República del Ecuador

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

Artículo Científico en Opción al título de Magister en:
Sistemas de Información Gerencial

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

Autor:
Ing. Evelin María Saltos Ramírez

Director de Artículo Científico:
PHD. José EnriqueTownsend Valencia, Msc.

Septiembre 2018

Guayaquil - Ecuador

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

Ing. Evelin María Saltos Ramírez

Candidata a Magister en Sistemas de Información Gerencial, Facultad de Posgrados, Universidad Tecnologica Empresarial de Guayaquil, Urdesa Central Guayacanes 520 y la 5ta, Guayaqui, Ecuador
evelinmsr@gmail.com

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

Se realiza la verificación de modelos fundamentados en las normas ISO, estándares y mecanismos de seguridad de la información e informática, se basa en el Estándar Cloud Security Alliance Cloud Controls Matrix, se analiza las variables intervinientes como la garantía, gobernanza, identidad y control de acceso, gestión de riesgos, servicio, despliegue, cumplimiento, producto del modelo definido para la seguridad informática y aplicabilidad de cloud computing.

El proceso de esta investigación es cualitativo y también cuantitativo por lo que se orienta a un tipo de estudio descriptivo y correlacional; se aplica los métodos inductivo, analítico, sintético; se utiliza además las técnicas estadísticas, documental y de campo para la recolección de información en las industrias de la ciudad de Manta Provincia de Manabí.

La población de estudio corresponde a las empresas del sector industrial de la ciudad de Manta, en función de los datos estadísticos obtenidos del Instituto Nacional de Estadísticas y Censo (INEC) y por la Superintendencia de Compañías del Ecuador.

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

Abstract: The present research work covers topics about the applicability of cloud computing, the way in which affects the security of the industrial sector of the city of Manta, examines the impact of these factors, contributing to the applicability of cloud computing using the appropriate model is security for cloud computing.

Is the verification of models based on ISO standards, standards and mechanisms of security of information and computer science, analyzes the intervening variables such as the warranty, governance, identity and access control, risk management, service, deployment, compliance, product of the model defined for computer security and applicability of cloud computing.

This research process is also quantitatively and qualitatively so it focuses on a type of descriptive and correlational study; apply inductive, analytic, synthetic methods, In addition the statistical techniques used documentary and field for the collection of information on the industries of the city of Manta province of Manabí.

The study population corresponds to the companies of the industrial sector of the city of Manta, according to the statistical data of the Statistics and census (INEC) and the Superintendency of Companies of Ecuador.

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

Introducción

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

La seguridad informática en el cloud es un servicio que ha crecido rápidamente y promete numerosas funciones que ofrece la seguridad de TI tradicional. En esto se incluye la protección de la información crítica frente al robo, la filtración de los datos y la eliminación de los mismos. Asimismo al optar por los servicios en la nube se puede operar a escala y tener protección. En la actualidad existe una similitud en el modo que se administra la seguridad, aunque existen formas adicionales de proporcionar soluciones de seguridad para otros aspectos preocupantes.

El problema de la investigación busca encontrar la respuesta a: ¿De qué manera que incide la aplicabilidad del cloud computing en la seguridad informática del sector industrial en la ciudad de Manta de la provincia de Manabí?, para ello se plantea las siguientes interrogantes que ayudarán a dar solución al problema de investigación: ¿ Es necesario que exista control de acceso a servicios y aplicaciones en el cloud computing?, ¿ Es indispensable para una organización la seguridad y privacidad de la información en todo momento?, ¿ Puede existir falla de los servicios y aplicaciones en el cloud computing?, ¿ Es posible ser víctimas de ataques informáticos debido a la divulgación de información confidencial?. La investigación tiene como objetivo determinar los factores que inciden en la seguridad informática y su aplicabilidad en el cloud computing, para las empresas del sector industrial de la ciudad de Manta en la Provincia de Manabí; los objetivos específicos son identificar los modelos de seguridad informática y analizar su aplicabilidad en el cloud computing, establecer a partir del modelo seleccionado los riesgos informáticos, amenazas y vulnerabilidades, evaluar los servicios que ofrece la tecnología del cloud computing para las empresas del sector industrial de la ciudad de Manta en la provincia de Manabí.

Esta investigación implica el análisis de los modelos de seguridad informática aplicables en el cloud computing para el sector industrial en la ciudad de Manta de la provincia de Manabí; ayudará a identificar el modelo apropiado identificando las teorías científicas sobre la seguridad informática y aplicabilidad en la tecnología cloud computing, y de esta manera responder a la pregunta de investigación planteada.

Marco Teórico

El control de la seguridad en la nube es aplicable a diversos niveles y recomendado de forma personalizada para los servicios que allí se ejecuten, definiendo claros protocolos de seguridad, controles y auditorias periódicas, capacitación adecuada al personal a cargo e innovación en tecnología, es el aporte de Robles C, Ramírez M. Rodríguez M., González M., Gayo R., (2014).

Modelos de Seguridad informática aplicables en el cloud computing

Un modelo de seguridad proporciona una representación científica acerca de las propiedades funcionales y estructurales de seguridad de un sistema de información. Para Aguilera (2010) define la seguridad informática como la disciplina que diseña normas, procedimientos, métodos y técnicas que están destinados a conseguir un sistema de información seguro y confiable.

Laudon y Laundon (2012) identifica seis tipos de sistemas de información, como los Sistemas para el Procesamiento de Transacciones, TPS, Sistemas del Trabajo del Conocimiento, KWS, Sistemas de Automatización de Oficinas, OAS, Sistemas de Información Gerencial, MIS, Sistemas de apoyo a la toma de decisiones, DSS, Sistemas de apoyo a Ejecutivos, ESS. Asimismo existen autores como De Pablos, López, Romo, Medina, Montero y Nájera (2006) agregan dos tipos de sistemas de información: Sistemas de Planificación de Recursos Empresariales, ERP, Sistemas Expertos (SE). En el cuadro 1.1 se detalla los autores más desatacados en los modelos teóricos de la seguridad informática.

Cuadro No. 1.1 PRINCIPALES MODELOS CONCEPTUALES DE LA SEGURIDAD INFORMÁTICA

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

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

Modelos formales para la seguridad informática de Landwher: Como indica Landwher (1981), los modelos imponen controles para cualquier operación en un sistema o aplicación. Este autor recopila varios modelos orientados a la seguridad como la protección contra observación, modificación no autorizada o inapropiada de la información procesada y la denegación de un servicio como el Modelo matriz de acceso, el Control de acceso basado en roles, el Modelo formal de confidencialidad Bell LaPadula, el Modelo formal de integridad Biba, el Modelo Clark-Wilson, el Modelo flujo de Información.

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

Para Whitman y Mattord (2014) define las dimensiones encontradas en el modelo apoyado en el análisis de Johnston (2004) que describe las principales características en tres dimensiones con sus atributos aplicables a cualquier entorno. Según Whitman y Mattord (2014) considera además como características de información críticas como Identificación y autenticación, Autorización, Confidencialidad y privacidad, Integridad, Auditoría, No repudio**.**

Modelo propuesto con base en el Estándar Cloud Security Alliance Cloud Controls Matrix (CSA CCM) (Matriz de controles en la nube): Está diseñado para proporcionar los principios de seguridad, guiar a proveedores y ayudar a clientes potenciales en la nube a evaluar el riesgo general de seguridad de un proveedor; CSA (2011) indica que tiene relación a otras normas de seguridad, reglamentos, y controla los marcos tales como la ISO 27001/27002, ISACA COBIT, PCI, NIST, entre otras. Se basa en 14 dominios de control según Cloud Security Alliance (2017) presentados en dos categorías como son gobierno y operaciones. En el cuadro 1.2 se presenta los dominios de gobierno, que abordan estrategias y políticas.

Cuadro No. 1.2 DOMINIOS DE GOBIERNO EN UN ENTORNO DE CLOUD COMPUTING

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

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

En el cuadro 1.3 se presenta los dominios operacionales, se centran en la seguridad de la información e implementación dentro de una arquitectura.

Cuadro No. 1.3 DOMINIOS OPERACIONALES EN UN ENTORNO DE CLOUD COMPUTING

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

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

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

Presenta elementos para obtener medidas en la privacidad y seguridad en la nube de parte de los proveedores (Jansen y Grance, 2011).

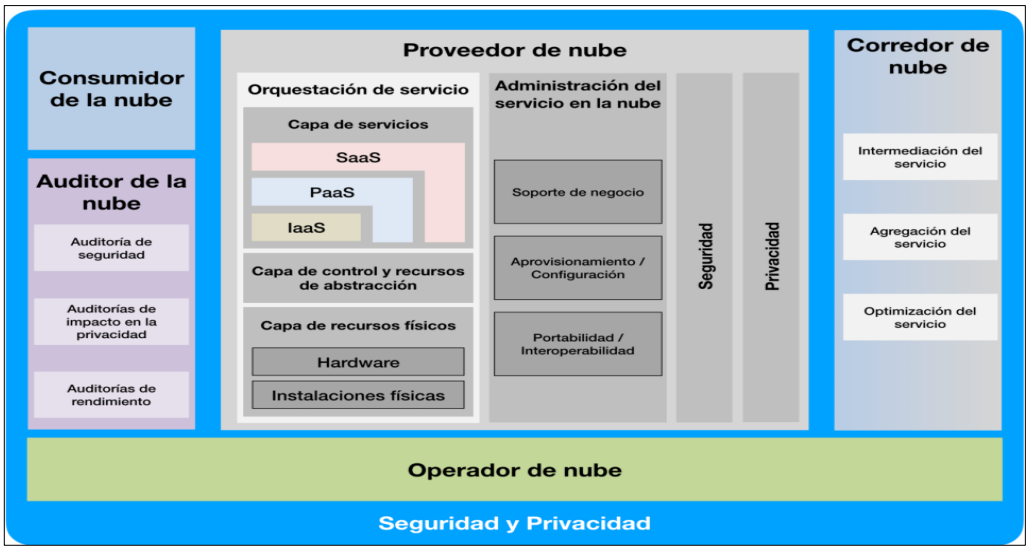
Cuadro No. 1.4 RECOMENDACIONES MODELO PROPUESTO NIST 800-144

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

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

En el cuadro 1.5 se presenta el marco de referencia conceptual propuesto por NIST 500-292 para el manejo de seguridades en el cloud computnig:

Cuadro No. 1.5 MODELO CONCEPTUAL DE REFERENCIA CLOUD COMPUTING NIST 500-292



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

Modelos de servicio

Software como servicio (SaaS): Para Liu, Tong, Mao, Bohn, Messina, Badger, y Leaf (2011) el consumidor utiliza pero no administra ni controla la infraestructura. Proporciona un entorno de trabajo independiente.
Platforma como sevicio (PaaS): El consumidor despliega en la infraestructura del proveedor aplicaciones creadas o adquiridas; tiene control sobre aplicaciones y de ser posible de configuraciones. (Liu et al., 2011)
Infraestructura como servicio (IaaS): El consumidor aprovisiona recursos de almacenamiento, procesamiento, redes y otros, puede desplegar y correr software, suele incluir sistemas operacionales y aplicaciones. (Liu et al., 2011)

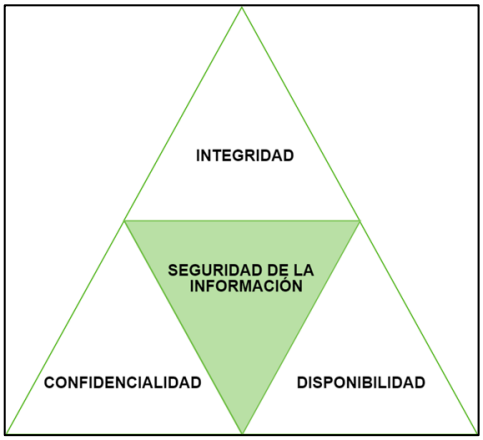
Modelos de despliegue

Nube privada: Administrada por una organización o por un tercero y puede existir dentro o fuera de la misma. (Liu et al., 2011)
Nube comunitaria: Compartida por varias organizaciones (Liu et al., 2011) aseguran que puede ser administrada por una organización o por un tercero y puede existir dentro o fuera de la misma.
Nube pública: Para el público o grupos de industrias, la infraestructura la provee una organización dedicada a vender servicios (Liu et al., 2011)
Nube híbrida: Se compone de dos o más nubes, (Liu et al., 2011) indica como entidades únicas, les permite compartir datos o aplicaciones.

Modelo basado en las Normas Técnicas ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional): Las normas ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización a nivel mundial. (ISO, 2013). A través del uso de las normas las

organizaciones pueden desarrollar e implementar un marco para la gestión de la seguridad de sus activos de información. Cabe mencionar que la seguridad de la información basada en las normas 27000 se fundamenta en la preservación de la confidencialidad, integridad y disponibilidad (medidas conocidas como CIA) como se observa en el cuadro 1.6, originalmente norma ISO 17799, además abarca términos que forman la base para un Sistema de Gestión de Seguridad de la Información.

Cuadro No. 1.6 SEGURIDAD DE LA INFORMACIÓN SEGÚN LA NORMA ISO/IEC 17799

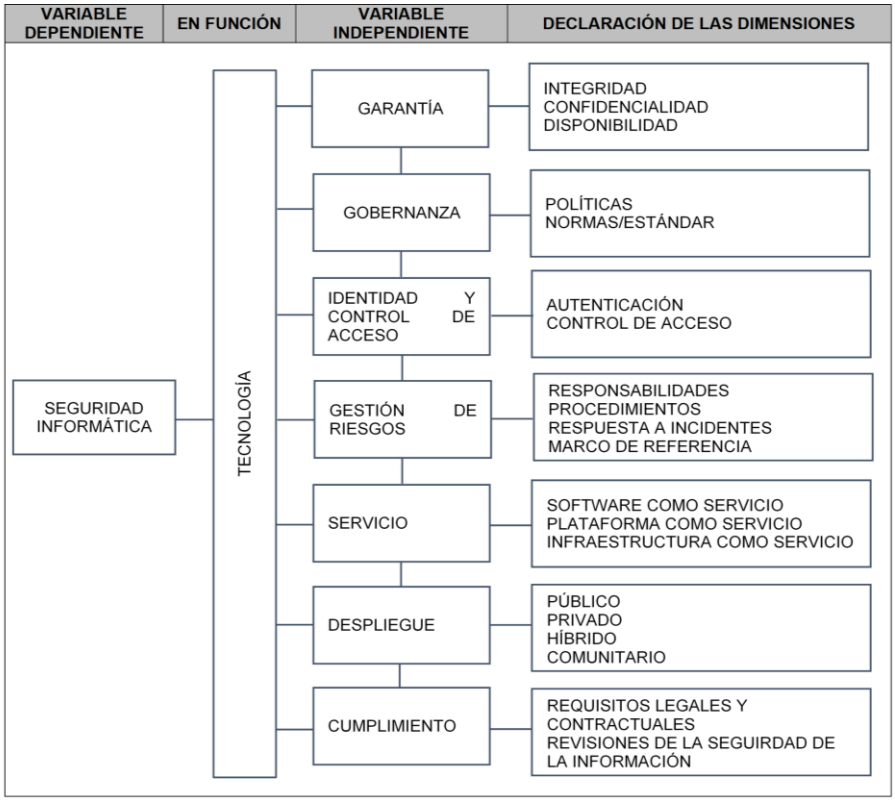


Fuente: Gómez, A. (2014). Enciclopedia de la Seguridad Informática, 2da Edición. Madrid: España. Editorial RA-MA.
Elaborado por: Autor

NORMA ISO / IEC 27001:2013: Según la Norma ISO 27001 (2013) específica los requisitos para establecer, implementar, mantener y mejorar consecutivamente un sistema de gestión de seguridad de la información. Contiene requisitos de evaluación y tratamiento de los riesgos de seguridad, una certificación ISO demuestra que cumple con todos los requisitos de la norma ISO 27001 (2013) o con un subconjunto específico de los controles.
NORMA ISO / IEC 27002:2013: Para la Norma ISO 27002 (2013) especifica directrices para los estándares y prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el medio ambiente. Consta de un anexo que incluye una guía con 14 dominios y 37 controles mapeados y enfocados a estos entornos.
NORMA ISO / IEC 27017:2015: Según la Norma ISO 27017 (2015) proporciona directrices que fomentan la aplicación de controles apropiados, dependen de una evaluación de riesgos y todos los requisitos de seguridad de información, legal, contractual, regulatorias u otras del sector nube.
NORMA ISO / IEC 27018:2014: Según Norma ISO 27018 (2014) define controles y directrices para la implementación de las medidas de protección de información de identificación personal (PII), según los principios de privacidad. También incluye directrices basadas en la norma ISO 27002.

Diagrama del modelo de evaluación propuesto
El cuadro No. 1.7 presenta el modelo conceptual de seguridad informática basado en diferentes teorías, normas y modelos investigados, considerando como instrumento científico al modelo del Instituto Nacional de Normas y Tecnología, NIST junto con el marco de referencia del Cloud Security Alliance que destaca las dimensiones del modelo del cloud computing.

Cuadro No. 1.7 MODELO DE LA SEGURIDAD INFORMÁTICA Y SU APLICABILIDAD TECNOLOGÍA CLOUD COMPUTING



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

Garantía: Todo proceso dentro de los servicios del cloud computing se mantengan protegidos, mediante la medición la Integridad para garantizar que la información no sea alterada en el contenido. La Confidencialidad para asegurar control de accesos a la información y la Disponibilidad para garantizar el alcance de forma oportuna y precisa, considerando fallos temporales, prolongados y permanentes, denegación de servicio, valor concentrado.
Gobernanza: Control y supervisión de políticas de seguridad, procedimientos y estándares para desarrollar aplicaciones.
Identidad y control de acceso: Métodos de autenticación para la identificación de usuarios y mecanismos para el control de accesos.
Gestión de riesgos: Medir y valorar los riesgos en la empresa, procedimientos para el monitoreo continuo del estado de seguridad de la información.
Servicio: Hace referencia al software, plataforma e infraestructura entregadas al consumidor como un servicio.
Despliegue: Modelo de implementación para la ejecución de un servicio, nube pública a disposición general o industria en que una organización es propietaria de la venta de servicios. Nube privada tiene un servicio de propiedad o de alquiler por una empresa. Nube híbrida combina las características de las nubes públicas y privadas. Nube comunitaria es compartida por organizaciones sobre requisitos de seguridad, políticas y cumplimiento legales.
Cumplimiento: Medir el grado de cumplimiento de estándares, normas o leyes.

Marco Metodológico

El proceso de esta investigación es cualitativo y también cuantitativo por lo que se orienta a un tipo de estudio descriptivo por la información independiente de conceptos o variables, permitiendo reflejar la situación real midiendo conceptos con sus componentes y correlacional por la relación o grado de asociación entre dos o más conceptos, categorías o variables en un contexto en particular.

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

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

Esta investigación empleó hechos registrados en el 2015, 2016 y 2017 en la seguridad informática de las grandes y medianas empresas del sector industrial de la ciudad de Manta. También se empleó el método de la medición debido a que se obtuvo información numérica y estadística del objeto de estudio de bases de datos para obtener conclusiones con un sustento más concreto.

Unidad de análisis, población y muestra

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

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

que el 45% de empresas utilizan el servicio de internet, el 23,6% correspondientes al sector de manufactura CIIU 10 ha realizado inversión en Tecnología, éstos datos conllevan a interrogantes sobre el manejo de seguridad informática debido a la inversión y ayudan a determinar los factores del objeto de estudio identificando el software de facturación como sistema de información aplicable a la tecnología cloud computing, utilizado en empresas del sector industrial manufacturero grande y mediana empresa, actividad económica C10 de la ciudad de Manta. Se realizó la revisión de información lo que permitió analizar las dimensiones de la seguridad informática.

Fuentes y técnicas e instrumentos para la recolección de información

Al ser una investigación tipo documental se utilizó fuentes primaria y secundaria de organismos gubernamentales y no gubernamentales afines a la información. Las Fuentes primarias se identificó la información procedente de revisión de informes emitidos por el INEC desde el 2010 al 2016, información de la Cámara de Industrias y Cámara de Comercio Manta, datos Superintendencia de Compañías, Valores y Seguros del Ecuador y modelos de seguridad Las Fuentes secundarias mediante información estadística y documental de otras fuentes de información, información de artículos científicos y revistas oficiales, página web del Instituto Nacional de Estándares y Tecnología (NIST), informes de estándares ISO, publicaciones de tesis de investigación científica revisión literaria sobre el tema.

Técnicas para la recolección de información.

Técnica de investigación estadística: Se consideró esta técnica de investigación para poder extraer información del fenómeno de estudio, a través de base de datos públicos de diferentes organismos gubernamentales y no gubernamentales involucrados con la información; para levantar información de los indicadores fijados en el estudio.
Técnica de investigación documental: Se consideró esta técnica de investigación para poder recopilar información relacionada al tema de investigación y de todas las fuentes disponibles, tesis, revistas, páginas web, libros, informes técnicos, artículos científicos y toda aquella fuente válida, de las variables garantía, gobernanza, identidad y control de acceso, gestión de riesgos, servicio, despliegue, cumplimiento.
Técnica de investigación de campo: Esta investigación recolectó información del objeto de estudio mediante el instrumento de encuesta sobre la aplicabilidad de la tecnología cloud computing en la seguridad informática. En el anexo 4 constan las columnas “técnica”, “instrumento”, “fuente de información” con la clasificación en la investigación de cada variable.

Escala aplicada para la evaluación de las variables: Se empleó la escala de Likert para medir y registrar cada uno de los indicadores asociados a la investigación. Esta escala posee un conjunto de ítems figuradas en proposiciones positivas, de hechos o fenómenos sociales o naturales, comportamientos individuales y colectivos de instituciones o personas, en donde la muestra sometida a observación expresa su opinión o actitud. Cada

ítem tiene grados de respuestas que van de lo más favorable a lo menos favorable y obtener de la muestra, resultados de forma objetiva y precisa.

Cuadro No. 1.8 ESCALA DE LIKERT PARA LA MEDICIÓN DE LA SEGURIDAD INFORMÁTICA Y APLICABILIDAD EN EL CLOUD COMPUTING

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

Fuente: Marco teórico de la investigación
Elaborado por. Autor

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

Resultados

Correlación de las variables cualitativas: Se estable la asociación aplicando tablas de contingencia para variables cualitativas inversión en tecnología y el uso de algún tipo de software de seguridad.

Cuadro No. 1.9 NIVEL DE ASOCIACIÓN ENTRE VARIABLES

tic17_firma_digital*tic135_seguridad tabulación cruzada

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

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

El cuadro 1.9 determina el grado de asociación lineal, estableciendo la relación entre la integridad con la firma digital y algún tipo de software de seguridad.

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

Cuadro No. 1.10 PRUEBA DE CHI CUADRADO SOBRE DATOS CUALITATIVOS

Pruebas de chi-cuadrado

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

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

b. Sólo se ha calculado para una tabla 2x2

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

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

Cuadro No. 1.11 NIVEL DE ASOCIACIÓN COEFICIENTE DE CONTINGENCIA

Medidas simétricas

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

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

En el cuadro 1.11 se observa una asociación débil debido al valor resultante 0,267 que se encuentra en la zona de aceptación entre la integridad con la firma digital y algún tipo de software de seguridad.

COEFICIENTE DE CRAMER.- Mide el nivel de asociación de variables nominales o cualitativas cuando sus categorías son de dos o tres clases. El valor varía entre 0 y 1. En el cuadro 1.12 se observa una asociación relativamente débil y la independencia de las variables.

Cuadro No. 1.12 NIVEL DE ASOCIACIÓN COEFICIENTE DE CRAMER

Medidas simétricas

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

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

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

Resultado de la aplicación del modelo sobre la muestra.

Cuadro No. 1.13 RESULTADO DE LA INVESTIGACIÓN

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

Fuente: Datos de la investigación
Elaborado por: Autor

En el cuadro 1.13 se presenta el resultado de la ponderación de la escala de Likert sobre las 20 variables con las respectivas dimensiones. Se observa que 12 indicadores se encuentran en los niveles de aceptación de la seguridad y el resto de los indicadores representa el 35% requieren de atención adyacente por no cumplir con las garantías de la seguridad informática en los sistemas de gestión de facturación electrónica aplicable a la tecnología cloud computing.

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

Conclusiones

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

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

informática y aplicabilidad en la tecnología cloud computing cumpliendo con los objetivos de la investigación.

Dimensiones como factores que inciden en la seguridad informática y su aplicabilidad en el cloud computing, para las empresas del sector industrial Integridad (53,3 %), Confidencialidad (60 %), Plataforma como servicio (20 %). Infraestructura como servicio (22,2 %), Público (53,3 %), Privado (60 %), Comunitario (46,7 %). Además se determinó la correlación de las variables observando la correspondencia de los datos recopilados, tomando para efecto del análisis las dimensiones integridad y control de acceso mediante pruebas estadísticas de tablas de contingencia, chi cuadrado, coeficiente de contingencia (karl pearson) y coeficiente de cramer, en el cual se midió el grado de asociación lineal.

Se estableció que dentro de los entornos de TI como lo es la aplicabilidad del cloud computing y los sistemas de información, están presente los riesgos informáticos debido a las vulnerabilidades y amenazas, mediante el análisis de las variables y dimensiones según la escala de Likert.

Recomendaciones

Las iniciativas de adopción o migración de la infraestructura de TI a la tecnología cloud computing debe garantizar la seguridad de la información por lo que se sugiere realizar con optimización y así lograr familiarizarse con el paradigma tecnológico del cloud.

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

Este trabajo de investigación servirá de aporte en futuras investigaciones considerando aspectos en los factores encontrados, considerando la necesidad de controles de accesos a servicios y aplicaciones en el cloud computing. Es recomendable que la organización que adapte un modelo de seguridad informática tenga como base y principio en las políticas internas asegurar la privacidad de la información como el activo valioso de la misma.

A medida que aparecen nuevas aplicaciones o servicios será necesario la gestión y manejo de riesgos para contrarrestar y mitigar posibles fallos en el funcionamiento y aplicabilidad del cloud computing. Es necesario que las empresas definan lineamientos y políticas internas fuertes para evitar ser víctimas de ataques informáticos debido a la divulgación de información confidencial en el manejo de la tecnología cloud computing.

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

Bibliografía

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mieres, J. (2009). Ataques Informáticos Debilidades de seguridad comúnmente explotadas. Recuperado de: https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

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

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

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

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

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

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

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

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

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

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

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

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