se realizó la revisión de información lo que permitió analizar las dimensiones de la seguridad informática.

2.4. Variables de la investigación, operacionalización

Variable dependiente (VD).

Seguridad informática: Es la variable del trabajo de investigación que permite determinar el nivel de incidencia.

Variable Independiente (VI).

Garantía (VI01): Variable para valorar preservación de seguridad basada en los principios de Disponibilidad, Confidencialidad e Integridad.

Gobernanza (VI02): Variable para valorar el control de las políticas, los procedimientos y los estándares aplicados, mediante Políticas y Normas ISO.

Identidad y control de acceso (VI03): Variable para valorar protecciones en la autenticación, la autorización y las funciones de control de acceso.

Gestión de riesgos (VI04): Variable identificada para medir y valorar los riesgos en la empresa, los procedimientos para el monitoreo continuo del estado de seguridad de la información sistema, Responsabilidades, Procedimientos, Respuesta a incidentes y Marco de referencia.

Servicio (VI05): Variable identificada para medir el uso de servicios o aplicaciones en cloud coputing siendo Plataforma como servicio, Software como servicio o Infraestructura como servicio.

Despliegue (VI06): Variable identificada para valorar un servicio o aplicación de cloud en entorno Público, Privado, Híbrido o Comunitario.

Cumplimiento (VI07): Variable identificada para valorar y medir el cumplimiento de estándares, normas o leyes establecidas, a través de Requisitos legales y contractuales y Revisiones de la seguridad de la información.

2.5. Fuentes y técnicas e instrumentos para la recolección de información

2.5.1. Fuentes de información

Al ser una investigación tipo documental se utilizó fuentes primaria y secundaria de organismos gubernamentales y no gubernamentales afines a la información.

Fuentes primarias: Se identificó la información procedente de:

- Revisión de informes emitidos por el INEC desde el 2010 al 2016.
- Información de la Cámara de Industrias y Cámara de Comercio Manta.
- Datos Superintendencia de Compañías, Valores y Seguros del Ecuador.
- Modelos de seguridad

Fuentes secundarias:

- Información estadística y documental de otras fuentes de información.
- Información de artículos científicos y revistas oficiales.
- Página web del Instituto Nacional de Estándares y Tecnología (NIST), informes de estándares ISO.
- Publicaciones de tesis de investigación científica.
- Revisión literaria sobre el tema.

2.5.2. Técnicas para la recolección de información.

2.5.2.1. Técnica de investigación estadística.

Se consideró esta técnica de investigación para poder extraer información del fenómeno de estudio, a través de base de datos públicos de diferentes organismos gubernamentales y no gubernamentales involucrados con la información; para levantar información de los indicadores fijados en el estudio.

2.5.2.2. Técnica de investigación documental.

Se consideró esta técnica de investigación para poder recopilar información relacionada al tema de investigación y de todas las fuentes disponibles, tesis, revistas, páginas web, libros, informes técnicos, artículos científicos y toda aquella fuente válida, de las variables garantía, gobernanza, identidad y control de acceso, gestión de riesgos, servicio, despliegue, cumplimiento.

2.5.2.3. Técnica de investigación de campo.

Esta investigación recolectó información del objeto de estudio mediante el instrumento de encuesta sobre la aplicabilidad de la tecnología cloud computing en la seguridad informática. En el anexo 4 constan las columnas “técnica”, “instrumento”, “fuente de información” con la clasificación en la investigación de cada variable.

Escala aplicada para la evaluación de las variables: Se empleó la escala de Likert para medir y registrar cada uno de los indicadores asociados a las propiedades del fenómeno de investigación. Esta escala posee un conjunto de ítems figuradas en proposiciones positivas, de hechos o fenómenos sociales o naturales, comportamientos individuales y colectivos de instituciones o personas, en donde la muestra sometida a observación expresa su opinión o actitud. Cada ítem tiene grados de respuestas que van de lo más favorable a lo menos favorable y obtener de la muestra, opinión y parecer de forma objetiva y precisa.

Cuadro No. 2.1 ESCALA DE LIKERT PARA LA MEDICIÓN DE LA SEGURIDAD INFORMÁTICA Y APLICABILIDAD EN EL CLOUD COMPUTING

ESCALA	CRITERIO	RANGO	
5	En total acuerdo con la seguridad	81%	100%
4	En acuerdo con la seguridad	61%	80%
3	Ni en acuerdo ni en desacuerdo con la seguridad	41%	60%
2	En desacuerdo con la seguridad	21%	40%
1	En total desacuerdo con la seguridad	0%	20%

Fuente: Marco teórico de la investigación
Elaborado por. Autor

2.6. Tratamiento de la información

Para el tratamiento de la información numérica se empleó la herramienta estadística IBM SPSS lo cual ayudó a establecer los resultados estadísticos, permitiendo realizar las comparaciones para comprender el tema de investigación. Se emplearon técnicas de medidas de tendencia central y de posición, como análisis de tabla de distribución de frecuencias, descriptivos, análisis de varianza y tabla de contingencia (tabla cruzada), gráficos de sectores, barras e histograma. Para el caso de las muestras se validó la base de datos empleando sólo los datos necesarios para el análisis, ejecutando y aplicando técnicas de selección de datos que brinda el software IBM SPSS.

CAPÍTULO III. RESULTADOS Y DISCUSIÓN

3.1. Análisis de la situación actual.

3.1.1. Breve reseña histórica de la seguridad informática y la tecnología del cloud computing en el Ecuador.

Según la investigación realizada, hace una década atrás existe una revolución orientada a la gestión de la información, producto del acceso al internet e integración de procesos en tola la red a nivel global.

Las interacciones entre los usuarios, siendo estos consumidores o proveedores, en la infraestructura que brinda el internet, o el cloud computing, es una tendencia tecnológica con gran avance en la actualidad, al tener muchas ventajas y competitividad. Por tal motivo el Ecuador lleva a cabo iniciativas como el gobierno en línea que está orientada a la transparencia de la gestión pública, consolidación de información y realización electrónica de trámites. Por su parte la entidad privada y las grandes empresas también han realizado innovaciones importantes en tecnología que les ha permitido la evolución empresarial y retorno de la inversión tecnológica.

Por todo este avance tecnológico también se tiene que evaluar aspectos sobre la seguridad informática, ya que al intercambiar información en internet, se puede ver afectado el activo más valioso, la información. La seguridad informática se ha convertido en una de los principales objetivos a preservar y mantener, por las diversas amenazas tanto físicas como lógicas, se puede vulnerar los sistemas de información ocasionando pérdida de información y afectando la empresa, medidas de seguridad y accesos vulnerados, dependencia en el control de aplicaciones y servicios en línea, reclamos de usuarios.

Según datos del Ministerio de Telecomunicaciones y de la Sociedad de la información (2015) a través de su página web menciona que en el Ecuador utilizan la red de Internet las micro, pequeñas y medianas empresas (MYPIMES)

representando un 52,8%, para la venta de productos, servicios, el uso el correo electrónico o redes sociales. Para el 2015 se obtuvo un 27,4% de empresas con presencia en la web, cabe mencionar que ciertas Mipymes no promocionan productos por la naturaleza de de clasificación perecibles, sin embargo dicho estudio establece que el uso de Internet es necesario para la interconexión con proveedores y clientes, obteniendo agilidad a actividades comerciales. Además menciona que el uso de las TIC, como el uso del Internet, ayudó a mejorar la gestión empresarial, representando un total de 95% de Mipymes, situadas en Quito, Guayaquil, Ambato, Cuenca, Machala, Manta, entre otras ciudades.

Actualmente la Secretaría Nacional de Administración Pública, considerando que las TIC son herramientas imprescindibles para el desempeño de institucional e interinstitucional, y como respuesta a la necesidad gestionar de forma eficiente y eficaz la seguridad de la información en las entidades públicas, emitió los Acuerdos Ministeriales No. 804 y No. 837, de 29 de julio y 19 de agosto de 2011 respectivamente, mediante los cuales creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicaciones; se realizó un análisis de la situación respecto de la gestión de la Seguridad de la Información en las Instituciones de la Administración Pública Central, Dependiente e Institucional, llegando a determinar la necesidad de aplicar normas y procedimientos para seguridad de la información, adaptando una nueva cultura y procesos institucionales para su gestión.

3.1.2. Descripción de los sistemas de información que utilizan las empresas del sector industrial.

Hace unos años los sistemas de información tradicionales han venido evolucionando e integrando los procesos de toda la empresa para permitir un mejor control de la información, con innovación en tecnología y además implementación de nuevos y eficientes sistemas empresariales integrales.

La finalidad de los sistemas de información es lograr las metas corporativas, la excelencia operacional, desarrollar nuevos productos y servicios, ayudar en la toma de decisiones y obtener una ventaja competitiva. La seguridad de los

sistemas de información se evalúa según los elementos por lo que está compuesta la organización, la tecnología y la administración, procesos que aportan para la funcionalidad de una empresa en procesos como manufactura y producción, finanzas y contabilidad, ventas y marketing, y por su puesto recursos humanos.

En el cuadro 3.1 se detalla los diferentes sistemas de información que se utilizan actualmente y varias funcionalidades aplicadas en las grandes empresas del sector industrial manufacturero C10.

Cuadro No. 3.1 TIPOS DE SISTEMAS DE INFORMACIÓN APLICABLES AL CLOUD COMPUTING

SISTEMA DE INFORMACIÓN	DESCRIPCIÓN
Sistemas de planificación de recursos empresariales (ERP)	Integran los procesos de negocios en manufactura y producción, finanzas y contabilidad, ventas y marketing, y recursos humanos en un solo sistema de software. Cuentan con un conjunto de módulos de software integrados y una base de datos central que permite compartir datos entre muchos procesos de negocios y áreas funcionales diferentes en toda la empresa
Sistemas de administración de relaciones con el cliente (CRM)	Proveen información para coordinar todos los procesos de negocios que tratan con los clientes en ventas, marketing y servicio para optimizar los ingresos, la satisfacción de los clientes, ayuda a las empresas a identificar, atraer y retener los clientes más rentables; a proveer un mejor servicio a los consumidores existentes; y a incrementar las ventas.
Sistemas de administración de la cadena de suministro (SCM)	Ayuda a administrar las relaciones con los proveedores, empresas de compras, distribuidores y compañías de logística a compartir información sobre pedidos, producción, niveles de inventario, y entrega de productos y servicios, de modo que puedan surtir, producir y entregar bienes y servicios con eficiencia.
Sistemas de administración del conocimiento (KMS)	Permiten a las organizaciones administrar mejor los procesos para capturar y aplicar el conocimiento y la experiencia. Estos sistemas recolectan todo el conocimiento y experiencia relevantes en la empresa, para hacerlos disponibles en cualquier parte y cada vez que se requieran para mejorar los procesos de negocios y las decisiones gerenciales. También enlazan a la empresa con fuentes externas de conocimiento.
Sistemas de procesamiento de transacciones (TPS)	Efectúa y registra las transacciones diarias de rutina necesarias para realizar negocios.
Sistemas para inteligencia de negocios (BIS)	Se refiere a los datos y herramientas de software para organizar, analizar y proveer acceso a la información para ayudar a la toma decisiones más documentadas, incluyen los Sistemas de procesamiento de transacciones (TPS), Sitemas de información gerencial (MIS), Sistemas de soporte de decisiones (DSS), Sistemas de apoyo a ejecutivos (ESS)
Sistemas específicos	Muchos sistemas no son clasificables y por esto se llaman sistemas específicos o a medida. Una gestión de ganado, un control de stock, un sistema de facturación electrónica, enre otros. Son específicos porque fueron hechos para atender a una situación específica y no a toda la empresa como ocurre con el ERP.

Fuente: Datos de la investigación
Elaborado por: Autor

Ciertas empresas del sector industrial manufacturero, consideradas grandes empresas, utilizan éstos sistemas en la medida de disponibilidad de inversión tecnológica asequible y se desarrolle mecanismos de seguridad informática se incrementará el uso de los servicios en el cloud. Los sistemas de información que más se utiliza en las empresas del sector industrial tienen relación con el sistema de planificación recursos empresariales mediante el software de facturación electrónica, permitiendo a la empresa alcanzar objetivos en beneficio de la misma siendo competitiva en el sector.

En el cuadro 3.2 se visualiza los diferentes tipos de sistemas de información que utilizan las empresas del sector industrial manufacturero, actividad económica CIIU 10:

Cuadro No. 3.2 SISTEMAS D INFORMACIÓN UTILIZADOS POR EMPRESAS SECTOR INDUSTRIAL CIIU 10

INDUSTRIA MANUFACTURERA CIIU 10	SISTEMAS DE INFORMACIÓN						
	Sistemas de planificación de recursos empresariales (ERP)	Sistemas de administración de relaciones con el cliente (CRM)	Sistemas de administración de la cadena de suministro (SCM)	Sistemas de administración del conocimiento (KMS)	Sistemas de procesamiento de transacciones (TPS)	Sistemas para inteligencia de negocios (BIS)	Sistemas específicos (Software de facturación electrónica)
Conservas Isabel Ecuatoriana S.A.	✓	✓	×	×	×	×	✓
Industria Ecuatoriana Productora de Alimentos CA INEPACA	✓	✓	×	×	×	×	✓
Seafman Sociedad Ecuatoriana de Alimentos y Frigoríficos Manta C.A.	✓	✓	×	×	×	×	✓
Empacadora Bilbo S.A. Bilbosa	✓	✓	×	×	×	×	✓
Promopesca S.A.	✓	✓	×	×	×	×	✓
Productos Balanceados Coprobalan S.A.	×	×	×	×	×	×	✓
Usafish S.A.	✓	✓	×	×	×	×	✓
Panificadora Industrial Cia Ltda	×	×	×	×	×	×	✓
Oleaginosas del Puerto Olipuerto S.A.	×	×	×	×	×	×	✓
Ensuperior S.A.	×	×	×	×	×	×	✓
Mareroce Export Import Cia. Ltda.	×	×	×	×	×	×	✓
Dulcremo S.A.	×	×	×	×	×	×	✓
Aldanacorp S.A.	×	×	×	×	×	×	✓
Industria Atunera Arrecifes-Marinos S.A.	×	×	×	×	×	×	✓
Exportadora Pacifico Exportpacific S.A.	×	×	×	×	×	×	✓

Fuente: Datos de la investigación
Elaborado por. Autor

3.1.3. Descripción de un software de facturación electrónica como un sistema de información aplicable en tecnología cloud computing.

Los sistemas específicos como el software de facturación electrónica y los sistemas de planificación de recursos empresariales (ERP) y Sistemas de administración de relaciones con el cliente (CRM) son los más empleados por las grandes empresas, buscando garantizar la seguridad de la información, identidad y control de riesgos en los servicios y despliegue ligados al marco del cumplimiento legal.

Las empresas del sector industrial manufacturero, actividad económica CIIU 10, dispone de sistemas de información con la finalidad de brindar servicio y cuidar los intereses de toda la empresa, y como estrategia para el incremento de sus

ventas y la fidelización de clientes, también para garantizar la seguridad y control de la información además de salvaguardar datos personales de los clientes, con la finalidad de lograr mayor confiabilidad, aplicando tecnología de vanguardia y con las seguridades que rigen las normas, estándares y políticas de seguridad para las nuevas tecnologías.

Los sistemas de información siendo software dinámico dentro de los sistemas empresariales, pueden presentar vulnerabilidades ocasionando la materialización de amenazas que conllevan a la pérdida de la información y se pueden derivar de varios factores organizacionales, técnicos y ambientales debido a malas decisiones gerenciales; bajo esta situación se establece mecanismos de seguridad y control de la información.

3.1.3.1. Descripción del sistema de facturación electrónica bajo el contexto de los Sistemas de Planificación de recursos empresariales (ERP).

Las características esenciales del software de facturación electrónica son:

- Puntualidad.
- Ahorra suministros de oficina (papel, tinta, etc.) y tiempo.
- Facilidad en los procesos de auditoría.
- Mayor seguridad en el resguardo de documentos.
- Menor probabilidad de falsificación.
- Agilidad en la localización de información.
- Eliminación de espacios para almacenar documentos históricos.
- Procesamiento rápido y eficiente.
- Aportación en pro del medio ambiente.
- Registra un mayor control para recaudación de impuestos

Dentro de las características de tiene un sistema empresarial están:

- Control de actividades empresariales.
- Incrementos de imagen institucional.
- Software de gestión de facturación para ventas y compras, transacción comercial.

- Distribución de información general de la empresa.
- Integración de los sistemas de información de todos los procesos.
- Manejo seguro de transacciones electrónicas como transferencia bancarias, comercio electrónico, entre otras.
- Control de proveedores

3.1.4. Análisis de las tres dimensiones de la variable GARANTÍA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing

La variable independiente GARANTÍA mide la seguridad mediante las tres dimensiones Integridad: garantiza que la información no sea alterada en el contenido. Confidencialidad: asegura control de accesos para el acceso a la información. Disponibilidad: garantiza el alcance de forma oportuna y precisa, Se debe considerar fallos temporales, fallos prolongados y permanentes, denegación de servicio, valor concentrado. Se analizan a continuación:

3.1.4.1. Análisis de la dimensión INTEGRIDAD en función de la variable independiente GARANTÍA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión INTEGRIDAD se tomó la variable de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones en empresas por sectores económicos año 2015, aplicando el análisis estadístico de frecuencias determinando el porcentaje del uso de la firma electrónica como mecanismo para mantener la integridad de la información.

Nombre de la variable: tic17_firma_digital, tic135_seguridad.
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.3 DATOS DE LA VARIABLE tic17_firma_digital

Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	13	86,7	86,7	86,7
	NO	2	13,3	13,3	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.3 se identifica el uso de la firma electrónica con un porcentaje de 86,7% de aceptación. Para establecer una relación para las medidas de integridad aplicadas como la firma electrónica y algún software de seguridad se aplicó la técnica tabla de contingencia o tabla cruzada para obtener el porcentaje total y medir la dimensión integridad.

Cuadro No. 3.4 Tabla cruzada para medir la relación de integridad aplicada

tic135_seguridad*tic17_firma_digital tabulación cruzada

			Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet		
			SI	NO	Total
Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	SI	Recuento	8	2	10
		% del total	53,3%	13,3%	66,7%
	NO	Recuento	5	0	5
		% del total	33,3%	0,0%	33,3%
Total		Recuento	13	2	15
		% del total	86,7%	13,3%	100,0%

Los porcentajes y los totales se basan en respuestas.

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.4 se identifica los resultados de la tabla cruzada en donde se utilizó el uso de la firma electrónica y software de seguridad representando un porcentaje de 53,3% de utilización considerando las dos variables, y según la escala de Likert tiene un criterio de 3 puntos que significa que se está **NI EN ACUERDO NI EN DESACUERDO** con la seguridad considerando el principio de integridad mediante el uso de la firma electrónica y software de seguridad.

3.1.4.2. Análisis de la dimensión CONFIDENCIALIDAD en función de la variable independiente GARANTÍA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Se tomó las variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos año 2015, aplicando el análisis estadístico de frecuencia determinando el uso de una intranet como medio para identificar aspectos de confidencialidad.

Nombre de la variable: tic16_intranet.
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.5 DATOS VARIABLE TIC16_INTRANET PARA ANÁLISIS DE CONFIDENCIALIDAD

Su empresa ¿Contaba con intranet en el 2015?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	9	60,0	60,0	60,0
	NO	6	40,0	40,0	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.5 se identifica el uso de una intranet como medida para controlar las conexiones con un valor de 60% y de esa manera asegurar la confidencialidad, según la escala de Likert tiene un criterio de 3 puntos que significa **NI EN ACUERDO NI EN DESACUERDO** con la seguridad en el uso de una intranet para controlar los roles de usuarios mediante el acceso a la misma.

3.1.4.3. Análisis de la dimensión DISPONIBILIDAD en función de la variable independiente GARANTÍA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión DISPONIBILIDAD se aplicó la técnica documental analizando la importancia de la disponibilidad dentro de un sistema de información para garantizar la seguridad informática y la forma cómo manejarla.

La disponibilidad se mide por el tiempo de reparación cuando un sistema no está disponible debido a Fallos temporales, Fallos prolongados y Denegación del servicio. Para calcular el porcentaje de disponibilidad se aplica el cálculo basado en el manual de ITIL v3 referente a la Gestión de Niveles de Servicio y Gestión de la Disponibilidad.

Cuadro No. 3.6 FÓRMULA PARA EL PORCENTAJE DE DISPONIBILIDAD

$$\%\text{Disponibilidad} = \frac{\text{Tiempo de Disponibilidad Acordado (AST) - Interrupción del Servicio durante el tiempo el tiempo de Disponibilidad Acordado (DT)}}{\text{Tiempo de Disponibilidad Acordado}}$$

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

La disponibilidad mantiene un fuerte impacto en todo entorno de TI, el elemento clave que caracteriza a esta dimensión es la fiabilidad que se basa en la redundancia para mayor tolerancia a los fallos, y equivale en la escala de Likert un valor de 5 puntos que significa se está **EN TOTAL ACUERDO** con la seguridad considerando el principio de disponibilidad como elemento fundamental en todo sistema de información como el software de facturación electrónica.

3.1.5. Análisis de las dos dimensiones de la variable GOBERNANZA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente GOBERNANZA mide la seguridad mediante las dos dimensiones políticas y normas/estándar, se plantea las normas como un conjunto de lineamientos, reglas, recomendaciones y controles a seguir para garantizar la seguridad en cualquier entorno de TI; y las políticas como una forma

de comunicación ya que constituyen un canal formal de actuación. Se analizan a continuación:

3.1.5.1. Análisis de la dimensión NORMAS/ESTÁNDAR en función de la variable independiente GOBERNANZA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión NORMAS/ESTÁNDAR se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la investigación referentes a los aspectos principales de las normas y estándares dentro de un sistema de información como el software de facturación para garantizar la seguridad informática.

Nombre de la variable: VI02gobernanza13
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.7 VALORACIÓN EN LA IMPORTANCIA DE LA NORMA ISO 27002
VI02goberanza13

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Alta	3	20,0	20,0	20,0
	Muy alta	12	80,0	80,0	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.7 se valora la importancia de la norma ISO 27002 en los sistemas de información como el software de facturación electrónica, basándose en recomendaciones y controles de las mejores prácticas de gestión, que representa un 80% de importancia y equivale en la escala de Likert a un valor de 4 puntos que significa que se está **EN ACUERDO** con la seguridad para iniciar, implementar o mantener los sistemas de gestión de seguridad.

3.1.5.2. Análisis de la dimensión POLÍTICAS en función de la variable independiente GOBERNANZA en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión POLÍTICAS se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la investigación referentes políticas y procedimientos internos para el manejo de seguridad de un sistema de información como el software de facturación.

Nombre de la variable: VI07cumplimiento_rev2
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.8 IMPORTANCIA DE POLÍTICAS DE SEGURIDAD Y PROCEDIMIENTOS INTERNOS VI07cumplimiento_rev2

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	En acuerdo	13	86,7	86,7	86,7
	En total acuerdo	2	13,3	13,3	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.8 se mide la importancia de las políticas de seguridad informática y procedimientos internos que representa un 86,7% de aceptación con esta medida para la empresa, y equivale en la escala de Likert a un valor de 5 puntos que significa que se está **EN TOTAL ACUERDO** con la seguridad considerando la importancia de las políticas y procedimientos para el buen manejo de la seguridad.

3.1.6. Análisis de las dos dimensiones de la variable IDENTIDAD Y CONTROL DE ACCESO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente IDENTIDAD Y CONTROL DE ACCESO mide la seguridad mediante las dos dimensiones autenticación y control de acceso, se

plantea las medidas empleadas como método de autenticación y la conexión a intranet, control de acceso, firmas digitales para garantizar la seguridad en cualquier entorno de TI. Se analizan a continuación:

3.1.6.1. Análisis de la dimensión AUTENTICACIÓN en función de la variable independiente IDENTIDAD Y CONTROL DE ACCESO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión AUTENTICACIÓN se tomó las variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos año 2015, aplicando el análisis estadístico de frecuencia determinando la existencia de mecanismos de autenticación y para el manejo de seguridad a través de software de seguridad.

Nombre de la variable: tic135_seguridad
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.9 DATOS DE LA VARIABLE tic135_seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	10	66,7	66,7	66,7
	NO	5	33,3	33,3	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.9 se identifica el uso de software de seguridad que representa un 66,7% de utilización de software, y equivale en la escala de Likert a un valor sobre los 4 puntos que significa que se está **EN ACUERDO** con la seguridad, dónde se emplean mecanismos de autenticación como el uso de usuarios y contraseñas para el acceso del software.

3.1.6.2. Análisis de la dimensión CONTROL DE ACCESO en función de la variable independiente IDENTIDAD Y CONTROL DE ACCESO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión CONTROL DE ACCESO se tomó la variable de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones (TIC) en empresas por sectores económicos año 2015, aplicando medidas de tendencia central y de posición estadísticas determinando el uso del internet e intranet como medio para identificar aspectos de confidencialidad.

Nombre de la variable: control_accesos_var compuesta por tic5_conexion_internet, tic16_intranet, tic17_firma_digital, c_accesos
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.10 MEDICIÓN DEL CONTROL DE ACCESO variable control_accesos_var

$control_accesos_var frecuencias

		Respuestas
		Porcentaje
$control_accesos_var[a]	SI	86,7%
	NO	13,3%
Total		100,0%

a. Grupo

$control_accesos_var frecuencias

		Respuestas
		Porcentaje
[a]	¿Disponía su empresa de conexión a internet en el 2015?	38,5%
	Su empresa ¿Contaba con intranet en el 2015?	23,1%
	Para realizar gestión electrónica completa, sin necesidad de ningún trámite adicional en papel	38,5%
Total		100,0%

a. Grupo de dicotomía tabulado en el valor 1.

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

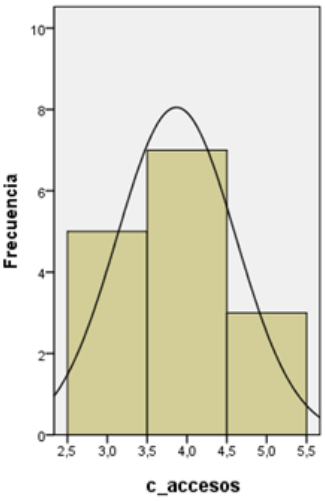
En el cuadro 3.10 se identifica el uso de respuestas múltiples para determinar medir el control de acceso a través de las variables, representando un 86,7% de confirmación sobre el manejo del control de acceso, y equivale en la escala de Likert a un valor sobre los 5 puntos que significa que se está **EN TOTAL**

ACUERDO con la seguridad conforme al personal que utiliza computadoras para el uso de internet e intranet para el control de accesos.

Cuadro No. 3.11 ESTADÍSTICAS DE MEDIDAS DE TENDENCIA CENTRAL

c_accesos

N	Válido	15
	Perdidos	0
Media		3,87
Error estándar de la media		,192
Mediana		4,00
Moda		4
Desviación estándar		,743
Varianza		,552
Asimetría		,227
Error estándar de asimetría		,580
Curtosis		-,970
Error estándar de curtosis		1,121
Suma		58



Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.11 se empleó las medidas de tendencia central sobre la muestra, que indica diferentes cantidades para cada una de las variables.

N VÁLIDO: Este valor representa la cantidad de datos que se analizaron en la muestra y representan la adopción de seguridad aplicada en las empresas del sector industrial en el año 2015.

ASIMETRÍA: El valor de 0,227 indica que la seguridad tiene asimetría negativa debido a que se encuentra sobre la media aritmética.

CURTOSIS: El valor de -0,970 representa una curva platicúrtica debido a que existe menor concentración de los datos en relación a la media.

MEDIA: Con el valor de 1,55 representa que 10 empresas han adoptado un tipo de seguridad.

MODA: Con el valor de 4 representa que más se repite que se haya adoptado algún tipo de seguridad.

MEDIANA: Con el valor de 4 siendo el promedio resultante de la suma dividida por el número de casos.

VARIANZA: El valor de 0,552 representa una baja dispersión de los datos.

3.1.7. Análisis de las cuatro dimensiones de la variable GESTIÓN DE RIESGOS en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente GESTIÓN DE RIESGOS mide la seguridad informática en cuatro dimensiones: responsabilidades, procedimientos, respuesta a incidentes, marco de referencia, los cuales se analizan a continuación:

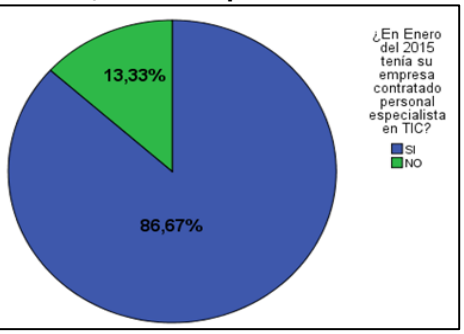
3.1.7.1. Análisis de la dimensión RESPONSABILIDADES en función de la variable independiente GESTIÓN DE RIESGOS en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión RESPONSABIIDADES se tomó variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones (TIC) en empresas por sectores económicos año 2015, aplicando la comparación de medias determinando el porcentaje de especialistas tics en la empresa, además de determinar la cantidad de hombres y mujeres.

Nombre de la variable: tic14_especialistas_tic, tic141_especialistas_tic_m, tic142_especialistas_tic_h
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.12 PORCENTAJE DE ESPECIALISTAS TICS EN LAS EMPRESAS
tic14_especialistas_tic, tic141_especialistas_tic_m, tic142_especialistas_tic_h

¿En Enero del 2015 tenía su empresa contratado personal especialista en TIC?		Mujeres especialistas en TIC	Hombres especialistas en TIC
SI	N	13	13
	Suma	12	49
	% de N total	86,7%	86,7%
NO	N	2	2
	Suma	0	0
	% de N total	13,3%	13,3%
Total	N	15	15
	Suma	12	49
	% de N total	100,0%	100,0%



Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.12 se identifica la cantidad de personal que son especialistas en tecnología, que representa un 86,67% de los cuales 12 son mujeres y 49 son hombres, y equivale en la escala de Likert a un valor de 5 puntos que significa que se está **EN TOTAL ACUERDO** con la seguridad evidenciando la importancia para una empresa contar con personal especializado en tecnología.

3.1.7.2. Análisis de la dimensión PROCEDIMIENTOS en función de la variable independiente GESTIÓN DE RIESGOS en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing

Para el análisis de la dimensión PROCEDIMIENTOS se aplicó la técnica documental analizando la importancia según la escala de Likert considerando el sistema de gestión de facturación aplicable en el cloud. Es necesario establecer los procedimientos adecuados para reducir y controlar las posibles amenazas.

Cuadro No. 3.13 Procedimientos para reducir y controlar posibles amenazas

Items	Procedimientos en función de la variable independiente gestión de riesgos en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing				
	Respuestas				
	En total acuerdo	En acuerdo	Ni en acuerdo ni es desacuerdo	En total desacuerdo	Porcentaje
1. Se realiza el plan de contingencia	✓				100%
2. Se debe identificar los requisitos legales y contractuales	✓				100%
3. Características escenciales del entorno	✓				100%
4. Se realiza la definición de políticas internas	✓				100%
5. Se debe establecer controles de acceso físico y lógico	✓				100%
6. Se debe documentar cada etapa a ejecutar	✓				100%
7. Debe existir comunicación entre las partes	✓				100%
				Puntuación total	100%

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

En el cuadro 3.13 se identifica que los procedimientos mantienen un fuerte impacto en la variable independiente gestión de riesgos que representa el 100%, por lo que equivale en la escala de Likert un valor de 5 puntos que significa se está **EN TOTAL ACUERDO** con la seguridad para la evaluación de los sistemas empresariales.

3.1.7.3. Análisis de la dimensión RESPUESTA A INCIDENTES en función de la variable independiente GESTIÓN DE RIESGOS en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing

La dimensión RESPUESTA A INCIDENTES busca que la empresa esté preparada para resolver eventualidades en el manejo de la gestión de riesgos.

Cuadro No. 3.14 PASOS EN LA RESPUESTA A INCIDENTES ANTE POSIBLES AMENAZAS EN EL MANEJO DE GESTIÓN DE RIESGOS

Items	Pasos en la respuesta ante incidentes				
	Respuestas				
	En total acuerdo	En acuerdo	Ni en acuerdo ni es desacuerdo	En total desacuerdo	Porcentaje
1. Se realiza la verificación	✓				100%
2. Se realiza un análisis del ataque	✓				100%
3. Se debe considerar la contención	✓				100%
4. Se realiza la recolección de evidencias	✓				100%
5. Se debe establecer la aplicación de soluciones	✓				100%
6. Se debe realizar la restauración del servicio	✓				100%
				Puntuación total	100%

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

En el cuadro 3.14 la respuesta a incidentes es un aspecto importante para saber solucionar y resolver los eventos ante amenazas y controlar las vulnerabilidades y mantiene un fuerte impacto en la variable independiente gestión de riesgos en la evaluación de los sistemas empresariales como lo es la facturación electrónica y representa el 100% por lo que equivale en la escala de Likert un valor de 5 puntos que significa se está **EN TOTAL ACUERDO** con la seguridad.

3.1.7.4. Análisis de la dimensión MARCO DE REFERENCIA en función de la variable independiente GESTIÓN DE RIESGOS en el uso de la facturación

electrónica en el software de gestión de facturación aplicable en el cloud computing

La dimensión MARCO DE REFERENCIA busca mejorar la eficiencia y eficacia de los sistemas de información gracias al aporte de procesos estandarizados y probados por empresas de diferentes sectores, y además la aplicación de metodologías y buenas prácticas en el manejo de la gestión de riesgos.

Cuadro No. 3.15 TIPOS DE MARCO DE REFERENCIA EN LA GESTION DE LA SEGURIDAD DE SISTEMAS DE INFORMACIÓN

MARCOS DE REFERENCIA		
DESCRIPCIÓN	**EVALUACIÓN**	**AUDITORÍA**
Cloud Security Matrix, matriz de controles de referencia para la seguridad propuesto por CloudSecurity Alliance, CSA	✓	✓
COBIT, Objetivos de control para la información y tecnologías relacionadas, propuesto por ISACA.	✓	✓
Norma ISO 27001-27002, Normas de seguridad de la información. Código de prácticas para los controles de seguridad de la información	✓	✓
ITIL, Biblioteca de Infraestructura de Tecnologías de la Información)	✓	✓

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

La adopción de un marco de referencia es un aspecto importante en una evaluación de riegos y auditoría y mantiene un fuerte impacto en la variable independiente gestión de riesgos en la evaluación de los sistemas empresariales como lo es la facturación electrónica, por lo que equivale en la escala de Likert un valor de 5 puntos que significa se está **EN TOTAL ACUERDO** con la seguridad.

3.1.8.Análisis de las tres dimensiones de la variable SERVICIO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente SERVICIO mide la seguridad informática en tres dimensiones: plataforma, software e infraestructura como servicio, los cuales se analizan a continuación:

3.1.8.1. Análisis de la dimensión PLATAFORMA COMO SERVICIO en función de la variable independiente SERVICIO en el uso de la facturación

electrónica en el software de gestión de facturación aplicable en el cloud computing

Para el análisis de la dimensión PLATAFORMA COMO SERVICIO se tomó variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones (TIC) en empresas por sectores económicos año 2015, aplicando la tabla de frecuencias determinando los servicios tipo plataforma como servicio.

Nombre de la variable: tic117_id
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.16 USO DE SERVICIO O APLICACIÓN PLATAFORMA COMO SERVICIO APLICANDO COMPARACIÓN DE MEDIAS

Negocio electrónico - Investigación y desarrollo		Software Libre - Sistemas Operativos (p. e. LINUX)	Software Libre - Navegadores de Internet (p. e. Mozila Firefox, Chrome, Opera, Safari)	Software Libre - Aplicaciones ofimáticas (p. e. Open Office)	Software Libre - Aplicaciones de código abierto para el procesamiento automático de información del tipo ERP o CRM	Software Libre - Otras, como sofware de seguridad (p. e. Open SSL, SSH), plataformas de aprendizaje (Moodie)
SI	N	3	3	3	3	3
	% de N total	20,0%	20,0%	20,0%	20,0%	20,0%
NO	N	9	9	9	9	9
	% de N total	60,0%	60,0%	60,0%	60,0%	60,0%
NO APLICA	N	3	3	3	3	3
	% de N total	20,0%	20,0%	20,0%	20,0%	20,0%
Total	N	15	15	15	15	15
	% de N total	100,0%	100,0%	100,0%	100,0%	100,0%

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.16 se identifica que existe un alto índice de no realizar investigación y desarrollo electrónica aplicado a una plataforma como servicio, y la utilización de aplicaciones de forma tradicional, por lo tanto representa un 20% de investigación y desarrollo para aplicaciones que no se aplican, por lo que equivale en la escala de Likert un valor de 1 punto que significa se está **EN TOTAL DESACUERDO** con la seguridad considerando la no utilización de la plataforma como servicio.

3.1.8.2. Análisis de la dimensión SOFTWARE COMO SERVICIO en función de la variable independiente SERVICIO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing

Para el análisis de la dimensión SOFTWARE COMO SERVICIO se tomó variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones (TIC) en empresas por sectores económicos año 2015, aplicando tablas de frecuencia determinando los servicios tipo software como servicio.

Nombre de la variable: tic8_web,tic10_interaccion_adm_pub, tic101_obtener_info_publicas,tic102_impreso_publicos,tic103_devolver_impresos,tic104_gestion_electronica,tic105_declaracion_impuestos,tic106_tramites_iess,tic107_portal_compras_publicas,tic111_gestion_cliente,tic112_control_pedidos, tic113_gestion_inventarios, tic114_gestion_finanzas, ic115_gestion_rrhh, tic116_soporte_ventas,tic117_id,tic118_gestion_conocimiento,tic122_correo_electronico, tic123_redes_sociales tic17_firma_digital
Técnica de investigación: Estadística
Instrumento: Base de datos 2015_TICEMPRESAS_BDD
Fuente: Secundaria

Cuadro No. 3.17 USO DE SERVICIO O APLICACIÓN SOFTWARE COMO SERVICIO

$saas frecuencias

		Respuestas
		Porcentaje
$saas[a]	SI	68,7%
	NO	24,0%
	NO APLICA	7,3%
Total		100,0%

a. Grupo

$saas frecuencias

		Respuestas
		Porcentaje
$saas[a]	Disponía su empresa de sitio o página web en el 2015?	7,3%
	¿Utilizó el internet para interaccionar con la administración pública?	7,3%
	Para obtener información a través de las páginas web de las Administraciones Públicas	6,8%
	Para conseguir impresos o formularios de las páginas web de las Administraciones Públicas	6,8%
	Para devolver impresos finalizados	5,3%
	Para realizar gestión electrónica completa, sin necesidad de ningún trámite adicional en papel	7,3%
	Declaración de impuestos	7,3%
	Trámites vinculados con el IEES	7,3%
	Acceder a documentación y especificaciones de artículos del Portal de Compras Públicas con el fin de participar en una licitación	1,0%
	Negocio electrónico - Gestión de relaciones con los clientes	4,4%
	Negocio electrónico - Control y seguimiento de pedidos	2,4%
	Negocio electrónico - Gestión de la cadena de suministros, logística, control de inventarios	2,9%
	Negocio electrónico - Gestión de finanzas y presupuestos	5,3%
	Negocio electrónico - Gestión de los recursos humanos	5,3%
	Negocio electrónico - Servicio y soporte de ventas	1,5%
	Negocio electrónico - Investigación y desarrollo	1,5%
	Negocio electrónico - Gestión del conocimiento	3,4%
	Medios de comunicación - Correo eléctrónico	7,3%
	Medios de comunicación - Redes Sociales	3,4%
	Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet	6,3%
Total		100,0%

a. Grupo de dicotomía tabulado en el valor 1.

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

En el cuadro 3.17 se identifica que existen varios servicios y aplicaciones que se utilizan en las actividades de las empresas que representa un 68,7% que emplean servicios o aplicaciones, por lo que equivale en la escala de Likert un valor de 4 puntos que significa se está **EN ACUERDO** con la seguridad considerando las aplicaciones utilizadas.

3.1.8.3. Análisis de la dimensión INFRAESTRUCTURA COMO SERVICIO en función de la variable independiente SERVICIO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing

Para el análisis de la dimensión INFRAESTRUTURA COMO SERVICIO se tomó variables de la base de datos del Instituto Nacional de Estadísticas y Censos referente al recurso Participación de Tecnologías de Información y Comunicaciones (TIC) en empresas por sectores económicos año 2015, aplicando tablas de frecuencia determinando los servicios tipo infraestructura como servicio que se ejecutan.

Nombre de la variable: tic131_sistemas_operativos, tic133_aplicaciones_ofimaticas, tic135_seguridad.

Técnica de investigación: Estadística

Instrumento: Base de datos 2015_TICEMPRESAS_BDD

Fuente: Secundaria

Cuadro No. 3.18 USO DE SERVICIO O APLICACIÓN INFRAESTRUCTURA COMO SERVICIO

$iaas frecuencias

		Respuestas
		Porcentaje
$iaas[a]	SI	77,8%
	NO	22,2%
Total		100,0%

a. Grupo

$iaas frecuencias

		Respuestas
		Porcentaje
$iaas[a]	Software Libre - Sistemas Operativos (p.e. LINUX)	37,1%
	Software Libre - Aplicaciones ofimáticas (p.e. Open Office)	34,3%
	Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	28,6%
Total		100,0%

a. Grupo de dicotomía tabulado en el valor 1.

Fuente: Datos recolectados de la investigación – Base de datos 2015_TICEMPRESAS_BDD
Elaborado por: Autor

Dentro de una infraestructura como servicio se ejecutan máquinas virtuales, servidores, almacenamiento, balanceo de carga, dispositivos de red, pero no se gestiona ni controla la infraestructura en el cloud sólo aplicaciones que utiliza; según la revisión bibliográfica es un riesgo alto que tienen las empresas además de la fuerte inversión. Asimismo al analizar los resultados de la base de datos se identifica el uso de infraestructura tradicional a través de sistemas operativos y servidores físicos, y es inversamente proporcional al uso de la infraestructura como servicio, mientras que el 22,2% se refiere a la no utilización de ésta, por lo tanto según la escala de Likert se da un valor de 2 puntos que significa se está **EN DESACUERDO** con la seguridad.

3.1.9. Análisis de la dimensión DESPLIEGUE en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente DESPLIEGUE mide la seguridad informática en cuatro dimensiones: Público, Privado, Híbrido, Comunitario; los cuales se analizan a continuación:

3.1.9.1. Análisis de la dimensión PÚBLICO en función de la variable independiente DESPLIEGUE en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión PÚBLICO se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la investigación referente a la importancia servicios o aplicaciones ejecutadas en un despliegue público.

Nombre de la variable: VI06despliegue_publico
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.19 VALOR DE IMPORTANCIA DE APLICACIONES O SERVICIOS EN UN DESPLIEGUE PÚBLICO

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy baja	2	13,3	13,3	13,3
	Baja	5	33,3	33,3	46,7
	Medio	8	53,3	53,3	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.19 se identifica que existe una valoración media que representa el 66,7% sobre los accesos a servicios o aplicaciones gratuitas o de pago en un despliegue público, por lo que equivale en la escala de Likert un valor de 3 puntos que significa se está **NI EN ACUERDO NI EN DESACUERDO** con la seguridad considerando un despliegue público.

3.1.9.2. Análisis de la dimensión PRIVADO en función de la variable independiente DESPLIEGUE en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión PRIVADO se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la

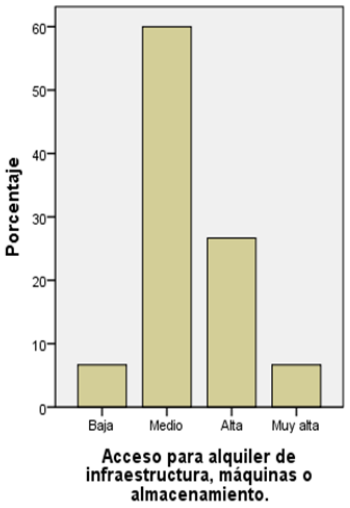
investigación referente a la importancia servicios o aplicaciones ejecutadas en un despliegue privado.

Nombre de la variable: VI06despliegue_privado
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.20 VALOR DE IMPORTANCIA DE UN DESPLIEGUE PRIVADO

VI06despliegue_privado

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Baja	1	6,7	6,7	6,7
	Medio	9	60,0	60,0	66,7
	Alta	4	26,7	26,7	93,3
	Muy alta	1	6,7	6,7	100,0
	Total	15	100,0	100,0	



Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.20 se identifica que existe una valoración muy alta que representa el 60% sobre los accesos para alquiler de infraestructura, máquinas o almacenamiento en un despliegue privado, por lo que equivale en la escala de Likert un valor de 3 puntos que significa se está **NI EN ACUERDO NI EN DESACUERDO** con la seguridad considerando un despliegue privado.

3.1.9.3. Análisis de la dimensión HÍBRIDO en función de la variable independiente DESPLIEGUE en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión HÍBRIDO se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la investigación

referente a la importancia servicios o aplicaciones ejecutadas en un despliegue híbrido, aplicando la tabla de frecuencia.

Nombre de la variable: VI06despliegue_hibrido
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.21 VALOR DE IMPORTANCIA DE UN DESPLIEGUE HÍBRIDO

VI06despliegue_hibrido

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy baja	1	6,7	6,7	6,7
	Baja	3	20,0	20,0	26,7
	Medio	10	66,7	66,7	93,3
	Alta	1	6,7	6,7	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.21 se identifica que existe una valoración muy alta que representa el 66,7% sobre si los ser vicios y datos se ejecutan de forma pública y privada, por lo que equivale en la escala de Likert un valor de 4 puntos que significa se está **EN ACUERDO** con la seguridad considerando un despliegue híbrido.

3.1.9.4. Análisis de la dimensión COMUNITARIO en función de la variable independiente DESPLIEGUE en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

Para el análisis de la dimensión COMUNITARIA se realizó una investigación de campo, la cual consistió en realizar una encuesta basada en los datos de la investigación referente a la importancia servicios o aplicaciones ejecutadas en un despliegue comunitario, aplicando la tabla de frecuencia.

Nombre de la variable: VI06despliegue_comunitario
Técnica de investigación: Recolección de campo
Instrumento: Encuesta
Fuente: Primaria

Cuadro No. 3.22 VALOR DE IMPORTANCIA DE DESPLIEGUE COMUNITARIO

VI06despliegue_comunitario

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Baja	3	20,0	20,0	20,0
	Medio	7	46,7	46,7	66,7
	Alta	3	20,0	20,0	86,7
	Muy alta	2	13,3	13,3	100,0
	Total	15	100,0	100,0	

Fuente: Datos recolectados de la investigación – Encuesta
Elaborado por: Autor

En el cuadro 3.22 se identifica que existe una valoración media que representa el 46,7% de importancia sobre recursos compartidos de forma comunitaria, por lo que equivale en la escala de Likert un valor de 3 puntos que significa se está **NI EN ACUERDO NI EN DESACUERDO** con la seguridad.

3.1.10. Análisis de la dimensión CUMPLIMIENTO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La variable independiente CUMPLIMIENTO mide la seguridad informática en dos dimensiones: requisitos legales y contractuales y revisiones de la seguridad de la información, los cuales se analizan a continuación:

3.1.10.1. Análisis de la dimensión REQUISITOS LEGALES Y CONTRACTUALES en función de la variable independiente CUMPLIMIENTO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La dimensión REQUISITOS LEGALES Y CONTRACTUALES busca evitar el incumplimiento de cualquier ley, obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad que ponga en peligro a la empresa, se deben aplicar cinco controles:

Cuadro No. 3.23 Controles en el cumplimiento legal para el entorno de seguridad informática

Controles en el cumplimiento legal
Identificación de la legislación aplicable.
Derechos de propiedad intelectual (DPI).
Protección de los registros de la organización.
Protección de datos y privacidad de la información personal.
Regulación de los controles criptográficos.

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

En el cuadro 3.22 los requisitos legales y contractuales son importantes ya que se deben definir y cumplir con los requisitos legales, por lo que equivale en la escala de Likert un valor de 5 puntos que significa se está **EN TOTAL ACUERDO** con la seguridad.

3.1.10.2. Análisis de la dimensión REVISIONES DE LA SEGURIDAD de la información en función de la variable independiente CUMPLIMIENTO en el uso de la facturación electrónica en el software de gestión de facturación aplicable en el cloud computing.

La dimensión REVISIONES DE LA SEGURIDAD de la información se realiza según las políticas de seguridad adecuada y realizar auditoría a las plataformas técnicas y sistemas de información para el cumplimiento de estándares para organización de la seguridad y controles documentados. Se aplican tres controles para las revisiones:

Cuadro No. 3.24 Controles para las revisiones de la seguridad informática

Controles para las revisiones de la seguridad informática
Revisión independiente de la seguridad de la información.
Cumplimiento de las políticas y normas de seguridad.
Comprobación del cumplimiento.

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

En el cuadro 3.24 las revisiones de seguridad se deben realizar con regularidad en todos los sistemas de información, por lo que equivale en la escala de Likert un valor de 4 puntos que significa se está **EN ACUERDO** con la seguridad.

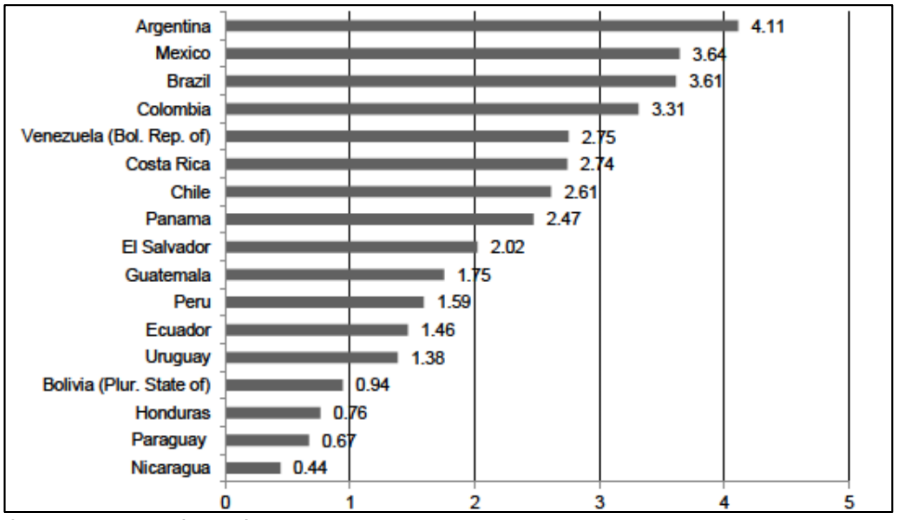
3.2. Análisis comparativo, evolución, tendencias y perspectivas

3.2.1. Análisis Evolutivo del Cloud Computing en el Ecuador

En Ecuador no se registran datos estadísticos del número de empresas que utilizan servicios de Cloud Computing, pero es evidente que se utilizan los servicios de Cloud gratuitos disponibles desde hace muchos años, se pueden mencionar: correos electrónicos, redes sociales, herramientas de almacenamiento como Google Drive, Dropbox, modificación de documentos en línea Google Docs, etc., control de ordenadores remotos; lo que ha evidenciado un desconocimiento sobre el uso de servicios de Cloud Computing.

Los servicios que ofrece la tecnología Cloud Computing son herramientas poco conocidas con características que pueden facilitar el trabajo y además ahorrar recursos a diversas empresas del Ecuador; en este país la tecnología cada vez evidencia mejoras de procesos productivos, por ende es vital un buen asesoramiento, implementación y desarrollo para lograr los objetivos tecnológicos e innovación y proteger la información. Basándose en el informe de CEPAL (2014) en referencia a la situación del Cloud Computing en América Latina, refleja que Ecuador tiene un nivel de adopción de un 1,46% lo que quiere decir que según el informe que considera una escala de 0 a 7, a Ecuador le falta muchos aspectos importantes para enfrentar la tecnología del cloud computing.

Cuadro No. 3.25 SITUACIÓN DEL CLOUD COMPUTING EN AMÉRICA LATINA



Fuente: Informe CEPAL (2014)
Elaborado por: CEPAL

La nueva legislación contempla varios artículos que están orientados a la protección de la información. Adicionalmente existen proveedores que están incursionando en el cloud computing ofreciendo servicios orientados a una IaaS, y SaaS, además de la facturación electrónica que brinda muchas ventajas.

3.2.2. Análisis FODA

Cuadro No. 3.26 ANÁLISIS FODA

FORTALEZAS	OPORTUNIDADES
Costes controlados	Incremento en estabilidad
Alcance del cliente	Nuevas tecnologías
Escalabilidad en infraestructura tecnológica	Certificaciones en seguridad de la información
Especialistas en el área de tecnología	Aumento del acceso a la inormación
Aumento de rentabilidad	Se integra a aplicaciones como ERP, CRM, etc
Reducción de costes en TI	Integración de tecnologias
DEBILIDADES	**AMENAZAS**
Alta inversión y mantenimiento de infraestructura	Fallo de seguridad, disponibilidad, confidencialidad, privacidad
Resistencia al cambio	Mercado en desarrollo
Desconfianza en nuevas tecnologías	Pérdida de control en los datos
Presencia de vulnerabilidades	Proveedores sin certificados en estándares de seguridad de la información
Poco conocimiento sobre la tecnología del cloud computing	Falta de regulación en seguridad de los datos
Falta de cultura en seguridad informática	Dependencia técnica de empresa

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

En el cuadro anterior se analizó la seguridad informática en función del sistema de gestión de facturación aplicable en la tecnología cloud computing desde la figura de la matriz FODA identificando los puntos relevantes.

3.2.3. Análisis de la matriz FOFA-DODA

En el cuadro siguiente se detalla las estrategias que se determinan a partir del análisis FODA en la seguridad informática en función del sistema de gestión de facturación aplicable en la tecnología cloud computing.

Cuadro No. 3.27 ANÁLISIS FOFA-DODA

MATRIZ FODA	OPORTUNIDADES	AMENAZAS
	O1. Incremento en estabilidad, seguridad en internet O2. Nuevas tecnologías O3. Certificaciones en seguridad de la O4. Aumento del acceso a la inormación 05. Soporte en uso de aplicaciones como ERP, CRM, etc O6. Integración de tecnologias	A1. Fallo de seguridad, disponibilidad, confidencialidad, privacidad A2. Mercado en desarrollo A3. Pérdida de control en los datos A4. Proveedores sin certificados en estándares de seguridad de la información A5. Falta de regulación en seguridad de los datos A6. Dependencia técnica de empresa
FORTALEZAS	**F.O**	**F.A**
F1. Despliegue de software, plataforma e infraestructura F2. Costes controlados y al alcance del cliente F3. Escalabilidad en infraestructura tecnológica F4. Especialistas en el área de tecnología F5. Aumento de rentabilidad F6. Reducción de costes en TI	F4. O3. O5. Contratar servicios de consultoría en seguridad de la información con personal certificado en normativas y estándares ISO 27000, COBIT, PCI, etc O4. F3. F5. O6. Planificar la implementación de nuevas tecnologías F1. O5 F3. O2. Aprovechar el poder adquisitivo de la tecnología cloud computing	F1. A2. A5. Promover la difusión de la importancia de la seguridad de la información F4. A1. A3. Promover la cultura de implementación de políticas de seguridad en tecnologías de la información y comunicaciones y utilización de buenas prácticas.
DEBILIDADES	**D.O**	**D.A**
D1. Alta inversión y mantenimiento de infraestructura D2. Resistencia al cambio D3. Desconfianza en nuevas tecnologías D4. Presencia de vulnerabilidades D5. Poco conocimiento sobre la tecnología del cloud computing D6. Falta de cultura en seguridad informática	O2. O5. D4. D6. Normar roles, funciones y perfiles de usuario. D6. O6. O3. D5. Desarrollar política internas de seguridad de la información.	D1. A1. A3. Adquirir tecnología de calidad para gestionar los procesos de la empresa D3. A2. D5. A4. Recibir capacitación para enfrentar los retos de las nuevas tecnologías A4.D1. Contar con proveedores confiables para resguardar la información

Fuente: Datos recolectados de la investigación
Elaborado por: Autor

3.3. Presentación de resultados y discusión

3.3.1. Correlación de las variables cualitativas.

Se estable la asociación aplicando tablas de contingencia para variables cualitativas inversión en tecnología y el uso de algún tipo de software de seguridad, tal como se muestra en el siguiente cuadro:

Cuadro No. 3.28 NIVEL DE ASOCIACIÓN ENTRE VARIABLES

tic17_firma_digital*tic135_seguridad tabulación cruzada

			tic135_seguridad		
			SI	NO	Total
tic17_firma_digital	SI	Recuento esperado	8,7	4,3	13,0
		% dentro de tic17_firma_digital	61,5%	38,5%	100,0%
		% dentro de tic135_seguridad	80,0%	100,0%	86,7%
		% del total	53,3%	33,3%	86,7%
	NO	Recuento esperado	1,3	,7	2,0
		% dentro de tic17_firma_digital	100,0%	0,0%	100,0%
		% dentro de tic135_seguridad	20,0%	0,0%	13,3%
		% del total	13,3%	0,0%	13,3%
Total		Recuento esperado	10,0	5,0	15,0
		% dentro de tic17_firma_digital	66,7%	33,3%	100,0%
		% dentro de tic135_seguridad	100,0%	100,0%	100,0%
		% del total	66,7%	33,3%	100,0%

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

El cuadro 3.28 determina el grado de asociación lineal, estableciendo la relación entre la integridad con la firma digital y algún tipo de software de seguridad.

CHI CUADRADO.- El estadístico observado 1,154 tiene una distribución de 1 grado de libertad (gl= 1) con una probabilidad de asociación de significancia de 0,283, lo que indica que existe una relación de independencia entre la integridad con la firma digital y algún tipo de software de seguridad.

Cuadro No. 3.29 PRUEBA DE CHI CUADRADO SOBRE DATOS CUALITATIVOS

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	1,154[a]	1	,283
Corrección de continuidad[b]	,072	1	,788
Razón de verosimilitud	1,772	1	,183
Prueba exacta de Fisher			
Asociación lineal por lineal	1,077	1	,299
N de casos válidos	15		

a. 3 casillas (75,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,67.

b. Sólo se ha calculado para una tabla 2x2

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

COEFICIENTE DE CONTINGENCIA C (KARL PEARSON).- Medida para el grado de aceptación de asociación entre dos conjuntos considerando la misma escala nominal en la tabla de contingencia (tabla cruzada), siendo el intervalo entre 0 y 1. El valor de 0 indica la independencia de la variable y el valor de 1 indica asociación de ambas, lo que resulta que mientras mayor es la medida indica intensidad de las variables.

Cuadro No. 3.30 NIVEL DE ASOCIACIÓN COEFICIENTE DE CONTINGENCIA

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	Coeficiente de contingencia	,267	,283
N de casos válidos		15	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el cuadro 3.30 se observa una asociación débil debido al valor resultante 0,267 que se encuentra en la zona de aceptación entre la integridad con la firma digital y algún tipo de software de seguridad.

COEFICIENTE DE CRAMER.- Mide el nivel de asociación de variables nominales o cualitativas cuando sus categorías son de dos o tres clases. El valor varía entre 0 y 1.

Cuadro No. 3.31 NIVEL DE ASOCIACIÓN COEFICIENTE DE CRAMER

Medidas simétricas

		Valor	Aprox. Sig.
Nominal por Nominal	V de Cramer	,277	,283
N de casos válidos		15	

Fuente: Datos de la investigación – Base de datos SPSS
Elaborado por: Autor

En el cuadro 3.31 se observa una asociación relativamente débil y la independencia de las variables.

COEFICIENTE PHI.- Este tipo de correlación no se aplica ya que la asociación es válida para variables tipo binario.

3.3.2. Resultado de la aplicación del modelo sobre la muestra.

Cuadro No. 3.32 RESULTADO DE LA INVESTIGACIÓN

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	DESCRIPCIÓN DE LA VARIABLE	EN TOTAL ACUERDO	EN ACUERDO	NI EN ACUERDO NI EN DESACUERDO	EN DESACUERDO	EN TOTAL DESACUERDO
					(5)	(4)	(3)	(2)	(1)
Seguridad informática	Garantía	1	Integridad	Detalle de medidas aplicadas para asegurar la integridad de la información			3		
		2	Confidencialidad	Disponibilidad de una intranet como medida en los roles de usuarios			3		
		3	Disponibilidad	Descriptión del iempo promedio de disponibilidad de un servicio	5				
	Gobernanza	4	Políticas	Políticas de seguridad informática	5				
		5	Normas/Estándar	Normas de seguridad informática					
	Identidad y control de acceso	6	Autenticación	Detalle de medidas empleadas como método de autenticación		4			
		7	Control de Acceso	Se cuenta o no con conexión a intranet, control de acceso, firmas digitales	5				
	Gestión de riesgos	8	Responsabilidades	Cantidad de personas que son especialistas en el uso de TIC.	5				
		9	Procedimientos	Procedimientos como medida en la gestión de riesgos	5				
		10	Respuesta a incidentes	Descripción de actividades como respuesta a incidentes en la gestión de riesgos	5				
		11	Marco de referencia	Tipos de marco de referencia	5				
	Servicio	12	Plataforma como servicio	Tipos de aplicaciones o servicios					1
		13	Software como servicio	Tipos de aplicaciones o servicios		4			
		14	Infraestructura como servicio	Tipos de aplicaciones o servicios				2	
	Despliegue	15	Público	Importancia del despliegue en la nube pública			3		
		16	Privado	Importancia del despliegue en la nube privada			3		
		17	Híbrido	Importancia del despliegue en la nube híbrida		4			
		18	Comunitario	Importancia del despliegue en la nube comunitaria			3		
	Cumplimiento	19	Requisitos legales y contractuales	Controles de requisitos legales y contractuales	5				
		20	Revisiones de la seguridad de la información	Controles de revisiones de seguridad de información		4			

Fuente: Datos de la investigación
Elaborado por: Autor

En el cuadro 3.32 se presenta el resultado de la ponderación de la escala de Likert sobre las 20 variables con las respectivas dimensiones. Se observa que 12 indicadores se encuentran en los niveles de aceptación de la seguridad y el resto de los indicadores que representa el 35% requieren de atención adyacente por no cumplir con las garantías de la seguridad informática en los sistemas de gestión de facturación electrónica aplicable a la tecnología cloud computing.

Entre los indicadores que requieren atención inmediata se encuentran garantizar la integridad, confidencialidad, evaluar la plataforma e infraestructura como servicio en un despliegue público, privado y comunitario según las diferentes aplicaciones que se utilicen.

CONCLUSIONES

El objetivo planteado en la investigación si permite identificar la relación de los modelos de seguridad informática fundamentados por los principios básicos de modelo de referencia de (Liu *et al.,* 2011) presentado por el Instituto Nacional de Normas y Tecnología, NIST, además se tomó información de la guía de seguridad para áreas críticas enfocadas a la seguridad en el cloud computing, publicada por el Cloud Security Alliance (2017) y la aportación de otros modelos.

La evaluación de este modelo mediante las veinte variables en función de la aplicabilidad de la tecnología del cloud computing fue a través de pruebas estadísticas, análisis relativos y cálculos porcentuales, se estableció una escala de valor por cada dimensión. La aplicación de la escala ayudó a identificar las dimensiones consideradas como un factor crítico que incide en la seguridad informática y su aplicabilidad en la tecnología cloud computing cumpliendo con los objetivos de la investigación.

Se evidencia que existen debilidades en las medidas para garantizar la seguridad informática, lo demuestra la garantía en la dimensión INTEGRIDAD, donde el valor de 3 puntos representa una ponderación de 53,3% asimismo lo demuestra la dimensión CONFIDENCIALIDAD con un valor de 3 puntos que representa una ponderación del 60%, ocupando en la escala una relación media en comparación a las 20 variables.

Para la variable SERVICIO se identificó dos dimensiones con puntaje bajo en relación a la escala aplicada, las cuales son PLATAFORMA COMO SERVICIO E INFRAESTRUCTURA COMO SERVICIO.

Según la valoración de la variable DESPLIEGUE la cual refiere al tipo de implementación donde se ejecuta un servicio o aplicación, se consideró tres dimensiones PÚBLICO, PRIVADO y COMUNITARIO representando en la escala una relación media representando 3 puntos cada una en la escala de Likert.

Además se determinó la correlación de las variables que permitió determinar la correspondencia de los datos recopilados, tomando para efecto del análisis las dimensiones INTEGRIDAD y CONTROL DE ACCESO mediante pruebas estadísticas de tablas de contingencia, chi cuadrado, coeficiente de contingencia (karl pearson) y coeficiente de cramer, en el cual se midió el grado de asociación lineal.

Se estableció que dentro de los entornos de tecnologías de la información como lo es la aplicabilidad del cloud computing y los sistemas de información, está presente los riesgos informáticos debido a las vulnerabilidades y amenazas, mediante el análisis de las variables y dimensiones según la escala de Likert; se determinó que existe debilidades para garantizar la seguridad y la privacidad de la información.

RECOMENDACIONES

Las iniciativas de adopción o migración de la infraestructura de TI a la tecnología cloud computing debe garantizar la seguridad de la información por lo que se sugiere realizar con optimización en sistemas, aplicaciones o datos que no son de criticidad y así lograr familiarizarse con el paradigma tecnológico del cloud.

Es necesario que exista una fuente de información oficial sobre el uso del cloud computing en las pequeñas, medianas y grandes empresas, con registros de los servicios, despliegue, gobernanza, gestión de riesgos y cumplimiento legal, como base de datos importante en el manejo de nuevas políticas y leyes que ayuden a la regularización y protección de los datos personales y de empresas.

Este trabajo de investigación servirá de aporte en las futuras investigaciones y se recomienda considerar los aspectos en los factores encontrados, considerando la necesidad de controles de accesos a servicios y aplicaciones en el cloud computing.

Es recomendable que la organización que adapte un modelo de seguridad informática tenga como base y principio en las políticas internas asegurar la privacidad de la información como el activo valioso de la misma.

A medida que aparecen nuevas aplicaciones o servicios será necesario la gestión y manejo de riesgos para contrarrestar y mitigar posibles fallos en el funcionamiento y aplicabilidad del cloud computing.

Es necesario que las empresas definan lineamientos y políticas internas fuertes para evitar ser víctimas de ataques informáticos debido a la divulgación de información confidencial en el manejo de la tecnología cloud computing.

Se recomienda considerar los elementos del modelo presentado basado principalmente en la disponibilidad, confidencialidad e integridad para garantizar y proveer de seguridad los entornos de tecnologías de la información en las empresas del sector industrial de la ciudad de Manta en la gestión empresarial.

REFERENCIAS BIBLIOGRÁFICAS

Agencia Europea de Seguridad de las Redes y de la Información, ENISA. (2009). Computación en Nube: Beneficios, riesgos y recomendaciones para la seguridad de la información. Madrid: España. Recuperado de https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish

Aguilera, L. P. (2010). Seguridad Informática. Recuperado de https://books.google.es/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=bell+seguridad+inofrmatica&ots=PpsqOyBDX0&sig=CK9G8FTiTTITGBUUUxpEHuManUM#v=onepage&q=bell&f=false

Areitio, B. (2008). Seguridad de la Información Redes, informática y sistemas de información. Madrid: España. Editorial Paraninfo S.A.

Blacio, K. (2015). Análisis y entrega de un plan para la gestión de seguridad de la información para empresas multinacionales de seguros con presencia en Ecuador. Recuperado de Repositorio Institucional de la Universidad de Guayaquil: http://repositorio.ug.edu.ec/handle/redug/11729

Cabrera, A. (2013). Estudio para implementación de servicios de data. Universidad de Cuenca, Cuenca. Recuperado de http://dspace.ucuenca.edu.ec/bitstream/123456789/4667/1/Tesis.pdf

Carmen de Pablos, José Joaquín López Hernández, Santiago Martín Romo, Sonia Medina. (2004). Informática y Comunicaciones en la empresa. Madrid, España. Editorial ESIC.

Casasola, R.M., Maqueo, R. M., Molina, R., Moreno, G.J., Recio, G.M. (2014). La nube: nuevos paradigmas de privacidad. Obregón: México. Editorial CIDE.

Comité de Seguridad de la Información. (2016). Esquema gubernamental de seguridad de la Informacion egsi. Recuperado de https://www.politica.gob.ec/wp-content/uploads/2017/04/EGSI.pdf

CSA, C. S. (2011). “Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0”. Recuperado de http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

CLOUD SECURITY ALLIANCE. (2017). The Security Guidance for Critical Areas of Focus in Cloud Computing v4.0 (“Guidance v4.0”). Cloud Security Alliance. Recuperado de https://cloudsecurityalliance.org/download/securityguidance-v4/

CLOUD SERVICES MEASUREMENT INITIATIVE CONSORTIUM, CSMIC. (2014). Introducing the service measurement index (SMI). California: Estados Unidos Recuperado de http://csmic.org/downloads/SMI_Overview_TwoPointOne.pdf.

Denning, P. (1971). Third Generation Computer Systems. New York: Estados Unidos. Editorial: ACM Computing Surveys.

Echenique J. A. (1990). Auditoría Informática. México: McGraw-Hill Interamericana.

Glossary, I. (2000). National information systems security (infosec) glossary.

Gonzáles L. Aspectos de seguridad informática en la utilización de cloud Computing. Recuperado de http://hdl.handle.net/10596/6173

Gómez, V. A. (2014). Enciclopedia de la Seguridad Informática, 2da Edición. España: RA-MA.

Gradiante. (3 de septiembre de 2010). Gradiante. Obtenido de Seguridad y privacidad en cloud computing. Recuperado de https://www.gradiant.org/noticia/seguridad-y-privacidad-en-cloud-computing-2/

Graham, G. y Denning P. (1972). Protection-Principles and Practice (Vol. 40). New Yersey: Estados Unidos Editorial: AFIPS Press.

Grance , T., & Mell, P. (2011). The NIST Definition of Cloud - Recommendations of the National Institute. NIST Special Publication 800-145. Recuperado de http://dx.doi.org/10.6028/NIST.SP.800-145

INSTITUTO NACIONAL DE ESTADÍSTICAS Y CENSOS. (2015). INEC. Recuperado de Instituto Nacional de Estadísticas y Censos:http://produccion.ecuadorencifras.gob.ec/QvAJAXZfc/opendoc.htm?document=empresas_test.qvw&host=QVS%40virtualqv&anonymous=true

INTECO. (2011). Seguridad y privacidad del cloud computing. Recuperado de http://www.inteco.es/file/2KMNG7mbyKb6gqdnJquPKw

ISACA. (2012 de 2012). IT Control Objectives for Cloud Computing. Recuperado de https://www.isaca.org/chapters2/kampala/newsandannouncements/Documents/IT%20contro%20objectives%20for%20Cloud%20computing.pdf

Jansen, W., Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing. Computer Security. NIST. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Jara, J. (2012). Guía para el análisis de factibilidad en la implantación de tecnologías de cloud computing en empresas del Ecuador. Quito: EPN. Recuperado de bibdigital.epn.edu.ec/bitstream/15000/4649/1/CD-4281.pdf

Johnston, S. (2004). Modeling security concerns in service-oriented architectures. Somers, Nueva York, Estados Unidos: IBM Corporation. Recuperado de https://pdfs.semanticscholar.org/4c59/4dbd2c45cd6779551f3961174053c59b78b9.pdf

Joyanes, A. (2013). Computación en la nube. Notas para una estrategia española en cloud computing. España: Revista del Instituto Español de Estudios Estratégicos. Recuperado de https://cover.vectorsf.net/index.php/ieee/article/view/10

Lampson, B. (1971). Protection. Princeton: ACM SIGOPS Operating Syst. New York: Estados Unidos.

Landwher, E. C. (1981). A survey of formal model for computer security. Washington: CSUR.

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. y Leaf, D. (September de 2011). NIST Cloud Computing Reference Architecture. Recommendations of the National. Gaithersburg: Estados Unidos. Editorial Natl. Inst. Stand. Technol. Spec.

Medina F. (2011). Arquitectura y Modelos de Seguridad. Recuperado de http://seguridad.capacitacionentics.com/2012-1-Seguridad_Informatica_Tema3.pdf

Mieres, J. (2009). Ataques Informáticos Debilidades de seguridad comúnmente explotadas. Recuperado de evilfingers:

https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Ministerio de Telecomunicaciones y Sociedad de la información. (2015). Obtenido de https://www.telecomunicaciones.gob.ec/el-823-de-mipymes-en-el-ecuador-utilizan-internet/

Organización Internacional de Normalización, ISO (2013). Organización Internacional para la Estandarización ISO/IEC 27001. Recuperado de https://www.iso.org/isoiec-27001-information-security.html

Organización Internacional de Normalización, ISO (2013). Organización Internacional para la Estandarización ISO/IEC 27002. Recuperado de https://www.iso.org/standard/54533.html

Organización Internacional de Normalización, ISO (2014). Organización Internacional para la Estandarización ISO/IEC 27018. Recuperado de https://www.iso.org/standard/61498.html

Organización Internacional de Normalización, ISO (2015). Organización Internacional para la Estandarización ISO/IEC 27017. Recuperado de https://www.iso.org/standard/43757.html

Organización Internacional de Normalización, ISO. (2009). ISO27000. Recuperado de http://www.revistavirtualpro.com:http://www.revistavirtualpro.com/biblioteca/iso-27000

Cloud Special Interest Group y PCI Security Standards Counci. (2013). Information Supplement: PCI DSS Cloud Computing Guidelines. Recuperado de https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Ponniah, P. (2002). Data Warehousing Fundamental: A comprehensive guide for IT. New York: Estados Unidos. Editorial John Whiley & Sons Inc.

Solórzano, L, Rezabala, J, Aranda, A. (2013). Estudio sobre el estado del arte de la seguridad informática en el Ecuador y sus necesidades reales. Recuperado de DSpace en ESPOL: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/24298

Tescari, J. (2011). Definición y Características de la Seguridad de la Información. Recuperado de http://749jesus.blogspot.com.co/2011/04/definicion-ycaracteristicas-de-la.html

Whitman, M. M. (2014). Management of Information Security Forth Edition. Standford: Estados Undios. Esitorial Cengage Learnig.

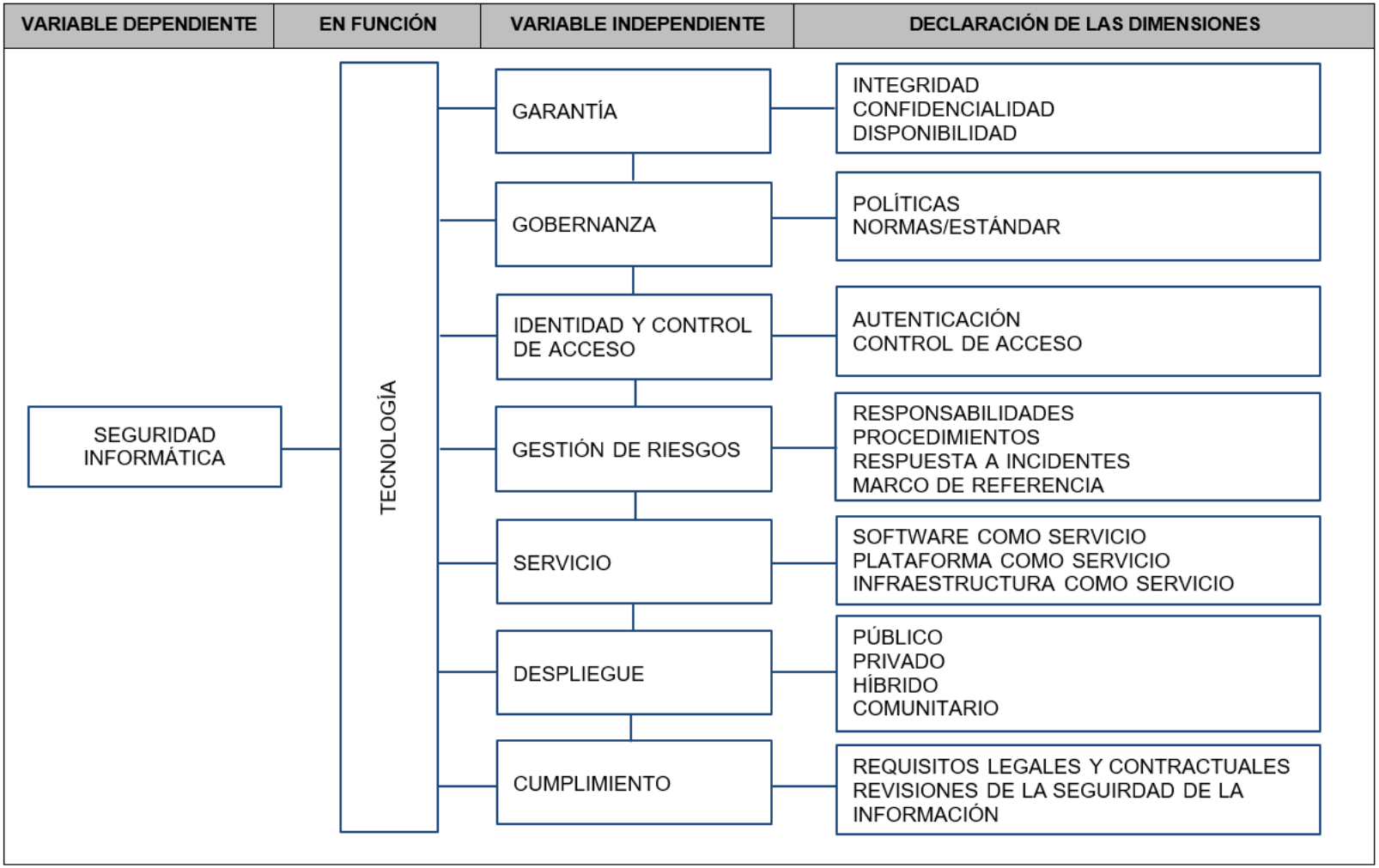
Youseff, L. Butrico M. y Da Silva D. (2015). Toward a Unified Ontology of cloud computing. California Santa barbara: Estados Unidos. Editorial IEEE

Anexo 1 Matriz auxiliar de operación en el diseño del trabajo de investigación

PROBLEMA	OBJETIVO	OPERACIONALIZACIÓN DE VARIABLES			
FORMULACIÓN DEL PROBLEMA	**GENERAL**	**VARIABLE DEPENDIENTE**	**VARIABLE INDEPENDIENTE**	**DIMENSIÓN**	**INDICADOR**
¿De qué manera incide la aplicabilidad del cloud computing en la seguridad informática de las empresas del sector industrial en la ciudad de Manta de la provincia de Manabí?	Estudiar los factores que inciden en la seguridad informática y su aplicabilidad en el cloud computing, para las empresas del sector industrial de la ciudad de Manta en la Provincia de Manabí	**Seguridad informática**	Garantía	Integridad	Permisos de usuarios
				Confidencialidad	Roles de usuarios
				Disponibilidad	Porcentaje de disponibilidad Tiempo promedio de falla. Tiempo promedio de recuperación
			Gobernanza	Políticas	Políticas aplicadas/Total Políticas adecuadas
				Normas/Estándar	Número de norma/estándar para el cloud
SISTEMATIZACIÓN	**ESPECÍFICOS**		Identidad y control de acceso	Autenticación	Métodos de autenticación
				Control de Acceso	Mecanismos de control de acceso
¿Es necesario que exista control de acceso a servicios y aplicaciones en el cloud computing? ¿Es indispensable para una organización la seguridad y privacidad de la información en todo momento? ¿Puede existir falla de los servicios y aplicaciones del cloud computing? ¿Es posible ser víctimas de ataques informáticos debido a la divulgación de información confidencial?	Analizar teóricamente los modelos de seguridad informática y su aplicabilidad en el cloud computing. Identificar las principales amenazas en los sistemas de información. Identificar las principales vulnerabilidades en los sistemas de información. Determinar los riesgos informáticos en el servicio de cloud computing. Determinar los principales mecanismos de seguridad informática para la protección de la información en el cloud computing. Analizar los servicios que ofrece la tecnología del cloud computing para las empresas del sector industrial de la ciudad de Manta en la provincia de Manabí. Indicar la regulación, normatividad y/o leyes, existente en el país para la tecnología del Cloud Computing		Gestión de riesgos	Responsabilidades	Personal especialistas en área de tecnología
				Procedimientos	Técnica y Procedimiento
				Respuesta a incidentes	Actividades de respuesta
				Marco de referencia	Marco de referencia
			Servicio	Plataforma como servicio	Propiedad de servicio como plataforma
				Software como servicio	Propiedad de servicio como software
				Infraestructura como servicio	Propiedad de servicio como infraestructura
			Despliegue	Público	Recursos asociados automatizados
				Privado	Recursos con arrendamientos
				Híbrido	Elementos compartidos
				Comunitario	Recursos compartidos
			Cumplimiento	Requisitos legales y contractuales	Requisitos legales
				Revisiones de la seguridad de la información	Revisión de cumplimiento

Fuente: Datos de la Investigación
Elaborado por: Autor

Anexo 2 Modelo conceptual aplicado a la investigación



Fuente: Datos recopilados de la investigación a partir del modelo NIST500-592 y otros modelos teóricos para determinar factores que inciden en la seguridad informática y su aplicabilidad en la tecnología cloud computing.
Elaborado por. Autor

Anexo 3 Antecedentes bibliográficos de las variables, dimensiones e indicadores

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	N°	DIMENSIÓN	INDICADORES	ANTECEDENTES TEÓRICOS
Seguridad informática	Garantía	1	Disponibilidad	Permisos de usuarios	Lampson, B.W., (1971). Protection. Editorial ACM SIGOPS Operating Syst. Princeton
		2	Confidencialidad	Roles de usuarios	Denning, P.S., (1971). Third Generation Computer Systems. Editorial ACM Computing Surveys
		3	Integridad	Porcentaje de disponibilidad Tiempo promedio de falla Tiempo promedio de recuperación	Gradiante. (3 de septiembre de 2010). Gradiante. Obtenido de Seguridad y privacidad en cloud computing
	Gobernanza	4	Políticas	Políticas aplicadas/Total Políticas adecuadas	Aguilera L., P, (2010). Seguridad Informática. Editorial EDITEX
		5	Normas ISO	Número de norma/estándar para el cloud	Medina L. F. (20 de septiembre de 2011). Arquitectura y Modelos de Seguridad.
	Identidad y control de acceso	6	Autenticación	Métodos de autenicación	Jansen Wayne, Grance Timothy (2011). Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144
		7	Control de Acceso	Mecanismos de control de acceso	Grance , T., & Mell, P. (2011). The NIST Definition of Cloud - Recommendations of the National Institute. NIST Special Publication 800-145.
	Gestión de riesgos	8	Responsabilidades	Personal sspecialistas en área de tecnología	Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. & Leaf, D., (2011). NIST Cloud Computing Reference Architecture Recommendations of the National. Natl. Inst. Stand. Technol. Spec. Gaithersburg
		9	Procedimientos	Técnica y Procedimieno	ISACA (2012). IT Control Objectives for Cloud Computing.
		10	Respuesta a incidentes	Actividades de respuesta	NORMA ISO. (2013). Organización Internacional para la Estandarización ISO/IEC 27001.
		11	Marco de referencia	Marco de referencia	NORMA ISO. (2013). Organización Internacional para la Estandarización ISO/IEC 27002.
	Servicio	12	Plataforma como servicio	Propiedad de servicio como plataforma	INEN ISO/IEC, 2. (2013). Esquema Gubernamental de Seguridad de la Información EGSI.
		13	Software como servicio	Propiedad de servicio como software	NORMA ISO. (Agosto de 2014). Organización Internacional para la Estandarización ISO/IEC 27018.
		14	Infraestructura como servicio	Propiedad de servicio como infraestructura	Whitman, M., Mattord, H. (2014). Management of Information Security Forth Edition. Estados Unidos: Standford. Editorial Cengage Learnig basado en la teoría de John MacCumber (1991). Assessing and Managing Security Risk in IT Systems a Structured Methodology
	Despliegue	15	Público	Recursos asociados automatizados	NORMA ISO. (2015). Organización Internacional para la Estandarización ISO/IEC 27017.
		16	Privado	Recursos con arrendamientos	PCI, DSS, Cloud Special Interest Group Y PCI Security Standars Council (2013).
		17	Híbrido	Elementos compartidos	CSMIC, Carnegie Mellos University Silicon Valley (2014). Introducing the service measurement index (SMI). Editorial Moffett Field. CA USA
		18	Comunitario	Recursos compartidos	Blacio, K. (2015). Análisis y entrega de un plan para la gestión de seguridad de la información para empresas multinacionales de seguros con presencia en Ecuador.
	Cumplimiento	19	Requisitos legales y contractuales	Requisitos legales	Youseff, L. Butrico, M., Da Silva, D., (2015). Toward a Unified Ontology of cloud computing. Santa Clara
		20	Revisiones de la seguridad de la información	Revisión de cumplimiento	Information Supplement: PCI DSS Cloud Computing Guidelines.

Fuente: Datos de la Investigación
Elaborado por: Autor

Anexo 4 Parte A Variables de la investigación, operacionalización

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	INDICADORES	NOMBRE VARIABLE INDEPENDIENTE	PREGUNTAS O ITEMS	TÉCNICAS	INSTRUMENTO	FUENTE	PROCESAMIENTO	TIPO DE INFORMACIÓN
Seguridad informática	Garantía	1	Integridad	Permisos de usuarios	VI01	¿Cuáles son las medidas aplicadas para asegurar la integridad de la información?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		2	Confidencialidad	Roles de usuarios		¿Cuáles son las medidas para el control de roles de usuarios que garantizan la confidencialidad?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		3	Disponibilidad	Porcentaje de disponibilidad Tiempo promedio de falla Tiempo promedio de recuperación		¿La disponibilidad es un factor importante para los servicios en el cloud computing?/ ¿Cuál es el porcentaje de disponibilidad de un servicio?/ ¿Cuál es el intervalo de tiempo promedio de falla de un servicio? / ¿Cál es el tiempo promedio necesario para reparar las fallas?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA
	Gobernanza	4	Políticas	Políticas aplicadas/Total Políticas adecuadas	VI02	¿Aplica las políticas y buenas prácticas para la seguridad en el cloud computing?	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
		5	Normas/Estándar	Número de norma/estándar		¿Aplica las normas que rigen en la seguridad informática?	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
	Identidad y control de acceso	6	Autenticación	Medidas de autenicación	VI03	¿Qué medidas aplica como método de autención en el control de accesos?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		7	Control de Acceso	Mecanismos de control de acceso		¿Qué medidas utiliza como mecanismo en el control de acceso?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
	Gestión de riesgos	8	Responsabilidades	Personal sspecialistas en área de tecnología	VI04	¿Tiene personal contratado especialista en tecnologías de la información y comunicaciones?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		9	Procedimientos	Técnica y Procedimiento		¿Qué procedimientos se aplican en la gestión de riesgos para el cloud computing?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA
		10	Respuesta a incidentes	Actividades de respuesta		¿Qué actividades se aplican para la restauración de un servicio?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA
		11	Marco de referencia	Marco de referencia		¿Qué marco de referencia se aplica en la tecnología cloud computing?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA

Fuente: Marco teórico y datos de la Investigación
Elaborado por: Autor

Anexo 4 Parte B Variables de la investigación, operacionalización

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	INDICADORES	NOMBRE VARIABLE INDEPENDIENTE	PREGUNTAS O ITEMS	TÉCNICAS	INSTRUMENTO	FUENTE	PROCESAMIENTO	TIPO DE INFORMACIÓN
Seguridad informática	Servicio	12	Plataforma como servicio	Elementos de servicio como plataforma	VI05	¿Cuál son los servicios o aplicaciones que utiliza en la plataforma como servicio?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		13	Software como servicio	Elementos de servicio como software		¿Cuál son los servicios o aplicaciones que utiliza en el software como servicio?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
		14	Infraestructura como servicio	Elementos de servicio como infraestructura		¿Cuál son los servicios o aplicaciones que utiliza en la infraestructura como servicio?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	CUANTITATIVA
	Despliegue	15	Público	Recursos asociados automatizados	VI06	¿Qué tan importante es el despliegue de la implementación de la nube pública?	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
		16	Privado	Recursos con arrendamientos		¿Qué tan importante es el despliegue de la implementación de la nube privada?	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
		17	Híbrido	Elementos compartidos		¿Qué tan importante es el despliegue de la implementación de la nube híbrida	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
		18	Comunitario	Recursos compartidos		¿Qué tan importante es el despliegue de la implementación de la nube comunitaria?	Recolección de campo	Encuesta	Primaria	No aplica	CUALITATIVA
	Cumplimiento	19	Requisitos legales y contractuales	Requisitos legales	VI07	¿Cuáles son los controles para el cumplimiento de los requisitos legales y contractuales para el uso del cloud?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA
		20	Revisiones de la seguridad de la información	Revisión de cumplimiento		¿Cuáles son los controles para el cumplimiento de revisiones de la seguridad de la información?	Documental	Investigación bibliográfica	Secundaria	No aplica	CUALITATIVA

Fuente: Marco teórico y datos de la Investigación
Elaborado por: Autor

Anexo 5 Parte A Matriz de conversión de datos

VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	PREGUNTAS O ITEMS	TÉCNICAS	INSTRUMENTO	FUENTE	NOMBRE VARIABLE	PROCESAMIENTO	TIPO DE FUENTE	TIPO DE INFORMACIÓN	DESCRIPCIÓN DE LA VARIABLE
Garantía	1	Integridad	¿Cuáles son los permisos de usuarios como mecanismo de asegurar la integridad?	Estadística	Base de datos	Secundaria	tic17_firma_digital, tic135_seguridad	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Detalle de medidas aplicadas para asegurar la integridad de la información
	2	Confidencialidad	¿Cuáles son las medidas para el control de roles de usuarios que garantizan la confidencialidad?	Estadística	Base de datos	Secundaria	tic16_intranet	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Disponibilidad de una intranet como medida en los roles de usuarios
	3	Disponibilidad	¿La disponibilidad es un factor importante para los servicios en el cloud computing?/ ¿Cuál es el porcentaje de disponibilidad de un servicio?/ ¿Cuál es el intervalo de tiempo promedio de falla de un servicio? / ¿Cál es el tiempo promedio necesario para reparar las fallas?	Documental	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Descriptión del iempo promedio de disponibilidad de un servicio
Gobernanza	4	Políticas	¿Aplica las políticas y buenas prácticas para la seguridad en el cloud computing?	Recolección de campo	Encuesta	Primaria	VI07cumplimiento_rev2	No aplica	No aplica	CUALITATIVA	Políticas de seguridad informática
	5	Normas/Estándar	¿Aplica las normas que rigen en la seguridad informática?	Recolección de campo	Encuesta	Primaria	VI02goberanza13	No aplica	No aplica	CUALITATIVA	Normas de seguridad informática
Identidad y control de acceso	6	Autenticación	¿Qué medidas aplica como método de autención en el control de accesos?	Estadística	Base de datos	Secundaria	tic135_seguridad	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Detalle de medidas empleadas como método de autenticación
	7	Control de Acceso	¿Qué medidas utiliza como mecanismo en el control de acceso?	Estadística	Base de datos	Secundaria	tic16_intranet, tic17_firma_digital, VI03control_acceso, c_accesos	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Se cuenta o no con conexión a intranet, control de acceso, firmas digitales
Gestión de riesgos	8	Responsabilidades	¿Tiene personal contratado especialista en tecnologías de la información y comunicaciones?	Estadística	Base de datos	Secundaria	tic14_especialistas_tic, tic141_especialistas_tic_m, tic142_especialistas_tic_h	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Cantidad de personas que son especialistas en el uso de TIC.
	9	Procedimientos	¿Qué procedimientos se aplican en la gestión de riesgos para el cloud computing?	Documental	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Procedimientos como medida en la gestión de riesgos
	10	Respuesta a incidentes	¿Qué actividades se aplican para la restauración de un servicio?	Documental	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Descripción de actividades como respuesta a incidentes en la gestión de riesgos
	11	Marco de referencia	¿Qué marco de referencia se aplica en la tecnología cloud computing?	Documental	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Tipos de marco de referencia

Fuente: Marco teórico y datos de la Investigación
Elaborado por: Autor

Anexo 5 Parte B Matriz de conversión de datos

VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	PREGUNTAS O ITEMS	TÉCNICAS	INSTRUMENTO	FUENTE	NOMBRE VARIABLE	PROCESAMIENTO	TIPO DE FUENTE	TIPO DE INFORMACIÓN	DESCRIPCIÓN DE LA VARIABLE
Servicio	12	Plataforma como servicio	¿Cuál son los servicios o aplicaciones que utiliza en la plataforma como servicio?	Estadística	Base de datos	Secundaria	tic117_id	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Tipos de aplicaciones o servicios
	13	Software como servicio	¿Cuál son los servicios o aplicaciones que utiliza en el software como servicio?	Estadística	Base de datos	Secundaria	tic8_web, tic9_transacciones, tic104_gestion_electronica, tic111_gestion_cliente, tic112_control_pedidos, tic113_gestion_inventarios, tic114_gestion_finanzas, tic115_gestion_rrhh, tic116_soporte_ventas, tic122_correo_electronico	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Tipos de aplicaciones o servicios
	14	Infraestructura como servicio	¿Cuál son los servicios o aplicaciones que utiliza en la infraestructura como servicio?	Estadística	Base de datos	Secundaria	tic131_sistemas_operativos tic133_aplicaciones_ofimaticas tic135_seguridad	Instituto Nacional de Estadísticas y Censos	Participación de Tecnologías de Información y Comunicación (TIC) en empresas por sectores económicos	CUANTITATIVA	Tipos de aplicaciones o servicios
Despliegue	15	Público	¿Qué tan importante es el despliegue de la implementación de la nube pública?	Recolección de campo	Encuesta	Primaria	VI06despliegue_publico	No aplica	No aplica	CUALITATIVA	Importancia del despliegue en la nube pública
	16	Privado	¿Qué tan importante es el despliegue de la implementación de la nube privada?	Recolección de campo	Encuesta	Primaria	VI06despliegue_privado	No aplica	No aplica	CUALITATIVA	Importancia del despliegue en la nube privada
	17	Híbrido	¿Qué tan importante es el despliegue de la implementación de la nube híbrida	Recolección de campo	Encuesta	Primaria	VI06despliegue_hibrido	No aplica	No aplica	CUALITATIVA	Importancia del despliegue en la nube híbrida
	18	Comunitario	¿Qué tan importante es el despliegue de la implementación de la nube comunitaria?	Recolección de campo	Encuesta	Primaria	VI06despliegue_comunitario	No aplica	No aplica	CUALITATIVA	Importancia del despliegue en la nube comunitaria
Cumplimiento	19	Requisitos legales y contractuales	¿Cuáles son los controles para el cumplimiento de los requisitos legales y contractuales para el uso del cloud?	Recolección de campo	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Controles de requisitos legales y contractuales
	20	Revisiones de la seguridad de la información	¿Cuáles son los controles para el cumplimiento de revisiones de la seguridad de la información?	Recolección de campo	Investigación bibliográfica	Secundaria	No aplica	No aplica	No aplica	CUALITATIVA	Controles de revisiones de seguridad de información

Fuente: Marco teórico y datos de la Investigación
Elaborado por: Autor

Anexo 6 Estructura de variables

PROGRAMA ESTADÍSTICO IBM SPSS

	Nombre	Tipo	Medida	Anchura
1	tic31_computadoras	Numérico	Escala	20
2	tic5_conexion_internet	Numérico	Nominal	1
3	tic8_web	Numérico	Nominal	1
4	tic9_transacciones	Numérico	Nominal	1
5	tic104_gestion_electronica	Numérico	Nominal	1
6	tic111_gestion_cliente	Numérico	Nominal	1
7	tic112_control_pedidos	Numérico	Nominal	1
8	tic113_gestion_inventarios	Numérico	Nominal	1
9	tic114_gestion_finanzas	Numérico	Nominal	1
10	tic115_gestion_rrhh	Numérico	Nominal	1
11	tic116_soporte_ventas	Numérico	Nominal	1
12	tic117_id	Numérico	Nominal	1
13	tic118_gestion_conocimiento	Numérico	Nominal	1
14	tic122_correo_electronico	Numérico	Nominal	1
15	tic123_redes_sociales	Numérico	Nominal	1
16	tic131_sistemas_operativos	Numérico	Nominal	1
17	tic132_navegador_internet	Numérico	Nominal	1
18	tic133_aplicaciones_ofimaticas	Numérico	Nominal	1
19	tic134_erp_crm	Numérico	Nominal	1
20	tic135_seguridad	Numérico	Nominal	1
21	tic14_especialistas_tic	Numérico	Nominal	1
22	tic141_especialistas_tic_m	Numérico	Escala	20
23	tic142_especialistas_tic_h	Numérico	Escala	20
24	tic16_intranet	Numérico	Nominal	1
25	tic17_firma_digital	Numérico	Nominal	1
26	control_acceso_var	Numérico	Escala	8
27	v01servicios_saas	Numérico	Nominal	8
28	c_accesos	Numérico	Nominal	8
29	VI02gobernanza13	Numérico	Nominal	1
30	VI06despliegue_publico	Numérico	Nominal	1
31	VI06despliegue_privado	Numérico	Nominal	1
32	VI06despliegue_hibrido	Numérico	Nominal	1
33	VI06despliegue_comunitario	Numérico	Nominal	1

Elaborado por: Autor

Anexo 7 Listado de Industrias activas registradas en la Superintendencia de Compañías, Valores y Seguros y afiliadas a la Cámara de Industrias de Manta

NOMBRE	TIPO COMPAÑIA	ACTIVIDAD ECONÓMICA	TAMAÑO
Conservas Isabel Ecuatoriana S.A.	Anónima	C1020.02	Grande
Industria Ecuatoriana Productora de Alimentos CA INEPACA	Anónima	C1020.02	Grande
Seafman Sociedad Ecuatoriana De Alimentos Y Frigoríficos Manta C.A.	Anónima	C1020.02	Grande
Empacadora Bilbo S.A. Bilbosa	Anónima	C1020.01	Grande
Promopesca S.A.	Anónima	C1010.21	Grande
Productos Balanceados Coprobalan S.A.	Anónima	C1080.02	Grande
Usafish S.A.	Anónima	C1020.02	Grande
Panificadora Industrial Cia Ltda	Responsabilidad limitada	C1071.01	Grande
Oleaginosas Del Puerto Olipuerto S.A.	Anónima	C1040.11	Mediana
Ensuperior S.A.	Anónima	C1061.11	Mediana
Mareroce Export Import Cia. Ltda.	Responsabilidad limitada	C1020.01	Mediana
Dulcremo S.A.	Anónima	C1071.02	Mediana
Aldanacorp S.A.	Anónima	C1030.11	Mediana
Industria Atunera Arrecifes-Marinos S.A.	Anónima	C1020.04	Mediana
Exportadora Pacifico Exportpacific S.A.	Anónima	C1020.02	Mediana

Fuente: Superitendencia de Compañías, Valores y Seguros 2017, Cámara de Industrias de Manta 2016
Elaborado por: Autor

Anexo 8 Formato de encuesta aplicada a las Empresas del sector industrial de la ciudad Manta, provincia Manabí.

ENCUESTA

Universidad Tecnológica Empresarial de Guayaquil - UTEG
Facultad de Estudios de Postgrado
Tesis en Opción al título de Magister en Sistemas de Información Gerencial
Tema: "Factores que Inciden en la Seguridad Informática y Aplicabilidad en el Cloud Computing de las Empresas del Sector Industrial en la Ciudad de Manta, Provincia de Manabí"

*Obligatorio

NOTA

A continuación se presenta un conjunto de ítems relacionados a la problemática de investigación: "aplicabilidad de la tecnología cloud computing en la seguridad informática"; se aplica como instrumento de evaluación la Escala de Likert que sirve para medir y registrar con precisión y objetividad datos sobre las variable y dimensiones de la investigación, las cuales comprenden lo siguiente:

GARANTÍA: Disponibilidad, Confidencialidad e Integridad.
GOBERNANZA: Políticas y Normas /Estándar.
IDENTIDAD Y CONTROL DE ACCESO: Autenticación y Control de Acceso.
GESTIÓN DE RIESGOS: Responsabilidades, Procedimientos, Respuesta a incidentes y Marco de referencia.
SERVICIO: Plataforma como servicio, Software como servicio o Infraestructura como servicio.
DESPLIEGUE: Público, Privado, Híbrido o Comunitario.
CUMPLIMIENTO: Requisitos legales y contractuales y Revisiones de la seguridad de la información.

Objetivo:

Determinar los factores que Inciden en la Seguridad Informática y su Aplicabilidad en el Cloud Computing de las Empresas del Sector Industrial en la Ciudad de Manta, Provincia de Manabí

Dirigido a:

Empresas del Sector Industrial en la Ciudad de Manta, Provincia de Manabí

Tiempo Aproximado

De 10 a 15 minutos

Consultas y Contacto

Ing. Evelin Saltos R. - evelinmsr@gmail.com
Teléfono: 0969061890

Preliminar

1. **1. Computadoras que tiene la empresa** *
Marca solo un óvalo.

- ◯ Menor a 25
- ◯ Entre 25 y 50
- ◯ Mayor a 50
- ◯ No tiene
- ◯ No sabe/No conoce

2. **2. El uso del internet en la empresa es importante para el desarrollo organizacional** *
Marca solo un óvalo.

- ◯ En total acuerdo
- ◯ En acuerdo
- ◯ Ni en acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ En total desacuerdo

3. **3. ¿Qué tipo de conexión utiliza la empresa para acceder a internet?** *
Marca solo un óvalo.

- ◯ Satelital
- ◯ Fibra óptica
- ◯ Conexión inalámbrica
- ◯ ADSL
- ◯ No sabe/No conoce
- ◯ Otro: _____

4. **4. ¿Para qué servicios y/o actividades utiliza el internet?** *
Selecciona todos los que correspondan.

- ☐ Comunicación (correos electrónicos)
- ☐ Banca electrónica y otros servicios financieros
- ☐ Transacciones con organismos gubernamentales
- ☐ Servicio al cliente
- ☐ Distribuidor de productos en línea
- ☐ Publicidad y marketing
- ☐ Búsqueda de información
- ☐ Actividades de investigación y desarrollo
- ☐ Social media, redes sociales, etc
- ☐ Otro: _____

5. **5. La tecnología del cloud computing o nube computacional ofrece servicios a través de Internet, por lo que las empresas pueden obtener una ventaja competitiva, ofrecer un mejor servicio a los clientes y reducir costos.** *

Marca solo un óvalo.

- En total acuerdo
- En acuerdo
- Ni en acuerdo ni en desacuerdo
- En desacuerdo
- En total desacuerdo

Sección VI01. Se evalúa la variable GARANTIA, y sus dimensiones en la seguridad informática la Integridad, Confidencialidad y Disponibilidad

6. **1. Valore las siguientes caracteríscicas.**

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
La Integridad es un principio fundamental para garantizar la seguridad informática mediante la asignación de permisos a usuarios.					
El rol de usuario es una medida de confidencialidad para garantizar la seguridad informática en un entorno de TI					
La disponibilidad es importante para garantizar la seguridad informática					

Sección VI02. Se evalúa la variable GOBERNANZA y sus dimensiones políticas de seguridad informática, normas/estándar

7. **2. Para las siguientes medidas de seguridad, valore la importancia que tiene a la hora de seleccionar un servicio/proveedor en el cloud computing.** *

Marca solo un óvalo por fila.

	Muy alta	Alta	Media	Baja	Muy baja
El país en el que está físicamente ubicada la información.					
Los controles tecnológicos de seguridad asociados a las plataformas cloud (Ejemplo: copias de seguridad, monitorización, antivirus, cortafuegos, etc.)					
La garantía de continuidad de negocio en caso de incidencia o desastre.					
Las certificaciones de la empresa proveedora (tanto a nivel de empresa como del personal técnico).					
Garantía de cumplimiento de políticas y normativas propias del cliente y de la legislación.					
La existencia de un ANS (Acuerdo de nivel de servicio) con una descripción clara de las características y compromisos de seguridad.					
Las posibilidades para recuperar los datos, una vez finalizado el serviciio, facilitando la migración a otro proveedor o la internalización del servicio.					
El derecho a auditar el servicio y/o la plataforma del CSP (Proveedor de soluciones en la nube) por parte del cliente.					
La adecuación del servicio a las exigencias de la legislación nacional e internacional de protección de datos de carácter personal.					
Que el contrato sea suscrito directamente con el CSP que presta el servicio y no con un intermediario.					
Integración de controles de seguridad del CSP en sistemas de monitorización, control interno y/o seguridad específicos del cliente.					
La aplicación de políticas de seguridad y buenas prácticas son medidas para el desarrollo de aplicaciones, así como el diseño, la implementación, las pruebas y la monitorización de los servicios.					
Importancia sobre la norma ISO 27002 que se basa en recomendaciones y controles de las mejores prácticas en la gestión de la seguridad de la información para iniciar, implementar o mantener sistemas de gestión de la seguridad de la información, aplicable a cualquier entorno de TI.					

Sección VI03. Se evalúa la variable IDENTIDAD Y CONTROL DE ACCESO como medidas para la seguridad informática

8. **3. Valore la importancia del control de acceso como medida de seguridad informática en el uso de la tecnología cloud computing.** *
Marca solo un óvalo por fila.

	Muy alta	Alta	Media	Baja	Muy baja
Dentro de las medidas de seguridad de la información es importante aplicar mecanismo de autenticación como el uso de contraseñas, validaciones a través de correos electrónicos u otros.	◯	◯	◯	◯	◯
Permitir o negar el acceso a un recurso, se valida una autenticación antes de permitir un acceso.	◯	◯	◯	◯	◯

Sección VI04. Se evalúa la variable GESTIÓN DE RIESGOS

9. **4. Valore la importancia sobre la gestión de riesgos** *
Marca solo un óvalo por fila.

	Muy alta	Alta	Media	Baja	Muy baja
Realización de evaluación de riesgos.	◯	◯	◯	◯	◯
Implementación de una estrategia de mitigación de riesgos.	◯	◯	◯	◯	◯
Empleo de técnicas y procedimientos para el monitoreo del estado de seguridad de la información.	◯	◯	◯	◯	◯
Respuesta a incidentes incluye la verificación, análisis, contención, recolección, medidas de solución y restauración.	◯	◯	◯	◯	◯
Marco de referencia para evaluación y auditoría como NORMA ISO 27001-27002, Clous Security Matrix, COBIT	◯	◯	◯	◯	◯

Sección VI05. Se evalúa la variable SERVICIO haciendo referencia al tipo de servicio cloud contratado

10. **5. La contratación de un servicio en el cloud computing es parte de un nuevo modelo de negocio para las empresas** *
Marca solo un óvalo.

- ◯ En total acuerdo
- ◯ En acuerdo
- ◯ Ni en acuerdo ni en desacuerdo
- ◯ En desacuerdo
- ◯ En total desacuerdo

11. **6. Valore el grado de utilización de servicios que accede la empresa mediante la tecnología cloud computing.** *

Marca solo un óvalo por fila.

	Muy alta	Alta	Media	Baja	Muy baja
Almacenamiento					
Servidores					
Redes					
Centro de datos					
Aplicaciones de gestión: ERP, CRM, etc					
Recursos colaborativos					
Aplicaciones de negocios					
Aplicaciones ofimáticas					
Correo electrónico: gmail. hotmail. outlook, etc					
Portales y/o aplicaciones web					
Lenguajes de programación					
Base de datos					
Desarrollo de aplicaciones					
Middleware					

Sección VI06. Se evalúa la variable DESPLIEGUE, según el tipo de nube existente.

12. **7. De acuerdo a la tipología de cloud: pública, privada, híbrida y comunitaria, valore el grado de utilización en el empresa** *

Marca solo un óvalo por fila.

	Muy alto	Alto	Media	Baja	Muy baja
Acceso a servicios o aplicaciones gratuitas o de pago					
Acceso para alquiler de infraestructura, máquinas o almacenamiento.					
Varios servicios y datos de forma pública, y otros de forma privada					
Recursos informativos compartidos en la nube.					

Sección VI07. Se evalúa la variable CUMPLIMIENTO haciendo referencia a los requisitos legales y revisiones de seguridad de la información.

13. **8. Valore la importancia sobre las medias legales para el cumplimiento de normativas.** *
Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
Basarse en requisitos legales y contractuales referentes a la adopción de un servicio de cloud computing.	◯	◯	◯	◯	◯
Revisiones de la seguridad de la información	◯	◯	◯	◯	◯
Auditorías periódicas sobre la seguridad informática.	◯	◯	◯	◯	◯
Políticas y procedimientos internos	◯	◯	◯	◯	◯

Información de segmentación

14. **9. Nombre de la empresa:** *

_____

15. **10. Número aproximado de empleados.** *
Marca solo un óvalo.

- ◯ Menos de 10
- ◯ 11 a 50
- ◯ 51 a 500
- ◯ Más de 500
- ◯ No sabe/No conoce

16. **11. Función dentro de la empresa.** *
Marca solo un óvalo.

- ◯ Gerente General
- ◯ Director de Tecnología y Comunicaciones
- ◯ Director Financiero
- ◯ Responsable de Departamento
- ◯ Jefe de Proyecto
- ◯ Administrador de Sistemas
- ◯ Desarrollador de Sistemas
- ◯ No sabe/No conoce
- ◯ Otro (especifique)

17. **12. ¿Cómo considera el tiempo que le ha llevado completar esta encuesta?** *

Marca solo un óvalo.

- ◯ La encuesta es demasiado larga.
- ◯ La encuesta tiene una longitud adecuada.
- ◯ La encuesta es demasiado corta.
- ◯ No sabe/No conoce