República del Ecuador

Universidad Tecnológica Empresarial de Guayaquil - UTEG

Facultad de Estudio de Postgrados

Tesis en opción al título de Magister en:

Sistemas de Información Gerencial

Tema de Tesis:

Incidencias de las Normas ISO en la Seguridad Informática para la protección de datos usada por proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil

AUTOR:

Ing. Brayan Javier Pinargote Acosta

Director de Tesis:

José Townsend Valencia, Ph.D.

Agosto 2021

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. Brayan Javier Pinargote Acosta
CI. 0930008693

DEDICATORIA

Todos los esfuerzos, triunfos y logros son dedicados a Dios por la vida, por guiarme día a día por el camino correcto, por la sabiduría que me brinda y las bendiciones que derrama en mí cada día. A mis padres por el apoyo incondicional que me dan y a todos aquellos que aportaron en mi un granito de arena para permitir lograr mis metas y ayudarme a crecer profesionalmente.

AGRADECIMIENTO

Agradezco principalmente a Dios por darme la sabiduría necesaria y los conocimientos para poder culminar esta carrera, a mis padres por creer en mí y por apoyarme en mis sueños y proyectos, a mis compañeros por todas las experiencias vividas y los conocimientos aprendidos.

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.

A las empresas que de alguna manera apoyaron con la información requerida para cumplir los objetivos planteados en esta tesis.

Finalmente agradezco al personal docente de la "Universidad Tecnológica Empresarial de Guayaquil" por haber compartido sus conocimientos a lo largo de la maestría, por creer en los esfuerzos de formar en mí un mejor profesional.

Resumen

En los últimos años el internet ha crecido enormemente brindándonos muchas formas y métodos para poder simplificar la ejecución de distintas tareas, actividades, y acciones. La evolución constante en los servicios que el Internet ofrece se presenta por las distintas necesidades que van adquiriendo las personas. Existe una cantidad innumerable de servicios, los cuales no necesariamente están instalados en un computador o servidor físico, sino en la nube; pero, ¿qué hay detrás de ello, qué riesgos podemos tener al usar esta tecnología?

Este proyecto tiene como objetivo determinar cómo inciden las Normas ISO en la seguridad informática para la protección de datos de proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil. Se analizaron modelos de Seguridad Informática existentes y su aplicabilidad en el Cloud Computing; a partir del modelo de Normas ISO se evaluó cuáles son los beneficios que ofrece la tecnología de Cloud Computing para la protección de datos brindada por los proveedores que ofrecen este servicio en la ciudad de Guayaquil; se analizó características específicas de las normas ISO, Cloud Security Alliance, Cloud Control Matrix y demás autores, además se analizó variables como garantía, control de acceso, cumplimiento, gestión de incidentes y continuidad del negocio, servicio y despliegue, lo cual fue el resultado del modelo definido y su aplicabilidad en el cloud computing.

La investigación se basa en el estudio de tipo descriptivo - correlacional, se aplica métodos analítico, inductivo, sintético; y se usa las técnicas estadísticas, documental y de campo.

Palabras claves: seguridad informática, tecnología, cloud computing, protección de datos, normas ISO

Abstract

Over the last years, the Internet has grown enormously, offering us many ways and methods to simplify the execution of different tasks, activities, and actions. The constant evolution in the services that the Internet offers is presented by the different needs that people are acquiring. There is an innumerable amount of services, which are not necessarily installed on a physical computer or server, but in the cloud; however, what is behind it, what risks can we have when using this technology?

This project aims to determine how the ISO Standards affect computer security for the protection of data of providers that offer Cloud Computing services in the city of Guayaquil. Existing Computer Security models and their applicability in Cloud Computing were analyzed; based on the ISO Standards model, it was evaluated what are the benefits offered by Cloud Computing technology for data protection given by the providers that offer this service in the city of Guayaquil. In addition, specific characteristics of the ISO, Cloud Security Alliance, Cloud Control Matrix and other authors were analyzed, as well as variables such as guarantee, access control, compliance, incident management and business continuity, service and deployment, which was the result of the defined model and its applicability in Cloud Computing.

The research is based on the descriptive-correlational study; analytical, inductive, and synthetic methods are applied; and statistical, documentary and field techniques are used.

.

Keywords: computer security, technology, cloud computing, data protection, normas ISO

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

A lo largo del tiempo el internet ha crecido enormemente mostrándonos muchas formas y maneras de poder simplificar tareas, labores cotidianas, y acciones. El uso de servicios tales como: redes sociales, web mail, plataformas de streaming, mensajería instantánea, almacenamiento de datos, etc., se han vuelto parte de la vida cotidiana y el hombre se ha ido adaptando de acuerdo a estos avances que el internet va mostrando día a día.

Debido a estos avances que se vienen dando de manera rápida y exponencial, los servidores o bases de almacenamiento necesitan crecer en cuanto a capacidad de memoria y disco, lo cual representa una dificultad a corto y largo plazo para los administradores de los centros de cómputo y para las empresas, ya que conforme va creciendo esta última, se deben aumentar los recursos de los servidores y su mantenimiento cada vez será más costoso.

Una alternativa para solventar este problema, que se viene dando desde décadas pasadas, es el Cloud Computing. Esta es una excelente opción para las empresas, ya que no se encontrarán ligadas a un equipo físico con capacidades cortas y reducirán su miedo de crecimiento por considerar que el rendimiento del equipo se deteriore. Además, es una ventaja significativa para los usuarios ya que tendrán acceso a sistemas de información, personales y de la compañía para la que trabajan, desde cualquier sitio solo con mantener una conexión a internet, y las empresas ya no se ocuparán de mantenimientos de equipos, adiciones de recursos y demás.

El objetivo de esta investigación es poder identificar qué modelo de sistema de seguridad informática, en base a lo indicado en las normas ISO, deben utilizar los proveedores que ofrecen servicio de Cloud Computing en Guayaquil para asegurar la protección de los datos brindando seguridad, confidencialidad e integridad. Se analizarán los factores determinantes que los usuarios deben tomar en cuenta de los proveedores de Cloud Computing previa a la contratación del servicio, y se mostrará qué incidencias pueden repercutir .

CAPITULO I. MARCO TEORICO CONCEPTUAL

1.1 Antecedentes de la Investigación

La gestión de eventos, incidencias y de los problemas resulta esencial e importante a la hora de asegurar el correcto funcionamiento y mantenimiento de los sistemas informáticos y la continuidad de las actividades laborales en los ámbitos públicos y privados. Los avances en tecnología y la aparición de nuevos sistemas, como la computación en la nube, suponen un trabajo de revisión y mejora constante de los procedimientos que afectan a estas gestiones.

El 11 de septiembre del 2020 en la Universidad de Alcalá, España, Jorge Benítez Abad realizó el siguiente proyecto de investigación: “Cloud Computing: Gestión de Eventos, Incidencias y Problemas” (Abad, 2020). El objetivo principal de este proyecto era estudiar a profundidad los entornos Cloud y la gestión de eventos, incidencias y problemas que han sido descritos por los procesos definidos por ITIL, adicional procedió con la creación de los procesos necesarios para abordar satisfactoriamente el curso de los eventos, incidencias o problemas que puedan surgir, adaptando los procesos de ITIL que están definidos para cada una de las incidencias o alertas, y creando un procedimiento que pueda abordar estas alertas de forma conjunta.

El estudio teórico fue orientado en entornos Cloud e ITIL, mientras el desarrollo de pasos y procedimientos fue orientado para sistemas poco complejos. El alcance del proyecto pretendía conseguir una visión más amplia de los sistemas Cloud y de la creación de sus procedimientos de gestión, con la finalidad de mostrar los factores que se deben tener en cuenta a la hora de crear los procedimientos para gestionar eventos, problemas o incidencias de algún sistema determinado. Como resultado de los procedimientos vistos en ITIL para la gestión de alertas, Benítez comprobó cómo se adaptan perfectamente a cualquier escenario que se pueda dar, tal como: Durante la gestión de problemas, realiza una clasificación entre problemas graves y no graves, para así darle prioridad a la resolución de los problemas graves.

El 14 de septiembre del 2020 en la Escuela Superior Politécnica de Chimborazo, Ecuador, Tenelema Arias Esthela Nataly realizó el siguiente proyecto de investigación: “Implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambiente de almacenamiento en la nube con base en las normas ISO 27017 y 27018” (Nataly, 2020). El objetivo principal de este proyecto fue plantear la implementación de un modelo de seguridad, en el cual se analizaron controles expuestos en las normas ISO 27017 (Controles de Seguridad para Servicios Cloud) y 27018
(Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud), estos controles de seguridad tuvieron un enfoque en tres principales objetivos: Conocer & Limite de Acceso, Seguridad del Entorno y Detección y Respuesta.

El modelo implementado logró establecer una estructura con bases en: estructura de la información general del control, definiciones principales del control y adicional la implementación de una guía; la cual tuvo su implementación y desarrollo de almacenamiento en la nube basados en un prototipo. Con el desarrollo de este estudio se pudo implementar un modelo definido con estrategias de seguridad, las cuales, desde la visión de la puesta en marcha, operación y finalmente la respuesta ante posibles incidentes, para así lograr mitigar de manera exhaustiva los problemas comunes que se presentan en los almacenamientos en la nube.

1.2 Planteamiento del Problema

La tecnología Cloud Computing proporciona un modelo que va a permitir el acceso a información bajo demanda a través de internet a un sinnúmeros de recursos los cuales pueden ser compartidos y configurables; estos recursos pueden ser aplicaciones, servidores, servicios, almacenamiento y redes, los cuales pueden ser rápida y gradualmente asignados, ejecutados y liberados, todo esto puede ser posible con tan solo una mínima gestión realizada por el proveedor del servicio. (Grance, 2011).

El talento humano es el miembro más importante con el que cuentan las empresas para lograr un manejo correcto de la seguridad de la información, es esencial para su funcionamiento eficiente; ya que al no concientizar al personal que hace parte de esta, terceros pueden aprovechar el desconocimiento o forma de actuar para que de manera directa o indirecta puedan masificarse posibles brechas en busca de aprovechamiento de vulnerabilidades existentes para hurtar o alterar información con fines indebidos (Castro Páez, 2015)

Si bien es cierto que todas las ventajas del uso del Cloud Computing, descritas anteriormente, sirven de apoyo para las empresas; hay que tomar en consideración que se pueden presentar problemas de seguridad en la nube y pueden traer grandes complicaciones debido a el desconocimiento, lo cual generaría a su vez grandes pérdidas, y podrían presentarse casos de hurto de información privada, y pérdida de servicios y aplicaciones a corto y largo plazo.

Steve Riley, director de investigación de Gartner, en su informe “Staying Secure in the Cloud is a shared responsibility” (Riley, 2016) manifiesta que la seguridad en la nube es una responsabilidad compartida, el trasladar los servicios a la nube disminuye el alcance de seguridad tradicional necesario, mas no lo elimina; desplazar procesos de trabajo a la nube no los hace más seguros automáticamente.

En su estudio realizado, Riley también indica que aproximadamente para el 2018, el 60% de las empresas que puedan implementar herramientas y normas adecuadas de visibilidad y control de la nube podrían experimentar un tercio menos de errores de seguridad (Riley, 2016).

En la actualidad, las empresas cuentan con múltiples alternativas para dar seguridad a sus datos e información, como lo es el Cloud Computing, pero a su vez este presenta riesgos en cuanto a sus servicios o información se vean comprometidos, y puedan causar pérdidas económicas graves; de estos riesgos los más comunes que podemos encontrar son: acceso a información por personal no autorizado, que la información no se encuentre disponible en

momentos estrictamente necesarios, pérdida total de la información y servicio. (González Hernández, 2016)

Por lo antes expuesto nos damos cuenta que existen ciertos peligros y vulnerabilidades en cuanto a la seguridad y privacidad de la información almacenada, y por ende se generan las interrogantes: ¿qué hay detrás del Cloud Computing?, ¿qué riesgos podemos tener al usar esta tecnología?, ¿nuestra información está totalmente asegurada?, ¿existe integridad en nuestros datos almacenados?

De acuerdo a lo indicado en la Encuesta Global de Seguridad de la Información de 2014 (PwC, 2013), el 37% de las empresas no tienen conocimiento real de los posibles riesgos tecnológicos que se puedan presentar al usar esta herramienta, y el 56% no están preparadas para detectar y mitigar un posible cibercrimen.

SÍNTOMAS

- Falta de conocimiento de las empresas (Vieites, 2014)
- Falta de seguridad y privacidad (González Hernández, 2016)
- Divulgación de la información (Castro Páez, 2015)

CAUSAS

- Presencia de ataques Informáticos en la red
- Existencia de brechas de seguridad
- Ingeniería Social

PRONÓSTICO

- Pérdida de información
- Accesos y servicios vulnerados
- Desprestigio de la empresa, reclamo de clientes

1.2.1 Formulación del Problema

¿De qué manera inciden la aplicabilidad de las Normas ISO en la Seguridad Informática para proteger los datos en el Cloud Computing de proveedores que ofrecen este servicio en la ciudad de Guayaquil?

1.2.2 Sistematización del Problema

- ¿Existe la posibilidad de que se presenten fallas de los servicios y aplicaciones en el Cloud Computing?

- ¿Es fundamental asegurar la privacidad de la información de las organizaciones en todo momento?

- ¿Pueden existir accesos no autorizados a servicios y aplicaciones en el Cloud Computing?

- ¿Al almacenar datos en la nube, es posible que las organizaciones queden expuestas a ataques informáticos?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Determinar cómo inciden las Normas ISO en la seguridad informática para la protección de datos de proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil.

1.3.2 Objetivos Específicos

- Analizar los modelos de Seguridad Informática existentes y su aplicabilidad en el Cloud Computing

- Identificar a partir del modelo de Normas ISO los riesgos, amenazas y vulnerabilidades.

- Evaluar cuáles son los beneficios que ofrece la tecnología Cloud Computing al aplicar correctamente las Normas ISO para la protección de datos brindada por los proveedores que ofrecen este servicio en la ciudad de Guayaquil.

1.4 Justificación de la Investigación

1.4.1 Justificación Teórica

En la actualidad la mayoría de los servidores se encuentran en grandes computadoras en las que solo se utiliza una pequeña parte del CPU, lo cual representa un desaprovechamiento de recursos. El Cloud Computing nos permite evitar estos problemas dado que algunos de los servicios de Cloud Computing que son ofertados por proveedores intermediarios ofrecen ventajas significativas como: rapidez, seguridad, disponibilidad, crecimiento tecnológico, etc.; las cuales están siendo aprovechadas por empresas privadas y gubernamentales de acuerdo a sus requerimientos, pero esto no implica que no existan riesgos de seguridad ya que el usuario no sabe exactamente dónde está almacenada la información; trasladar toda la información a la nube significa desplazar la seguridad a terceros lo que puede ser preocupante (Aguilar, 2009).

1.4.2 Justificación Práctica

Vivimos en una era tecnológica que está en constante ascenso mediante la cual podemos acceder a información desde cualquier momento, lugar con tan solo una conexión a internet; sin embargo estamos expuestos a ataques informáticos que pueden ocasionar hurtos, fraudes entre otros; por lo tanto el propósito del presente proyecto de investigación sobre incidencias de las

Normas ISO en la Seguridad Informática para la protección de datos nos va ayudar a estudiar a fondo el modelo de Normas ISO y sus beneficios al cumplir con estos y así poder responder la pregunta de investigación planteada.

1.5 Marco de Referencia de la Investigación

1.5.1 Marco Teórico

1.5.1.1 Cloud Computing

El Cloud Computing no tiene una definición exacta, pero podemos describirlo como las nubes o un conjunto de clústeres distribuidos que brindan recursos y servicios bajo demanda con solo tener acceso a internet y con la escala y fiabilidad de un centro de datos (Grossman, 2009).

Para Gartner (Daryl C. Plummer, 2008) el Cloud Computing se integra como un modelo de computación en el cual la TI escala y sus capacidades y se entregan "como un servicio" a clientes externos que utilizan tecnologías de Internet para cumplir con sus necesidades Tecnológicas.

Los autores Mell y Grance (Grance, 2011) indican que la computación en la nube se trata de un modelo el cual va a permitir acceder a la red de manera omnipresente y bajo demanda en la cual se encontrarán recursos informáticos configurables tales como: redes, servidores, equipos de almacenamiento, aplicaciones, servicios, etc.; los cuales se podrán aprovisionar y liberar de manera rápida realizando un esfuerzo mínimo en el cual se incluya interacción con el proveedor de servicios.

1.5.1.1.1 Características Esenciales del Cloud Computing

A continuación, se muestran cinco características esenciales del Cloud Computing las cuales fueron definidas por los autores Mell y Grance (Grance, 2011)

Autoservicio bajo demanda

Mell y Grance (Grance, 2011) indican que un consumidor puede aprovisionar unilateralmente ciertas capacidades informáticas las cuáles pueden ser tiempo y almacenamiento de red según lo requiera de manera automática sin solicitar la interacción del proveedor de servicios.

Amplio Acceso a la Red

Los servicios y capacidades están disponibles a través de la red, Mell y Grance (Grance, 2011) también agregan que el acceso a esta se lo puede realizar a través de mecanismos que promueven el uso de plataformas sean estas tabletas, teléfonos móviles, estaciones de trabajo, computadoras portátiles, etc.

Conjunto de Recursos

Mell y Grance (Grance, 2011) expresan que los recursos informáticos del proveedor están agrupados para responder a los múltiples consumidores estableciendo diferentes recursos físicos y virtuales de manera dinámica de acuerdo a la demanda que se vaya presentando; además Mell y Grance (Grance, 2011) también indican que aunque el cliente generalmente no tenga control o conocimiento sobre l ubicación de los recursos brindados si podrá ser capaz de especificar la ubicación de los recursos como por ejemplo: almacenamiento, memoria, ancho de banda, etc.

Rápida Elasticidad

Mell y Grance (Grance, 2011) aseguran que las capacidades de los recursos se pueden aprovisionar y liberar elásticamente y en ciertos casos de manera automática, estas capacidades que se encuentran disponibles para el cliente a menudo aparecen ser delimitadas y pueden ser aprovisionadas la cantidad deseada en cualquier momento.

Servicio Medido

Los sistemas en la nube controlan y optimizan de manera automática el uso de recursos aprovechando la capacidad de medición adecuada al tipo de servicio como, por ejemplo: almacenamiento, ancho de banda, procesamiento y cuentas de usuario activas. Mell y Grance (Grance, 2011) establecen también

que este uso de recursos puede ser monitoreado, controlado e informado de manera transparente.

1.5.1.1.2 Conceptos de Cloud Computing escritos por diferentes autores

Podemos encontrar diferentes definiciones sobre Cloud Computing, a continuación, se muestran algunas de estas definiciones en la tabla 1.1.

Tabla 1.1

Conceptos de Cloud Computing por diferentes autores

Año	Autores	Conceptos definidos por el autor
2008	Gartner	Gartner define la computación en la nube como "un estilo de computación en el que la TI es escalable capacidades se entregan "como un servicio" a clientes externos que utilizan tecnologías de Internet."
2009	Robert L. Grossman	La computación en la nube aún no tiene una definición estándar, pero una buena descripción de la misma es decir que las nubes, o clústeres de equipos distribuidos, proporcionan recursos y servicios bajo demanda a través de una red, normalmente Internet, con la escala y fiabilidad de un centro de datos.
2011	Raj Kumar Buyya James Broberg Andrzej Goscinski	La computación en la nube ha surgido recientemente como una de las palabras de moda en las TIC Industria. Numerosos proveedores de TI prometen ofrecer computación, almacenamiento, y servicios de alojamiento de aplicaciones y para proporcionar cobertura en varios continentes.
2012	NIST	La tecnología Cloud Computing proporciona un modelo que va a permitir el acceso a información bajo demanda a través de internet a un sinnúmeros de recursos, los cuales pueden ser aplicaciones, servidores, servicios, almacenamiento, etc.; todo esto puede ser posible con tan solo una mínima gestión realizada por el proveedor del servicio
2012	ISACA	El Cloud Computing brinda la posibilidad de obtener beneficios nivel empresarial y de negocios los cuales pueden ser: agilidad, contención de costos, arquitectura de multiempresa, confiabilidad y escalabilidad.

Fuente: Elaborado por autor

1.5.1.2 Seguridad Informática

1.5.1.2.1 Seguridad

Según Aguilera (Lopez, 2011), se puede definir a la seguridad informática como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad.

La seguridad puede definirse como el conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la información o los sistemas ante una eventual amenaza que se pueda suscitar (Aguirre, 2006).

A continuación, en la tabla 1.2 podemos encontrar diferentes conceptos de seguridad con sus respectivos autores y año de publicación.

Tabla 1. 2

Conceptos de Seguridad por diferentes autores

Año	Autores	Conceptos definidos por el autor
2013	Eduardo Caballero Juan Pablo Vera	La Seguridad Informática está relacionada con diferentes modelos y factores de los sistemas de procesamiento y almacenamiento de datos, esto ayuda a brindar una garantía para que la información se mantenga íntegra, confiable y disponible en todo momento.
2014	Álvaro Gómez Vieites	Se define como una de las medidas que va ayudar a impedir que se ejecuten operaciones no autorizadas en los sistemas informáticos, ya que al realizarse este tipo de operaciones podría causar daños sobre la información, y a su vez alterar la misma, como por ejemplo el bloqueo de usuarios que si tienen acceso al sistema y problemas en los servicios y rendimiento de los equipos.
2016	Gabriel Baca Urbina	Indica que la Seguridad Informática establece la disciplina que, con conocimientos de normas y políticas de la empresa, ayudará a la protección de la integridad y privacidad de la información la cual se encuentre en algún tipo de almacenamiento conocido, esto se lo realiza ante cualquier amenaza, con el objetivo de disminuir riesgos a los que se encuentra expuesta.
2017	Silvia M. David G.	El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable.

Fuente: Elaborado por autor

1.5.1.2.2 Informática

A. Prieto, Antonio L. y Juan Carlos T. (A. Prieto, 2002) indican que la informática se trata de un conjunto de técnicas y conocimientos que estudia el tratamiento de la información por medio de máquinas automáticas.

La informática es el estudio de la estructura, comportamiento e interacciones de los sistemas computacionales naturales o artificiales (Gutierrez, 1993). A

continuación, en la tabla 1.3 se encuentran diferentes conceptos de informática detallando los autores y el año de publicación.

Tabla 1. 3

Conceptos de Informática por diferentes autores

Año	Autores	Conceptos definidos por el autor
1989	Barchini	La informática estudia el tratamiento sistemático de la información con bases automatizadas en los sistemas y redes establecidas.
1992	Diccionario de la Lengua Española de la Real Academia	Define a la Informática como el conjunto de técnicas que hacen posible que la información se pueda tratar automáticamente con base en conocimientos científicos a través de ordenadores.
2004	De Pablos, López, Romo y Medina	La informática establece un estudio de la información manteniendo su atención en tratamientos automáticos y racionales de la misma, así como también estudia la ciencia de los ordenadores.
2005	R. Cañedo, R Ramos, J. Guerrero	Estudia la estructura, el comportamiento y la interacción de los sistemas naturales y las tecnologías de la información. Abarca, tanto el arte y la ciencia como la dimensión humana de las tecnologías de la información

Fuente: Elaborado por autor

1.5.1.3 Modelos de Seguridad Informática

1.5.1.3.1 Principales Modelos de Seguridad Informática

El enfoque de los modelos formales de seguridad va a permitir el diseño que fomenta eficientes mecanismos para definir e implementar controles que están dirigidos a reconocer los diferentes niveles de riesgo que se encuentran presentes en un sistema y a su vez define las acciones que se deben implementar para reducirlos. Para (Figueroa, Suarez, Obando, & Saltos Gomez, 2017) la seguridad informática se compone de un conjunto de métodos, técnicas o procedimientos que se usan para la protección de los sistemas informáticos (redes e infraestructura) y la información en formato digital que estos almacenen, a su vez dentro de esta categoría se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos.

Según consultores en Seguridad de la Información (CSI, 2016) la Seguridad Informática o Seguridad de Tecnologías de la información es el campo de la informática que radica en garantizar que los recursos del sistema de

información (aplicaciones o programas) de una organización sean utilizados de manera correcta; el trabajo de estos tipos de seguridad son diversos, y consiste en lo general en la restricción del acceso al sistema o parte del sistema, el acceso solo es permitido a ciertas personas que se encuentren acreditadas, así como su modificación dentro de los límites de su autorización

Elena Riuz Larrocha (Ruiz Larrocha, 2017) en su libro Nuevas Tendencias en los Sistemas de Información nos habla de 6 etapas en la evolución de los sistemas de información las cuales son:

Primera Etapa:

Sistema Manual y Semimecanizado, los sistemas de información solo pretendían realizar procedimientos de tipo manual o con máquinas elementales ara organizar los documentos que generaba la administración de la empresa.

Segunda Etapa:

Sistema de Procesamiento de Transacciones, estaban al nivel de gestión inferior de la empresa, el nivel operativo, procesando los datos históricos que se producen en la actividad cotidiana (compras, ventas, pagos, cobros, movimientos de almacén, etc.)

Tercera Etapa:

Sistemas Integrados de Información para la Gestión, estos sistemas facilitaban la información necesaria para la planificación, gestión y control de las actividades de la empresa, generando como subproductos los informes contables y financieros.

Cuarta Etapa:

Sistemas Integrados en Tiempo Real, permiten la actualización y la consulta en tiempo real de las bases de datos corporativas y la incorporación instantánea de información externa, facilitando el control de las operaciones corrientes, la gestión por excepción (toma de decisiones no estructuradas), el establecimiento de correlaciones y relaciones cruzadas entre los datos y una mejor toma de decisiones.

Quinta Etapa:

Sistemas Distribuidos, integran la información en la estrategia corporativa utilizando las TIC para conseguir nuevas formas de diseño, producción y comercialización de productos y servicios.

Sexta Etapa:

El Presente, en la actualidad todos los sistemas de información están viviendo un momento de total disrupción, la inteligencia artificial, los vehículos autónomos, las redes sociales, etc.

A continuación, los autores (Carmen de Pablos, Lopez, Hermoso, & Medina, 2004) indican los sistemas de información basados en dos tipos los cuales son :

Sistemas de Planificación de Recursos Empresariales, (ERP): Estos sistemas van ayudar a realizar y automatizar aquellos procesos de negocio que se encuentran en áreas funcionales, los mismos que pueden ser implementados mediante una plataforma o recurso de tecnología de la información.

Sistemas Expertos (SE): Estos sistemas van ayudar a solucionar posibles problemas a través de la aplicación del conocimiento de (IA) inteligencia artificial.

A continuación, se muestran propuestas de autores más relevantes sobre modelos de la seguridad informática en la tabla 1.4.

Tabla 1. 4

Modelos teóricos de la Seguridad Informática

Año	Autor	Propuesta
1981	Carl E. Landwehr	Modelos formales para la Seguridad Informática
1992	Comité de Sistemas de Seguridad Nacional (CNSS), creado por John McCumber Cube	Presenta un modelo integral de análisis de información crítica basado en tres dimensiones.
2011	Cloud Security Alliance (CSA)	Establece un modelo basado en cinco características, de las cuales tres modelos corresponden a servicios en la

		nube y cuatro basados en modelos de implementación.
2011	Fang L., Jin T., Jian M., Robert B., John M., Lee B. y Dawn L. (National Institute of Standards and Technology NIST)	Establece modelos basados en Seguridad y Privacidad.
2013	Normas ISO/ IEC	Propone modelos establecidos en normas ISO/IEC 17799 – ISO/IEC 270001 – ISO/IEC 27002 – ISO/IEC 27017 – ISO/IEC 27018

Fuente: Elaborado por autor

1.5.1.3.2 Modelos formales para la Seguridad Informática de Landwehr

De acuerdo a lo mencionado por (Landwehr, 1981) por lo general en los modelos se aplican controles más rígidos que el control del entorno real y cada una de las operaciones informáticas que se encuentren en las estructuras del modelo serán seguras según las definiciones establecidas, y otras operaciones no permitidas deben ser consideradas fuera del modelo formal. El autor muestra varios modelos que se encuentran orientados a la seguridad, denegación de un servicio, modificación de información no autorizada.

Modelo High-Water-Mark

El sistema ADEPT-50 fue construido en la Corporación de Desarrollo del Sistema a finales de la década de 1960, fue uno de los primeros en el cual se intentó implementar controles de software para información clasificada; sus controles se basaron en un modelo formal de seguridad militar. En el mismo se definieron cuatro tipos de objetos los cuales son: usuarios, terminales, trabajos y archivos, cada objeto se lo describe como Autoridad (A), Categoría (C) y Franquicia (F) en el a los dos primeros corresponden a nivel de sensibilidad y un conjunto de compartimientos; el tercero se trata de un conjunto de designaciones de usuario y los conjuntos de franquicias se los usa para implementar controles discrecionales de necesidad de saber. Los valores de las asignaciones A, C y F son usados para controlar las propiedades asignadas a nuevos objetos (ejemplo: archivos recién creados) y también para determinar si las operaciones solicitadas se permitirán. (Landwehr, 1981)

Modelo de Matriz de Acceso

Este modelo para la protección informática se basa más en la abstracción de las estructuras del sistema operativo que en los conceptos de seguridad. Fue proporcionado por (Lampson, 1974), (Denning , 1971) y Graham (1972) el mismo ha sido ampliamente utilizado ya que permite un conjunto de varias técnicas de implementación demostrando tres componentes principales: un conjunto de objetos, un conjunto de sujetos activos (los cuales pueden manipular los objetos) y un conjunto de reglas. El modelo de matriz de acceso correctamente interpretado corresponde muy bien a una amplia variedad de implementaciones reales del sistema informático; por ejemplo, la protección de un archivo de información es de responsabilidad del propietario del archivo, así como también el modelo separa cuidadosamente los mecanismos para aplicación de la política aplicada

Modelo Bell and LaPadula

El modelo (Bell, D. E. LaPadula, Leonard J. , 1973) establece la confidencialidad con la cual a través de una política de acceso de seguridad podrá definir y establecer un conjunto de reglas y modos entre las cuales se encuentran: lectura, escritura y también lectura y escritura; a su vez también establece un control en el flujo de información de un sistema en el cual usa reglas de control de acceso para manejarlas.

Modelo de Flujo de Información

Controla el flujo de información seguro en el sistema modelado el cual ayuda a garantizar que la información real que fluya entre objetos no infringe el flujo especificado; se lo conoce como un modelo flexible el cual ayuda a la implementación de políticas de seguridad.

1.5.1.3.3 Modelo McCumber Cube propuesto por el Comité de Sistemas de Seguridad Nacional (CNSS)

Según (Whitman & Mattord, Management of Information Security, 2014) describen un modelo integral de seguridad de la información que se convertirá en un estándar de evaluación ampliamente aceptado para la seguridad de los

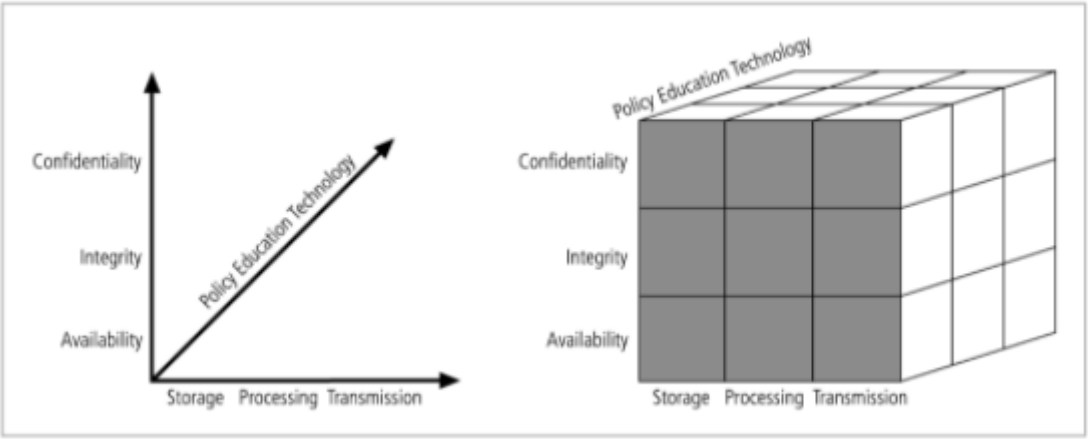
sistemas de información; en el cual describe las principales características en tres dimensiones las cuales son aplicables en cualquier entorno cuyo objetivo es identificar vulnerabilidades que puedan ser corregidas por medidas de seguridad.

Este modelo creado por (McCuber, 1991) se lo conoce también como Cubo de McCumber, establecido por el CNSS (Committe on National Security System) o también llamado NSTISSC (National Security Telecommunications and Information Systems Security Committe) el cual ayuda a proporcionar una representación gráfica del enfoque arquitectónico ampliamente utilizado en la seguridad informática y de la información.

En la figura 1.1 se muestran tres dimensiones, las cuales si se extrapolan las tres dimensiones de cada eje se convierte en un cubo de 3x3x3 con 27 celdas que representan áreas que deben dirigirse para proteger los sistemas de información actuales y garantizar la seguridad del sistema.

Figura 1. 1

Modelo Tres Dimensiones McCumber Cube



Fuente: Elaborado por autor. Tomado de (McCuber, 1991)

Adicional (Whitman & Mattord, Management of Information Security, 2014) consideran que la intersección entre tecnología, integridad y el almacenamiento requiere un control o salvaguardia el cual aborda la necesidad de utilizar la tecnología para proteger la integridad de la información durante el almacenamiento; uno de esos controles podría ser el sistema.

1.5.1.3.4 Modelo propuesto por el Cloud Security Alliance (CSA) Cloud Controls Matrix (CSA CCM)

Fue creado para prestar una guía a proveedores y ayudar a posibles clientes potenciales en la nube proporcionando principios de seguridad, identificando y reduciendo posibles vulnerabilidades y amenazas y a su vez fortaleciendo los entornos que se encuentran en la nube. Parte de su diseño se centra en establecer una búsqueda con el cual se pueda normalizar ciertas expectativas de seguridad, contemplando algunos términos y medidas que fueron implementadas.

Según la (CSA, 2011) este modelo establece una relación con otras normas de seguridad entre las cuales se encuentran: ISACA COBIT, ISO 27001/27002, NIST, PCI, entre otras, además la (CSA, Security Guidance for Critical Areas of Focus in Cloud Computing v.4., 2017) establece que mantienen una base en 14 dominios de control los cuales se presentan en dos categorías como lo son gobierno y operaciones.

Los dominios de gobierno son amplios ya que abordan estrategias y políticas dentro de un entorno de cloud computing, a continuación, en la tabla 1.5 se muestran los dominios de gobierno en un entorno de cloud computing.

Tabla 1. 5

Dominios de Gobierno en un entorno de Cloud Computing

Dominios de Gobierno	Descripción
Gobernanza y Gestión de Riesgos en la empresa	Establece como una organización tiene la capacidad para poder gobernar y establecer medidas que impidan el riesgo empresarial introducido por cloud computing, de la misma manera establece algunos puntos entre los cuales se encuentran la precedencia legal, la capacidad de usuarios que puedan evaluar adecuadamente los riesgos de un proveedor de cloud y también la responsabilidad que mantienen para así poder proteger los datos confidenciales.
Aspectos Legales: Contratos y descubrimiento Electrónico	Se analizan los posibles problemas legales que se tienen al usar cloud computing, adicionalmente se incluyen otros temas tales como: leyes de divulgación de infracciones de seguridad, validación de requisitos para poder proteger la información y los sistemas informáticos, , informes de requisitos reglamentarios, diseños de requisitos de privacidad, aplicación de leyes

	internacionales, etc.
Cumplimiento y auditoria	Al usar el cloud computing se debe mantener y evaluar como el cloud computing afecta el cumplimiento de las políticas de seguridad, adicional en el dominio se incluyen algunas directrices para probar el cumplimiento durante una auditoria.
Gestión de Información y Seguridad de Datos	Administración de datos que se colocan en el cloud así como la compensación de controles que pueden ser utilizados para hacer frente a la pérdida de control físico al mover datos al cloud; adicional otros elementos que se discuten son: responsabilidad, confidencialidad, integridad y disponibilidad.
Portabilidad e Interoperabilidad	La capacidad de mover datos o servicios de un proveedor a otro o llevarlos completamente de vuelta a casa, en conjunto con los problemas relacionados con la interoperabilidad entre proveedores.

Fuente: Elaborado por autor

Los dominios operativos se centran más en los problemas de seguridad táctica e implementación dentro de la arquitectura, a continuación, en la tabla 1.6 se muestran los dominios operativos en un entorno de cloud computing.

Tabla 1. 6

Dominios Operativos en un entorno de Cloud Computing

Dominios Operativos	Descripción
Seguridad tradicional, Continuidad de Negocio y Recuperación ante Desastres.	Como afecta la computación en la nube a los procesos y procedimientos operativos, actualmente usada para implementar la seguridad, la continuidad del negocio y la recuperación ante desastres. Se enfoca en discutir y examinar los posibles riesgos del cloud computing; además la sección muestra cómo ayudar a las personas a identificar donde el cloud computing puede ayudar a disminuir ciertos riesgos de seguridad.
Operaciones de DataCenter	Como evaluar en un proveedor su arquitectura y las operaciones del Datacenter. Se centra principalmente en ayudar a usuarios a identificar las características comunes del Datacenter que podrían ser perjudiciales para los servicios en curso, así como las características que son fundamentales para la estabilidad a largo plazo.
Respuesta, Notificación y Remediación ante Incidentes	Intenta abarcar aquellos elementos que deben permanecer en su lugar basados en ambos niveles sean estos proveedor y usuario con lo cual permitirá el manejo adecuado ante posibles incidentes y forenses. Este dominio permitirá comprender las distintas complejidades que proporciona el cloud y también, maneja un programa de atención a incidentes.
Seguridad de Aplicaciones	Este incluye elementos para validar un escenario apropiado, en el cual se puedan migrar rediseñar las aplicaciones que se ejecutan en la nube y de esta manera; lograr indicar qué tipo de plataforma en la nube resulta el más apropiado a implementar sean estos (SaaS, PaaS o IaaS).
Cifrado y Gestión de Claves	Identificar el uso adecuado del cifrado y la administración escalable de claves ya que se necesitan discutir porque se necesitan identificar los problemas que surgen en el uso de claves tanto para proteger el acceso a los recursos, así como para proteger los datos.

Gestión de Identidades y Accesos	Lograr una administración y aprovechamiento de identidades entre los cuales se muestran servicios de directorio con el cual se proporcionan control de acceso. El enfoque se centra en los problemas encontrados al extender la identidad de una organización en el cloud, adicional se proporciona información sobre la evaluación de la disposición a llevar a cabo, la identidad, el derecho y el acceso basados en la nube Gestión (IdEA)
Virtualización	Las direcciones de dominio, elementos como riesgos asociados como alquiler múltiple, aislamiento de máquina virtual, vulnerabilidades de hipervisores, etc. Este dominio se centra en la seguridad, problemas relacionados con la virtualización del sistema/hardware, en lugar de una encuesta de todas las formas de virtualización.
Seguridad como Servicio	Proporcionar a terceras garantías de seguridad, gestión de incidentes, certificación de cumplimiento y supervisión de identidad y acceso. La seguridad como servicio es la delegación de detección, reparación y gobernanza de la seguridad; los usuarios de este servicio obtienen el beneficio de la experiencia dedicada y tecnología de vanguardia en la lucha por asegurar y endurecer los negocios sensibles.

Fuente: Elaborado por autor

1.5.1.3.5 Modelo propuesto por el National Institute of Standards and Technology (NIST)

NIST (NIST 500-292, y otros, 2011) tiene como estrategia crear una hoja de ruta de tecnología de computación en la nube en la cual sus requisitos prioritarios sean seguridad, interoperabilidad y portabilidad y a su vez desarrollar normas y directrices con organismos en el cual participen el sector privado y otras partes interesadas. Este programa computación en la nube NIST fue lanzado formalmente en noviembre 2010 con esfuerzo del gobierno para incorporar la computación en la nube como reemplazo o mejora del sistema de información y modelos cuando sea apropiado.

Los autores (Jansen & Grance, 2011) nos presentan algunas recomendaciones que se deben considerar dentro del modelo propuesto

Gobernanza

Los autores (Jansen & Grance, 2011) indican que la gobernanza establecen un control y una supervisión de normas, procedimientos y políticas para continuar con el desarrollo de aplicaciones entre las cuales se encuentran: propuesta, diseño, puesta en marcha, pruebas y finalmente supervisión de servicios.

Cumplimiento

Establece una especificación de la conformidad establecida para la regulación o ley, (Jansen & Grance, 2011) mencionan que al existir varios tipos de leyes y regulaciones de seguridad y privacidad en los diferentes países se puede volver un problema complicado para el cloud computing.

Confianza

Bajo el esquema de cloud computing se establece que las organizaciones renuncian al control directo de muchos aspectos de la seguridad por lo cual se logra un nivel alto de confianza al proveedor. (Jansen & Grance, 2011) nos indican algunos de estos aspectos: acceso a la información privilegiada, datos privados, servicios compuestos, visibilidad, gestión de riesgos.

Arquitectura

Se trata de la arquitectura de los sistemas de software usados para ofrecer servicios en la nube comprendiendo hardware y software, (Jansen & Grance, 2011) indican que esta infraestructura es determinada por el proveedor de cloud al igual que la implementación, soporte y escalabilidad que conlleva.

Identidad y Control de Acceso

Trata de la sensibilidad de los datos y la privacidad de la información las cuales se han convertido en un área de accesos no autorizados por lo que representa una preocupación importante al mantener datos en la cloud. (Jansen & Grance, 2011) mencionan que un problema recurrente es que la identificación de la organización y el marco de autenticación no pueden extenderse naturalmente a la nube lo cual puede ser difícil.

Aislamiento de Software

(Jansen & Grance, 2011) establecen que se necesita un nivel alto de throughput en las plataformas de cloud para lograr la flexibilidad prevista del aprovisionamiento bajo demanda de los servicios y beneficios de acuerdo a lo requerido.

Protección de Datos

(Jansen & Grance, 2011) indican que los datos almacenados en la nube normalmente residen en un entorno compartido con datos de otros clientes, ya que las organizaciones trasladan los datos sensibles a la nube.

Disponibilidad

Se trata de la medida en que el conjunto completo de recursos computacionales ya sean aplicaciones, datos o servicios son accesibles y utilizables en el tiempo requerido. (Jansen & Grance, 2011) indican también que esta disponibilidad puede verse afectada temporal o permanentemente estableciendo pérdidas parciales o completa debido a amenazas como: ataques de denegación de servicio, cortes de servicio y desastres naturales son algunas de las amenazas que afectan la disponibilidad.

Respuesta a Incidentes

Tal como lo indica su nombre la respuesta a incidentes implica un mecanismo organizado y establecido para determinar las consecuencias y reestablecerse de un ataque contra la seguridad de un sistema informático. (Jansen & Grance, 2011) indican que el papel del proveedor de cloud es vital en la realización de actividades de verificación, análisis y respuesta a incidentes; recopilación y preservación de datos y a su vez la restauración del servicio.

Tabla 1. 7

Recomendaciones del modelo NIST 800-144

Elementos	Características
Gobernanza	Establecimiento mecanismos e implementación de herramientas de auditoria para ayudar a determinar el almacenamiento de los datos, como protegerlos, y como se utilizan, con la validación de los servicios y finalmente poder verificar las políticas ya aplicadas.
Cumplimiento	Establece la aplicación de una revisión exhaustiva de las medidas aplicadas por el proveedor que tienen relación con las necesidades y prioridades de la organización.
Confianza	Realizar un control de los procesos y control de privacidad de los empleados del proveedor.
Arquitectura	Reconocer las tecnologías utilizadas por el proveedor ara poder establecer controles técnicos de seguridad y privacidad.
Identidad y Control de Acceso	Establecer mecanismos para asegurar la autenticación y control de acceso.
Aislamiento de Software	Comprender las herramientas de aislamiento y virtualización que mantiene el proveedor para establecer los riesgos que estas

	implican.
Protección de Datos	Los clientes deben de tener en cuenta los medios por los cuales se controla el acceso a los datos para determinar el grado de seguridad.
Disponibilidad	Asegurarse que las operaciones y servicios se encuentren disponibles inmediatamente en un tiempo determinado luego de una interrupción presentada.
Respuesta a Incidentes	Comprender minuciosamente los contratos de los proveedores en los cuales presenta un mecanismo de respuesta a incidentes para la disponibilidad de los servicios.

Fuente: Elaborado por autor

La arquitectura de referencia de cloud computing NIST 500-292 (NIST 500-292, y otros, 2011) define cinco actores principales los cuales son: consumidor, proveedor, operador, auditor y agente en el que cada actor es una entidad (una persona u organización) que participa en el proceso de tareas de cloud computing; a continuación, en la tabla 1.8 nos muestran la descripción de la función de cada uno de ellos.

Tabla 1. 8

Principales actores de Cloud Computing del modelo NIST 500-292

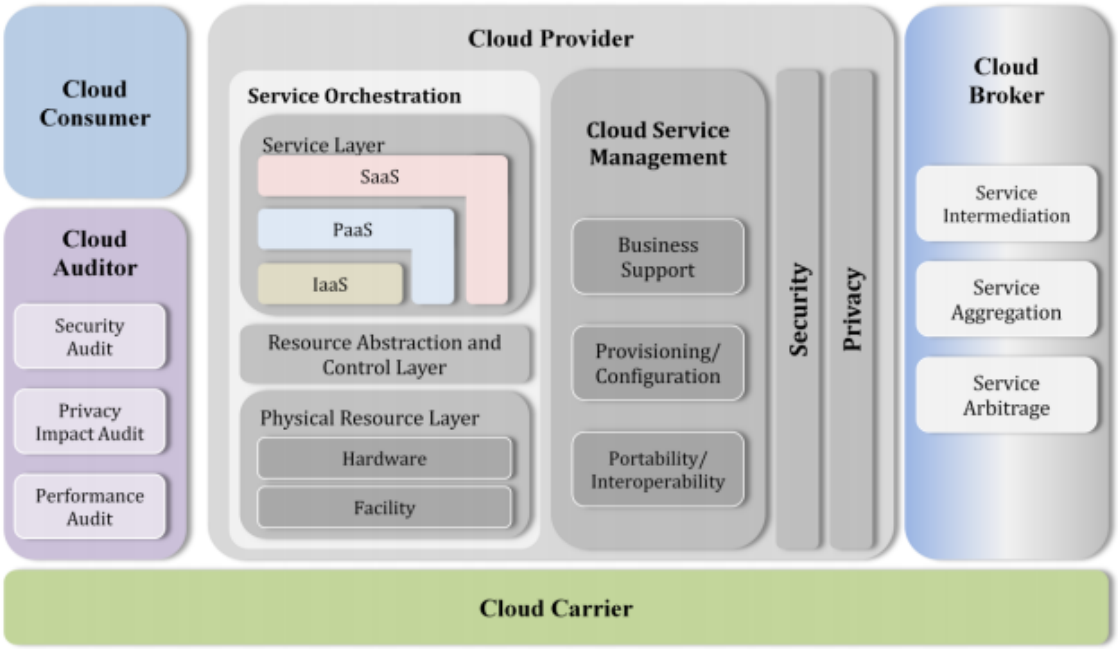
Actor	Definición
Consumidor Cloud	Persona u organización que mantiene una relación comercial utilizando servicios en la nube.
Proveedor Cloud	Persona u organización responsable de mantener un servicio a disposición de los interesados.
Operador Cloud	Entidad que administra el uso, rendimiento y entrega de los servicios en la nube.
Auditor Cloud	Persona o entidad que lleva a cabo una evaluación independiente de los servicios en la nube, sean estos rendimiento, seguridad, operación e implementación.
Agente Cloud	Intermediario que proporciona conexión y transporte en la nube.

Fuente: Elaborado por autor

Los autores (NIST 500-292, y otros, 2011) nos muestran en la figura número 1.2 una visión general de la arquitectura de referencia de computación en la nube NIST la cual identifica cada uno de sus actores importantes, actividades y funciones en el cloud computing.

Figura 1. 2

Modelo conceptual de referencia Cloud Computing NIST 500-292



Fuente: Elaborado por autor. Tomado de (NIST 500-292, y otros, 2011)

1.5.1.3.5.1 Modelos de Servicio

Software como Servicio (SaaS)

Los autores (NIST 500-292, y otros, 2011) indican que se trata de la capacidad proporcionada al consumidor para poder gestionar aplicaciones o servicios que se ejecutan en un entorno o infraestructura cloud; estas gestiones se pueden realizar desde varios dispositivos del cliente a través de una interfaz como por ejemplo navegador web o correo electrónico basado en web.

Plataforma como Servicio (PaaS)

La capacidad que se le proporciona al consumidor son aplicaciones creadas o adquiridas por el consumidor de infraestructura en la nube las cuales son creadas mediante programación y herramientas compatibles con el proveedor, los autores (NIST 500-292, y otros, 2011) también mencionan que el consumidor carece de control y gestión de la infraestructura de nube, sin embargo; mantiene un control sobre las aplicaciones ya implementadas y de ser el caso gestión del entorno de configuración de las aplicaciones.

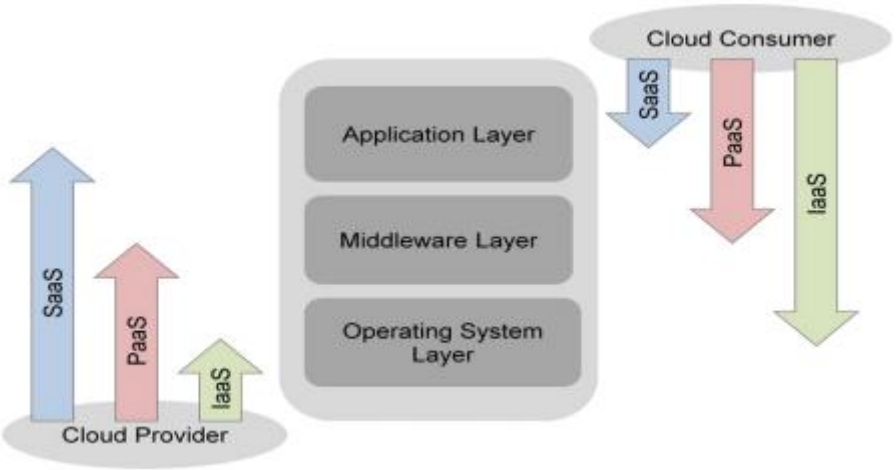
Infraestructura como Servicio (IaaS)

(NIST 500-292, y otros, 2011) indican que la capacidad que se le proporciona al consumidor se encuentran: almacenamiento y procesamiento de redes y también de otros recursos informáticos que sean fundamentales con el cual el consumidor debería ser capaz de poder implementar y ejecutar ciertos sistemas operativos, aplicaciones y software; el consumidor no posee administración ni control de la infraestructura en la cloud, pero si se le brinda control sobre las aplicaciones implementadas y los sistemas operativos y a su vez posiblemente un control limitado del uso de componentes de red entre los cuales pueden estar host, firewall, etc.

En la figura 1.3 se muestra el alcance existente de los controles entre proveedor y consumidor definida por (NIST 500-292, y otros, 2011)

Figura 1. 3

Alcance de los controles entre Proveedor y Consumidor



Fuente: Elaborado por autor. Tomado de (NIST 500-292, y otros, 2011)

1.5.1.3.5.2 Modelos de Despliegue

Nube Privada

Este tipo de nube es aquella cuya infraestructura es operada únicamente para una organización, es gestionada por la organización o un tercero y pueden existir bajo premisa o fuera de premisa (NIST 500-292, y otros, 2011).

Nube Comunitaria

Según el (NIST 500-292, y otros, 2011) en este tipo de nube varias organizaciones comparten la infraestructura, y también pueden ser administradas por la organización que adquiere los servicios o por un tercero y a su vez establecer si se mantienen bajo premisa o fuera de premisa.

Nube Pública

Según lo indicado por (NIST 500-292, y otros, 2011) es la nube más común ya que su infraestructura está a disposición del público en general sean estos: organizaciones, industrias, unidades educativas o personas en general y es de propiedad de organizaciones que venden servicios en la nube.

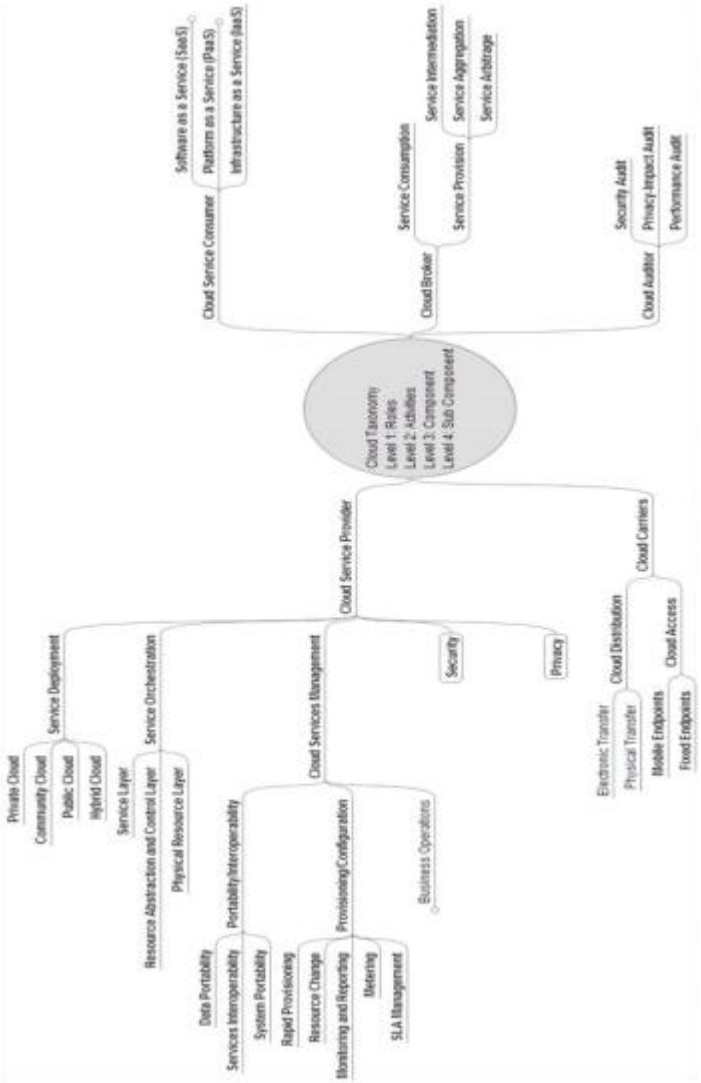
Nube Híbrida

(NIST 500-292, y otros, 2011) mencionan que este tipo de son el resultado de diferentes composiciones, como, por ejemplo: dos o más nubes privadas, nubes comunitarias o nubes públicas que siguen formando parte de entidades únicas, pero a su vez están unidas por tecnología con esto se plantea que permite la portabilidad de datos y aplicaciones.

A continuación, en la figura 1.4 NIST nos muestra una taxonomía asociada con la arquitectura de referencia de cloud computing en la cual se muestran cuatro niveles para describir los conceptos claves e cloud computing; los niveles se dividen en rol, actividad, componentes y subcomponentes.

Figura 1. 4

Taxonoma de Cloud Computing



Fuente: Elaborado por autor. Tomado de (NIST 500-292, y otros, 2011)

1.5.1.3.6 Modelo ISO basado en Normas Técnicas (Organización Internacional de Estandarización) e IEC (Comisión Electrotécnica Internacional)

ISO (Organización Internacional de Estandarización, s.f.) y la IEC (Comisión Electrotécnica Internacional, s.f.) forman el sistema especializado para la normalización mundial. Las siglas ISO no hacen referencia solamente a las normas, sino que ISO es la mayor organización mundial desarrolladora de normas internacionales la cual nació en el año 1947 y hasta la actualidad lleva publicado más de 20000 normas internacionales; estas normas están

orientadas a establecer un orden en las gestión de las empresas en cada uno de sus diferentes ámbitos ya sean estos: productivos, humanos y tecnológicos; cuentan con su sede en Ginebra, y se trata de un conjunto de organismos nacionales, entre los cuales se encuentran (AFNOR, s.f.) Francia, (AENOR, s.f.) España, (DIN, s.f.) Alemania entre otros.

Las normas ISO (ISO/IEC, ISO, s.f.) tienen como objetivo asegurar que tanto los productos como los servicios alcancen la calidad deseada ya que a través de ella las organizaciones puedan establecer un desarrollo y poder implementar un marco que permita la gestión de la seguridad y utilizarla como instrumento la cual les va a permitir minimizar costos por medio de la reducción de errores y a su vez incrementar la productividad. Se menciona también que la seguridad de la información establece sus bases en las normas 27000 la cual está profundamente fundamentada en factores como: confidencialidad, integridad y disponibilidad, esta fundamentación de medidas es conocida como CIA.

1.5.1.3.6.1 Norma ISO/IEC 17799

Según la norma ISO/IEC 17799 (Vieites, 2014) este estándar se lo define como un conjunto de guías de seguridad de la información reconocidas y aceptadas internacionalmente ya que proporciona una base para desarrollar normas y procedimientos de seguridad dentro de las organizaciones, las mismas se pueden aplicar a cualquier tipo de organización independientemente de la actividad, sector o tamaño; esta norma fue basada en el estándar BS 7799-1, la cual se la publicó en 1995 por el British Standard Institute (BSI, Instituto de Estándares Británico) la misma se la consideró como una norma No Certificable.

En la ISO/IEC 17799 (Vieites, 2014) se establece la definición de la información como un activo el cual representa valor para la organización por lo cual requiere de una protección adecuada. De la misma manera la Seguridad de la Información la definen como "la preservación de su confidencialidad, su integridad y su disponibilidad" cuyo objetivo es proteger de manera correcta

este activo para asegurar la continuidad del negocio, reducir daños a la organización e incrementar el retorno de las inversiones y oportunidades de negocio.

El 15 de junio de 2005 se publicó una nueva versión de esta norma la cual se nombró ISO/IEC 17799:2005 (Vieites, 2014) tras mantener un proceso de revisión de tres años se estableció esta versión cuyo contenido consta de 11 dominios, 39 objetivos de seguridad y 133 controles específicos, a su vez incorporó una "guía de implantación" para cada control. Adicional en esta nueva versión se incluyeron temas sobre análisis de riesgos y gestión de incidentes.

1.5.1.3.6.2 Norma ISO/IEC 27001:2013

La Norma (ISO 27001, 2013) establece una serie de requisitos los cuales van a permitir especificar las implementaciones, el mantenimiento y así poder mejorar adecuadamente los sistemas de gestión de seguridad de la información. Con la implementación de requisitos para así poder lograr evaluar y realizar un análisis y tratamiento de los riesgos de seguridad con los que se cuenta de acuerdo a las necesidades y prioridades de la organización.
Esta Norma (ISO 27001, 2013) fue llevada a cabo en el cual se facilita un formato y un conjunto de alineación el cual permite seguir con el desarrollo documental de los sistemas de gestión. En la tabla 1.9 se muestra las características de la nueva estructura

Tabla 1. 9

Características de la nueva estructura Norma ISO 270001:2013

Características
Introducción
Alcance
Referencias Normativas
Términos y Definiciones
Contexto de la Organización
Liderazgo
Planificación
Soporte
Operación
Evaluación del desempeño
Mejora

Fuente: Elaborado por autor

1.5.1.3.6.3 Norma ISO/IEC 27002:2013

La Norma (ISO 27002, 2013) se publicó desde el 1 de julio de 2007 la cual fue creada para renombrar la ya publicada ISO 17799:2005. Esta norma describe una guía de buenas prácticas en las cuales se establecen diferentes objetivos de control y a su vez se establecen controles recomendables a aplicar para la protección de la seguridad de la información; este diseño mantiene un enfoque el cual puede ser utilizado por las organizaciones o empresas que requieren seleccionar controles específicos para poder iniciar el proceso de implementación de un Sistema de Gestión de Seguridad de la Información el cual mantiene sus bases en ISO, IEC 27001.

Esta edición 2013 estableció un estándar actualizado y reestructurando el contenido logrando así un total de 14 Dominios, 35 Objetivos de Control y 114 controles. A continuación, en la tabla 1.10 se muestran la lista de los dominios según la Norma (ISO 27002, 2013)

Tabla 1. 10

Dominios según la Norma ISO 270002:2013

ID	Dominio
5	Políticas de Seguridad
6	Enfoque de aspectos Organizativos de la Seguridad de la Información
7	Enfoque de Seguridad ligada a los Recursos Humanos
8	Administración y Gestión de Activos
9	Gestión y Control de Accesos
10	Cifrado
11	Enfoque de Seguridad Física y Ambiental
12	Enfoque de Seguridad en la Operativa
13	Enfoque de Seguridad en las Telecomunicaciones
14	Gestión de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información
15	Enfoque de relaciones con Suministradores
16	Gestión de Incidentes en la Seguridad de la Información
17	Gestión de aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio
18	Cumplimiento

Fuente: Elaborado por autor

De acuerdo a lo indicado por la (ISO 27000, 2009) esta norma que a principios se denominaba ISO 17799 fue revisada en el año 2000 pasando a nombrarse después (ISO 27002, 2005) desde el mes de junio de 2007

1.5.1.3.6.4 Norma ISO/IEC 27017:2015

La Norma (ISO 27017, 2015) fue publicada el 15 de diciembre de 2015 y conforma una guía de seguridad para Cloud Computing la cual se encuentra alineada con la ISO/IEC 27002 y establece controles adicionales específicos aplicables a los entornos de nube. La selección de cada uno de estos controles y la aplicación de la guía dependerán de la evaluación de riesgos y cada uno de los requisitos de seguridad de información regulatorio, legal u otras del entorno cloud. En los controles adicionales de la Norma (ISO 27017, 2015) se tratan los siguientes puntos:

- Responsable de lo que sucede entre el proveedor del servicio y el cliente cloud.
- La eliminación o devolución de activos al disolverse el contrato de la prestación de servicios.
- Gestión de protección y separación del entorno virtual del cliente.
- Implementación y Configuración de máquina virtual.
- Gestión de operaciones y procedimientos administrativos relacionados con el entorno en la nube.
- Gestión de seguimiento de todas las actividades de los clientes en la nube.
- Administración de la alineación del entorno de la red virtual con la nube.

1.5.1.3.6.4.1 Beneficios para los clientes de Servicio Cloud 27017

De acuerdo a lo establecido por (ISO 27017, 2015) los gerentes de tecnología y las personas del departamento técnico podrán minimizar los riesgos que se encuentren presentes y así poder asegurar las responsabilidades de cada parte y con eso poder tomar mejores decisiones concernientes a la migración de la información de la organización a la nube.

1.5.1.3.6.4.2 Beneficios para los proveedores de Servicio Cloud 27017

La implantación de la Norma (ISO 27017, 2015) podrá también beneficiar a los proveedores que ofrecen servicio de cloud ya que con las normas establecidas

se proporcionará mayor seguridad y protección de datos lo cual les ayudará a establecer una ventaja competitiva dentro del mercado aumentando la reputación de marca por mantener un estándar de ISO para servicio cloud reconocido a nivel mundial y garantizando el cumplimiento de las normas locales legales.

1.5.1.3.6.5 Norma ISO/IEC 27018:2014

La Norma (ISO 27018, 2014) nació con el objetivo de proteger los datos personales en la nube definiendo controles y directrices según los principios de privacidad (PII). Los proveedores que administran información personal (PII) de sus clientes en la nube tienen que operar sus servicios de manera que permitan a ambas partes cumplir con los requisitos de la legislación y regulaciones aplicables que cubren la protección de (PII).

La Norma (ISO 27018, 2014) se la utiliza en conjunto a los objetivos y controles de seguridad de la Norma ISO/IEC 27002, cuya misión es crear un conjunto común de categorías y controles de seguridad que puedan ser implementados por un proveedor de Cloud Computing.
De acuerdo a lo establecido en la Norma (ISO 27018, 2014) se definen los siguientes objetivos los cuales se muestran en la tabla 1.11

Tabla 1. 11

Objetivos según la Norma ISO 27018:2014

Objetivo	Descripción
1	Ayudar al proveedor de servicios de Cloud Computing a cumplir con las obligaciones aplicables al actuar como procesador (PII).
2	Lograr que le procesador (PII) de Cloud Computing sea transparente en asuntos relevantes con el objetivo de que los clientes puedan seleccionar servicios de procesamiento de (PII) basados en cloud bien gobernados.
3	Lograr un acuerdo contractual entre el proveedor y cliente de servicios de Cloud Computing.
4	Brindar a los clientes de servicios cloud un mecanismo con el cual puedan ejercer los derechos y responsabilidades de cumplimiento y auditoria.

Fuente: Elaborado por autor

1.5.1.4 Otras teorías y modelos de Seguridad Informática en el Cloud Computing

De lo expuesto anteriormente podemos encontrar una variedad de dimensiones en común a través de los diferentes modelos y aplicaciones desarrolladas para poder cumplir la seguridad en el Cloud, cada uno de ellos nos describe una estructura de como poder implementar y mantener un servicio en el Cloud aplicando normas, controles y buenas prácticas las cuales han sido desarrolladas conforme va avanzando la tecnología y se van sumando nuevos requerimientos y obligaciones que conforman el sistema Cloud.

La seguridad informática tiene como objetivo asegurar los sistemas de información ya que se extiende en abarcar la información en todas sus formas, además de brindar protección ante cualquier incidente que se presente en la red. En resumen, el núcleo de la seguridad informática se basa en implantar medidas de integridad, confidencialidad y disponibilidad cumpliéndolos de manera ética y responsable en los procesos de auditoria que se presenten manteniendo principios como lo son la autenticación autorización y privacidad generando tranquilidad a las organizaciones. A continuación, en la tabla 1.12 presentamos otras teorías y modelos de seguridad informática que se pueden presentar al usar los servicios de Cloud Computing.

Tabla 1. 12

Otros modelos de Seguridad Informática que resaltan en los servicios de Cloud Computing

Año	Autores	Descripción
1985	TCSEC (Trusted Computer System Evaluatión Criteria)	Fue desarrollado en 1985 por el Centro de Seguridad Informática Nacional de Estados Unidos el cual fue responsable de los Sistemas de Seguridad definiéndolos en siete clases según su nivel: • Clase D (Sin Seguridad) • Clase C1 (Control de acceso Discrecional) • Clase C2 (Protección de acceso controlado) • Clase B1 (Seguridad Etiquetada) • Clase B2 (Protección Estructurada) • Clase B3 (Dominios de Seguridad) • Clase A (Protección verificada)
2003	ENISA (European Network and Information Security Agency)	Tuvo su creación en el 2003 para hacer cumplir los siguientes objetivos: • Obtener un consenso en materias de Seguridad Informática en Europa para mantener la

		disponibilidad y seguridad en las redes y los sistemas de información de las organizaciones. • Asistir para la aplicación de nuevas normativas en el campo de la Seguridad Informática. • Dirigir el desarrollo en esta materia. • Realizar un aviso y coordinación acerca de la información recopilada y analizada. • Brindar soporte a la certificación y estandarización del mercado. • Facilitar el contacto con terceros países.
2012	ISACA (Information System Audit and Control Association)	Brinda principios fundamentales para la adopción y el uso de la nube con el objetivo de poder brindar una ayuda a las empresas del camino correcto a elegir. • Gestión de Capacitación • Comparación de relación Costo-Beneficio • Estudio de riesgo para la Empresa • Gestión de Responsabilización • Enfoque de Capacidad • Implementación de Confianza
2013	Cloud Special Interest Group PCI Security Standards Council	Fue creado en 2013 teniendo como objetivo establecer un conjunto de normas para asegurar que las organizaciones que tengan vínculos con tarjetas de crédito se mantengan en un entorno que cumpla con seguridad • Verificación PCI DSS Gestión de Control por el proveedor de cloud • Verificación y validación de servicios y componentes • Facilidades y seguridad física • Seguridad de datos • Seguridad técnica • Soberanía de datos y consideraciones legales • Gobierno, riesgo y cumplimiento
2014	SMI (Service Measuremente Index)	Diseñado para evaluar y medir servicios cloud en base a requerimientos técnicos y especificaciones establecidas en el cual define un conjunto de funciones para evaluar las características de los proveedores de servicio cloud • Responsabilidad • Garantía • Seguridad • Agilidad • Finanzas • Usabilidad

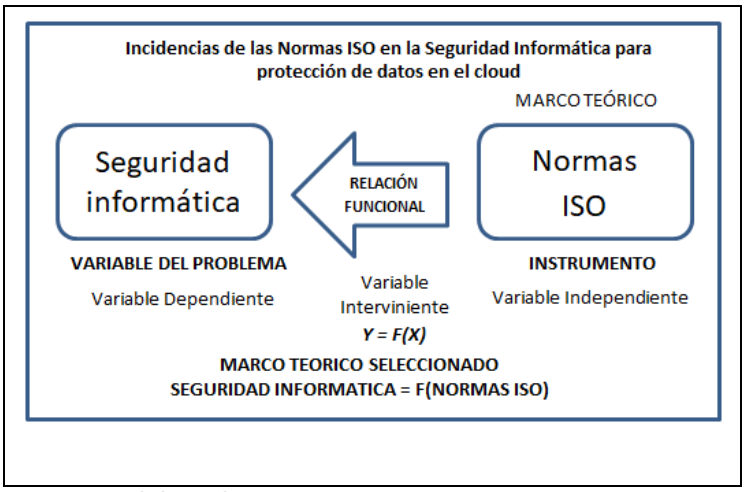
Fuente: Elaborado por autor

1.5.2 Diseño del modelo de evaluación

1.5.2.1 Definición y enfoque de la problemática de seguridad informática con el uso de un instrumento

Tabla 1. 13

Diseño de la relación de variable Dependiente y variable Independiente



Fuente: Elaborado por autor

Para poder identificar cómo inciden las Normas ISO en la Seguridad Informática para proteger los datos del Cloud Computing es necesario determinar ciertos factores importantes empleando el instrumento de estudio de investigación científica. Según (Hernández, Fernández, & Baptista, 2010) este instrumento de estudio se lo sustenta mediante conceptos, modelos, teorías que fueron desarrollados por los autores a partir de un objetivo y el planteamiento de un problema.

1.5.2.2 Definición de la variable independiente basada en el modelo de Normas ISO 27000

Según la (ISO 27000, 2009) la seguridad de la información es uno de los recursos más importantes de las organizaciones, con el avance de la tecnología es necesario que las organizaciones protejan sus datos críticos para garantizar la confianza establecida entre los socios y clientes; estas empresas que alinean sus prácticas de seguridad de la información con un estándar ISO

27000 gozarán de varios beneficios que fortalecerán la unión entre cliente-proveedor.

Para definir las variables independientes se tomó en consideración lo mencionado en las Normas ISO, iniciando con la Norma (ISO 27000, 2009) ya que en esta norma se establecen principios básicos de seguridad para los sistemas de información en el cual se resaltan la disponibilidad, integridad y confidencialidad.

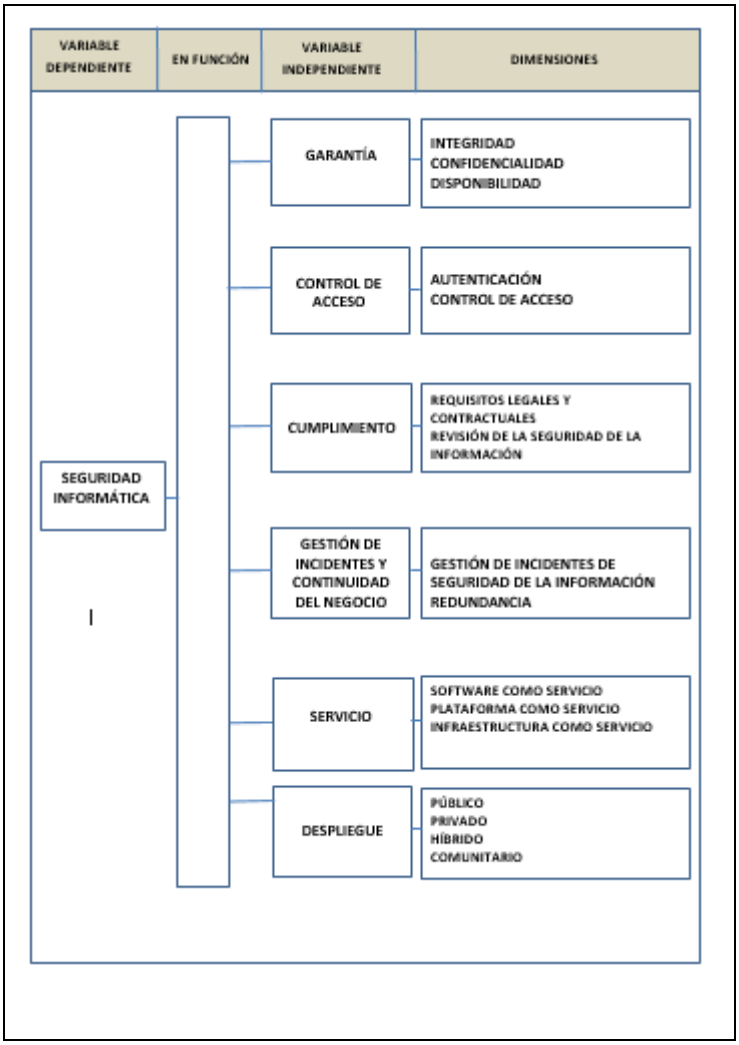
Continuando con la Norma (ISO 27002, 2013) vamos a encontrar una guía de buenas prácticas con el objetivo de establecer controles tales como la gestión y control de acceso a los recursos de los usuarios, cumplimiento y gestión de la continuidad del negocio. Para complementar el presente proyecto se consideró también los principios básicos tomados por el modelo de referencia del Instituto Nacional de Normas y Tecnología (NIST 500-292, y otros, 2011) en el mismo se establecen modelos de servicios y modelos de despliegue que se implementan en los ambientes Cloud.

1.5.2.3 Diagrama del modelo de evaluación propuesto

En la tabla 1.14 mostraremos un diagrama del modelo de evaluación propuesto el cual se basa en las teorías, normas del modelo de Normas ISO 27000 y el modelo NIST 500-292 que son aplicables en Cloud Computing.

Tabla 1. 14

Modelo de evaluación propuesto



Fuente: Elaborado por autor

Garantía

Asegurar que todos los procesos que se encuentren dentro de los servicios de Cloud Computing permanezcan protegidos.

- Integridad: Garantizar la no alteración de la información.
- Confidencialidad: Garantizar que la información sea accesible solo para usuarios autorizados.
- Disponibilidad: Asegurar que los servicios puedan ser usados sin interrupciones por el usuario final.

Control de Acceso

Uso de mecanismos y métodos de autenticación para identificar los usuarios que requieran acceso a la información.

Cumplimiento

Garantizar el cumplimiento de normas, leyes y estándares a través de los requisitos legales y contractuales y realizar una revisión de la Seguridad de la Información.

Gestión de Incidentes y Continuidad del Negocio

Definir y Planificar estrategias para verificar, revisar y evaluar la seguridad de la información notificando eventos y estableciendo respuestas ante incidentes, adicional contar con disponibilidad de instalaciones para el procesamiento de la información.

Servicio

Se refiere al software, plataforma e infraestructura que recibe el cliente como servicio.

- SaaS (Software como Servicio): Se le entregan al usuario aplicaciones, pero no pueden ser gestionadas ni controladas.
- PaaS (Plataforma como Servicio): Se le entregan al usuario aplicaciones para su gestión y control, pero no puede realizar lo mismo con la infraestructura subyacente ya sean estos (redes, sistemas operativos, servidores, etc.).
- IaaS (Infraestructura como Servicio): Se le entrega al usuario control sobre almacenamiento, procesamiento, instalación y ejecución de software, pero no puede gestionar ni controlar la infraestructura subyacente.

Despliegue

Se refiere al modelo de implementación que se usa para ejecutar un servicio.

- Nube Pública: Se encuentra a disposición general en la que una industria u organización es propietaria de la venta de servicios.
- Nube Privada: Cuenta con servicios los cuales son operados únicamente para una organización.
- Nube Híbrida: Combinación de las características de las nubes privadas, comunitarias o públicas manejando responsabilidades de gestión.
- Nube Comunitaria: Varias organizaciones comparten la infraestructura cumpliendo requisitos de seguridad y políticas.

CAPITULO II. MARCO METODOLÓGICO

2.1 Tipo de diseño, alcance y enfoque de la investigación

2.1.1 Tipo de estudio

La realización de la siguiente investigación es de tipo de estudio cualitativo y cuantitativo.

Estudio descriptivo

La presente investigación recopiló información independiente de conceptos, métodos y variables que permitieron reflejar la situación real y a su vez realizando la medición de sus conceptos y componentes.

Estudio correlacional

La aplicación del estudio correlacional permitió identificar la existencia de la relación de asociación entre dos o más métodos, conceptos o variables de un contexto o enfoque en particular.

2.1.2 Metodología de investigación

2.1.2.1 Enfoque de la investigación

Esta investigación realizó un enfoque cuantitativo, en el cual se procedió a la recolección y análisis de los datos recopilados con la aplicación de métodos estadísticos en la investigación científica para su posterior procesamiento y presentación de resultados,

2.2 Métodos de investigación

Método deductivo

En la presente investigación se aplicó el uso del método deductivo el cual a partir de la aplicación de un modelo teórico permitirá poder observar cómo

inciden las Normas ISO para proteger los datos del Cloud estableciendo una medición cualitativa y a su vez cuantitativa a través del uso de la seguridad informática.

Método histórico

La presente investigación empleó registros obtenidos en el 2019 y 2020 de las empresas que ofrecen servicio de cloud computing en la ciudad de Guayaquil; también se hiso uso del método de medición con la ayuda de la información y bases de datos de los organismos gubernamentales.

2.3 Unidad de análisis, población y muestra

Esta investigación permitió analizar 11 empresas que ofrecen servicio de cloud computing en la ciudad de Guayaquil provincia del Guayas. De acuerdo a los datos obtenidos de la Superintendencia de Compañías, Valores y Seguros año 2020 (Superintendencia de Compañias, Valores y Seguros, 2020), en la sección de Directorio de Compañías existen 410 empresas del sector Telecomunicaciones CIIU J6, C3 y G4, código CIIU basado en la clasificación Nacional de Actividades Económicas como lo indica el Instituto Nacional de Estadísticas y Censos INEC (2012) (Instituto Nacional de Estadísticas y Censos, 2019) ; Para efectos de esta investigación se determinó a 11 empresas comprendidas entre grandes y medianas dedicadas a la actividad económica CIIU J6, C3 y G4 con el objetivo de identificar cómo inciden las Normas ISO en la seguridad informática para la protección de datos de proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil

2.4 Variables de la investigación y su operacionalización

Variable Dependiente (VD)

Seguridad informática: Es la variable principal de la investigación con la cual se van a iniciar los análisis respectivos.

Variable Independiente (VI)

Garantía (VI01): Es la variable usada para preservar la seguridad la cual se encuentra basada en disponibilidad, confidencialidad e integridad.

Control de Acceso (VI02): Es la variable para valorar funciones como autenticación, autorización y las demás funciones de control de acceso.

Cumplimiento (VI03): Es la variable con al cual se va a valorar y medir el cumplimiento de las normas, estándares y leyes establecidas a través de los requisitos legales y contractuales.

Gestión de incidentes y continuidad del negocio (VI04): Es la variable con la cual se va a valorar las estrategias para asegurar la continuidad de la seguridad de la información.

Servicio (VI05): Es la variable con la cual se va a indicar cuan frecuentemente se usan aplicaciones o servicios en un entorno cloud siendo estas: SaaS, PaaS e IaaS.

Despliegue (VI06): Es la variable con la cual se va a valorar un servicio o aplicación en los entornos Público, Privado, Híbrido o Comunitario.

2.5 Fuentes, técnicas e instrumentos para la recolección de información

2.5.1 Fuentes de información

La presente investigación es de tipo documental por lo cual se utilizó fuentes primarias y secundarias de organismos gubernamentales y no gubernamentales.

Fuentes Primarias

Se recopiló información de las siguientes fuentes:

- Revisión de informes emitidos por el INEC.

- Informes y Datos de la Superintendencia de Compañías, Valores y Seguros del Ecuador.
- Información y Datos de modelos de Seguridad.

Fuentes Secundarias:

- Información y Datos de artículos científicos y revistas oficiales.
- Información de libros de Seguridad Informática.
- Páginas web del Instituto Nacional de Estándares y Tecnología (NIST), Organización Internacional de Normalización (ISO) y Comisión Electrotécnica Internacional (IEC).
- Publicaciones de tesis sobre investigación científica, Cloud Computing y seguridad de la información.

2.5.2 Técnicas para la recolección de información

2.5.2.1 Técnica de investigación estadística

Esta técnica nos va a permitir extraer información del fenómeno de estudio, haciendo el uso de bases de datos públicos de los diferentes organismos gubernamentales y no gubernamentales escogidos.

2.5.2.2 Técnica de investigación documental

Esta técnica nos va a permitir recolectar información relacionada al tema de investigación ya sean estas: tesis, revistas, libros, artículos científicos, páginas web y otras fuentes válidas.

2.5.2.3 Técnica de investigación de campo

Para la investigación de campo se recopiló información del objeto de estudio mediante el instrumento de encuesta sobre las incidencias que tienen las Normas ISO en la Seguridad Informática.

Evaluación y aplicación de las variables

La medición y registro de los indicadores que se encuentran asociados al fenómeno de investigación se empleó la escala de Likert ya que permite el análisis de hechos y acciones naturales, sociales. o individuales de personas u organizaciones. Los grados de respuesta de los ítems van desde lo más favorable a lo menos favorable.

A continuación, en la tabla 2.1 se muestra la medición de la seguridad informática de acuerdo a las variables seleccionadas de las Normas ISO para proteger los datos del Cloud.

Tabla 2. 1

Escala de Likert para la medición de la Seguridad Informática de acuerdo a las variables seleccionadas de las Normas ISO para proteger los datos del 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: Elaborado por autor

2.6 Tratamiento de la información

La herramienta estadística IBM SPSS permitió realizar ciertos tipos de comparaciones con el objetivo de establecer una comprensión del tema de investigación; y a su vez poder realizar un análisis de tablas de distribución de frecuencias implementando medidas de tendencia central mostrada en gráficos, barras e histogramas.

CAPITULO III. RESULTADOS Y DISCUSIÓN

3.1 Análisis de la situación actual

De acuerdo a las investigaciones realizadas en cuanto a las interacciones entre los usuarios ya sean estos consumidores o proveedores en los servicios de internet como el cloud computing se observa que hay una tendencia que se viene acogiendo con mayor auge en lo que va de la última década en el Ecuador; dado que actualmente los servicios de IT ofrecen muchas alternativas y ventajas que generan competitividad.

Estas innovaciones se presentan tanto en las pequeñas y grandes empresas sean estas públicas o privadas, innovaciones importantes en tecnología que les permiten evolucionar empresarialmente y a su vez les ofrece un retorno de la inversión tecnológica realizada.

3.1.1 Impacto de la Economía Digital en los Sectores Productivos

Según lo indicado por el INEC (Instituto Nacional de Estadísticas y Censos, 2019), en el Ecuador más del 90% de las empresas son micro por lo cual se establece la importancia de la adopción de las TIC ya que ayudará a mejorar negocios e incrementar en tamaño; de las encuestas realizadas por el INEC de 2012-2014 resaltan que la inversión en TIC no alcanza el 50% del total de las empresas encuestadas. En 2015 el 96,6% de las empresas a las que se les realizó las encuestas tenían acceso a internet, por lo consiguiente el 66,7% realizan inversiones en TIC; del porcentaje antes mencionado solo el 24,6% corresponde a empresas industriales o de manufactura.

En el 2020 el Gobierno Nacional elaboró una propuesta de Ley de Conectividad y Transformación Digital la cual ayudará a fomentar la transformación digital de las empresas públicas, privadas y de la sociedad con el objetivo de impulsar la economía digital, la eficiencia y el bienestar social.

De acuerdo a la publicación realizada por el MINTEL (MINTEL, 2019) en su página web en la sección de la Agenda Digital del Ecuador 2021-2022 indica que el Cloud Computing es reconocido como una tecnología emergente por parte del Gobierno Nacional por el cual establecerá proyectos dentro del denominado programa3: Tecnologías Emergentes para el Desarrollo Sostenible; en el informe indican que es muy importante de la implementación de tecnologías en las organizaciones a corto plazo y de los datos obtenidos de la encuesta de Ernst & Young en el 2020 y en el informe "Tendencias Tecnológicas de mayor impacto en el Ecuador para el 2020" indican que el 69% planean implementar Cloud Computing, el 73% Big Data/Data Analytics, 44% Inteligencia Artificial y Machine Learning, 41% Robotic Processes Automation (RPA), 28% IoT, 17% Blockchain, 11% Realidad Virtual/Aumentada, 9% uso de drones y 3% impresión en 3D.

Por lo antes citado se deben realizar evaluaciones de aspectos que engloban la seguridad informática ya que el almacenado de información en internet o el intercambio de información en la web puede verse afectado si no se toman las debidas medidas correspondientes. Unas de las principales amenazas tanto físicas como lógicas suceden debido a la vulneración de los sistemas de información lo cual trae pérdidas económicas a las empresas y a su vez reclamos de usuarios afectados quienes ya no verán con buen auge al proveedor que le ofrece el servicio.

3.1.2 Panorama actual del Cloud Computing en el Ecuador

Según la revista (Lideres, 2012) Nubis Partners en la actualidad ofrece servicios en la nube a cerca de 50 empresas en el Ecuador a través de Google, estos servicios los reciben empresas del sector de tecnología, banca, medios de comunicación, servicios de construcción, etc. Según Sebastián Pérez gerente en Ecuador de Nubis Partners indica que "En Ecuador estamos atrasados en el tema, recién estamos entrando con herramientas básicas como Google Apps. Pero las empresas se están dando cuenta de que pasar a la nube implica un cambio de estrategia de toda la organización".

En una publicación realizada por la revista (Lideres, 2012) indican que una de las compañias de las que usa los servicios en la nube es Humana una firma de medicina prepagada, su gerente de Gestión de Tecnologías de la Información Marco Puente indica que en los dos años que utilizan el servicio la experiencia ha valido la pena indicando textualmente que "Los procesos se agilitaron y mejoramos el procesamiento de datos que genera la fuerza de ventas, copuesta por 100 personas".

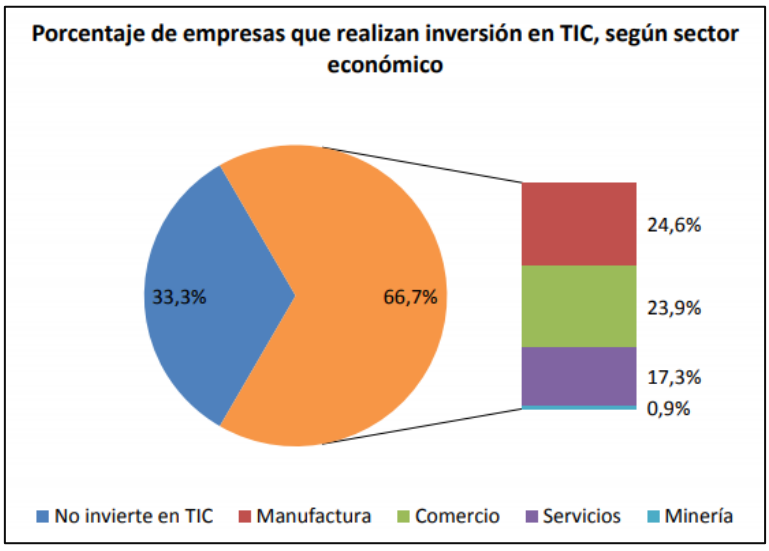
La revista (Lideres, 2012) también indica en su publicación que en el país Microsoft también ofrece servicio para 300 mipymes, además unas 3000 compañias conocen los beneficios de estar en la nube.

3.1.3 Inversiones en TIC (Tecnologías de la Información y la Comunicación) en el Ecuador

Según el informe del INEC (Instituto Nacional de Estadísticas y Censos, 2019) realizado en el 2015 sobre Tecnologías de la Información y la Comunicación, de las 3245 empresas existentes 958 de ellas que están orientadas a Servicios han invertido en TIC, adicional el 17,3% de las empresas orientadas a servicios invierten en TIC.

Figura 3. 1

Porcentaje de empresas que realizan inversión en TIC, según sector económico

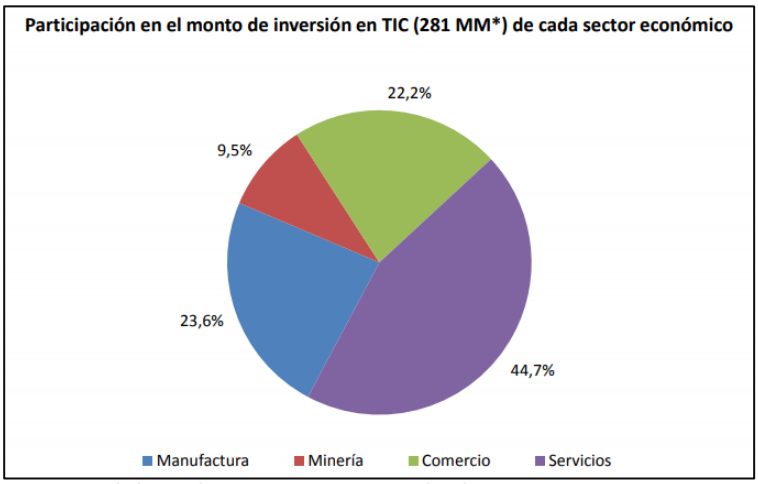


Fuente: Elaborado por autor. Tomado de https://www.ecuadorencifras.gob.ec/documentos/webinec/Estadisticas_Economicas

El informe del INEC (Instituto Nacional de Estadísticas y Censos, 2019) también nos muestra que de las empresas investigadas que realizaron inversión en TIC, las que mayor aporte en monto invertido son las de servicios con un 44,7% del total de la inversión.

Figura 3. 2

Participación en el monto de inversión en TIC (281 MM) de cada sector económico*



Fuente: Elaborado por autor. Tomado de https://www.ecuadorencifras.gob.ec/documentos/webinec/Estadisticas_Economicas

Vady Guerra Director Comercial Mercado Corporativo de Claro menciona en un informe de la revista (Datta Business Innovation, 2019) publicado el 16 de Agosto del 2019 que en la medida de que este nuevo consumidor sea dominante en Ecuador e ingresen empresas con formatos digitales, va aumentar la competitividad del mercado.

La revista Datta (Datta Business Innovation, 2019) también indica en su informe que Ecuador aún es un mercado incipiente en lo que respecta a la adopción del cloud computing; y anuncia que de acuerdo a un estudio realizado por la Espol y Microsoft indican que cerca del 78% de empresas que fueron encuestadas usan servicio de computación en la nube, aunque solo el 8,3% establece que más del 75% de sus aplicaciones se encuentran en entornos cloud; así también el 42,2% manifiesta que mantienen menos del 25% de sus aplicaciones en la nube.

3.1.4. Análisis de Variables

3.1.4.1 Desarrollo de la variable GARANTÍA (VI01) y sus tres dimensiones Integridad, Confidencialidad y Disponibilidad

La variable Garantía va a medir que todos los procesos que se encuentren dentro de los servicios de cloud computing sean seguros mediante sus tres dimensiones como lo son Integridad: Garantiza la no alteración de la información, Confidencialidad: garantiza que la información sea accesible solo para usuarios autorizados, Disponibilidad: asegura que los servicios puedan ser usados sin interrupciones.

3.1.4.1.1 Desarrollo de la variable independiente GARANTÍA en su dimensión INTEGRIDAD

Este análisis de la dimensión INTEGRIDAD fue llevado a cabo con la variable obtenida de la base de datos del Instituto Nacional de Estadísticas y Censos en la cual existió un análisis de la Participación de Tecnologías de Información y Comunicaciones de las empresas por sector económico año en el año 2015, se aplicó la estadística de frecuencias como análisis para determinar en qué porcentaje usan la firma electrónica como un método para asegurar la integridad de la información.

Tabla 3. 1

Datos de la variable Garantía en función de la Integridad

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

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable tic17_firma_digital

Tabla 3. 2

Análisis de la Integridad con datos de la variable tic17_firma_digital

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

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Si	10	10.0	58.8	58.8
	No	7	7.0	41.2	100.0
	Total	17	17.0	100.0	
Missing	System	83	83.0		
Total		100	100.0		

Fuente: Elaborado por autor

En la tabla 3.2 se puede identificar que existe una aceptación del 58,8% del uso de la firma electrónica; Se aplicó también una relación de las variables seleccionadas firma digital y software de seguridad con el uso de la técnica tabla cruzada.

Tabla 3. 3

Medición de la dimensión de Integridad aplicada en tabla cruzada

Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet * Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie) Crosstabulation

			Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)		
			Si	No	Total
Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet	Si	Count	3	7	10
		% within Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet	30.0%	70.0%	100.0%
	No	Count	1	6	7
		% within Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet	14.3%	85.7%	100.0%
Total		Count	4	13	17
		% within Utilizó su empresa firma digital en comunicaciones enviadas? Solo si dispone de internet o intranet	23.5%	76.5%	100.0%

Fuente: Elaborado por autor

En la tabla 3.3 se puede observar la existencia de un 30.0% del uso de la firma electrónica y un software de seguridad, relacionando a la escala de Likert podemos establecemos un criterio de 2 puntos con lo que definimos que está **EN DESACUERDO CON LA SEGURIDAD** relacionado al principio de integridad con el uso de la firma electrónica y un software de seguridad.

3.1.4.1.2 Desarrollo de la variable independiente GARANTÍA en su dimensión CONFIDENCIALIDAD

Este análisis de la dimensión CONFIDENCIALIDAD fue llevado a cabo con la variable obtenida de la base de datos del Instituto Nacional de Estadísticas y Censos con el análisis de la Participación de Tecnologías de Información y Comunicaciones de las empresas por sector económico año en el año 2015, se aplicó la estadística de frecuencias como análisis del uso de una intranet como un método para garantizar la confidencialidad de la información.

Tabla 3. 4

Datos de la variable Garantía en función de la Confidencialidad

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

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable tic16_intranet

Tabla 3. 5

Análisis de la Confidencialidad con datos de la variable tic16_intranet

Su empresa ¿Contaba con intranet en el 2015?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Si	12	12.0	70.6	70.6
	No	5	5.0	29.4	100.0
	Total	17	17.0	100.0	
Missing	System	83	83.0		
Total		100	100.0		

Fuente: Elaborado por autor

En la tabla 3.5 se puede identificar que existe un 70,6% del uso de una intranet, en relación a la escala de Likert podemos definir un criterio de 4 puntos lo cual indica que está **EN ACUERDO CON LA SEGURIDAD** con el uso de una intranet como método para garantizar la confidencialidad aplicando roles a usuarios y de esta manera llevar un control de la seguridad de la información.

3.1.4.1.3 Desarrollo de la variable independiente GARANTÍA en su dimensión DISPONIBILIDAD

Este análisis de la dimensión DISPONIBILIDAD fue llevado a cabo con la técnica de Documental, cabe recalcar que se tomó como referencia el uso del manual de ITIL v3 el cual establece un enfoque a la Gestión de Niveles de Servicio y Gestión de la Disponibilidad el cual nos muestra una fórmula para el cálculo del porcentaje de la disponibilidad.

Tabla 3. 6

Fórmula para calcular el porcentaje de disponibilidad según ITIL

$$\text{Availability (\%)} = \frac{\text{Agreed Service Time (AST)} - \text{Downtime}}{\text{Agreed Service Time (AST)}} \text{ x}$$

Fuente: Elaborado por autor. Tomado de ITIL v3

La disponibilidad se la considera como uno de los elementos principales y fundamentales en un sistema de información ya que el mismo va a garantizar

que los servicios estén siempre activos; de acuerdo a la escala de Likert se le agrega un valor de 5 puntos lo cual indica que se está **EN TOTAL ACUERDO CON LA SEGURIDAD** con la aplicación de mecanismos de disponibilidad para mantener y resguardar la seguridad de la información.

3.1.4.2 Desarrollo de la variable CONTROL DE ACCESO (VI02) y sus dos dimensiones Autenticación y Control de Acceso

La variable Control de Acceso va a medir la seguridad aplicando mecanismos como lo son métodos de autenticación, firmas digitales y mecanismos que ayuden asegurar el control de acceso mediante sus dos dimensiones las cuales son Autenticación y Control de Acceso.

3.1.4.2.1 Desarrollo de la variable independiente CONTROL DE ACCESO en su dimensión AUTENTICACIÓN

Este análisis de la dimensión AUTENTICACIÓN fue llevado a cabo con la técnica de recolección de campo en la cual se analizó la importancia de implementar métodos de autenticación en los sistemas para asegurar la seguridad de la información.

Tabla 3. 7

Datos de la variable Control de Acceso en función de la Autenticación

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI02_ControldeAcceso_autenticación	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI02_ControldeAcceso_autenticación

Tabla 3. 8

Encuesta de variable Autenticación

7.Sección(VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso. [Se establecen mecanismos de autenticación como medida de seguridad de la información para los servicios brindados a los clientes.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	2	2.0	2.0	2.0
	En total acuerdo con la seguridad	98	98.0	98.0	100.0
	Total	100	100.0	100.0	

Fuente: Elaborado por autor

La autenticación es considerada importante en un sistema de información ya que el mismo va a garantizar que solo los usuarios registrados tengan acceso a la información, en la tabla 3.8 se observa un porcentaje de importancia de 98% que de acuerdo a la escala de Likert se le agrega un valor de 5 puntos lo cual indica que se está **EN TOTAL ACUERDO CON LA SEGURIDAD** de establecer mecanismos de autenticación para asegurar la seguridad de la información.

3.1.4.2.2 Desarrollo de la variable independiente CONTROL DE ACCESO en su dimensión CONTROL DE ACCESO

Este análisis de la dimensión CONTROL DE ACCESO fue llevado a cabo con la técnica de recolección de campo en la cual se analizó la importancia de establecer mecanismos para asegurar que los sistemas no sean vulnerados por personal no autorizado.

Tabla 3. 9

Datos de la variable Control de Acceso en Función del Control de Acceso

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI02_ControldeAcceso_controldeacceso	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI02_ControldeAcceso_controldeacceso

Tabla 3. 10

Encuesta de variable Control de Acceso

7.Sección(VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso. [Para los permisos o denegación de accesos a servicios, es necesario realizar una autenticación previa de usuario.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	3	3.0	3.0	3.0
	En total acuerdo con la seguridad	97	97.0	97.0	100.0
	Total	100	100.0	100.0	

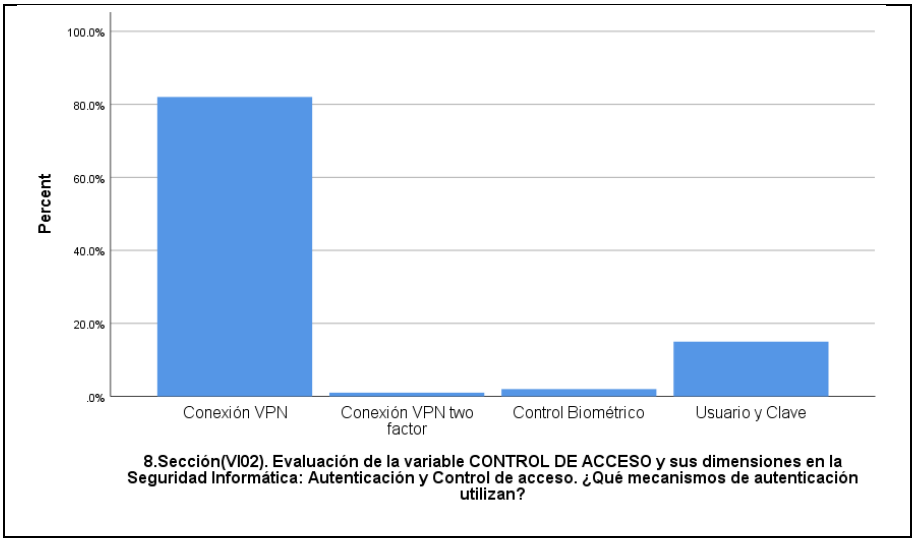
Fuente: Elaborado por autor

En la tabla 3.10 podemos observar como tiene una aceptación la implementación de mecanismos de control de acceso como autenticación previa de usuarios con un valor de 97% que de acuerdo a la escala de Likert se le agrega un valor de 5 puntos lo cual indica que se está **EN TOTAL ACUERDO CON LA SEGURIDAD** de implementar mecanismos de control de acceso para asegurar la seguridad de la información.

Adicional se realizó una encuesta donde consultaban que mecanismos de autenticación utilizan para el acceso a la información obteniendo los siguientes resultados

Tabla 3. 11

Encuesta de variable Autenticación y Control de Acceso



Fuente: Elaborado por autor

En los resultados de la tabla 3.11 se puede observar que el mecanismo de autenticación más utilizado es la conexión VPN con un valor de 82%, método utilizado para el resguardo de la seguridad de la información.

3.1.4.3 Desarrollo de la variable CUMPLIMIENTO (VI03) y sus dos dimensiones Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información

La variable CUMPLIMIENTO va a medir la seguridad informática mediante sus dos dimensiones las cuales son: Requisitos Legales y Contractuales y también la Revisión de la Seguridad de la Información.

3.1.4.3.1 Desarrollo de la variable independiente CUMPLIMIENTO en su dimensión REQUISITOS LEGALES Y CONTRACTUALES

Este análisis de la dimensión REQUISITOS LEGALES Y CONTRACTUALES fue llevado a cabo con la técnica documental en la cual se valida la importancia de cumplir con las normas, leyes y estándares para poder evitar poner en peligro a la empresa y resguardar la seguridad de la información evaluando cinco controles para el cumplimiento legal.

Tabla 3. 12

Controles para el Cumplimiento Legal en el entorno de Seguridad Informática

Controles para el cumplimiento Legal
Protección y Gestión de los registros de la organización
Protección y Gestión de datos y de información personal
Regulación y Gestión de los controles criptográficos
Derechos de propiedad Intelectual (DPI)
Identificación y Gestión de la legislación aplicable

Fuente: Elaborado por autor

Tabla 3. 13

Datos de la variable Cumplimiento en función de los Requisitos Legales y Contractuales

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI03_Cumplimiento_c VI03_Cumplimiento_d VI03_Cumplimiento_e VI03_Cumplimiento_f VI03_Cumplimiento_g	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de las variables: VI03_Cumplimiento_c, VI03_Cumplimiento_d, VI03_Cumplimiento_e, VI03_Cumplimiento_f, VI03_Cumplimiento_g

Tabla 3. 14

Encuesta de los controles para el Cumplimiento Legal en el entorno de Seguridad Informática

9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Proteger los registros de la organización.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En total acuerdo con la seguridad	100	100.0	100.0	100.0

9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Protección de datos y privacidad de información personal.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	2	2.0	2.0	2.0
	En total acuerdo con la seguridad	98	98.0	98.0	100.0
	Total	100	100.0	100.0	

9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Cumplir con controles para asegurar el entorno de la seguridad informática.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	9	9.0	9.0	9.0
	En total acuerdo con la seguridad	91	91.0	91.0	100.0
	Total	100	100.0	100.0	

9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Derechos de propiedad intelectual (DPI).]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	9	9.0	9.0	9.0
	En total acuerdo con la seguridad	91	91.0	91.0	100.0
	Total	100	100.0	100.0	

9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Identificar la legislación aplicable.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	13	13.0	13.0	13.0
	En total acuerdo con la seguridad	87	87.0	87.0	100.0
	Total	100	100.0	100.0	

Fuente: Elaborado por autor

En la tabla 3.14 podemos observar la aceptación de la importancia de los requisitos legales y contractuales, de acuerdo a la escala de Likert se le agrega una ponderación de 5 puntos indicando **EN TOTAL ACUERDO CON LA SEGURIDAD** del análisis planteado

3.1.4.3.2 Desarrollo de la variable independiente CUMPLIMIENTO en su dimensión REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Este análisis de la dimensión REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN fue llevado a cabo con la técnica documental en la cual se establecen controles que permitan cumplir con procesos de auditorías a plataformas o servicios, técnicas y sistemas de información según las políticas establecidas y así poder cumplir con los estándares existentes, se aplicaron tres controles para la revisión

Tabla 3. 15

Controles para la revisión de la Seguridad Informática

Controles para la revisión de la Seguridad Informática
Revisión de la seguridad de la información
Cumplimiento de políticas y normas de seguridad
Comprobación del cumplimiento

Fuente: Elaborado por autor

Tabla 3. 16

Datos de la variable Cumplimiento en función de la Seguridad Informática

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI03_Cumplimiento_i	Recolección de campo	Encuesta	Primaria

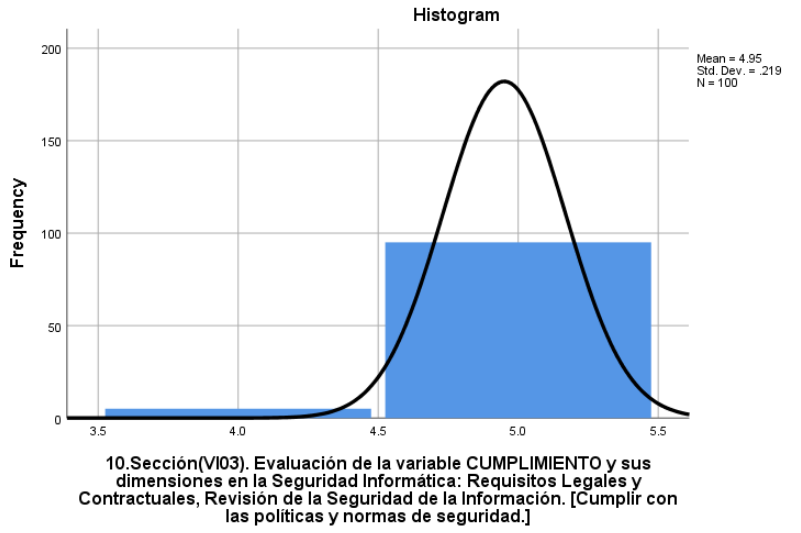
Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI03_Cumplimiento_i

Tabla 3. 17

Encuesta de los controles para la revisión de la Seguridad Informática

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	5	5.0	5.0	5.0
	En total acuerdo con la seguridad	95	95.0	95.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.17 podemos observar la aceptación de la importancia de cumplir con los controles de la seguridad informática, de acuerdo a la escala de Likert se le agrega un valor de 5 puntos lo cual indica que se está **EN TOTAL ACUERDO CON LA SEGURIDAD** con la seguridad.

3.1.4.4 Desarrollo de la variable GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO (VI04) y sus dos dimensiones Gestión de Incidentes de Seguridad de la Información y Redundancia

La variable Gestión de Incidentes y Continuidad del Negocio va a medir si existen planes de acción que se realizan para prevalecer la seguridad de la información aplicando estrategias como métodos de redundancia y notificaciones de eventos de seguridad y puntos débiles, esta medición se la realiza mediante sus dos dimensiones como lo son Gestión de Incidentes de Seguridad de la Información y Redundancia.

3.1.4.4.1 Desarrollo de la variable independiente GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO en su dimensión GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El análisis de la dimensión GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN fue llevado a cabo con la técnica recolección de campo en la cual se consultó si se establecían responsabilidades y procedimientos para asegurar la información y si se realizaban notificaciones de eventos y posibles puntos débiles de seguridad.

Tabla3. 18

Datos de la variable Gestión de Incidentes y Continuidad del Negocio en función de la Gestión de Incidentes de Seguridad de la Información

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI04_Gestióndeincidentes_ gestióndeincidentesdeseguridad	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI04_Gestióndeincidentes_gestióndeincidentesdeseguridad

Tabla 3. 19

Encuesta de la variable Gestión de Incidentes y Seguridad de la Información

11.Sección(VI04). Evaluación de la variable GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO y sus dimensiones en la Seguridad Informática: Gestión de Incidentes de Seguridad de la Información , Redundancia. [Se establecen responsabilidades y procedimientos para asegurar la información, realizando notificaciones de eventos y posibles puntos débiles de seguridad.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En total acuerdo con la seguridad	100	100.0	100.0	100.0

Fuente: Elaborado por autor

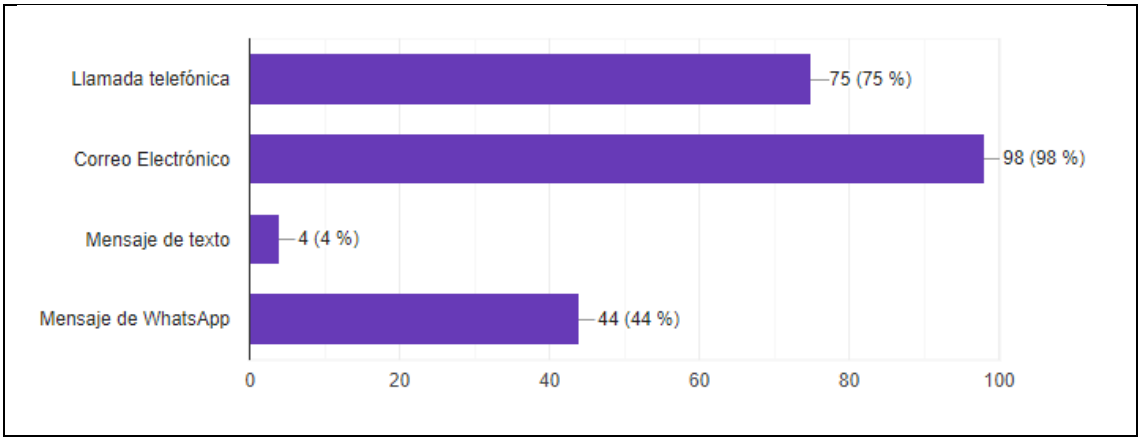
En la tabla 3.19 podemos observar la aceptación de establecer responsabilidades y procedimientos para asegurar la información, de acuerdo a la escala de Likert se le agrega un valor de 5 puntos lo cual indica que se está

EN TOTAL ACUERDO CON LA SEGURIDAD.

Adicional, en las encuestas se realizó la consulta también de cuáles eran los métodos más usados para realizar las notificaciones a los clientes antes posibles eventos de seguridad, mostrándonos los siguientes datos:

Tabla 3. 20

Encuesta de variable Gestión de Incidentes y Seguridad de la Información



Fuente: Elaborado por autor

En la tabla 3.20 se puede identificar que el medio más utilizado para realizar notificaciones de eventos de seguridad es el correo electrónico con un 98% de aceptación, seguido de la llamada telefónica con un 75% y en tercer lugar tenemos los mensajes de WhatsApp con un 44% y finalmente tenemos la opción de mensajes de texto con un 4% de aceptación lo cual indica que correo electrónico y llamadas telefónicas son los medios más utilizados para notificaciones de eventos.

3.1.4.4.2 Desarrollo de la variable independiente GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO en su dimensión REDUNDANCIA

El análisis de la dimensión REDUNDANCIA fue llevado a cabo con la técnica recolección de campo en la cual se mide la necesidad de definir y planificar estrategias que aseguren la seguridad de la información ante posibles fallas de elementos e instalaciones principales.

Tabla 3. 21

Datos de la variable Gestión de Incidentes y Continuidad del Negocio en función de la Redundancia

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI04_Gestióndeincidentes_ redundancia	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

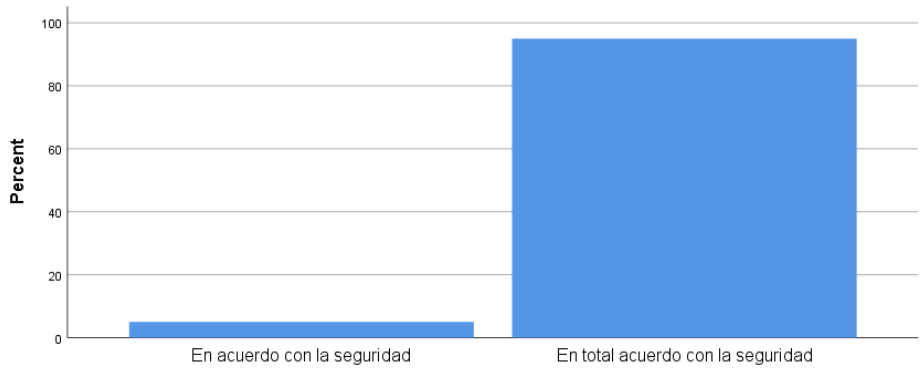
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI04_Gestióndeincidentes_redundancia

Tabla 3. 22

Encuesta de variable Gestión de Incidentes y Seguridad de la Información

11.Sección(VI04). Evaluación de la variable GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO y sus dimensiones en la Seguridad Informática: Gestión de Incidentes de Seguridad de la Información , Redundancia. [Es importante planificar y ejecutar estrategias que protejan la seguridad de la información ante posibles fallas de elementos e instalaciones principales.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En acuerdo con la seguridad	5	5.0	5.0	5.0
	En total acuerdo con la seguridad	95	95.0	95.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.22 podemos observar la aceptación estrategias que aseguren la seguridad de la información ante posibles fallas de elementos e instalaciones principales, con un 95% de aceptación que de acuerdo a la escala de Likert se

le agrega un valor de 5 puntos lo cual indica que se está **EN TOTAL ACUERDO CON LA SEGURIDAD**.

3.1.4.5 Desarrollo de la variable SERVICIO (VI05) y sus tres dimensiones Software como Servicio, Plataforma como Servicio e Infraestructura como Servicio

La variable Servicio va a medir la seguridad informática en tres dimensiones las cuales son: Software como Servicio, Plataforma como Servicio e Infraestructura como Servicio, a continuación, el análisis de las mismas.

3.1.4.5.1 Desarrollo de la variable independiente SERVICIO en su dimensión SOFTWARE COMO SERVICIO

En la dimensión SOFTWARE COMO SERVICIO se midió la importancia de que el proveedor tenga el control de las funciones de los servicios tales como actualizaciones para que estén siempre activos y seguros, se aplicó un análisis de frecuencia; a continuación, el resultado obtenido.

Tabla 3. 23

Datos de la variable Servicio en función del Software como Servicio

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI05_Servicio_SaaS	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI05_Servicio_SaaS

Tabla 3. 24

Encuesta de variable Servicio

14.Sección(VI05). Evaluación de la variable SERVICIO y sus dimensiones en la Seguridad Informática: Software como Servicio, Plataforma como Servicio, Infraestructura como Servicio. [El proveedor debe tener el control de las funciones y actualizaciones par

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Ni en acuerdo ni en desacuerdo con la seguridad	1	1.0	1.0	1.0
	En acuerdo con la seguridad	10	10.0	10.0	11.0
	En total acuerdo con la seguridad	89	89.0	89.0	100.0
	Total	100	100.0	100.0	

Fuente: Elaborado por autor

En la tabla 3.24 se puede identificar que existe una aceptación del 89% que se encuentra en total acuerdo, el 10% se encuentra en acuerdo y el 1% está marcado como: ni en acuerdo ni en desacuerdo, lo cual de acuerdo a la escala de Likert se le asigna un valor de 5 puntos lo cual tenemos como resultado **EN TOTAL ACUERDO CON LA SEGURIDAD**.

3.1.4.5.2 Desarrollo de la variable independiente SERVICIO en su dimensión PLATAFORMA COMO SERVICIO

En la dimensión PLATAFORMA COMO SERVICIO se midió la importancia de que el proveedor tenga el control del uso de herramientas, aplicaciones, lenguajes de programación, etc. Se aplicó un análisis de frecuencia; a continuación, el resultado obtenido.

Tabla 3. 25

Datos de la variable Servicio en función de la Plataforma como Servicio

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI05_Servicio_PaaS	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI05_Servicio_PaaS

Tabla 3. 26

Datos de la variable Servicio en función de la Plataforma como Servicio

14.Sección(VI05). Evaluación de la variable SERVICIO y sus dimensiones en la Seguridad Informática: Software como Servicio, Plataforma como Servicio, Infraestructura como Servicio. [La administración de la insfraestructura debe ser realizada únicamente po

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En desacuerdo con la seguridad	24	24.0	24.0	24.0
	Ni en acuerdo ni en desacuerdo con la seguridad	37	37.0	37.0	61.0
	En acuerdo con la seguridad	17	17.0	17.0	78.0
	En total acuerdo con la seguridad	22	22.0	22.0	100.0
	Total	100	100.0	100.0	

Fuente: Elaborado por autor

En la tabla 3.26 se puede identificar que existe una aceptación del 37% que se encuentra ni en acuerdo ni en desacuerdo, el 24% se encuentra en desacuerdo, el 22% se encuentra en total acuerdo y finalmente solo el 17% se encuentra en acuerdo, lo cual de acuerdo a la escala de Likert se le asigna un valor de 3 puntos lo cual nos muestra como resultado **NI EN ACUERDO NI EN DESACUERDO CON LA SEGURIDAD**.

3.1.4.5.3 Desarrollo de la variable independiente SERVICIO en su dimensión INFRAESTRUCTURA COMO SERVICIO

En la dimensión INFRAESTRUCTURA COMO SERVICIO se consultó si existían aspectos negativos para los clientes tales como: falta de control, dependencia, privacidad al mantener equipos y/o servicios en la infraestructura del proveedor, Se aplicó un análisis de frecuencia; a continuación, el resultado obtenido.

Tabla 3. 27

Datos de la variable Servicio en función de la Infraestructura como Servicio

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI05_Servicio_IaaS	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

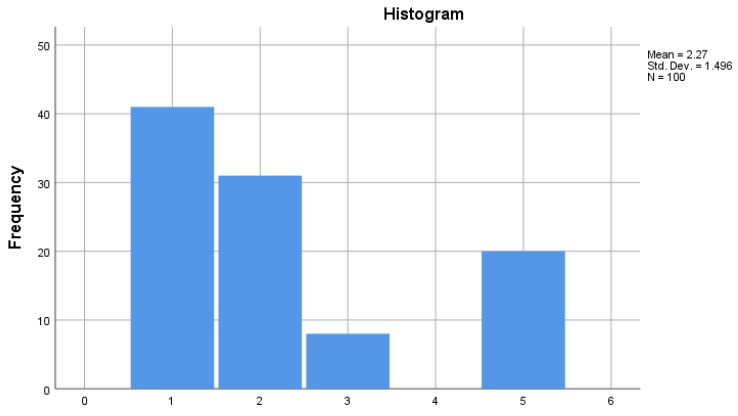
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI05_Servicio_IaaS

Tabla 3. 28

Datos de la variable Servicio en su Dimensión Infraestructura como Servicio

14.Sección(VI05). Evaluación de la variable SERVICIO y sus dimensiones en la Seguridad Informática: Software como Servicio, Plataforma como Servicio, Infraestructura como Servicio. [Al ofrecer el servicio de IaaS los clientes podrían experimentar aspectos

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	En total desacuerdo con la seguridad	41	41.0	41.0	41.0
	En desacuerdo con la seguridad	31	31.0	31.0	72.0
	Ni en acuerdo ni en desacuerdo con la seguridad	8	8.0	8.0	80.0
	En total acuerdo con la seguridad	20	20.0	20.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En un servicio tipo Infraestructura se ejecutan diferentes softwares y equipos sean estas máquinas virtuales, balanceadores de cargas, servidores de almacenamiento, dispositivos de red, firewalls, servidores de aplicaciones, etc. pero no hay una gestión ni control de la infraestructura cloud, solo de los servicios y aplicaciones que se usan lo cual es un riesgo. En el análisis de los

resultados obtenidos de la base de datos se puede identificar que el 41% está en total desacuerdo, el 31% en desacuerdo, el 20% en acuerdo y finalmente el 8% ni en acuerdo ni en desacuerdo; el 41% que está en total desacuerdo nos muestra que no existen aspectos negativos para los clientes tales como: falta de control, dependencia, privacidad al mantener equipos y/o servicios en la infraestructura del proveedor de acuerdo a la escala de Likert se asigna un valor de 3 lo cual indica que está **NI EN ACUERDO NI EN DESACUERDO CON LA SEGURIDAD.**

3.1.4.6 Desarrollo de la variable DESPLIEGUE (VI06) y sus cuatro dimensiones Público, Privado, Híbrido y Comunitario

La variable DESPLIEGUE va a medir la seguridad informática en cuatro dimensiones las cuales son: Público, Privado, Híbrido y Comunitario, a continuación, el análisis de las mismas.

3.1.4.6.1 Desarrollo de la variable independiente DESPLIEGUE en su dimensión PÚBLICO

Esta dimensión PÚBLICO fue llevado a cabo con la técnica recolección de campo en la cual se analizan la importancia del uso de servicios y/o aplicaciones en un despliegue público, a continuación, el resultado obtenido.

Tabla 3. 29

Datos de la variable Despliegue en función del Despliegue Público

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI06_Despliegue_público	Recolección de campo	Encuesta	Primaria

Fuente: Elaborado por autor

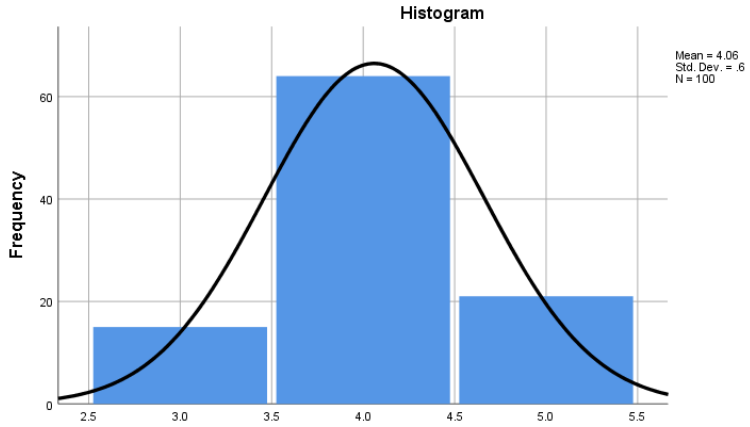
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de la variable VI06_Despliegue_público

Tabla 3. 30

Datos de la variable Despliegue en su dimensión Público

15.Sección(VI06). Evaluación de la variable DESPLIEGUE y sus dimensiones en la Seguridad Informática: Público, Privado, Híbrido y Comunitario. De acuerdo al despliegue cloud existente: público, privado, híbrido y comunitario valore el grado de demanda mas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Medio	15	15.0	15.0	15.0
	Alto	64	64.0	64.0	79.0
	Muy Alto	21	21.0	21.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.30 se puede identificar que existe una valoración del 64% sobre el acceso a servicios y/o aplicaciones gratuitas que se encuentran en una nube pública; de acuerdo a la escala de Likert se le agrega un valor de 4 puntos lo cual indica que se está **EN ACUERDO** con servicios y/o aplicaciones gratuitas que se encuentran en nube pública.

3.1.4.6.2 Desarrollo de la variable independiente DESPLIEGUE en su dimensión PRIVADO

Esta dimensión PRIVADO fue llevado a cabo con la técnica recolección de campo en la cual se analizan la importancia del acceso a infraestructura, equipos y/o servicios en un despliegue privado, a continuación, el resultado obtenido.

Tabla 3. 31

Datos de la variable Despliegue en función de la Dimensión Privado

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI06_Despliegue_privado	Recolección de Campo	Encuesta	Primaria

Fuente: Elaborado por autor

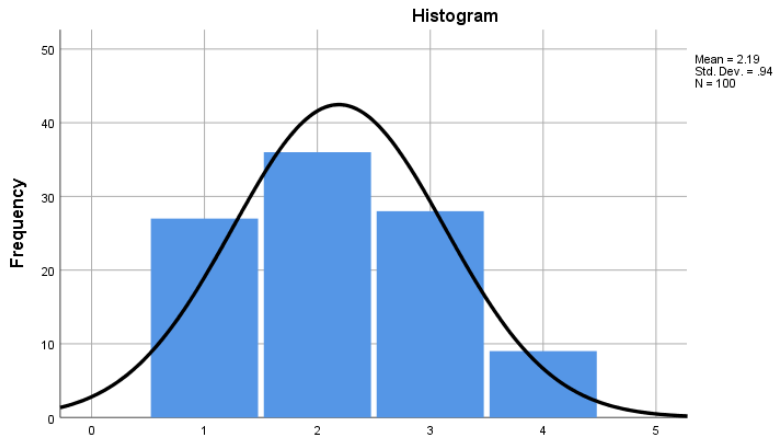
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de las variables VI06_Despliegue_privado

Tabla 3. 32

Datos de la variable Despliegue en su dimensión Privado

15.Sección(VI06). Evaluación de la variable DESPLIEGUE y sus dimensiones en la Seguridad Informática: Público, Privado, Híbrido y Comunitario. De acuerdo al despliegue cloud existente: público, privado, híbrido y comunitario valore el grado de demanda mas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Muy Bajo	27	27.0	27.0	27.0
	Bajo	36	36.0	36.0	63.0
	Medio	28	28.0	28.0	91.0
	Alto	9	9.0	9.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.32 se puede identificar que existe una valoración del 36% sobre la infraestructura, equipos y/o servicios que se encuentran en una nube privada; de acuerdo a la escala de Likert se le agrega un valor de 2 puntos lo cual indica

que se está **EN DESACUERDO** con equipos y/o servicios que se encuentran en una nube privada.

3.1.4.6.3 Desarrollo de la variable independiente DESPLIEGUE en su dimensión HÍBRIDO

Esta dimensión HÍBRIDO fue llevado a cabo con la técnica recolección de campo en la cual se analizan la importancia del acceso a servicios y/o datos en un despliegue híbrido; es decir público y privado, a continuación, el resultado obtenido.

Tabla 3. 33

Datos de la variable Despliegue en función de la dimensión Híbrido

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI06_Despliegue_híbrido	Recolección de Campo	Encuesta	Primaria

Fuente: Elaborado por autor

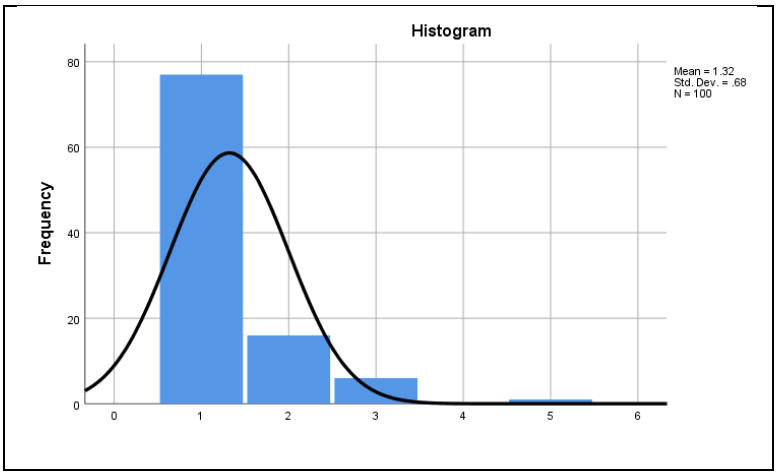
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de las variables VI06_Despliegue_híbrido

Tabla 3. 34

Datos de la variable Despliegue en su dimensión Híbrido

15.Sección(VI06). Evaluación de la variable DESPLIEGUE y sus dimensiones en la Seguridad Informática: Público, Privado, Híbrido y Comunitario. De acuerdo al despliegue cloud existente: público, privado, híbrido y comunitario valore el grado de demanda mas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Muy Bajo	77	77.0	77.0	77.0
	Bajo	16	16.0	16.0	93.0
	Medio	6	6.0	6.0	99.0
	Muy Alto	1	1.0	1.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.34 se puede identificar que existe una valoración del 77% sobre el acceso a servicios y/o datos que se encuentran en una nube híbrida; de acuerdo a la escala de Likert se le agrega un valor de 1 puntos lo cual nos muestra **EN TOTAL DESACUERDO** con la seguridad.

3.1.4.6.4 Desarrollo de la variable independiente DESPLIEGUE en su dimensión COMUNITARIO

Esta dimensión COMUNITARIO fue llevado a cabo con la técnica recolección de campo en la cual se analizan la importancia de ejecutar servicios y/o aplicaciones en un despliegue comunitario, a continuación, el resultado obtenido.

Tabla 3. 35

Datos de la variable Despliegue en función de la dimensión Comunitario

Nombre de la variable	Técnica de investigación	Instrumento	Fuente
VI06_Despliegue_comunitario	Recolección de Campo	Encuesta	Primaria

Fuente: Elaborado por autor

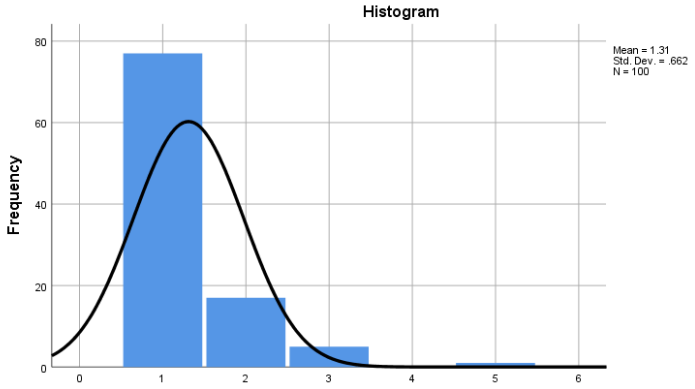
En la siguiente tabla se observa el resultado del análisis estadístico de frecuencias de las variables VI06_Despliegue_comunitario

Tabla 3. 36

Datos de la variable Despliegue en su dimensión Comunitario

15.Sección(VI06). Evaluación de la variable DESPLIEGUE y sus dimensiones en la Seguridad Informática: Público, Privado, Híbrido y Comunitario. De acuerdo al despliegue cloud existente: público, privado, híbrido y comunitario valore el grado de demanda mas

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Muy Bajo	77	77.0	77.0	77.0
	Bajo	17	17.0	17.0	94.0
	Medio	5	5.0	5.0	99.0
	Muy Alto	1	1.0	1.0	100.0
	Total	100	100.0	100.0	



Fuente: Elaborado por autor

En la tabla 3.36 se puede identificar que existe una valoración del 77% sobre la ejecución de servicios y/o aplicaciones que se encuentran en una nube comunitaria; de acuerdo a la escala de Likert se le agrega un valor de 1 puntos lo cual no muestra **EN TOTAL DESACUERDO** con la seguridad.

3.2 Análisis y enfoque comparativo, evolución, perspectivas y tendencias

3.2.1 Análisis de la evolución del Cloud Computing en el Ecuador

En la actualidad la mayoría de las personas utilizamos servicios de Cloud, algunas con conocimiento del mismo y otras no y Ecuador no es la excepción; estos tipos de servicios pueden ser los más comunes como son los gratuitos sean estos: redes sociales, herramientas de correo electrónico como: Gmail, Outlook, herramientas de almacenamiento tales como Dropbox, Google Drive, juegos en línea ya sean de las plataformas de PS, XBOX, y con la aparición de

la pandemia COVID-19 se empezó a impulsar el teletrabajo lo que trajo consigo el uso de plataformas de sesiones remotas sean estas TEAMS, CISCO WEBEX, ZOOM, etc. lo que no muestra un desconocimiento sobre el uso de servicios de Cloud Computing y tampoco tenemos registros en Ecuador de las empresas que usan este servicio.

El uso y aplicación de los servicios que ofrece Cloud Computing pueden llegar a facilitar trabajos, procesos y hasta ahorrar recursos a diferentes empresas en el Ecuador, pero para ello se necesita un excelente asesoramiento en el despliegue, implementación y desarrollo para que puedan lograr cumplir con todos los objetivos planteados sean estos de tecnología e innovación y a su vez pueda proteger la seguridad de la información. También se debe tomar en consideración el despliegue de los proveedores existentes en Ecuador, en la actualidad son pocas las empresas que ofrecen este servicio, pero de a poco se van sumando en brindar soluciones con esta tecnología; en muchos casos es necesario obtener certificaciones que avalen que el proveedor está capacitado para brindar este servicio; de acuerdo a un informe realizado por (Pyramid Research, 2014) sostiene que los servicios cloud a nivel empresarial sean estos SaaS, IaaS y UcasS han generado el 5% del total del ingreso en el sector de las telecomunicaciones en lo que comprende a Latinoamérica en 2014 y que podría aumentar al 14% hasta el final del 2019.

3.2.2 Principales proveedores de Cloud Computing en Ecuador

El (MINTEL, 2019) sostiene que como objetivo general para el 2019 es posicionar a CNT (Corporación Nacional de Telecomunicaciones) como la mejor proveedora de soluciones de cloud computing ya que esta cuenta con Data Centers en Guayaquil y Quito, los mismos brindan uso de una nube hiperconvergente 4.0.; servicios que van a estar disponibles para diferentes líneas de negocio las cuales estén orientadas a: recopilar, transportar, almacenar, procesar analizar y predecir información lo cual permitirá aumentar la productividad de las empresas y satisfacer sus necesidades tecnológicas. Dentro de las estrategias propuestas se encuentran las siguientes:

- Soluciones orientadas a la Seguridad de la Información
- Solución Big Data as a Service (BDaaS) enmarcados en la estrategia de MINTEL promoviendo el desarrollo de TIC’s en el país
- Soluciones que impulsen la Inteligencia Artificial (AI)

Entre las empresas privadas tenemos a Claro y Telconet quienes han desarrollado servicios de Cloud Computing con diferentes opciones para satisfacer la necesidad de sus clientes entre esas opciones se encuentran las siguientes:

La empresa Claro cuenta con su servicio llamado Claro Cloud (Claro Cloud, n.d.) el cual presenta múltiples soluciones en un centro de datos permitiendo utilizar archivos, aplicaciones e infraestructura de cómputo con tan solo acceso a internet; adicional cuenta con un portafolio servidores virtuales, espacios de almacenamiento, software, videoconferencias, cuentas de correos entre otros. Dentro de las ventajas de obtener estos servicios Claro indica que las empresas percibirán ahorros relacionados con:

- Inversión en equipos
- Sistemas de seguridad, monitoreo y respaldo
- Personal especialista y certificado
- Aumento de capacidad inmediata y dinámica
- Infraestructura redundante con una operación centralizada.

Por su parte Telconet cuenta con dos centros de datos avalados internacionalmente los cuales lo denominó (Telconet ClouDCenter, n.d.) TELCONET CLOUD CENTER I, el cual se encuentra localizado en la ciudad de Guayaquil y TELCONET CLOUD CENTER II ubicado en Quito ambos con una amplia infraestructura que van a permitir mejorar la productividad de las empresas ya que podrán optimizar recursos, maximizar beneficios y aumentar ingresos, cumpliendo con todos los estándares de calidad y seguridad; dentro de los servicios que ofrece se encuentran:

- Housing

- Cloud Mail
- Cloud RPA
- IaaS
- Office 365
- Web Hosting entre otros

Daniel Ramos analista senior en (Pyramid Research, 2014) indica que uno de los problemas principales que tienen las compañias de telecomunicaciones en Latinoamérica es llegar a una gran cantidad de negocios debido a la saturación del canal y mantiene que una forma efectiva de abordar al segmento Pyme es con plataformas de autoservicio.

Adicional cabe mencionar que en la actualidad Ecuador cuenta con 9 Datacenters los cuales están avalados con certificaciones internacionales otorgadas por él (Uptime Institute, 2017) lo cual confirman que cumplen con todas las funciones de administración de TI, ingeniería de centro de datos, y demás.

Tabla 3. 37

Certificaciones TIER para Ecuador

Compañía	Localización	Nombre del Centro de Datos	Certificación TIER
CenturyLink Ecuador S.A.	Quito, Ecuador	Quito Datacenter Carcelén	Tier III Certification of Design Documents
Conecel S.A.	Guayaquil, Ecuador	Data Xperience Center Durán	Tier III Certification of Design Documents
Conecel S.A.	Quito, Ecuador	Data Xperience Center Collaloma Salas 104 y 105	Tier III Certification of Design Documents
Corporación Nacional de Telecomunicaciones CNT E.P	Guayaquil Guayas, Ecuador	Centro de Datos CNT EP – Guayaquil	Tier III Certification of Design Documents
Corporación Nacional de Telecomunicaciones CNT E.P	Guayaquil Guayas, Ecuador	Centro de Datos CNT EP – Guayaquil, Phase 1	Tier III Certification of Constructed Facility
Corporación Nacional de Telecomunicaciones CNT E.P	Quito Pichincha, Ecuador	Centro de Datos CNT EP – Quito	Tier III Certification of Design Documents
Corporación Nacional de	Quito Pichincha, Ecuador	Centro de Datos CNT EP – Quito, Phase 1	Tier III Certification of Constructed Facility

Telecomunicaciones CNT E.P			
Telconet S.A.	Quito, Ecuador	Telconet Cloud Center II	Tier III Certification of Design Documents
Telconet S.A.	Guayaquil, Ecuador	Telconet Cloud Center I	Tier IV Certification of Design Documents

Fuente: Elaborado por autor. Tomado de (Uptime Institute, 2017)

3.2.3 Análisis FODA

Con el análisis FODA vamos a poder identificar y contrastar las Fortalezas y Debilidades contra las Oportunidades y Amenazas de la investigación realizada.

Tabla 3. 38

Análisis FODA

Fortalezas	**Oportunidades**
F1: Infraestructura escalable F2: Especialistas en el área tecnológica F3: Cumplimientos de las normas F4: Tecnología robusta F5: Costos Controlados	O1: Mercado en crecimiento O2: Integración de nuevas soluciones de servicios O3: Certificaciones en Seguridad de la información O4: Mayor rentabilidad O5: Asociación con proveedores líderes internacionales
Debilidades	**Amenazas**
D1: Riesgo de amenazas D2: Desconfianza de la tecnología D3: Resistencia al cambio D4: Costos altos de inversión y mantenimiento D5: Desconocimiento del Cloud Computing	A1: Dependencia del servicio de internet A2: Fallas inesperadas podrían afectar la seguridad A3: Falta de organismo de control en el país A4: No conocimiento de los estándares A5: Infringir directrices

Fuente: Elaborado por autor

El desarrollo del análisis FODA va a permitir a esta investigación transformar las debilidades en fortalezas y poder reducir el impacto de las amenazas y vulnerabilidades; para poder diseñar y mejorar estrategias a corto, mediano y largo plazo con el objetivo de fortalecer la adaptación de esta tecnología.

3.2.4 Análisis de Asimetría y Curtosis de Variables

3.2.4.1 Coeficientes de Asimetría y Curtosis

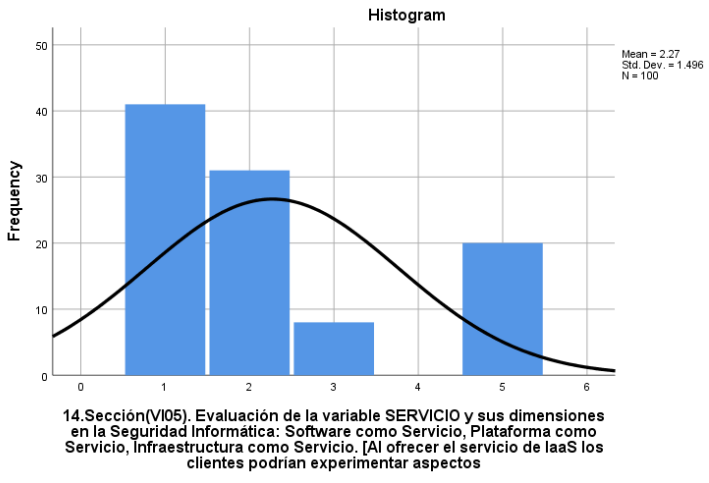
El coeficiente de Curtosis va a permitir identificar la existencia de una gran concentración de valores (Leptocúrtica), concentración normal de valores (Mesocúrtica) o una baja concentración de valores (Platicúrtica) lo cual muestra los valores de una variable que se encuentran alrededor de la zona céntrica de la distribución de frecuencias; este análisis es importante para las variables independientes que cuentan con mayor relevancia en el estudio.

3.2.4.2 Análisis de la variable independiente VI05

Tabla 3. 39

Análisis de la variable VI05

N	Valid	100
	Missing	0
Mean		2.27
Median		2.00
Mode		1
Std. Deviation		1.496
Variance		2.239
Skewness		1.001
Std. Error of Skewness		.241
Kurtosis		-.482
Std. Error of Kurtosis		.478



Fuente: Elaborado por autor

A continuación, observamos los siguientes resultados en la tabla 3.39:

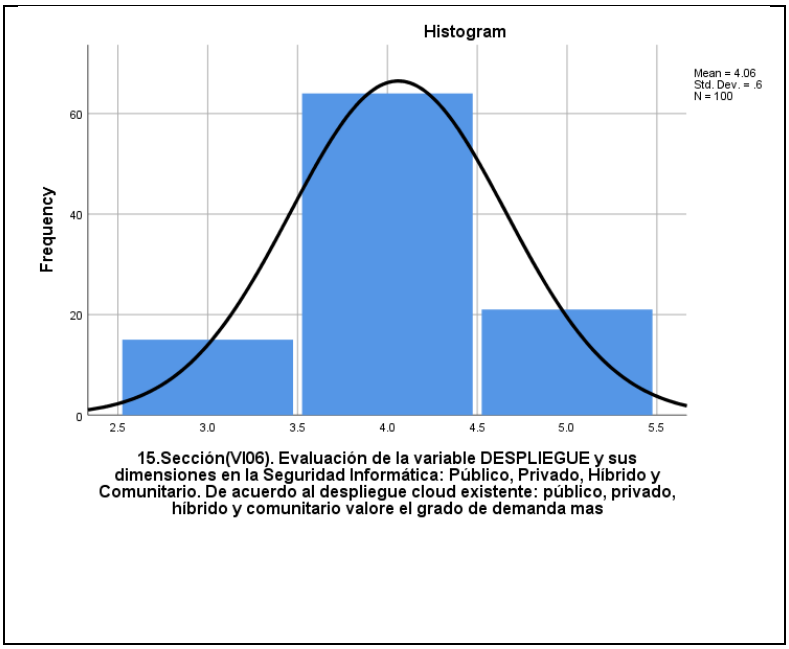
- **N. Válido:** Indica la cantidad de datos analizados (muestra) en el trabajo de investigación.
- **Asimetría:** El valor 1.001 indica que la variable independiente SERVICIO tiene una asimetría positiva.
- **Varianza:** El valor 2.239 indica una buena dispersión de los datos analizados.
- **Curtosis:** El valor -0.482 nos muestra una curva Platicúrtica lo que nos indica un menor porcentaje de datos concentrados entorno a la media.

3.2.4.3 Análisis de la variable independiente VI06

Tabla 3. 40

Análisis de la variable VI06

N	Valid	100
	Missing	0
Mean		4.06
Median		4.00
Mode		4
Std. Deviation		.600
Variance		.360
Skewness		-.021
Std. Error of Skewness		.241
Kurtosis		-.167
Std. Error of Kurtosis		.478



Fuente: Elaborado por autor

A continuación, observamos los siguientes resultados en la tabla 3.40:

- **N. Válido:** Indica la cantidad de datos analizados (muestra) en el trabajo de investigación.
- **Asimetría:** El valor -0.021 indica que la variable independiente DESPLIEGUE tiene una asimetría negativa encontrando su posición sobre la media aritmética.
- **Varianza:** El valor 0.360 indica una dispersión normal de los datos analizados.
- **Curtosis:** El valor -0.167 nos muestra una curva Platicúrtica lo que nos indica un menor porcentaje de datos concentrados entorno a la media.

3.2.5 Análisis Correlacional de las variables de investigación

3.2.5.1 Coeficiente de correlación de Pearson

El coeficiente de correlación de Pearson nos va ayudar a poder medir la fuerza y la dirección cuando se asocien dos variables cuantitativas aleatorias en conjunto con una distribución bivariada; es decir se buscará comprobar que cada una muestren una distribución normal univariada por sí solas. Los valores para el análisis de la correlación de Pearson van desde -1 siendo este un indicador que muestra menor correlación entre las variables, 1 muestra mayor

correlación entre las variables y finalmente 0 indicando que no existe correlación entre las variables.

Tabla 3. 41

Valores de Coeficiente de Correlación de Pearson

Valor	Significancia
0 y 0,2	Correlación Mínima
0,2 y 0,4	Correlación Baja
0,4 y 0,6	Correlación Moderada
0,6 y 0,8	Correlación Buena
0,8 y 1	Correlación muy Buena

Fuente: Elaborado por autor

3.2.5.2 Análisis correlacional de las variables Seguridad y Garantía

Tabla 3. 42

Asociación de coeficiente de correlación de Pearson de variables Seguridad y Garantía

Correlations

		Software Libre - Otras, como sofware de seguridad (p. e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	6.Sección (VI01). Evaluación de la variable GARANTÍA y sus dimensiones en la Seguridad Informática: Integridad, Confidencialidad y Disponibilidad. [Los roles asignados a usuarios se establecen como una medida de confidencialidad.]
Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	Pearson Correlation	1	.555*
	Sig. (2-tailed)		.021
	N	17	17
6.Sección(VI01). Evaluación de la variable GARANTÍA y sus dimensiones en la Seguridad Informática: Integridad, Confidencialidad y Disponibilidad. [Los roles asignados a usuarios se establecen como una medida de confidencialidad.]	Pearson Correlation	.555*	1
	Sig. (2-tailed)	.021	
	N	17	100

*. Correlation is significant at the 0.05 level (2-tailed).

Fuente: Elaborado por autor

El estadístico de Pearson mostrado en la tabla 3.42 muestra un valor resultante de significancia 0.555 lo cual de acuerdo a los valores de correlación indicados anteriormente se asigna una correlación moderada entre las variables

analizadas; es decir que existe una relación de seguridad en la asignación de un rol a los usuarios como medida de confidencialidad con el uso de un software.

3.2.5.3 Análisis correlacional de las variables Seguridad y Cumplimiento

Tabla 3. 43

Asociación de coeficiente de correlación de Pearson de variables Seguridad y Cumplimiento

Correlations

		Software Libre - Otras, como sofware de seguridad (p. e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	10.Sección (VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Debe existir por parte del cliente una auditoría de servicio y/o plataforma.]
Software Libre - Otras, como sofware de seguridad (p.e. Open SSL, SSH), plataformas de aprendizaje (Moodie)	Pearson Correlation	1	.658**
	Sig. (2-tailed)		.004
	N	17	17
10.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Debe existir por parte del cliente una auditoría de servicio y/o plataforma.]	Pearson Correlation	.658**	1
	Sig. (2-tailed)	.004	
	N	17	100

**. Correlation is significant at the 0.01 level (2-tailed).

Fuente: Elaborado por autor

El estadístico de Pearson en la tabla 3.43 muestra un valor resultante de significancia 0.658 lo cual de acuerdo a los valores de correlación indicados anteriormente se asigna una correlación buena entre las variables analizadas; es decir que existe una relación entre el cumplimiento de auditoria de servicios y/o plataformas existentes y softwares de seguridad.

3.2.5.4 Análisis correlacional de las variables Cumplimiento y Control de Acceso

Tabla 3. 44

Asociación de coeficiente de correlación de Pearson de variables Cumplimiento y Control de Acceso

Correlations

		10.Sección (VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Cumplir con las políticas y normas de seguridad.]	7.Sección (VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso. [Para los permisos o denegación de accesos a servicios, es necesario realizar una autenticación previa de usuario.]
10.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información. [Cumplir con las políticas y normas de seguridad.]	Pearson Correlation	1	.498**
	Sig. (2-tailed)		.000
	N	100	100
7.Sección(VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso. [Para los permisos o denegación de accesos a servicios, es necesario realizar una autenticación previa de usuario.]	Pearson Correlation	.498**	1
	Sig. (2-tailed)	.000	
	N	100	100

**. Correlation is significant at the 0.01 level (2-tailed).

Fuente: Elaborado por autor

El estadístico de Pearson en la tabla 3.43 muestra un valor resultante de significancia 0.498 lo cual de acuerdo a los valores de correlación indicados anteriormente se asigna una correlación moderada entre las variables analizadas; es decir que existe una relación entre el cumplimiento que debe existir con los controles para asegurar el entorno de la seguridad informática y las autenticaciones previas que se realizan.

3.3 Resultado del diseño y análisis del modelo sobre la muestra

Tabla 3. 45

Resultado de la aplicación 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
1	GARANTIA	1	INTEGRIDAD	Medidas aplicadas para asegurar la integridad de la información				2	
		2	CONFIDENCIALIDAD	Aplicación de roles para asegurar la privacidad de la información		4			
		3	DISPONIBILIDAD	Medición de tiempo de disponibilidad de un servicio	5				
	CONTROL DE ACCESO	4	AUTENTICACION	Medidas aplicadas como métodos de autenticación	5				
		5	CONTROL DE ACCESO	Ejecución de mecanismos para asegurar el control de acceso	5				
	CUMPLIMIENTO	6	REQUISITOS LEGALES Y CONTRACTUALES	Controles de requisitos Legales y Contractuales	5				
		7	REVISION DE LA SEGURIDAD DE LA INFORMACION	Controles de revisión de la Seguridad de la Información	5				
	GESTION DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO	8	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION	Planificación y definición de estrategias, plan de acción y notificaciones	5				
SEGURIDAD INFORMATICA		9	REDUNDANCIA	Disponibilidad de instalaciones para el procesamiento de la información	5				
	SERVICIO	10	SOFTWARE COMO SERVICIO	Tipos de software o servicio	5				
		11	PLATAFORMA COMO SERVICIO	Tipos de plataforma o servicio			3		
		12	INFRAESTRUCTURA COMO SERVICIO	Tipos de infraestructura o servicio			3		
	DESPLIEGUE	13	PUBLICO	Despliegue en nube Pública		4			
		14	PRIVADO	Despliegue en nube Privada				2	
		15	HIBRIDO	Despliegue en nube Híbrida					1
		16	COMUNITARIO	Despliegue en nube Comunitaria					1

Fuente: Elaborado por autor

A continuación, observamos el resultado de las 16 variables analizadas. Se observa que existen 10 indicadores los cuales se mantienen en niveles aceptables de la seguridad, por lo cual requieren una revisión los restantes indicadores que representan el 37% ya que no cumplen con las garantías de seguridad informática de acuerdo a los datos mostrados. Entre los indicadores que requieren atención inmediata que se encuentran en los rangos de nivel 3, 2 y 1 encontramos a integridad que es la variable que evalúa la no alteración de los datos que se encuentran en la nube, este indicador nos muestra un poco el temor de los usuarios de que su información sea alterada; continuando con la revisión de los resultados podemos observar que el despliegue público es el más usado por lo que se recomienda aplicar estrategias que puedan garantizar los servicios como plataforma e infraestructura que se encuentran en los despliegues privados, híbridos y comunitarios de acuerdo a las aplicaciones o equipos que utilicen. La adopción de la tecnología Cloud Computing es un proceso delicado que conlleva múltiples análisis, mostrando la importancia de la aplicación de las normas ISO en la tecnología Cloud Computing.

CONCLUSIONES

La relación de los modelos de seguridad informática que fueron fundamentados por el modelo de referencia de las normas ISO (ISO 27018, 2014) y por el modelo del Instituto Nacional de Normas y Tecnología NIST (NIST 500-292, y otros, 2011) fueron claves para poder cumplir con el objetivo planteado de la presente investigación. La evaluación del modelo planteado mediante las 16 variables escogidas fue realizado a través de pruebas estadísticas, análisis de campo y cálculos porcentuales para así poder establecer una escala de valor por cada dimensión planteada. El uso de la aplicación de escala permitió identificar cada una de las dimensiones que fue considerada influyente en el Cloud Computing y su entorno en la seguridad informática para poder cumplir con los objetivos planteados de la investigación.

Esta investigación logró analizar que existen debilidades en las que se debe trabajar para poder garantizar la seguridad informática al ofrecer esta tecnología; iniciamos este análisis con la variable GARANTÍA en función de la integridad, donde se obtuvo un valor de 2 puntos con una ponderación del 30% lo cual nos indica que está por debajo de la media en este campo, continuamos con la variable SERVICIO mostrándonos dos dimensiones con valores mínimos como lo son PLATAFORMA COMO SERVICIO seguido de INFRAESTRUCTURA COMO SERVICIO, el valor de estas variables fue de 3 puntos con un 37% y 41% respectivamente lo cual nos indica que son servicios que no son muy usados por los clientes por temor al riesgo que puedan presentar en las instalaciones de los proveedores.

Para la variable DESPLIEGUE la cual indica el tipo de implementación en la que se realizan los servicios y/o aplicaciones tenemos 3 dimensiones con puntuaciones bajas las cuales son PRIVADO con ponderación de 2 puntos lo cual nos indica un 36% de aceptación, el 36% de aceptación presentado en el despliegue PRIVADO nos muestra que existe aún una desconfianza de los clientes al usar la nube de los proveedores para alojar sus servicios y/o aplicaciones; y luego tenemos las dimensiones HÍBRIDO y COMUNITARIO con

ponderación de 1 punto respectivamente que nos indica el poco uso de la misma.

Se realizó también correlación de las variables GARANTÍA, CUMPLIMIENTO y CONTROL DE ACCESO las cuales permitieron determinar una correspondencia de los datos recopilados mostrando correlaciones buena y moderada respectivamente. Las variables seguridad y garantía mostraron una correlación moderada lo cual indica que existe una relación de seguridad en la asignación de un rol a los usuarios como medida de confidencialidad con el uso de un software, las variables seguridad y cumplimiento mostraron una correlación buena lo cual indica el cumplimiento de auditoria de servicios y/o plataformas existentes y softwares de seguridad; y finalmente las variables cumplimiento y control de acceso presentaron una correlación moderada analizando que existe una relación entre el cumplimiento que debe existir con los controles para asegurar el entorno de la seguridad informática y las autenticaciones previas que se realizan.

Las otras variables entre ellas CONTROL DE ACCESO, CUMPLIMIENTO, GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO obtuvieron valores muy buenos; lo cual da a entender que se está trabajando de mejor manera en este campo de la tecnología. La notificación de posibles incidentes presentados y la disponibilidad de instalaciones redundantes para el procesamiento de datos son puntos claves en los proveedores para ofrecer los servicios de Cloud Computing mostrando un 95% de aceptación, cabe indicar que también se consultó el medio más usado para realizar las notificaciones de incidentes en la cual lidera el correo electrónico seguido de las llamadas telefónicas y los mensajes de WhatsApp.

Concluyo que los riesgos informáticos se encuentran presentes en todos los entornos de tecnología y el Cloud Computing no es una excepción debido a las vulnerabilidades y amenazas existentes, de acuerdo a la escala de Likert se determina que existen debilidades que pueden influir en la seguridad de la información las cuales deben ser mejoradas.

RECOMENDACIONES

La implementación y uso de servicios, equipos y/o aplicaciones finales en un entorno Cloud Computing debe poder garantizar la seguridad de la información como prioridad en todos sus distintos factores por lo cual se recomienda a los proveedores que ofrecen este servicio en la ciudad de Guayaquil desarrollar más estrategias de seguridad a nivel de los servicios y despliegues.

Es necesario que exista una fuente oficial en la que se muestren los proveedores que ofrecen cloud computing con los diferentes servicios, despliegues, cumplimientos legales, gestión de incidencias como una base de datos pública para que así las empresas que desean optar por migrar a esta tecnología tengan un apoyo en cuanto a la toma de decisiones.

A medida va avanzando la tecnología van apareciendo nuevas aplicaciones y servicios con mejores prestaciones y de igual manera los riesgos y amenazas se potencializan por lo que se recomienda a las empresas que decidan adoptar esta tecnología elaboren lineamientos y políticas internas robustas para que eviten ser víctimas de divulgación de información y ataques informáticos.

Se recomienda promover más el despliegue de nube privado por parte de los proveedores estableciendo niveles altos de garantía y cumplimiento de acuerdo a las normas y leyes establecidas.

Las normas ISO fueron desarrolladas para garantizar el cumplimiento de las obligaciones legales como un código de buenas prácticas para los proveedores llamados y a su vez ofrece a los consumidores el derecho de auditar y verificar el cumplimiento de las mismas por lo que se recomienda a los proveedores y consumidores conocer los controles de las normas ISO para que los servicios a contratar y a recibir vayan de acuerdo a lo indicado en las normas.

Bibliografía

Abad, J. B. (2020). *Cloud Computing: Gestión de Eventos, Incidencias y Problemas.* Alcalá.

Aguilar, L. J. (2009). COMPUTACIÓN EN LA NUBE NOTAS PARA UNA ESTRATEGIA ESPAÑOLA EN CLOUD COMPUTING. *IEEE*. Obtenido de https://revista.ieee.es/article/view/406/706

Aguirre. (2006). *Libro Electrónico de Seguridad Informática y Criptografía.* Madrid.

Cañedo Andalia, R., Ramos Ochoa, R. E., & Guerrero Pupo, J. C. (2005). *La Informática, la Computación y la Ciencia de la Información: una alianza para el desarrollo.* La Habana: ISSN 1024-9435.

Carmen de Pablos, Lopez, J., Hermoso, S. M., & Medina, S. (2004). *Informática y Comunicaciones en la Empresa.* Madrid: ESIC EDITORIAL.

CSA. (2011). *Cloud Security Alliance*. Obtenido de http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Denning , P. J. (1971). *Third Generation Computer Systems.* ACM Computing Surverys.

ENISA. (2003). Obtenido de http://www.enisa.europa.eu/

González Hernández, L. F. (21 de Abril de 2016). *Aspectos de seguridad informática en la utilización de cloud computing.* Obtenido de https://repository.unad.edu.co/handle/10596/6173

Grance, P. M. (Sptember de 2011). *NIST.* Obtenido de National Institute of Standards and Technology: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

Grossman, R. L. (21 de Marzo de 2009). The Case for Cloud Computing. *IEEE*, *11*, 23-27. Obtenido de https://ieeexplore.ieee.org/abstract/document/4804045/authors#authors

Gutierrez, C. C. (1993). *Epistemología e Informática.* Obtenido de https://editorial.uned.ac.cr/book/U01999

Hernández, S. R., Fernández, C. C., & Baptista, L. P. (2010). *Metodología de la Investigación.* Mexico. Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

ISO 27002. (2013). Obtenido de https://www.iso.org/standard/54533.html

ISO 27018. (2014). Obtenido de https://www.iso.org/standard/61498.html

ISO 27017. (2015). Obtenido de https://www.iso.org/standard/43757.html

Jansen, W., & Grance, T. (Diciembre de 2011). *Guidelines on Security and Privacy in Public Cloud Computing.* Obtenido de NIST: https://csrc.nist.gov/publications/detail/sp/800-144/final

Lampson, B. W. (1974). *ACM SIGOPS Operating Systems Review.* Editorial ACM SIGOPS.

Landwehr, C. E. (1981). *Formal Models for Computer Security.* Washington: Naval Research Laboratory.

Lideres. (2012). Las empresas ecutorianas se proyectan a la nube. *Lideres*. Obtenido de https://www.revistalideres.ec/lideres/empresas-ecuatorianas-proyectan-nube.html

McCuber, J. (1991). *Assessing and Managing Security Risk in IT Systems.* NY: Taylor & Francis Group.

MINTEL. (2019). *Ministerio de Telecomunicaciones*. Obtenido de https://www.telecomunicaciones.gob.ec/

Nataly, T. A. (2020). *Implementación de un modelo de seguridad para mitigación de vulnerabilidades en ambiente de almacenamiento en la nube con base en las normaas ISO 27017 y 27018.* Chimborazo.

National Computer Security Center. (1987). *The Trusted Computer System Evaluation Criteria.* Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=o35NR7I_EQ8C&oi=fnd&pg=PR1&dq=TCSEC+(Trusted+Computer+System+Evaluati%C3%B3n+Criteria+)&ots=_Zr8W4ItEU&sig=H7nCrQrYcha_nZCERJrG1M2zJC4&redir_esc=y#v=onepage&q=TCSEC%20(Trusted%20Computer%20System%20Evaluati%C

NIST 500-292, Fang, L., Jin, T., Jian, M., Robert, B., John, M., . . . nist. (Septiembre de 2011). *NIST.* Obtenido de NIST 500-292: http://www.mofa-easj.dk/docs/cods/docs/NIST_Cloud_Computing_Reference_Architecture.pdf

PwC, C. M. (1 de 2 de 2013). *PWC.* Obtenido de https://www.pwc.com.ar/es/publicaciones-por-industria/assets/resultados-de-la-encuesta-global-de-seguridad-de-la-informacion-2014-final.pdf

Riley, S. (7 de April de 2016). *Gartner.* Obtenido de https://www.gartner.com/en/documents/3277620/staying-secure-in-the-cloud-is-a-shared-responsibility

Siegel, J., & Perdue, J. (24-27 de Julio de 2012). *Cloud Services Measures for Global Use: The Service Measurement Index (SMI).* Obtenido de https://ieeexplore.ieee.org/abstract/document/6311020

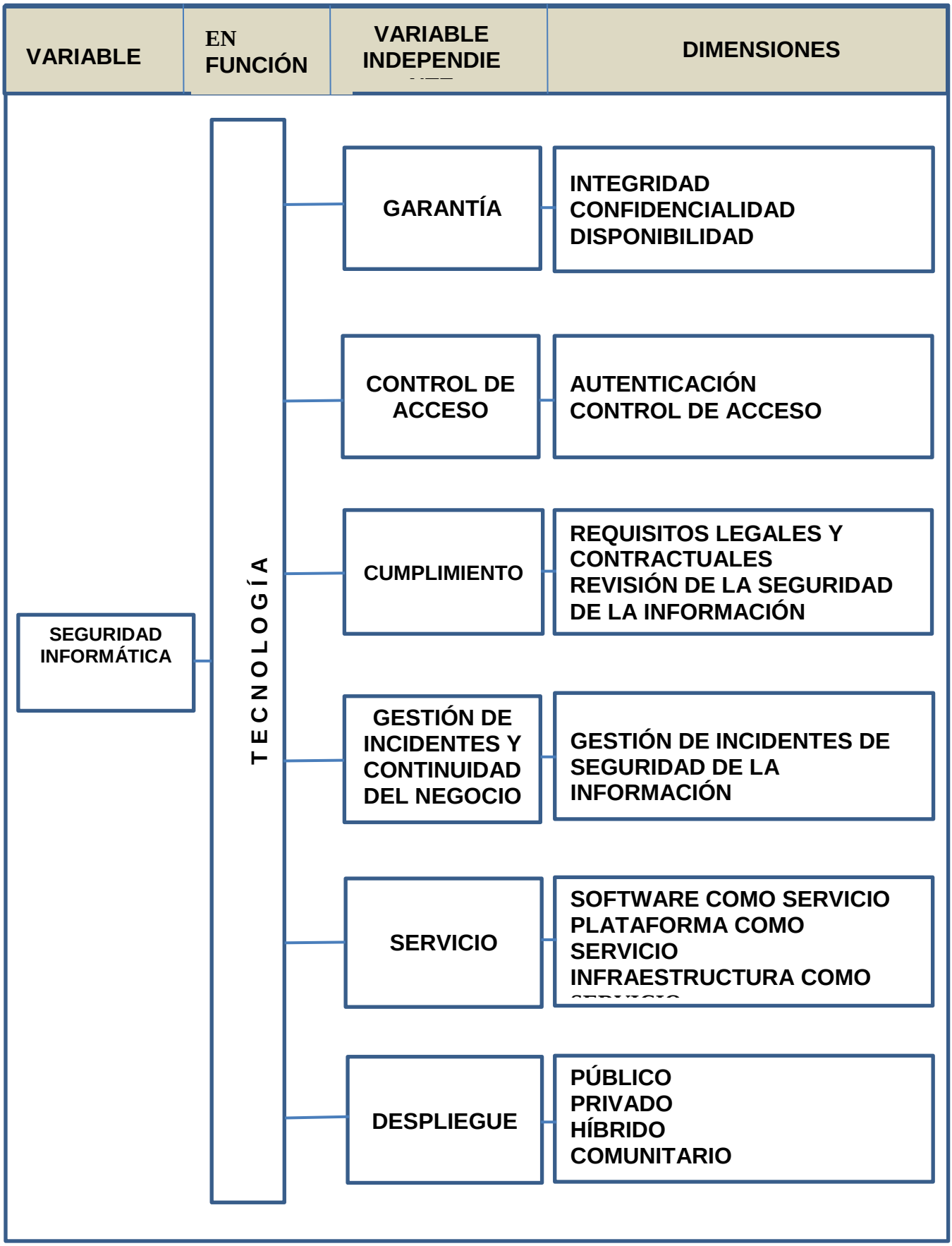
Superintendencia de Compañias, Valores y Seguros. (Diciembre de 2020). *Superintendencia de Compañias, Valores y Seguros*. Obtenido de https://www.supercias.gob.ec

Uptime Institute. (2017). *UPTIME INSTITUTE*. Obtenido de https://es.uptimeinstitute.com/

Vieites, Á. G. (2014). *ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA* (Segunda ed.). Madrid, España: RA-MA, S.A. Editorial y Publicaciones.

Whitman, M. E., & Mattord, H. J. (1992). *Principles of Informatión Security.* Boston.

Anexo1. Modelo conceptual aplicado a la investigación



Fuente: Datos de la investigación
Elaborado por: Autor

Anexo2. Antecedentes bibliográficos de las variables, dimensiones e indicadores

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	INDICADORES	ANTECEDENTES TEÓRICOS
SEGURIDAD INFORMÁTICA	GARANTÍA	1	INTEGRIDAD	Generación de permisos a usuarios	Lampson, B. W. (1974). ACM SIGOPS Operating Systems Review. Editorial ACM SIGOPS.
		2	CONFIDENCIALIDAD	Aplicación de roles a usuarios	Denning , P. J. (1971). Third Generation Computer Systems. ACM Computing Surverys.
		3	DISPONIBILIDAD	Medición de tiempo entre el inicio de una falla y recuperación	Whitman, M. E., & Mattord, H. J. (2014). Management of Information Security.
	CONTROL DE ACCESO	4	AUTENTICACIÓN	Implementación de métodos de autenticación	Vieites, Á. G. (2014). ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA (Segunda ed.). Madrid, España: RA-MA, S.A. Editorial y Publicaciones.
		5	CONTROL DE ACCESO	Ejecución de mecanismos para asegurar el control de acceso	Grance, P. M. (Sptember de 2011). NIST. Obtenido de National Institute of Standards and Technology
	CUMPLIMIENTO	6	REQUISITOS LEGALES Y CONTRACTUALES	Revisión de normas, leyes, estándares, etc.	CSA. (2017). Security Guidance for Critical Areas of Focus in Cloud Computing v.4. Cloud Security Alliance.
		7	REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Revisar y asegurar el cumplimiento	ISO 27001. (2013). ISO.
	GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO	8	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Planificación y definición de estrategias y plan de acción	CSA. (2011). Cloud Security Alliance.
		9	REDUNDANCIA	Pruebas de alta disponibilidad	Grossman, R. L. (21 de Marzo de 2009). The Case for Cloud Computing. IEEE, 11, 23-27
	SERVICIO	10	SOFTWARE COMO SERVICIO	Tenencia de servicio como software	ISO 27018. (2014)
		11	PLATAFORMA COMO SERVICIO	Tenencia de servicio como plataforma	ISACA. (2012). IT Control Objectives for Cloud Computing
		12	INFRAESTRUCTURA COMO SERVICIO	Tenencia de servicio como infraestructura	Jansen, W., & Grance, T. (Diciembre de 2011). Guidelines on Security and Privacy in Public Cloud Computing. Obtenido de NIST
	DESPLIEGUE	13	PÚBLICO	Recursos copartícipes	NIST 500-292, Fang, L., Jin, T., Jian, M., Robert, B., John, M., . . . nist.
		14	PRIVADO	Recursos arrendados	Cloud Special Interest Group PCI Security Standard. (Febrero de 2013). *PCI Security Standards Council.*
		15	HÍBRIDO	Componentes y elementos compartidos	Siegel, J., & Perdue, J. (24-27 de Julio de 2012). Cloud Services Measures for Global Use: The Service Measurement Index (SMI).
			COMUNITARIO	Recursos divididos	NIST 500-292, Fang, L., Jin, T., Jian, M., Robert, B., John, M., . . . nist.

Fuente: Datos de la investigación
Elaborado por: Autor

Anexo3. Matriz auxiliar de operación

FORMULACIÓN DEL PROBLEMA	GENERAL	VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	DIMENSIÓN	INDICADOR
¿De qué manera inciden la aplicabilidad de las Normas ISO en la Seguridad Informática para proteger los datos en el Cloud Computing de proveedores que ofrecen este servicio en la ciudad de Guayaquil?	Determinar cómo inciden las Normas ISO en la seguridad informática para la protección de datos de proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil.	SEGURIDAD INFORMÁTICA	GARANTÍA	INTEGRIDAD	Generación de permisos a usuarios
				CONFIDENCIALIDAD	Aplicación de roles a usuarios
				DISPONIBILIDAD	Medición de tiempo entre el inicio de una falla y recuperación
			CONTROL DE ACCESO	AUTENTICACIÓN	Implementación de métodos de autenticación
				CONTROL DE ACCESO	Ejecución de mecanismos para asegurar el control de acceso
SISTEMATIZACIÓN	**ESPECÍFICOS**		CUMPLIMIENTO	REQUISITOS LEGALES Y CONTRACTUALES	Revisión de normas, leyes, estándares, etc.
				REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Revisar y asegurar el cumplimiento
¿Existe la posibilidad de que se presenten fallas de los servicios y aplicaciones en el Cloud Computing? ¿Es fundamental asegurar la privacidad de la información de las organizaciones en todo momento? ¿Pueden existir accesos no autorizados a servicios y aplicaciones en el Cloud Computing? ¿Al almacenar datos en la nube, es posible que las organizaciones queden expuestas a ataques informáticos?	Analizar los modelos de Seguridad Informática existentes y su aplicabilidad en el Cloud Computing Identificar a partir del modelo de Normas ISO las incidencias, amenazas y vulnerabilidades. Determinar cuáles son los beneficios que tienen los proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil al aplicar correctamente las Normas ISO para la protección de datos.		GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Planificación y definición de estrategias, plan de acción y notificaciones
				REDUNDANCIA	Disponibilidad de instalaciones para el procesamiento de la información
			SERVICIO	SOFTWARE COMO SERVICIO	Tenencia de servicio como software
				PLATAFORMA COMO SERVICIO	Tenencia de servicio como plataforma
				INFRAESTRUCTURA COMO SERVICIO	Tenencia de servicio como infraestructura
			DESPLIEGUE	PÚBLICO	Recursos copartícipes
				PRIVADO	Recursos arrendados
				HÍBRIDO	Componentes y elementos compartidos
				COMÚNITARIO	Recursos divididos

Fuente: Datos de la investigación
Elaborado por: Autor

Anexo4. Variables de la investigación, operacionalización

VARIABLE DEPENDIENTE	VARIABLE INDEPENDIENTE	NO.	DIMENSIÓN	INDICADORES	NÚMERO DE VARIABLE INDEPENDIENTE	PREGUNTAS	TÉCNICAS	INSTRUMENTO	FUENTE	PROCESAMIENTO	TIPO DE INFORMACIÓN
SEGURIDAD INFORMÁTICA	GARANTÍA	**1**	INTEGRIDAD	Generación de permisos a usuarios	VI01	¿Qué medidas se aplican para asegurar la integridad de la información?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	Cuantitativa
		2	CONFIDENCIALIDAD	Aplicación de roles a usuarios		¿Qué medidas controlan los roles de usuarios para asegurar la confidencialidad?	Estadística	Base de datos	Secundaria	Instituto Nacional de Estadísticas y Censos	Cuantitativa
		3	DISPONIBILIDAD	Medición de tiempo entre el inicio de una falla y recuperación		¿Qué tan importante es la disponibilidad en los servicios de cloud computing?	Documental	Investigación bibliográfica	Secundaria	No aplica	Cualitativa
	CONTROL DE ACCESO	**4**	AUTENTICACIÓN	Implementación de métodos de autenticación	VI02	¿Qué medidas usa como método de autenticación?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		5	CONTROL DE ACCESO	Ejecución de mecanismos para asegurar el control de acceso		¿Qué procedimientos usa para el control de acceso?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
	CUMPLIMIENTO	**6**	REQUISITOS LEGALES Y CONTRACTUALES	Revisión de normas, leyes, estándares, etc.	VI03	¿Qué controles establecen para el cumplimiento de los requisitos legales y contractuales?	Documental	Investigación bibliográfica	Secundaria	No aplica	Cualitativa
		7	REVISIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Revisar y asegurar el cumplimiento		¿Qué controles establecen para el cumplimiento de la seguridad de la información?	Documental	Investigación bibliográfica	Secundaria	No aplica	Cualitativa
	GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO	**8**	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	Planificación y definición de estrategias, plan de acción y notificaciones	VI04	¿Se realizan notificaciones de eventos de seguridad y puntos débiles existentes?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa

SEGURIDAD INFORMÁTICA		**9**	REDUNDANCIA	Disponibilidad de instalaciones para el procesamiento de la información		¿Qué medidas usan para asegurar la continuidad de la seguridad de la información?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
	SERVICIO	10	SOFTWARE COMO SERVICIO	Tenencia de servicio como software	VI05	¿Qué servicios o aplicaciones son los más comunes en el software como servicio?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		11	PLATAFORMA COMO SERVICIO	Tenencia de servicio como plataforma		¿Qué servicios o aplicaciones son los más comunes en la plataforma como servicio?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		12	INFRAESTRUCTURA COMO SERVICIO	Tenencia de servicio como infraestructura		¿Qué servicios o aplicaciones son los más comunes en la infraestructura como servicio?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
	DESPLIEGUE	13	PÚBLICO	Recursos copartícipes	VI06	¿Cuán importante es el despliegue de la implementación de la nube pública?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		14	PRIVADO	Recursos arrendados		¿Cuán importante es el despliegue de la implementación de la nube privada?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
		15	HÍBRIDO	Componentes y elementos compartidos		¿Cuán importante es el despliegue de la implementación de la nube híbrida?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa
			COMUNITARIO	Recursos divididos		¿Cuán importante es el despliegue de la implementación de la nube comunitaria?	Recolección de campo	Encuesta	Primaria	No aplica	Cualitativa

Fuente: Datos de la investigación
Elaborado por: Autor

Anexo5. Listado de empresas registradas en la Superintendencia de Compañias, Valores y Seguros

NOMBRE	EXPEDIENTE	TIPO DE COMPAÑIA	ACTIVIDAD ECONÓMICA	TAMAÑO
CONSORCIO ECUATORIANO DE TELECOMUNICACIONES S.A. CONECEL	47845	ANÓNIMA	J6120.01	GRANDE
TELCONET S.A.	72951	ANÓNIMA	J6110.01	GRANDE
PUNTONET S.A.	48928	ANÓNIMA	J6190.04	GRANDE
CORPORACION NACIONAL DE TELECOMUNICACIONES CNT	161230	ANÓNIMA	J6010.02	GRANDE
COMUNICACIONES Y TELEFONIA MULTIPLES S.A. MULTICOM – TELEMOVIL	66196	ANÓNIMA	J6120.01	MEDIANA
OTECEL S.A.	47972	ANÓNIMA	J6120.01	GRANDE
TECHNOLOGY EQUINOCCIAL TECCIAL S.A.	102603	ANÓNIMA	J6202.10	MEDIANA
DATTA BUSINESS SOLUTIONS C.A.	316102	ANÓNIMA	J6202.10	GRANDE
MAINT S.A.	26340	RESPONSABILIDAD LIMITADA	C3312.91	GRANDE
COMPUTADORES Y EQUPOS COMPUEQUIP DOS S.A.	18185	ANÓNIMA	G4651.01	GRANDE
SUDAMERICANA DE SOFTWARE S.A. SASF	100887	ANÓNIMA	J6209.01	MEDIANA

Fuente: Datos de la investigación
Elaborado por: Autor

Anexo6. Formato de encuesta aplicada a empresas que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil.

ENCUESTA

Universidad Tecnológica Empresarial de Guayaquil - UTEG
Facultad de Estudios de Postgrado
Tesis para la obtención del título de Magister en Sistemas de Información Gerencial
Tema: "Incidencias de las Normas ISO en la Seguridad Informática para la protección de datos usada por proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil"

NOTA

A continuación se presentan un conjunto de ítems relacionados a la problemática de investigación:
GARANTÍA: Integridad, Confidencialidad, Disponibilidad
CONTROL DE ACCESO: Autenticación, Control de acceso
CUMPLIMIENTO: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información
GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO: Gestión de incidentes de Seguridad de la Información, Redundancia
SERVICIO: Software como Servicio, Plataforma como Servicio, Infraestructura como Servicio
DESPLIEGUE: Público, Privado, Híbrido, Comunitario

OBJETIVO

Determinar cómo inciden las Normas ISO en la seguridad informática para la protección de datos de proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil

DIRIGIDO A

Empresas que ofrecen Servicio de Cloud Computing en la ciudad de Guayaquil

TIEMPO APROXIMADO

10 a 15 minutos

CONSULTAS Y CONTACTO

Ing. Brayan Pinargote A.
celular: 0986382280
pinargotebryanj@gmail.com

1. 1.¿Qué cargo cumples en la empresa?

   Marca solo un óvalo.

   - Técnico
   - Ingeniero
   - Jefe
   - Gerente

2. 2.¿Qué tiempo llevas laborando en la empresa?

   Marca solo un óvalo.

   - Menor a 5 años
   - Entre 5 y 10 años
   - Entre 10 y 20 años
   - Mayor a 20 años

3. 3.La tecnología de Cloud Computing ofrece servicios a través de internet, lo que resulta una ventaja competitiva para las empresas en cuanto a reducción de costos y ofertas de mejores servicios a clientes.

   Marca solo un óvalo.

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

4. 4.¿Crees que existe un riesgo al almacenar datos de las empresas en la nube?

Marca solo un óvalo.

- ◯ No es riesgoso
- ◯ Existe un riesgo bajo
- ◯ Existe un riesgo medio
- ◯ Totalmente riesgoso

5. 5.Dentro de las dimensiones que ofrece el Cloud Computing a nivel de servicio, ¿cuál de los siguientes son los mas requeridos por los clientes?

Marca solo un óvalo.

- ◯ SaS (Software como Servicio)
- ◯ PaS (Plataforma como Servicio)
- ◯ IaS (Infraestructura como Servicio)

6. 6.Sección(VI01). Evaluación de la variable GARANTÍA y sus dimensiones en la Seguridad Informática: Integridad, Confidencialidad y Disponibilidad.

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 la base fundamental en la Seguridad Informática que nos garantiza la no alteración de la información.	◯	◯	◯	◯	◯
Los roles asignados a usuarios se establecen como una medida de confidencialidad.	◯	◯	◯	◯	◯
Se establecen mecanismos para calcular la disponibilidad de los servicios como el indicado en el manual de ITIL v3, el cual hace referencia a la Gestión de Niveles de Servicio y Gestión de la Disponibilidad.	◯	◯	◯	◯	◯

7. 7.Sección(VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso.

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
Se establecen mecanismos de autenticación como medida de seguridad de la información para los servicios brindados a los clientes.	◯	◯	◯	◯	◯
Para los permisos o denegación de accesos a servicios, es necesario realizar una autenticación previa de usuario.	◯	◯	◯	◯	◯

8. 8.Sección(VI02). Evaluación de la variable CONTROL DE ACCESO y sus dimensiones en la Seguridad Informática: Autenticación y Control de acceso. ¿Qué mecanismos de autenticación utilizan?

Marca solo un óvalo.

- ◯ Conexión VPN
- ◯ Conexión VPN two factor
- ◯ Control Biométrico
- ◯ Usuario y Clave
- ◯ Otros: _____

9. 9.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información.

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
Es necesario apoyarse en los lineamientos de los requisitos legales y contractuales relacionados a la contratación del servicio de Cloud Computing.	◯	◯	◯	◯	◯
Los contratos deben ser establecidos directamente con el proveedor de servicios, mas no con intermediarios.	◯	◯	◯	◯	◯
Cumplir con controles para asegurar el entorno de la seguridad informática.	◯	◯	◯	◯	◯
Identificar la legislación aplicable.	◯	◯	◯	◯	◯
Proteger los registros de la organización.	◯	◯	◯	◯	◯
Protección de datos y privacidad de información personal.	◯	◯	◯	◯	◯
Derechos de propiedad intelectual (DPI).	◯	◯	◯	◯	◯

10. 10.Sección(VI03). Evaluación de la variable CUMPLIMIENTO y sus dimensiones en la Seguridad Informática: Requisitos Legales y Contractuales, Revisión de la Seguridad de la Información.

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
Se debe establecer políticas y procedimientos internos que permitan realizar auditorías periódicas sobre la seguridad informática.	⬭	⬭	⬭	⬭	⬭
Cumplir con las políticas y normas de seguridad.	⬭	⬭	⬭	⬭	⬭
Debe existir por parte del cliente una auditoría de servicio y/o plataforma.	⬭	⬭	⬭	⬭	⬭
La empresa y los empleados deben tener una certificación para poder brindar y operar servicios de Cloud Computing.	⬭	⬭	⬭	⬭	⬭

11. 11.Sección(VI04). Evaluación de la variable GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO y sus dimensiones en la Seguridad Informática: Gestión de Incidentes de Seguridad de la Información , Redundancia.

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
Se establecen responsabilidades y procedimientos para asegurar la información, realizando notificaciones de eventos y posibles puntos débiles de seguridad.	⬭	⬭	⬭	⬭	⬭
Es importante planificar y ejecutar estrategias que protejan la seguridad de la información ante posibles fallas de elementos e instalaciones principales.	⬭	⬭	⬭	⬭	⬭

12. 12.Sección(VI04). Evaluación de la variable GESTIÓN DE INCIDENTES Y CONTINUIDAD DEL NEGOCIO y sus dimensiones en la Seguridad Informática: Gestión de Incidentes de Seguridad de la Información , Redundancia. ¿Qué medio utilizan para realizar notificaciones ante posibles incidentes?

Selecciona todas las opciones que correspondan.

- ☐ Llamada telefónica
- ☐ Correo Electrónico
- ☐ Mensaje de texto
- ☐ Mensaje de WhatsApp

Otros: ☐ _____

13. 13.Sección(VI04). Evaluación de la variable SERVICIO y sus dimensiones en la Seguridad Informática. De los siguientes servicios mencionados indicar cuáles son los que tienen más demanda por los clientes:

Selecciona todas las opciones que correspondan.

- [ ] Aplicaciones de Negocios
- [ ] Aplicaciones Ofimáticas
- [ ] Aplicaciones de Gestión: CRM, ERP
- [ ] Correo Electrónico: hotmail, gmail, outlook, etc
- [ ] Aplicaciones Web
- [ ] Base de Datos
- [ ] Lenguajes de Programación
- [ ] Antivirus

Otros: [ ] _____

14. 14.Sección(VI04). Evaluación de la variable SERVICIO y sus dimensiones en la Seguridad Informática: Software como Servicio, Plataforma como Servicio, Infraestructura como Servicio.

Marca solo un óvalo por fila.

	En total acuerdo	En acuerdo	Ni en acuerdo ni en desacuerdo	En desacuerdo	En total desacuerdo
El proveedor debe tener el control de las funciones y actualizaciones para garantizar que los servicios estén siempre activos y actualizados.	⬭	⬭	⬭	⬭	⬭
La administración de la insfraestructura debe ser realizada únicamente por el proveedor asi como el uso de herramientas y lenguajes de programación.	⬭	⬭	⬭	⬭	⬭
Al ofrecer el servicio de IaaS los clientes podrían experimentar aspectos negativos como: falta de control de recursos, dependencia y privacidad.	⬭	⬭	⬭	⬭	⬭

15. 15.Sección(VI04). Evaluación de la variable DESPLIEGUE y sus dimensiones en la Seguridad Informática: Público, Privado, Hibrido y Comunitario. De acuerdo al despliegue cloud existente: público, privado, hibrido y comunitario valore el grado de demanda mas utilizado por los clientes.

Marca solo un óvalo por fila.

	Muy Alto	Alto	Medio	Bajo	Muy Bajo
Acceso a servicios, aplicaciones y almacenamiento que se encuentran en una nube pública.	◯	◯	◯	◯	◯
Acceso a infraestructura, equipos o servicios que se encuentran en una nube privada.	◯	◯	◯	◯	◯
Accesos a servicios y datos de forma pública y privada.	◯	◯	◯	◯	◯
Recursos compartidos en la nube.	◯	◯	◯	◯	◯

16. 16.La Seguridad de la Información es responsabilidad únicamente del proveedor de servicio.

Marca solo un óvalo.

- ◯ En total acuerdo
- ◯ En acuerdo
- ◯ Ni en acuerdo ni es desacuerdo
- ◯ En desacuerdo
- ◯ En total desacuerdo
- ◯ Otros: _____

17. 17.¿Cómo consideras el avance del Cloud Computing en el Ecuador?

Marca solo un óvalo.

- Está avanzando rápidamente.
- Se encuentra en un proceso de transición normal.
- Está avanzando lentamente.
- La mayoría desconoce de la tecnología.

18. 18.¿Cuál es tu opinión sobre el tiempo que te tomó completar la encuesta?

Marca solo un óvalo.

- La encuesta fue demasiado larga.
- La encuesta estuvo dentro de los parámetros de tiempo adecuados.
- La encuesta estuvo demasiado corta.
- Irrelevante.

Fuente: Datos de la investigación
Elaborado por: Autor