ESCUELA DE INGENIERÍA EN SISTEMAS

Tema:

GUÍA DE IMPLEMENTACIÓN DE NORMAS DE AUTENTICACIÓN Y SEGURIDAD EN ENTORNOS CLOUD COMPUTING PARA PYMES.

Proyecto de investigación previo a la obtención del título de Ingeniero de Sistemas y Computación

Línea de Investigación:

SISTEMAS DE INFORMACIÓN Y/O NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN Y SUS APLICACIONES

Autor:

HOLGUER DARIO HARO CRIOLLO

Director:

ING. GALO MAURICIO LÓPEZ SEVILLA MG.

Ambato – Ecuador

Diciembre 2021

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

GUÍA DE IMPLEMENTACIÓN DE NORMAS DE AUTENTICACIÓN Y SEGURIDAD EN ENTORNOS CLOUD COMPUTING PARA PYMES

Línea de Investigación:

Sistemas de Información y/o Nuevas Tecnologías de la Información y Comunicación y sus aplicaciones

Autor:

HOLGUER DARIO HARO CRIOLLO

Galo Mauricio López Sevilla, Ing. Mg. f_____
CALIFICADOR

Liliana del Roció Mena Hernández, Ing. Mg. f_____
CALIFICADOR

Enrique Xavier Garces Freire, Ing. Mg. f_____
CALIFICADOR

Santiago Alejandro Acurio Maldonado, Ing. Mg. f_____
DIRECTOR ESCUELA DE SISTEMAS

Hugo Rogelio Altamirano Villaroel, Dr. f_____
SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Diciembre 2021

DECLARACIÓN Y AUTORIZACIÓN

Yo: HOLGUER DARIO HARO CRIOLLO, con CC.180474654-, autora del trabajo de graduación intitulado: "GUÍA DE IMPLEMENTACIÓN DE NORMAS DE AUTENTICACIÓN Y SEGURIDAD EN ENTORNOS CLOUD COMPUTING PARA PYMES", previa a la obtención del título profesional de **INGENIERO DE SISTEMAS Y COMPUTACIÓN**, en la escuela de **INGENIERÍA EN SISTEMAS**.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad

Ambato, octubre 2021

HOLGUER DARIO HRO CRIOLLO

CC. 180474654-1

AGRADECIMIENTO

A mis padres quienes me forjaron e inculcaron valores los, cuales, hoy me hacen la persona que soy; muchos de los logros se lo debo a ustedes, el más importante darme mis estudios. Como dice mi madre la mejor herencia que te puedo dar es el estudio.

De igual manera a mis hermanos los, cuales, me apoyaron cada vez que lo necesitaba, me daban ánimos para terminar y cumplir mis anhelos, el más importante mi sueño, culminar mi carrera universitaria.

DEDICATORIA

A mi abuelita, mamá Rosita quien me vio crecer, con quien pase toda mi vida la, cual, me enseño desde hacer un café, hasta cocer. Te dedico este logro mamá Rosita, que no daría por tenerte en aquí junto a mí, pero el destino es cruel y me dejaste, pero siempre te llevare en mi corazón, siempre vivirás ahí, hasta el último día de mi vida, este logro es gracias a ti.

Para ti Mamá Rosita.

RESUMEN

El presente trabajo de investigación tiene como objetivo desarrollar una Guía de implementación de normas de autenticación y seguridad en entornos *Cloud Computing* para PYMES. A través de las diferentes técnicas de investigación como analítico – sintético el, cual, permitió el estudio de los subcriterios que contempla la academia, así también las encuestas para identificar problemas al momento del manejo y recolección de información de importancia para la empresa. Se determina, que se utilizará *cloud computing* y sus diferentes servicios a mejor convenir a la empresa. Se utilizó y modifico la metodología cascada para la realización de la guía, las fases fueron de gran importancia, de estas dependió el éxito del proyecto, se obtuvo como resultado diferentes módulos: seguridad de la red, seguridad en entornos *cloud*, protección de datos en entornos *cloud*, *backup* y recuperación de datos, recomendaciones de uso y mantenimiento, finalmente términos y definiciones. El producto final fue validado a través de una evaluación general de las PYMES que permitió la contestación a las preguntas básicas del planteamiento del problema, un cuadro comparativo con los indicadores de la ISO/ IEC 27017 y los indicadores de la guía, el mismo que demostró que cumplió 5 de los 7 indicadores de la norma ISO/IEC 27017 y final mente por la técnica de IADOV la, cual, permitió valorar la satisfacción de los usuarios con la guía.

Palabras Clave: *Cloud computing, backup,* autenticación, normas, implementación y PYMES.

ABSTRACT

This present research aims to develop a Guide for the implementation of authentication and security standards in Cloud Computing environments for SMEs. Through the different research techniques such as analytical - synthetic, which resulted in the study of the sub- criteria contemplated by the academy, as well as surveys to identify problems in the management and collection of information in the company. It is determined that cloud computing and its different services can be used in the company. The cascade methodology was used and modified for the designed of the guide and the steps were of great importance for the success of the project. Different modules were obtained as a result: network security, security in cloud environments, protection of data in cloud environments, data backup and recovery, recommendations for use and maintenance, finally terms and definitions. The final product was valuable through a general evaluation of SMEs to obtain the answer to the basic questions of the problem statement, a comparative table with the indicators of ISO / IEC 27017 and the indicators of the guide, the same that demonstrated the reach of 5 from the 7 indicators of the ISO / IEC 27017 standard and finally by the IADOVtechnique, which provides the user satisfaction with the guide.

Keywords: Cloud computing, backup, authentication, standards, implementation and SMEs

Holguer Dario Haro Criollo
EIS-1286

ÍNDICE GENERAL DE CONTENIDOS

PRELIMINARES

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

En los Antecedentes del uso de *Cloud Computing* las PYMES (Pequeñas y Medianas Empresas) tienen acceso a una gran variedad de servicios para cubrir las necesidades, no es necesario hacer grandes inversiones en *hardware* y *software* por lo que la nube tiene todos estos beneficios y están listos para ponerse en marcha, de tal manera que ayuda a la empresa a logar una eficacia en todos sus procedimientos.

También se contempla que el uso de Cloud Computing es una alternativa para las pequeñas y medianas empresas debido a la escalabilidad y flexibilidad que esta brinda en el uso de los recursos, además, otorga la facilidad de poder usarlos si es preciso, de manera que los servicios estarán siempre en línea en todo momento (Orantes Jiménez, Aguillón Martínez, & Vázquez Álvarez, 2015).

Cloud Computing es una guía conveniente y bajo demanda de un grupo de recursos que son configurables, además, tiene la capacidad de brindar agilidad, disponibilidad y escalabilidad de tal manera que llegará a reducir costos para aquellas empresas que empiezan y desean estar totalmente actualizados en la tecnología y sus diferentes beneficios.

Cloud Security Alliance cuenta con las definiciones basadas en los trabajos publicados por los científicos del *National Institute of Standards and Technology* (en adelante NIST) y sus esfuerzos en torno a la definición del *Cloud Computing*.

Según lo mencionado anteriormente por (*CLOUD SECURITY ALLIANCE*, 2009), se dice que existen guías para la implementación de normas de seguridad en entornos *cloud*, por lo cual, este proyecto tendrá validez en cuantos a un nuevo modelo de ejecución de nuevas normas adaptadas a las necesidades de las pequeñas y medianas empresas.

La adoptación de servicios en la nube para sustentar servicios TIC, introduce varias ventajas, que se ha especificado anteriormente en la incorporación de nuevos recursos, sin embargo, la misma adquisición de nuevos recursos conllevan con nuevos riesgos que es imprescindible controlar que garantice los requisitos exigibles por la protección de datos personales, así como los requerimientos de seguridad de las organizaciones establezcan como necesarias. (Ministerio de hacienda y administraciones públicas, 2014).

(Ministerio de Tecnologías de la Información y las Comunicaciones, 2016), indica los debidos lineamentos y aspectos a tener en cuenta para el aseguramiento de la información de la nube que las entidades del estado llevarán a cabo, con el objetivo de mantener las seguridad de datos, se toma en cuenta lo citado es importante mantener la seguridad de los clientes al asumir que den su información con el fin de obtener un servicio por él, cual, pago además, las pequeñas y medianas empresas que desean llevar la información correctamente adquirirán equipos tecnológicos por tanto se comprometerán con los clientes que los datos entregados, no se use para sobornar a la empresa o a las usuarios.

El (Centro Criptológico Nacional, 2017), afirma que es necesario llevar de una manera adecuada los datos, que se entrega a las entidades por lo, cual, la cita da pautas, que se seguirán para evitar el robo de información, los pasos a seguir son: políticas de seguridad, normativa de seguridad, procedimientos operativos de seguridad y proceso de autorización. Al saber los pasos mencionados anteriormente la idea de ciertas normas que son posibles de aplicar a las PYMES se toma en cuenta la necesidad.

La implementación de *Cloud Computing* en PYMES beneficiará en el transcurso del tiempo y a su vez brindará la debida seguridad, por lo tanto, el costo

beneficio de poner en funcionamiento la tecnológica de Cloud Computing se podrá realizar la guía de implementación de normas de autenticación y seguridad en entornos *Cloud* para PYMES, que se procederá en el tema de investigación (Lovato, 2015).

El ambiente *Cloud Computing* y la disponibilidad de información, se tiene en cuenta los criterios para garantizar los servicios y la operatividad, brindará la ayuda para aplicar un tipo de *Cloud Computing* y de esta manera aplicar a las pequeñas y medianas empresas de tal manera que cubra los servicios y la operatividad exigida por la empresa (Toro Sánchez, Murcia Prieto, & Hernández Vega, 2014).

La gran importancia de Cloud Computing a nivel mundial, diversas organizaciones han puestos esfuerzos por el estudio y análisis de los tipos de servicios, arquitectura y las tecnologías que hoy en día se extinguen a gran medida por lo, cual, el campo de seguridad, no se dejará de lado por lo, cual, es necesario tener en cuenta todos los riesgos que a presentarse y de una manera poder mitigarlos, en este caso de investigación se aplica normas de autenticación y seguridad (Salazar, 2013).

La situación de las PYMES y necesidades principales del uso de *Cloud Computing* lleva a realizar una indagación de la información necesaria para sustentar las necesidades de las pequeñas y medianas empresas, y por ende inquirir en las normas que cumplirá las PYMES para implementar *Cloud* (Rodríguez, 2016).

Problema

Descripción del problema

Cloud Computing es una tecnología que ayuda a tener toda la información en el

internet y esta toma un gran protagonismo hoy en día en las grandes empresas, sin embargo, las pequeñas y medianas empresas no implementan ya que las normas de autenticación y seguridad existentes aplican a grandes empresas.

Como una de las causas de este problema se tiene que el auge de las aplicaciones de Cloud Computing es reciente en PYMES, en efecto las PYMES no implementan *Cloud Computing,* las normas de seguridad y autenticación tiene un costo elevado y una gran dificultad.

También la seguridad de la información no es aún una cultura empresarial o no es un tema prioritario y como consecuencia se tiene que los aspectos de seguridad pasan a segundo plano.

Preguntas básicas

¿Cómo aparece el problema, que se pretende solucionar?

No aplica

¿Por qué se origina?

El problema se origina porque las normas de autenticación y seguridad existentes se aplican a grandes empresas

- ¿Qué lo origina?

La expansión de las aplicaciones Cloud Computing es reciente en las pequeñas y medianas empresas

- ¿Cuándo se origina?

Se origina cuando las pequeñas empresas y medianas empresas no cuentan con las normas y recursos necesarios para poder implementar la infraestructura que requiere la subida de datos hacia la nube.

- ¿Dónde se origina? No aplica
- ¿Dónde se detecta? No aplica

Objetivo General

Desarrollar una guía de implementación de normas de autenticación y seguridad en entornos Cloud Computing para PYMES.

Específicos

1. Fundamentar teóricamente las normas de autenticación y seguridad, así como de los entornos *Cloud Computing* y las PYMES.
2. Realizar un diagnóstico acerca de los entornos *Cloud Computing* más utilizados en soluciones para PYMES.
3. Definir una guía de implementación de normas de autenticación y seguridad enmarcando los aspectos de importancia de *Cloud Computing.*
4. Validar la guía implementación mediante una técnica de satisfacción usuario y una comparativa con norma ISO.

Pregunta de Estudio, Meta y/o Hipótesis de Trabajo

Como meta para el tema de investigación es dar la ayuda necesaria con las normas, que se aplicarán a las PYMES para mantener las debidas seguridades de la información lo apoya la tecnológica *Cloud Computing*.

Metodóloga de investigación

Para el desarrollo del proyecto se apoyará de la metodología de la investigación. El experto (Sampieri, 2010) presenta diferentes enfoques lo, cuales, sirven para la recopilación de información que ayudarán en el desarrollo de este, de los conceptos, orientación, características, etc. Con el fin de llegar a unificar para obtener el objetivo.

Justificación

Las PYMES no tienen el presupuesto para poder dar la debida seguridad a sus empresas en servicios Cloud, además, las posibilidades de crecimiento y de aprovechamiento de la nube se han incrementado paulatinamente en la medida en que la mente visionaria de algunas empresas, ha marcado el camino con un ritmo de cambio exponencial y frente a una nueva era “sociedad globalizada”, en la que las fronteras desaparecen en beneficio de los intercambios de ideas, mensajes, productos, servicios, personas, etc., es imprescindible mantener la seguridad de datos y aplicaciones.

La guía de implementación medirá la eficiencia y eficacia del desarrollo de las pequeñas y medianas empresas en el ecuador, que cuenten con Cloud Computing, con la finalidad de ayudar a la toma de decisiones por parte de la gerencia.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1 Origen y evolución de *cloud computing*

La historia sobre la seguridad *cloud* se remonta específicamente en los inicios de la creación del mismo internet, a partir de 1990 como sistema de comunicación global, el concepto de nube se emplea en un entorno académico en 1997 por el profesor (Chellapa, 2019).

En el año 1950 la aparición de los *mainframes,* fue lo que se conoce hoy en día como el *cloud computing* donde una computadora central se conectaba con distintos usuarios, en décadas posteriores se desarrolló la virtualización que en la actualidad se conoce como servicios de nube. (Ionos, 2019)

Las primeras alertas de seguridad conllevan principalmente en la red en el año de 1983 nació la internet como tal, pues dichos sucesos naturales y alteraciones físicas en los servidores principales vulneraban el funcionamiento de la red, así en el transcurso de los años se abre la necesidad de tener dispositivos cada vez más sofisticados en seguridad informática, en dicho proceso universidades de estados unidos, ARPANET, entre otras instituciones públicas y privadas se unen para mejorar los sistemas de seguridad para la información informática. (Academia.edu, 2009).

La seguridad *cloud* es implementada para proteger la infraestructura de la red, la información contenida de los clientes y de las PYMES, donde se aprovechará los procedimientos de seguridad para la integridad de los datos sobre todo ha provocado daños personales y financieros importantes para las empresas, como pérdida de registros de facturación, inventario, errores de la data de los clientes, sustitución o duplicación de

información por usuarios no autorizados entre otros.Hay que tomar en cuenta que es necesario tener a nivel de hardware los componentes físicos como un modem, que es un dispositivo que sirve para modular la señal digital originada de un ordenador y convertira a una forma de onda, que sea asimilable por dispositivos de red como *switch* y router que interconectan el ordenador con el modem para facilitar el acceso a la web. Del cuál a continuación se especifica el sistema de seguridad a nivel físico.

1.2 Fundamentación teórica

1.3 Autenticación

Tabla 1. Concepto de autenticación

Autor	Definición
(Microsoft, 2005)	La autenticación es un método para verificar la identidad de un individuo mediante una prueba para cotejar Información de dicho individuo.
(IBM, 2018)	Es una técnica por la, cual, se corrobora la identidad con la ayuda de un ID usuario y contraseña.
(Mifsud, 2012)	Se define como la comprobación de la identidad del usuario, habitualmente si este ingresa a la red o a un sistema que tenga una base de datos.

Fuente: elaboración propia

Al tener la información segura se necesita la autenticación, es parte fundamental para la protección es necesario saber la definición de autenticación que brindan los siguientes autores:

Las definiciones mencionadas determinan que la autenticación es un método por él, cual, se valida la identidad de un individuo con la ayuda de un número de identificación (ID) y una contraseña, generalmente si ingresa a una red o a un

sistema que tenga una base de datos.

Características

Tiempo de espera

Según Morales (2015), el tiempo de espera “es la diferencia entre el tiempo de presionado y el de liberación de la tecla” (p.3), como se detalla, esta característica es de vital importancia dentro de un proceso de autenticación el tiempo de espera de 2 segundos.

Por lo tanto, destacar que el tiempo de espera hace referencia a la divergencia entre el lapso en el, cual, se presiona la tecla y se suelta la misma, por lo que el tiempo de presionado es de 2 segundos.

Latencia Alzado – Presionado

Esta característica dice que la diferencia entre el tiempo de presión de la tecla y el tiempo de alzado de la tecla (Morales, 2015).

En base a lo expuesto la latencia de alzado – presionado, existe una diferencia entre el lapso de presión y de alzado de botón.

Mecanismos

Autenticación de cliente a servidor de aplicaciones para el usuario Autenticación básica

Este tipo de mecanismo no permite el inicio de sesión único, es decir, el inicio de sesión único se da si el cliente da inicio a la sesión en un equipo con Windows, pues el beneficiario se autentica a un dominio y después posee acceso a los

recursos y aplicaciones del domino y no es necesario volver a escribir sus datos para tener acceso a la información, es decir, una vez ingresados los datos no es necesario volver a escribirlo, se guarda en la memoria cache (Microsoft, 2005).

Lo anteriormente expuesto dice que la autentificación básica es aquella que el usuario se autentica tiene accesos a todas la aplicaciones y recursos dentro de un dominio, de tal manera que no es necesario volver a realizar la autenticación.

Autenticación basada en formularios

Este mecanismo usa *cookie* para identificar al cliente si esté realice un inicio de sesión. Al usar esta *cookie* permite cerrar las sesiones inactivas, sin embargo, el usuario y contraseña siguen en la memoria cache al igual que a la autenticación básica (Microsoft, 2005).

La autenticación basada en formularios dice que si el usuario inicia sesión tiene accesos a los recursos, sin embargo, si el usuario deje de trabajar inmediatamente cierra sesiones que están inactivas, este tipo de autenticación hace uso de cookie, los, cuales, permiten realizar dichas acciones, además, cabe destacar que los usuarios y contraseñas están guardadas en la memoria cache.

Tabla 2. Tipos de autenticación

Tipo	Descripción
El identificador y la contraseña.	Este tipo de autenticación es el más popular. De tal manera que llegará a ser simple o robusta al depender de la complejidad de la contraseña que el usuario le dé.
El identificador y la contraseña OTP (*One-Time Password*).	OTP otorga un calculador al usuario que le proporciona al cliente una contraseña bajo cierto límite de tiempo y se lo usa para autenticación inicial.

Los certificados PKI (*Key Performance Indicator*) sobre tarjeta inteligente o token USB	Es una tecnología de vanguardia en la codificación que concede calcular o firmar sin necesidad de compartirlos. El certificado es público y es firmado, como resultado tiene una garantía por una autoridad de certificación comprobada.
Tecla Confidencial Defensa	Es una llave multifunciones que tiene acceso al almacenamiento de los certificados, información, requerimientos anterior mente mencionada.
El identificador y la contraseña sobre una tarjeta inteligente	Este tipo de almacenamiento por identificador y contraseña sobre una tarjeta inteligente proporciona la incorporación del proceso de autenticación. Es decir que no importa que tan compleja sea la contraseña o se cambian continuamente, sin esta tarjeta, no se podrá acceder a la contraseña.
Biométrica	Es basa en la comprobación de una parte del cuerpo del cliente (habitualmente la huella dactilar).
La definición sin contacto	Básicamente es una tarjeta que contiene información del cliente esta permite el acceso o inicio de sesión, si la tarjeta o el objeto que lleve el microchip está cerca del otro objeto que leerá los datos sin necesidad de entrar en contado esta dará paso al inicio de sesión o a la respectiva información necesaria.

Fuente: (EVIDAN, 2015)

Se toma en cuenta la tabla anterior, donde hay varios tipos de autenticación de los, cuales, se ha dado su debida conceptualización se basó en lo que el autor redactó en su proyecto de investigación.

Autenticación en entornos *Cloud Computing*

Cabe destacar, que se considerará la autenticación para aplicar en entornos *cloud* a continuación, el autor (Zapata, 2018). Al usar un sistema de autenticación se tomará en cuenta que el proveedor permita aplicar *Security Assertion Markuo Language (SAML)* la, cual, es aplicable en Google Apps. SAML es un estándar para realizar el intercambio de la autorización y autenticación entre dominios de seguridad.

A su vez se revisa los tipos de autenticación, que se realizará en la nube, sin olvidar, que se autenticará dos factores, ya sea algo que el usuario sepa (contraseña, código, etc.) y algo que le pertenezca (credencial, llave, etc.). A continuación, se describirá los tipos más populares:

Como consecuencia de lo expuesto se considerará, si se realiza la autenticación en entornos *cloud computing* el proveedor permita adaptar *Security Assertion Markuo Language (SAML)* la, cual, es compatible con Google App, se tomará en cuenta que SAML es un modelo para realizar la autenticación en la nube.

Basado en contraseña

Es el nivel más básico y poco seguro para la autenticación, es fácil de predecir y de interpretar, se tomará en cuenta que si se desea utilizar este tipo de autenticación es recomendable que el usuario utilice caracteres especiales, teclas alfanuméricas, de esta manera se podrá obtener una contraseña robusta.

De esta manera se dice que el nivel más bajo y poco seguro para realizar la autenticación es la, que se basa en contraseñas, muchas de las bese estas son predecibles, por lo, cual, es recomendable que los usuarios creen sus contraseñas con una combinación entre caracteres especiales, teclas alfanuméricas, con el objetivo de poder tener una contraseña robusta.

Certificados digitales

Usar este tipo de autenticación es una buena opción, incluye dos factores los, cuales, son el certificado y el pin de acceso. Una de las desventajas del uso, es que almacenará en algún lugar, se considerará que, si la ubicación de dicho certificado está en un ordenador, es de difícil acceso a él sí, no se tiene el equipo a su lado.

De este modo se dice que los certificados digitales son una de las mejores alternativas para realizar la autenticación, brinda dos elementos con los, cuales, se tiene acceso a la información. Sin embargo, existe una desventaja del uso de esta, el certificado está almacenado en una base de datos la, cual, no es transportable.

Código SMS

Es más aplicable en entidades bancarias, si se desea acceder a información personal siempre se pide introducir usuario y contraseña e inmediatamente envía un mensaje a su número de celular con él, cual, creo su cuenta de dicha entidad bancaria, de esta manera se accederá a la información personal, es una de las mejores formas de autenticar a un usuario.

De igual forma los códigos por mensaje brindan tres elementos de seguridad los, cuales, son el nombre de usuario, contraseña y además, la verificación por un código el, cual, se envía a su celular móvil, este tipo de autenticación es implementado principalmente en los bancos.

Norma de autenticación *Cloud Computing*

La norma ISO 27018 la, cual, fue publicada el 29 de Julio de 2014, ayuda en la protección de la información para el uso de *cloud computing,* esta norma se

anexa a las normas ISO/IEC 27001 e ISO/IEC 27002 las, cuales, ayudan en la gestión de la seguridad en los, cuales, van vinculados a los servicios en la nube (Redondo, 2015). Además, se apoyará de la norma IEEE la, cual, está vinculada con la seguridad y autenticación, que se mencionará más adelante.

Dentro de lo expuesto se toma en cuenta la norma anteriormente mencionada como base para poder realizar la autenticación para los servicios en la nube que ira de la mano con la norma IEEE la, cual, está relacionada con la autenticación.

1.4 Seguridad

Tabla 3. Concepto de seguridad

Autor	Definición
(Pérez, 2015)	Se dice que la seguridad es la carencia de peligros o advertencias, aplicable en el contorno individual de las personas.
(Seguridad, 2018)	Es la carencia de peligro, daño o riegos por otro lado se la denomina efecto de esperanza.
(Competencias e información especializadas en salud pública, 2018)	Se la define como una situación en la que las amenazas y las circunstancias llegará a causar males ya sea físico, psicológico o material.

Fuente: elaboración propia

En este sentido se dice que seguridad, es la carencia de riesgos o amenazas la, cual, se lo vincula como en el entorno o individual, además, a la seguridad se la contextualiza como esperanza.

Niveles

Según el autor (VERIDOS, 2018) afirma que existen tres tipos de niveles de seguridad.

- **Nivel 1:** Atributos de la seguridad por los sentidos del ser humano.

- **Nivel 2:** Atributos que solicitan herramientas sencillas de validación, como lámparas o lupas.
- **Nivel 3:** Atributos exclusivamente validados por herramientas aplicadas o laboratorios.

Lo expuesto indica que a la seguridad se la desglosa por niveles, en el primer nivel se tiene la seguridad basada en los sentidos del ser humano. En el nivel dos se aplican herramientas de validación para poder tener la debida seguridad. En el nivel tres se tiene a las herramientas explicitas para poder obtener la seguridad necesaria.

Seguridad en entornos *Cloud Computing*

La seguridad en la nube es una de las presencias que más tienen cuidado los suministradores de servicios y entornos cloud. Varios de los administradores de estos servicios como Microsoft, Amazon, IBM, etc. Procuran abastecer de medidas de seguridad hacia los consumidores. Se considerará que el suministrador no podrá eliminar las amenazas del todo, estas amenazas permanecerán como riesgos e incluso los entornos más robustos podrán caer ante las posibles contingencias (Portal, 2015).

Según lo anteriormente expuesto se dice que la seguridad en la nube es una entidad a la, cual, cuidará, aunque el proveedor de los servicios brinda ciertas políticas de seguridad. Sin embargo, no están totalmente cubiertas, existen riesgos que llegarán a convertirse en amenazas.

Normas de seguridad *Cloud Computing*

La norma ISO/IEC 27017 trabaja simultáneamente con la norma ISO 27001, la norma ISO 27017 brinda controles para los suministradores de servicios en la nube, así como los consumidores de estos, esta norma evidencia

funciones y obligaciones de tal manera que controla que los servicios en la nube sean tan seguros, así como los datos que la contiene. Además, la norma ISO/IEC 27017 ayuda a comprender las partes esenciales, así como los controles y también como se beneficiarán si desea mudar la información hacia *cloud* (bsi, 2018).

De este modo la norma ISO anteriormente mencionada da los respectivos controles de seguridad para poderlos implantar en los servicios que brinda la nube, a su vez da la certeza que las obligaciones y funciones sean desempeñadas de la mejor manera, de este modo se tendrá los datos seguros.

1.5 Cloud Computing

Origen y Evolución

Se considerará que para el estudio del proyecto de investigación se detallará el origen que tuvo *Cloud Computing,* así como su evolución se tomará en cuenta la información que brindan los autores. (ONTSI, 2012) y (Reyna, 2009)

Debido al gran avance que ha tenido la tecnología y así como la necesidad por saber cómo usarla se indagará en el origen de *Cloud Computing* (Computación en la nube).

Desde el inicio de la década de 1960, en ese entonces los inmensos y rústicos equipos informáticos estaban planteados para poder usar un único programa. Un quinquenio después se hizo popular el compartimiento a tiempo, es decir, que varios programas estén en funcionamiento simultáneo en un mismo equipo, gracias al poder de procesamiento y almacenamiento en un computador central.

Se popularizó de tal manera que las comunidades grandes se acogieron a usarla,

así como los científicos y/o estudiantes de las ciencias rigurosas requerían tener acceso a la previsión de la información. Durante los 80's se dio la evolución de las computadoras de hogar y esto dio como habito a los usuarios a operar con equipos personales. En el año 1981 se da la difusión de las computadoras personales, un equipo accesible para la gran demanda que había.

Tras varias investigaciones en la tecnología se implementaron los *clusters* (conjuntos de varios equipos en uno solo) basados en la tecnología de las PC, se tiene como resultado se obtuvo construcciones de cálculo de gran rendimiento a precios bajos la, cual, se extendió en la década de 1990.

Los *clusters* tuvieron un cambio para poder realizar cálculos, almacenamiento de información esencialmente en la universidad y los edificios de investigación.

Las instalaciones comenzaron a brindar los servicios a terceros, a través de un estándar, de tal manera, que se construyó una arquitectura denominada *grid* la, cual, es encaminada al almacenamiento de gran cantidad de información.

Las arquitecturas propuestas tuvieron una gran acogida en instituciones dedicadas a la investigación durante la mitad de la década de los 2000, sin embargo, por su complejidad de infraestructura, así como el uso de varios *grids* y los problemas de trasporte hicieron que, no se popularizara para otros objetivos que, no sean la investigación.

En la misma década se comenzó con la tecnología de la virtualización que hacía posible la implementación de máquinas virtuales, que permite replicar el ambiente de usuario sin tener que configurar todo el software. Este nuevo tipo de arquitectura permitía la distribución del trabajo de manera fácil lo,

> cual, no se pueda realizar en arquitectura *grid* de tal manera, que se abrió una nueva oportunidad para el cálculo distribuido, denominado *Cloud Computing*. El nuevo modelo conlleva un paradigma capas de facilitar medios de cálculo y almacenamiento, a su vez ayuda en el aprovechamiento comercial de la gigantesca capacidad de cómputo de abastecedores de servicios en internet.

Según lo anteriormente mencionado se pude decir que debido al auge de la tecnología y la necesidad de como poder aplicarlo al diario vivir, se tomará en cuenta los orígenes que tuvo la nube, a inicios de los años 60s existían inmensos equipos los, cuales, era rústicos, cuya funcionalidad era la de realizar un solo proceso, al avance que tuvo la tecnología se hizo popular el compartimiento de datos a tiempo, es decir, que varios de esos equipos se los unió para poder implementar más procesos así como obtener más almacenamiento en un solo equipo. Tuvo una gran acogida, varias entidades deseaban obtener dichos equipos los, cuales, era usados para cálculos. En la década de los 80s hubo un paso gigantesco hacia las computadoras de casa.

Sin embargo, después se dio el salto hacia las computadoras personales, además, de esto también se dio el auge de los *clusters* lo, cual, era el conjunto de varios equipos en uno solo y se los utilizaba para realizar grandes cálculos a precios accesibles.

Además, se popularizó el estándar al, cual, se lo denomino *grid*, estas tenían una gran capacidad de procesamiento, así como de almacenamiento, esta arquitectura tuvo una gran acogida en el año 2000, sin embargo, debido a la gran demanda que existía se dio otra evolución en la tecnología, en la misma década se popularizo la virtualización la, cual, permitía duplicar la interacción del usuario sin tener la necesidad de configurar todo el software, esta permitía realizar proceso de una forma más eficiente lo, cual, abrió un camino hacia la nueva arquitectura nombra Cloud Computing. Este nuevo modelo lleva a otro nivel la

capacidad de procesamiento, así como la del almacenamiento, así como poder acceder a datos desde cualquiera párate que el usuario se encuentre.

Modelos

Pública

La infraestructura y recursos están creados para el uso público en general a través de internet. Ser de un proveedor, administrador y/o ejecutada por una empresa y esta existe en el lugar del proveedor del servicio (Sánchez, 2017). Se dice que la nube pública es accesible para todos solamente con el uso del internet la, cual, administrará un suministrador de servicios.

Privada

La infraestructura y recursos están creadas para el uso de una sola institución, es decir, que solo los miembros de dicha organización tienen acceso a la información exteniente. Ser de un proveedor, administrador y/o ejecutada por una empresa (Sánchez, 2017).

El tipo de nube mencionada anteriormente esta creada para que una sola entidad pueda tener acceso a los servicios que ofrece el proveedor.

Comunitaria

La infraestructura y recursos están creadas para el uso de una o más organizaciones que tienen un convenio de tal manera que cumplan objetivos en común, con una seguridad y privacidad para las entidades que la conformen (Arenas, 2017).

La nube comunitaria es aquella que está ligada por medio de un convenio por

la, cual, estas entidades accederán a información compartida.

Híbrida

La infraestructura y recursos están basadas en unión de dos o más tipos de nubes anteriormente mencionadas, sin embargo, están asociadas por el uso de la tecnología estandarizada que da el acceso de aplicaciones e información (Arenas, 2017).

Esta infraestructura está relacionada en conjunción de dos o más tipos de nubes, las, cuales, están unidas por el tipo de tecnología, que se aplica.

Servicios

Software como servicio (Saas)

El termino software como servicio se refiere al software que está instalado en la nube al, cual, es accecible desde varios dispositivos a través una interfaz ágil como un navegador de internet (Bustamante, 2014).

Este servicio se basa a las aplicaciones que están previamente instaladas las, cuales, son dadas por el proveedor de la misma.

Infraestructura como servicio (Iaas)

Brinda la infraestructura indispensable para ejecutar aplicaciones. Este tipo de servicio proporciona almacenamiento, servidores, capacidad de proceso y equipamiento físico al, cual, se tiene acceso por pago. Contienen sistemas operativos y aplicaciones. El cliente no tiene acceso a la infraestructura de la nube, pero si tiene control en la aplicaciones y sistemas operativos por los, cuales, ha pagado (Bustamante, 2014).

Por consiguiente, la infraestructura como servicio es aquella en la, cual, se ejecutará aplicaciones, así como tener acceso a capacidad de proceso, almacenamiento y equipamiento para lo, cual, se tiene acceso solo si se paga por dichos servicios. Sin embargo, el cliente tiene control sobre las prestaciones que el proveedor le brinda.

Plataforma como servicio (Paas)

Hace referencia que el cliente adquirirá o creará aplicaciones dentro de la infraestructura que brinda el proveedor y a su vez es aplicaciones creadas por el cliente estarán soportadas por el lenguaje de programación y herramientas dadas por el proveedor de la infraestructura (Quintero & Florez Fuente, 2014).

Elaborar aplicaciones dentro de la nube, considerará que las aplicaciones que haga el consumidor compatible con los lenguajes que el suministrador tenga en su infraestructura.

1.6 PYMES

Características

Al hablar de las pequeñas y medianas empresas de considerará, cuales, son las características de estas, según (Logicbus, 2018).

- El patrimonio es suministrado por 2 o más personas que llegan a un acuerdo.
- Los propietarios de la empresa son quienes la administran.
- El número de empleados es de hasta 250 personas.
- Rinden y proveen no solo a nivel de la región, si no que podrán llegar a un nivel nacional e incluso internacional.
- Constantemente está en proceso de crecimiento al tener como meta ser una

empresa grande.

En cuanto a las características las más esenciales son:

- El capital es administrado por más de una persona.
- Por lo generar los jefes son los propietarios de las entidades.
- La cifra de funcionarios dentro de la empresa no excede de 250.
- Abastecen fuera y dentro de la su región, así como del país.
- Constantemente están en evolución para poder llegar a su meta la, cual, es ser una gran empresa.

Estructura

De constituye una empresa sea esta grande, mediana o pequeña, no siempre se sabe cómo organizarla, según (Zuluaga, 2015). Las PYMES, se estructuran de la siguiente manera:

Accionista /Dueño

Es aquella persona que indaga la forma para retribuir la transposición, a su vez este miembro contribuirá con la toma de resoluciones con el fin de poder aumentar su patrimonio y poder sustentar así al accionista y de igual manera a sus clientes.

Según lo mencionado, se dice que el dueño o accionista es la persona que investiga procesos para poder mantener o aumentar su inversión, además, es aquel que toma acciones con el fin de poder encaminar a la empresa por la mejor vía hacia el éxito.

Clientes

Las empresas son creadas con el fin de saciar las carencias de un mercado. Entonces para esto, se dirigirá a un grupo de personas las, cuales, necesiten de los servicios que la empresa brinda. Se denomina cliente aquella persona que busca una empresa que pueda solventar su necesidad a cambio de tarifa extra por lo financiado.

Mercado

Es el conjunto no tangible de los clientes en él, cual, se garantiza que los servicios y productos lleguen a satisfacer las necesidades de los consumidores. El mercado es el todo en él, cual, la empresa brindará cada uno de sus servidos y así solucionar los problemas de los clientes.

Colaboradores

Las PYMES asegurar el futuro crecimiento de la misma por los, cuales, es necesario tener un área de recurso humanos la, cual, ayudará en el desarrollo de la empresa.

Se define como colaboradores a quienes ayudan al crecimiento de la empresa de manera entera los, cuales, evalúan a las personas que, se contrataran para ofrecer los servicios.

Modelo de negocios

Existen varias variantes del modelo de negocio unas van por el camino de la cadena de valor y otra de las actividades. La cualidad del modelo de negocio hace referencia a su diseño los, cuales, englobarán todos y cada uno de los límites de la empresa. Se dice que el modelo de negocios

radica en los activos, actividades y la estructura del gobierno que tiene como meta incrustar la desigualdad entre el valor del servicio o producto para el consumidor y el costo establecido del mismo.

Sin dejar de lado el modelo de negocio, se dice que es la forma por la, cual, la empresa, se sustenta así misma como a los empleados y clientes de tal manera que genera ingresos para poder seguir brindados servicios para quienes lo necesitan (Morejón, Acosta, Ávila, Cabrero, & Cabrera, 2014).

Se expresa que el modelo de negocio es el camino o la forma por la, cual, la empresa llega a sustentarse a través de las prestaciones de servicios, además, se dice que está basada en el diseño por la, cual, la empresa mantendrá a los consumidores de una manera fiel.

Procesos y funciones

El proceso viene hacer un factor de gran importancia para poder conseguir una ampliación basada en la eficiencia y eficacia de tal manera que llegan a reducir los recursos, no es adecuado realizar cambios radicales ni hacer grandes adquisiciones. Lo recomendable es tener una percepción a lo que, se desea llagar a largo plazo (Diaz, 2015). Los procesos son aquellos por los, cuales, se destacan las empresas, al reducir los recursos sin afectar la calidad del servicio que ofrecen hacia el exterior.

Para varios inquisidores de teorías de administración la función fundamental es la de guiar hacia la mejora continua de las decisiones, inversiones y financiación. Además, cabe recalcar que la función financiera perdurar en su liquidez como las utilidades de las empresas (Blanchar, Portela, & Portela, 2015). Las funciones vienen dadas desde la administración por lo, cual, esta realizará un proceso de mejor permanente para sin dejar de lado la liquidez, que se mantendrá o incrementará.

Cloud Computing en PYMES

Cloud Computing fortalecerá el aceleramiento para que industria pueda desarrollarse ante su competencia. La computación en la nube es una opción fácil para que las pequeñas y medianas empresas puedan permitirse a tener acceso a soluciones eficientes y servicios tecnológicos que puedan incrementar la mejora en procesos y operaciones dentro de la empresa, de tal manera rivalizar con otra empresa (ONTSI, 2012).

La computación en la nube ayuda al crecimiento de las pequeñas y medianas empresas, no son tan costadas de implantar, sin dejar de lado que realizará como varios procesos, almacenamiento y gestión dentro de la nube, además, este tipo de tecnología está en auge para las PYMES por lo, cual, es de importancia tener en cuenta su factibilidad.

Las TIC con enfoque a las PYMES

Según él (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2016) dice:

Para impulsar la infraestructura y la conectividad en el territorio ecuatoriano se asegurará que los sacrificios marquen de una forma económica y social al país.

Puesto que la implantación de TIC (Tecnologías de la información y comunicación) en las empresas ofrecen diferentes ventajas entre las, cuales, se tiene eficiencia en el servicio, así como la disminución de recursos. Además, que en los servicios públicos brinda ayuda realizarán varios trámites desde su hogar por lo, cual, al aplicar TIC en las empresas, llevarán a un gran avance tecnológico al país puesto que al ciudadano ayuda en la disminución de recursos, así como ceder servicios de alta

calidad.

Por lo tanto, se afirma según lo anunciado anteriormente que con la implementación de las TIC en las pequeñas y medianas empresas en el Ecuador es de gran ayuda por lo que serán útiles en las eficiencia y eficacia en los servicios que las PYMES prestan hacia los consumidores. Además, se considerarán que si implantan las tecnologías de información y comunicación dentro en las empresas existentes en el Ecuador tendrán más posibilidades de competitividad hacía el mercado exterior.

CAPÍTULO II. DISEÑO METODOLÓGICO

En este capítulo se encuentra estructurado de la siguiente manera: primera parte, un marco conceptual de los tipos de investigación utilizados, así como métodos teóricos y prácticos, segunda parte una descripción de la metodología de desarrollo a utilizar.

2.1 Metodología de investigación

2.1.1 Enfoque de la investigación

(Sampieri, 2010), menciona la usabilidad que tiene el enfoque cualitativo y cuantitativo los que sirvieron para el desarrollo del tema de investigación los mismo se detallan más adelante.

Enfoque cualitativo

Sirve para modelar todo un procedimiento en al, cuales, se recolectan datos y poder tener una relación entre los integrantes de la investigación de tal manera poder obtener pruebas de lo, que se ha puesto a los participantes. Por lo tanto, este método ayudó a extraer información de las personas estrechamente relacionadas con el área de TI y su experiencia con el uso de los servicios de *cloud*.

Enfoque cuantitativo

Representa los procesos a seguir de un tema de investigación, la misma que tiene fases y no se evadirán, de esta manera podrá obtener preguntas y objetivos de la investigación. De manera que este enfoque sirvió para obtener interrogantes y aclarar metas, que se podrán evidenciar en forma de gráficos y

numero que sirvieron para el tema de investigación.

2.1.2 Método general de la investigación

Búsqueda Bibliográfica

Para la realización de una investigación es necesario una exploración bibliografía según (HEVIA M J, 2017). Manifiesta que la búsqueda bibliográfica es necesaria para aprender nuevos conocimientos o para excluir procedimientos y defunciones caducas. En la investigación, que se realizó la técnica bibliográfica la, cual, estuvo basado en el análisis de los documentos de Google académico, Repositorios, SciELO con el fin de recopilar información necesaria para el presente proyecto, en donde se ubicaron varios documentos referentes al tema, los que fueron analizados de forma particular.

Analítico- sintético

Además, se empleó el método analítico sintético que, como mencionan (Bastar, 2012); (Maya, 2014), consiste en separar por partes un todo de tal manera, que se pueda explorar e interpretar la información necesaria para el estudio y poder llegar a una síntesis y rehacer lo investigado. Este método, se lo uso para conocer sobre las pequeñas y medianas empresas, así como el uso de los servicios de la nube diferentes modelos de guías, normas de autenticación y seguridad, servicios en la nube, donde se pudo establecer las dimensiones e indicadores para la construcción de la guía propuesta.

Técnicas e instrumentos de recopilación de información

En el desarrollo del tema de investigación es importante la recolección de datos e información de manera, que se pueda constatar y solucionar el problema. (Torres, Paz, & Salazar, 2015), afirman que es fundamental obtener

información de manera ordenada y establecer objetivos los que servirán para acumular datos necesarios. El proyecto se usará la siguiente técnica.

- Encuesta

Instrumentos

Encuesta

(López & Fachelli, 2015) afirma que la encuesta se apoya en la extracción de información a las personas encuestadas. De tal manera se pretende obtener la debida información para poder dar solución al problema planteado. Para determinar las dificultades de las pequeñas y medianas empresas en la migración de datos hacia la nube se encuestará a los encargados del área TI de cada empresa.

Población

Para la realización del estudio se determinó las pequeñas y medianas empresas de la ciudad de Ambato las, cuales, se desglosaron en las siguientes categorías a su vez de determinó la población al ser esta de 157 la, cual, de detalla a continuación.

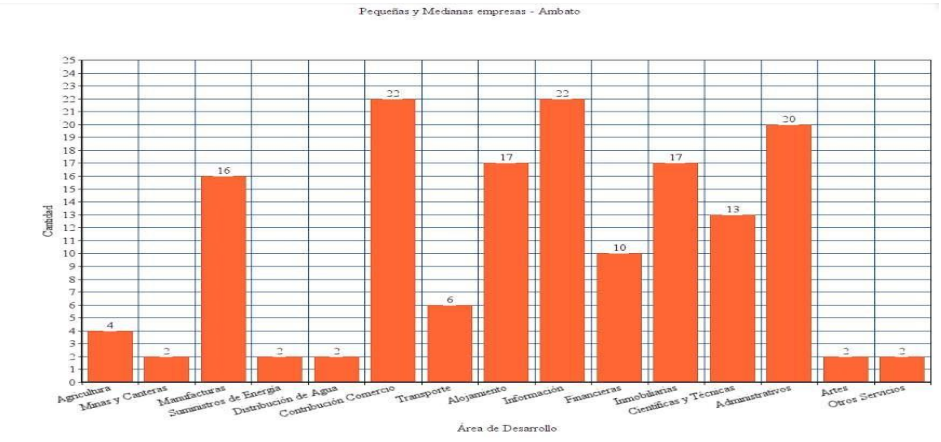
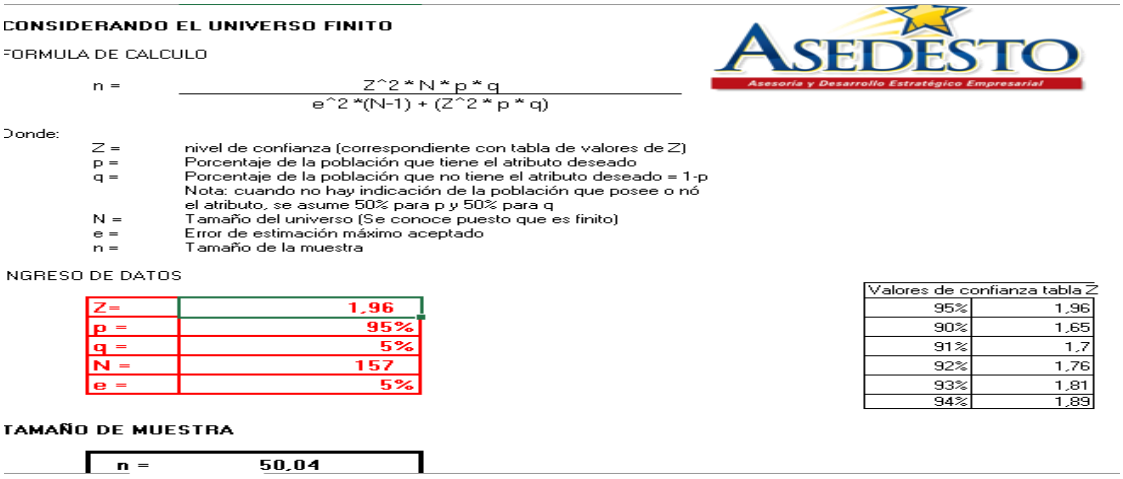


Gráfico 1: Pequeñas y medianas empresas en la ciudad de Ambato

Fuente: Elaboración propia

Muestra

Se consideró las pequeñas y medianas empresas (PYMES) de la ciudad de Ambato provincia de Tungurahua para aplicar la encuesta, que se realizará al personal encargado del área de TI, en este caso se aplicará la muestra, al ser la ciudad de Ambato se necesita un subconjunto la, cual, es representativa a la población de tal manera se podrá procesar información con una aproximación a la muestra de la población que fue de 50 empresas y se refleja en la fórmula a continuación.



CONSIDERANDO EL UNIVERSO FINITO

FORMULA DE CALCULO

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

Donde:

Z =	nivel de confianza (correspondiente con tabla de valores de Z)
p =	Porcentaje de la población que tiene el atributo deseado
q =	Porcentaje de la población que no tiene el atributo deseado = 1-p
	Nota: cuando no hay indicación de la población que posee o nó el atributo, se asume 50% para p y 50% para q
N =	Tamaño del universo (Se conoce puesto que es finito)
e =	Error de estimación máximo aceptado
n =	Tamaño de la muestra

INGRESO DE DATOS

Z=	1,96
p =	95%
q =	5%
N =	157
e =	5%

Valores de confianza tabla Z	
95%	1,96
90%	1,65
91%	1,7
92%	1,76
93%	1,81
94%	1,89

TAMAÑO DE MUESTRA

n =	50,04

Gráfico 2: Cálculo de la población

Fuente: (ASEDESTO, 2019)

2.2 Metodología de desarrollo

2.2.1 Metodología Cascada

Para el desarrollo del proyecto de investigación se usó la Metodología Cascada la, cual, consiste en, que se inicia una etapa hasta que esta llegue a su fin para así continuar con la siguiente etapa o fase. Sin embargo, esta metodología se usó de manera empírica, no desarrollará software. (Areba, 2001)

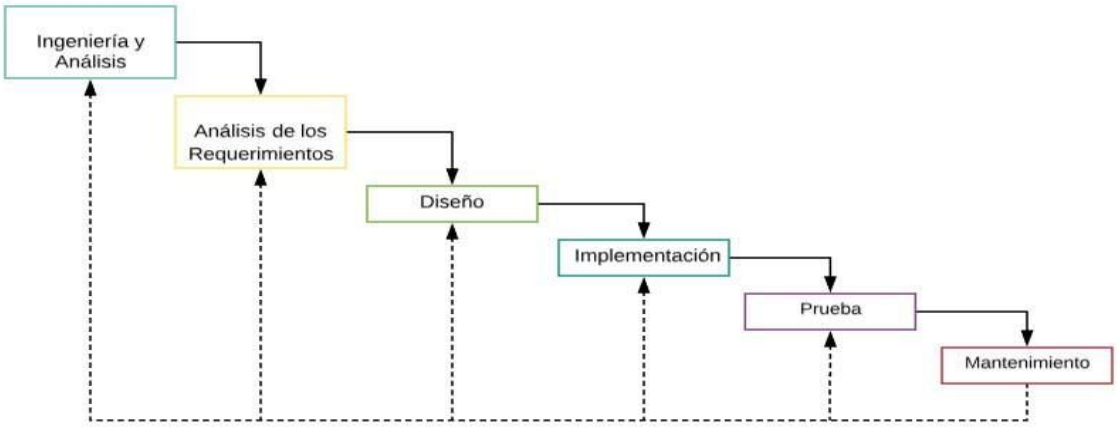


Gráfico 3: Fases metodología cascada

Fuente: Adaptado de (Richard Rojas, 2005)

- Análisis, se realizó una observación de las necesidades, que se deseará cubrir para determinar las características del producto final.
- Diseño, se desglosó y organizó los elementos, que se realizarán el desarrollo en equipo. La guía comprende tipos de VPN (Virtual Private Network) y su configuración; descripción del cifrado en VPN; contención de ataque DDoS (ataque distribuido denegación de servicio); protección contra programa maligno, habilitación y configuración del entorno *cloud* con el proveedor Azure y de igual forma la protección de los datos en la plataforma *cloud*.
- Implementación, se planteó los requerimientos previamente observados en la fase de análisis que sirvió para la elaboración de la guía de implementación de normas de autenticación y seguridad en entornos Cloud Computing para PYMES.
- Pruebas, como su nombre lo indica, una vez culminada la fase de implementación se realizará la respectiva evaluación para saber si cumplido los requerimientos del cliente. Se validará el producto propuesto por diferentes técnicas para llegar a cumplir las necesidades del cliente
- Mantenimiento, después de haber culminado las fases anteriores se inicia la revisión y mantenimiento del producto final. Se da inicio al producto y se valida si da los resultados esperados (Richard Rojas, 2005).

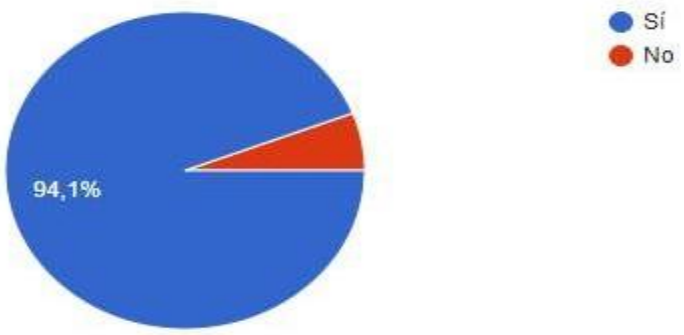
2.2.2 Análisis

Resultados de la encuesta

A continuación, se refleja el resultado obtenido de la encueta, que se realizaron a las personas encargadas de área de TI de cada una de las empresas, que se aplicó y se ejecutó un análisis a dichos datos obtenidos.

P01.- ¿Conoce el concepto del Cloud Computing o Computación en nube?

Gráfico 4: Conocimiento del concepto computación en la nube



Fuente: elaboración propia

Como se manifiesta en el gráfico se da a entender que el 5,9 % de las personas encuestadas no conoce el concepto de la computación en nube.

P02.- ¿La empresa contrata un servicio en la nube (Cloud Computing)?

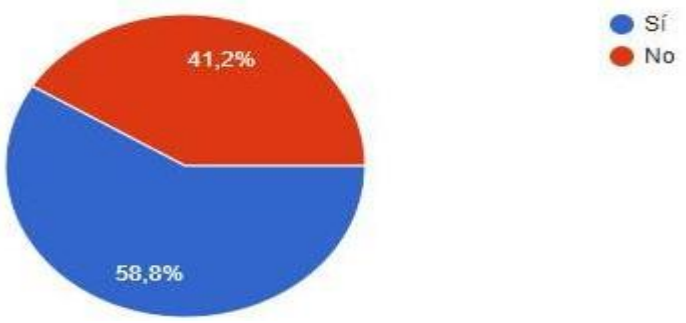


Gráfico 5: Contratación servicio en la nube

Fuente: elaboración propia

Se da entender que más de la mitad contrata servicios en la nube, sin embargo, cabe resaltar que no todas entienden el concepto de esta.

P03.- Describa tres motivos por las que no cuentan con un servicio de Cloud Computing.

Falta de conocimientos Falta de interés Falta de recursos
Presupuesto
Costos, velocidad y respaldo técnico
Dinero
Respaldo, seguridad y movilidad
Costos
Servicios Internet, Almacenamiento, Infraestructura
NINGUNA
Temor al cambio
No es necesario
Poco conocimiento, temor al cambio, precios

Gráfico 6: Motivos para no contratar servicios en la nube

Fuente: elaboración propia

Según lo observado se pudo resaltar que la mayoría de las personas encuestadas tienen en común el temor al cambio, precio y falta de conocimiento.

P04.-La empresa en la que usted labora cuenta con alguno de estos servicios.

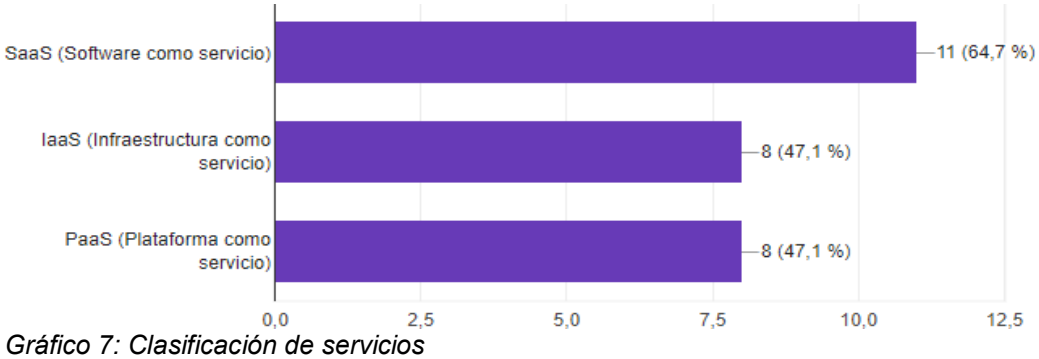


Gráfico 7: Clasificación de servicios

Fuente: elaboración propia

Como se muestra gráfico 7, un 64,7% de las personas encuestadas que tiene servicios en la nube usan software como servicio, sin dejar de lado que la infraestructura como servicio y plataforma como servicio están al mismo nivel.

P05.- Mencione algunos de los programas importantes que funcione dentro de la empresa

venture
Paquete de Office
Satjet
Bolsa de empleo
BestSystems
Cursos
amazon
Plataforma con servicio
TELCOS OS, OSS DIGITAL
Aws ec2, lambda, dynamodb, rds, sns, ses, cloudformation, s3
Sap
Sistemas de gestion estudiantil

Gráfico 8: Programas utilizados en la empresa

Fuente: elaboración propia

Se observa que los programas que tienen gran relevancia para las personas encuestadas están distribuidos en distintas zonas por lo, cual, se asegura que estos programas se podrán migrar hacia la nube.

P06.- Que áreas de la empresa cuenta con el servicio de Cloud Computing

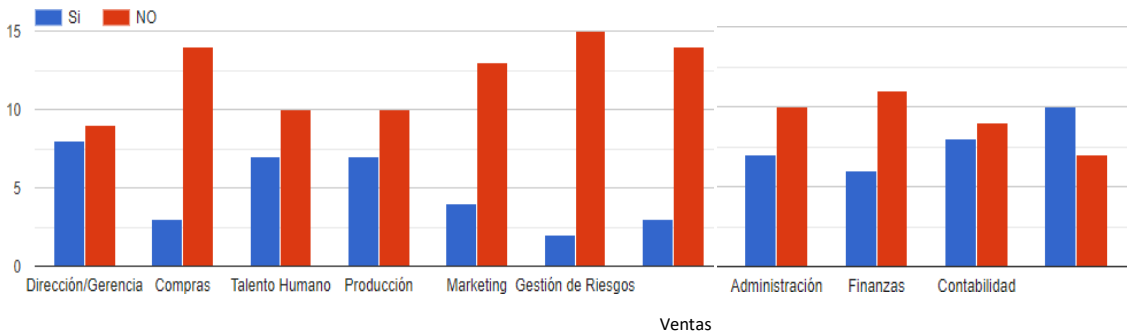


Gráfico 9: Áreas con servicios en la nube

Fuente: elaboración propia

En el gráfico 9 se observa que cuatro de las áreas que no cuentan con servicio en nube y tiene un porcentaje negativo son compras, marketing, gestión de riesgos y ventas.

P07.- ¿Conoce las ventajas que tiene el servicio de Cloud Computing para su empresa?

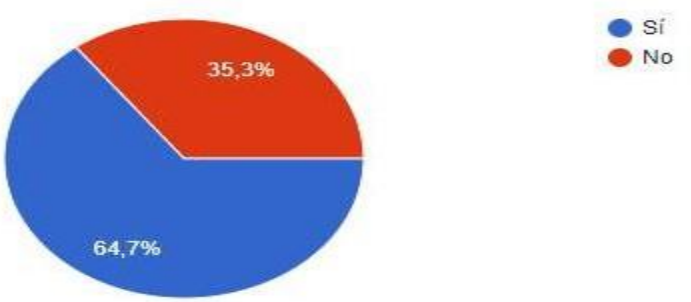


Gráfico 10: Ventajas de los servicios en la nube

Fuente: elaboración propia

Se destaca que el 64,7% de la población encuestada afirma que sabe el beneficio que tiene la computación en la nube, sin embargo, se presume que el restante no sabe los beneficios por falta de conocimiento de la nube.

P08.- ¿Cuáles son las principales ventajas que tiene la implementación de servicios en Cloud Computing para su empresa?

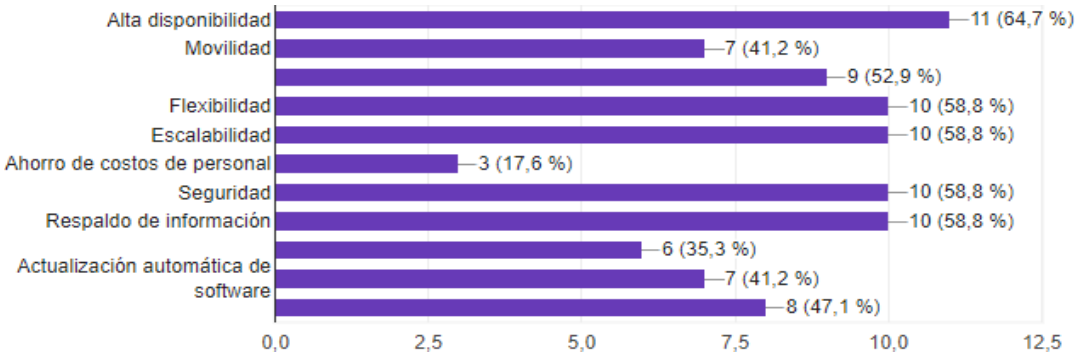


Gráfico 11: Ventajas de los servicios en la nube

Fuente: elaboración propia

Según los datos la flexibilidad, escalabilidad, seguridad y respaldo de información son las principales ventajas en común de las personas encuestadas, tiene un porcentaje más alto.

P09.- Cuáles serían las principales desventajas que tiene la implementación de servicios de Cloud Computing en su empresa

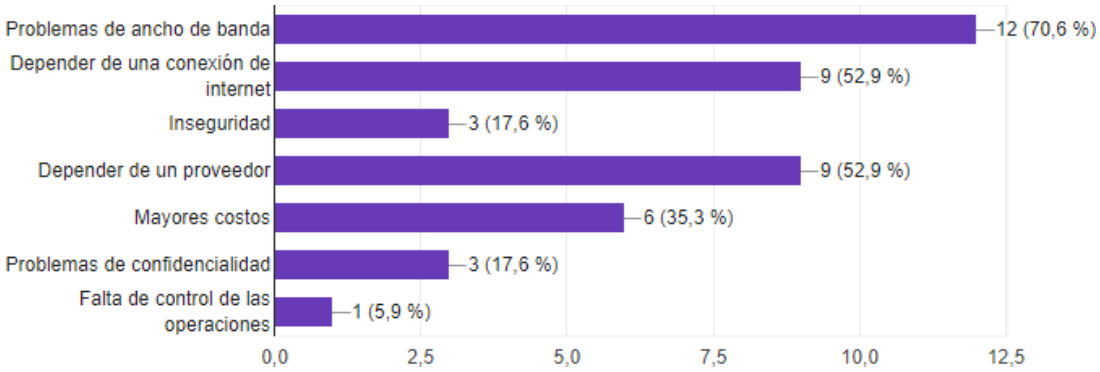


Gráfico 12: Desventajas de los servicios en la nube

Fuente: elaboración propia

Según los porcentajes obtenidos, los problemas de ancho de banda, depender de una conexión de internet y depender de un proveedor las principales razones por los encargados del departamento de TI no implementan computación en la nube.

P10.- Inversión anual en servicios en la nube de su empresa

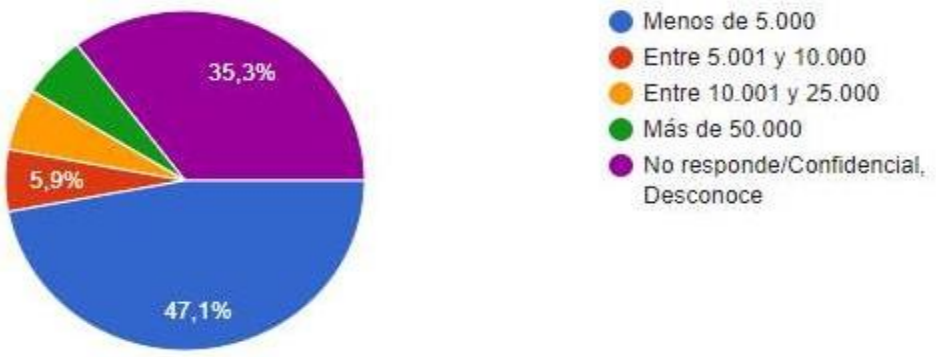


Gráfico 13: Inversión anual de los servicios en la nube

Fuente: elaboración propia

Se aprecia que en la gran mayoría de empresas encuestadas tiene una inversión inferior a los 5000 dólares anuales en servicios de computación en la nube.

P11.- Percepción del nivel de madurez de la Cloud Computing de su empresa

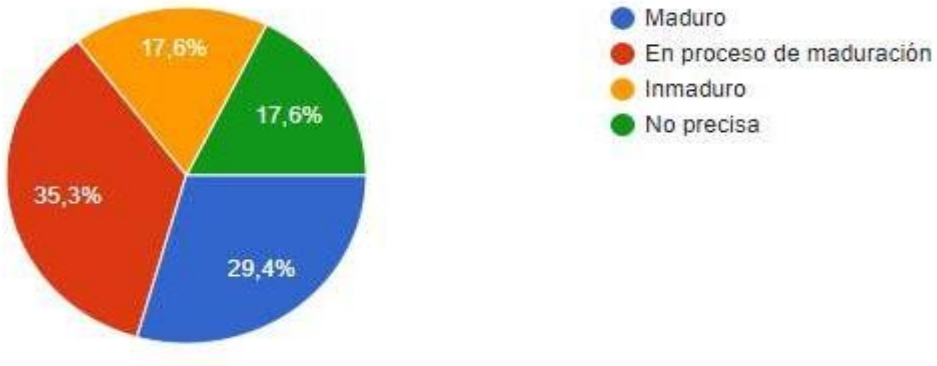


Gráfico 14: Nivel de madurez de la nube
Fuente: elaboración propia

Según lo observado se dice que el mayor porcentaje de empresas implementan los servicios en la nube, sin embargo, existen los porcentajes similares que no lo hacen, es por falta del conocimiento de los beneficios de la computación en la nube.

P12 ¿Conoce usted las seguridades que brinda la nube?

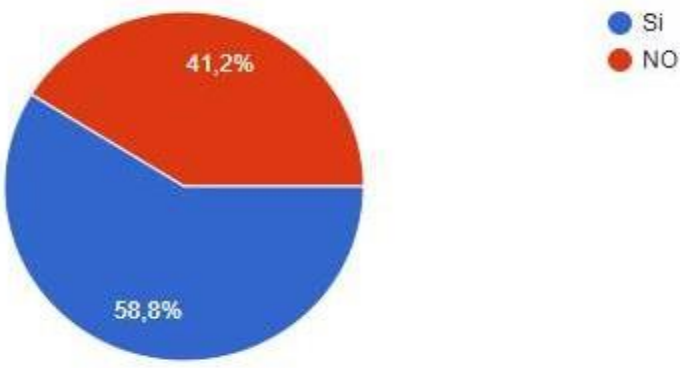


Gráfico 15: Seguridades de la nube
Fuente: elaboración propia

Mediante el gráfico 15 observado el 41,2 % de los encuestados no tiene conocimiento de las seguridades que brinda la nube por tanto se enfoca en la pregunta número dos la, cual, manifiesta que este porcentaje no contrata servicios en la nube.

P13 ¿Conoce normas de seguridad y autenticación, que se aplicarán en la nube?

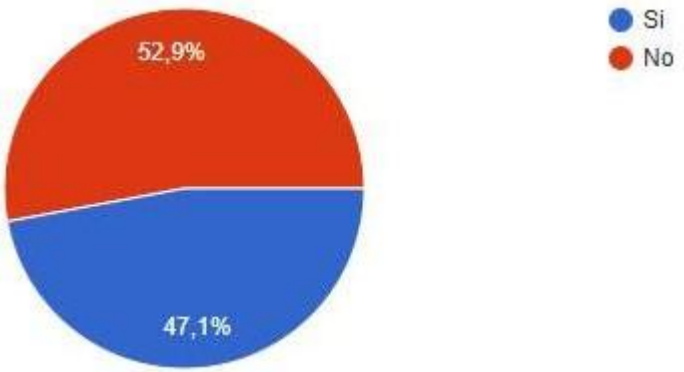


Gráfico 16: Conocimiento de las normas de autenticación y seguridad
Fuente: elaboración propia

Existe una leve diferencia entre el conocimiento de las normas, que se podrán aplicar en la nube, las respuestas e interpretaciones anteriores existe la posibilidad de cumplir dicha meta planteada en el tema de investigación.

2.2.3 Diseño

Después de observar las gráficas de las encuestas realizadas a las personas encargadas del área TI de cada una de las empresas pequeñas y medianas de la ciudad de Ambato se denota falta de conocimiento en la aplicación de las normas de seguridad y autenticidad en cuanto a la aplicación de las herramientas ofrecidas en la nube.

A continuación, se presenta la guía de implementación de normas de seguridad y autenticidad en *cloud computing* para Pymes, dirigido al equipo I.T de las

empresas pequeñas y medianas de la ciudad de Ambato; donde se toma en cuenta la metodología de cascada aplicada. Y tiene como objetivo educar y facilitar los conocimientos básicos de seguridad y autenticación de la nube, para que permita ser de soporte gerencial en la toma de decisiones de los cambios y recursos necesarios para la empresa. Los requisitos que una empresa necesita para implementar esta normativa dependen de la complejidad y el tipo de servicio que desee implementar, toda la infraestructura está en la nube, y se paga sólo por el servicio utilizado. A nivel *Hardware* es necesario un dispositivo de cómputo y conexión a internet para acceder a la infraestructura.

La tecnología *Cloud Computing* proporciona facilidad para la ejecución y administración de aplicaciones, pone al alcance al cliente todo el diseño de infraestructura que permite escalabilidad, flexibilidad, rendimiento, configuración de software y el mantenimiento y seguridad de todos los elementos necesarios para cubrir las necesidades del negocio. Esta guía inicia desde la seguridad de la red y de los dos tipos de VPN, que se utilizan. Restricciones / permisos vistos desde el proveedor de servicio *cloud* Azure en una máquina virtual donde se aloja un sitio web; hasta la creación, protección y autenticación de las cuentas de los usuarios que pertenecen al sistema, ejemplificados de manera tal, que se pueda evidenciar una breve descripción y uso de cada paso a seguir para el uso adecuado de las herramientas en *cloud computing.*

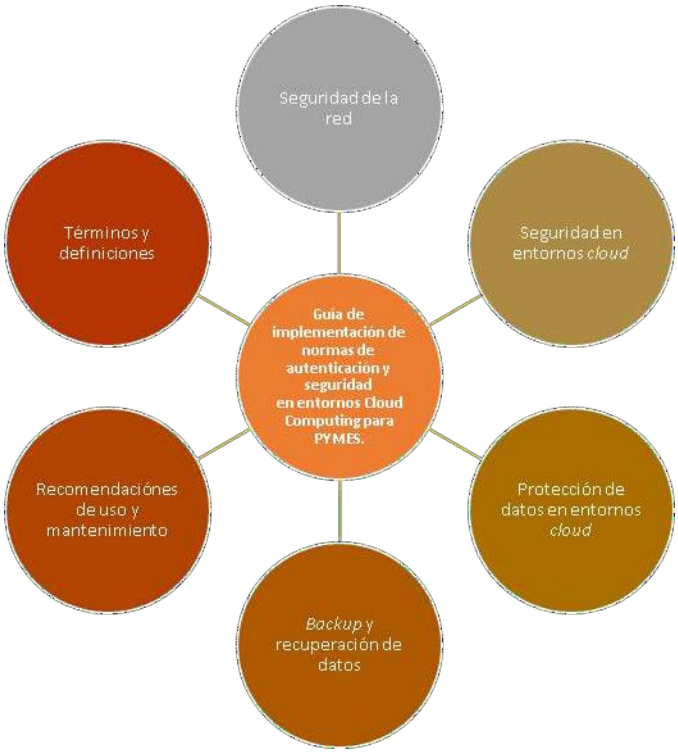


Gráfico 17: Organigrama de la guía de implementación
Fuente: elaboración propia

2.2.4 Implementación

A continuación, se presenta la guía planteada para el proyecto con su respectivo contenido.

2.2.4.1 Seguridad de la red

El sistema de seguridad de la red es manejado por una red interna que no está conectada directamente con la red externa como medida de seguridad y prevención. Los ataques a la red usualmente son controlados mediante el cifrado y el servicio de antivirus. Existen dos tipos de VPN, que se utilizarán para la protección la infraestructura de la empresa y la infraestructura de la nube contra ataques.

Tipos de VPN

(Krishnan, 2017), manifiesta que una de las virtudes de utilizar un VPN (Red Privada Virtual) es aumentar la rentabilidad en escenarios como, por ejemplo: si se tiene una sede principal en una ciudad que cuente con infraestructura el sitio principal que cuente con un directorio activo, un servidor de intercambio, un servidor de archivos, etc. Y tener sedes en otras ciudades una VPN les permitiría trabajar como si fuera parte de la red física de la sede principal sin la necesidad de invertir en servidores e infraestructura en las otras sedes y solo se tendría que mantener los servidores e infraestructura principal, además, de la conexión VPN que sería responsabilidad del equipo de administradores IT en la sede principal.

Site to site

Trujillo, E (2006), los servidores de las sucursales se conectan a internet mediante los servicios de su proveedor local de internet, típicamente mediante conexiones de banda ancha.

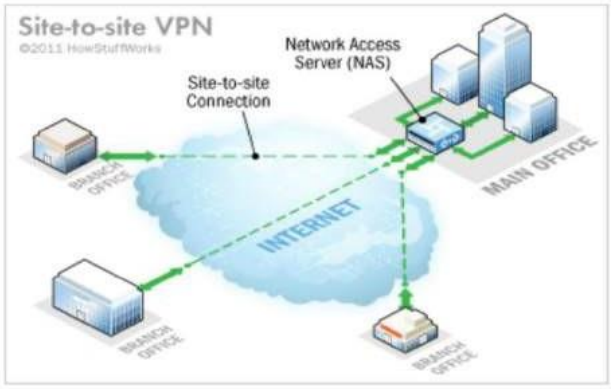


Gráfico 18: VPN Site To Site

Fuente: (Institute of Acoustics, Chinese Academy of Sciences, 2020)

El esquema empleado *site to site* es uno de los pocos difundidos, pero aun utilizados en las empresas como acceso remoto, como medio de conexión

mediante la red LAN (red de área local). Ejemplo de conexión VPN, como red segura para que las sucursales estén conectadas entre sí.

- Inicie sesión en la interfaz basada en web del *router*.

Gráfico 19: Interfaz principal *router*

Fuente: elaboración propia

- Configurar el servicio DNS dinámico o asignar una dirección IP estática para el puerto WAN del enrutador y síncrona la hora del sistema con Internet.
- En la dirección IP archivada del cliente, se ingresa el rango dedirecciones IP (hasta 10) que serán arrendadas a los dispositivos por el servidor VPN PPTP.
- Hacer clic en Avanzado para establecer el permiso de conexión PPTP de acuerdo con las necesidades.
- Seleccione, Permitir acceso a Samba (Network Place) para que el dispositivo VPN acceda al servidor Samba local.
- Seleccione, Permitir el paso a través de NetBIOS para permitir que el dispositivo VPN acceda al servidor Samba utilizando el nombre NetBIOS.
- Seleccione, Permitir conexiones sin cifrar para permitir conexiones sincifrar a su servidor VPN.
- Configure la cuenta de conexión PPTP VPN para el dispositivo remoto podrán crear hasta 16 cuentas.

Point to site

(Trujillo, 2006), Los protocolos del tipo de VPN *Point To Site*, es diseñado de modo modular para seleccionar un conjunto de algoritmos estándar para garantizar la integridad y autenticación de los datagramas IP.

Tabla 4. Protocolos más utilizados para una VP

PPTP	Soportado por PPP (Protocolo punto a punto), cifrado de 40 bits y 128 bits.
L2TP *(Layer 2 Tunneling Protocol)*	Soportado por PPP (Protocolo punto a punto), cifrado de 40 bits y 128 bits. Aplicable al *site to site*.

Fuente: Elaboración propia

Los protocolos de una VPN de *point to site* es el método más común que las organizaciones usan para conectar separación de la red local a la red virtual.

Permite el intercambio seguro de datos de un cliente a un servidor al formar una Red Privada Virtual, si se emplea una red de trabajo TCP/IP.

Esta conexión VPN se inicia en el nivel de firewall perimetral o enrutador.
Se ejemplifica la configuración de una VPN L2TP (*Layer 2 Tunneling Protocol*) al usar el UniFi gui con ubiquiti *Unifi Security Gateway* (USG)

1. Habilitar el servidor *Radius* (*Remote Authentication Dial-In User Service*), el, cual, se utiliza como demo para una conexión VPN, estos datos son los puertos que estarán configurados en ambos extremos al igual que el "*secret*" que es una clave que permitirá la conexión entre ambas.

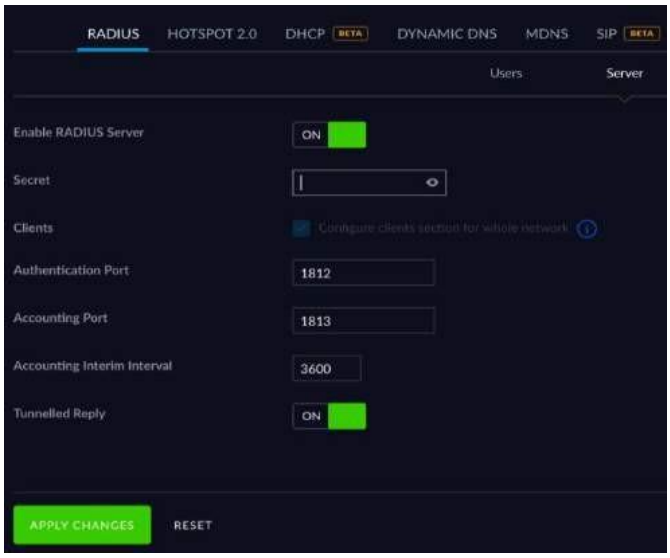


Gráfico 20: Sección *radius* del *router*

Fuente: elaboración propia

2. Crear un nuevo usuario y tomar en cuenta seleccionar el protocolo de túnel de 3 capas dos (L2TP) y Tipo medio de túnel: 1- IPv4 (versión IP 4)

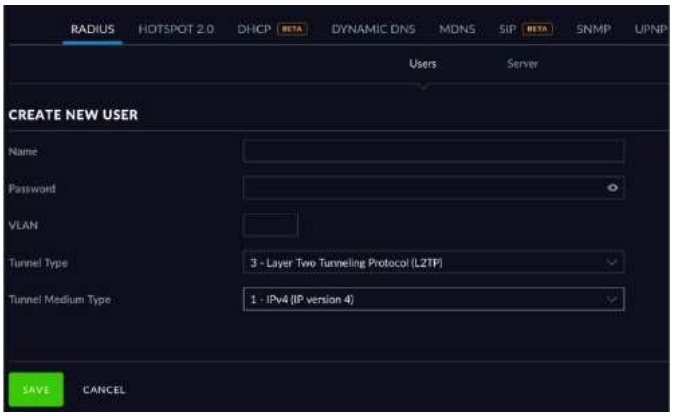


Gráfico 21: Sección *radius* del *router*

Fuente: elaboración propia

3. Crear una nueva red, en esta sección es necesario tomar en cuenta: tipo de VPN (en este caso L2TP), una clave alfanumérica para el ingreso, establecimiento de una máscara para un rango que sirve la puerta de enlace de la subred.

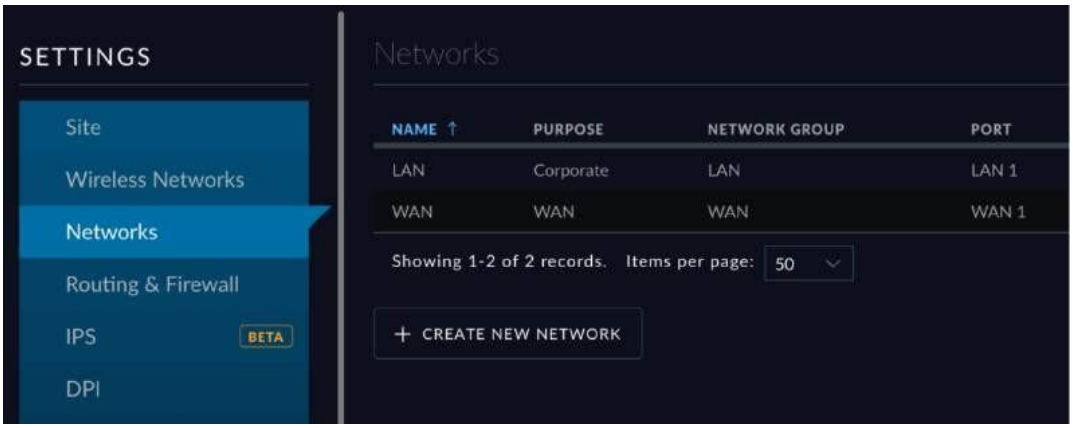


Gráfico 22: Interfaz de red del *router*

Fuente: elaboración propia

Configurar el cliente, en este último paso se determina el tipo: L2TP / IPSec (*Internet Protocol security*) PSK (*Phase Shift Keying*), dirección del servidor wan del firewall USG (*Unifi Security Gateway*), la clave previamente compartida IPsec ya establecida en el paso anterior.

Por lo tanto, las VPN proporcionan una solución excelente y rentable para que las empresas con varias sucursales, socios y usuarios remotos compartan datos y se conecten a su red corporativa de forma segura y privada.

Como la información de la red se transporta a través del internet los paquetes son detectados y leídos por cualquier persona. Sin embargo, el envío de datos a través de un túnel VPN encapsula todos los paquetes de datos que proporcionan un alto nivel de seguridad. Si los paquetes, que se enviaron de forma segura a través de Internet son interceptados, serían ilegibles y cualquier modificación sería detectada por la puerta de enlace VPN.

Cifrado del VPN

(Gani, 2011), indica que como parte del modelo de seguridad empleado en la red se utilizará el cifrado Asimétrico donde los usuarios del sistema poseen un par

de llaves desiguales, *Public Key y Private Key* las, cuales, matemáticamente están relacionadas donde la primera es usada para la encriptación y la segunda es utilizada para desencriptar la información de esta forma poder leerla.

La fuerza de este procedimiento es que *la Private Key* y *Public Key* del usuario están relacionadas, pero no es posible conseguir una llave con la otra. La *Private Key* se guardará como un secreto y se requiere buscar la *Public Key* en el repositorio público.

Al momento que el usuario A envía datos a un usuario B, el usuario A obtiene del repositorio la *Public Key* del usuario B y con esta encripta la información y la envía, el usuario B recibe la información y usa su *Private Key* para poder descifrar y leerla.

(Valle, 2014), denota que los sistemas simétricos basan su seguridad en el tamaño de la clave a aplicar, es decir, a mayor tamaño de la clave usada, mayor seguridad se otorga.

Es decir, que es un proceso de encriptación donde los usuarios del sistema usan la misma llave para encriptar y desencriptar la información. Por lo tanto, el usuario A y B poseerá la llave para poder encriptar y descifrar la información.

Alguno de los retos de este método es que tanto el que envía como el que recibe tendrá una llave la, cual, es cambiada con regularidad y los dispositivos necesarios tienden a ser engorrosos, además, de problemas de seguridad, si al receptor le es robada la clave el que envía no es informado de este suceso. Como ventaja se tiene que el poder computacional requerido es menor.

Ataque DoS (*denial of service*)

(Krishnan, 2017), expresa que para evitar un ataque DoS es necesario conocer a fondo el sistema operativo de la plataforma, limitar el acceso a la red (*firewall*), limitar el número de puntos de entrada (puertos), definir una política de seguridad interna (contraseñas, activación de archivos ejecutables) y hacer uso de utilidades de seguridad (registro).

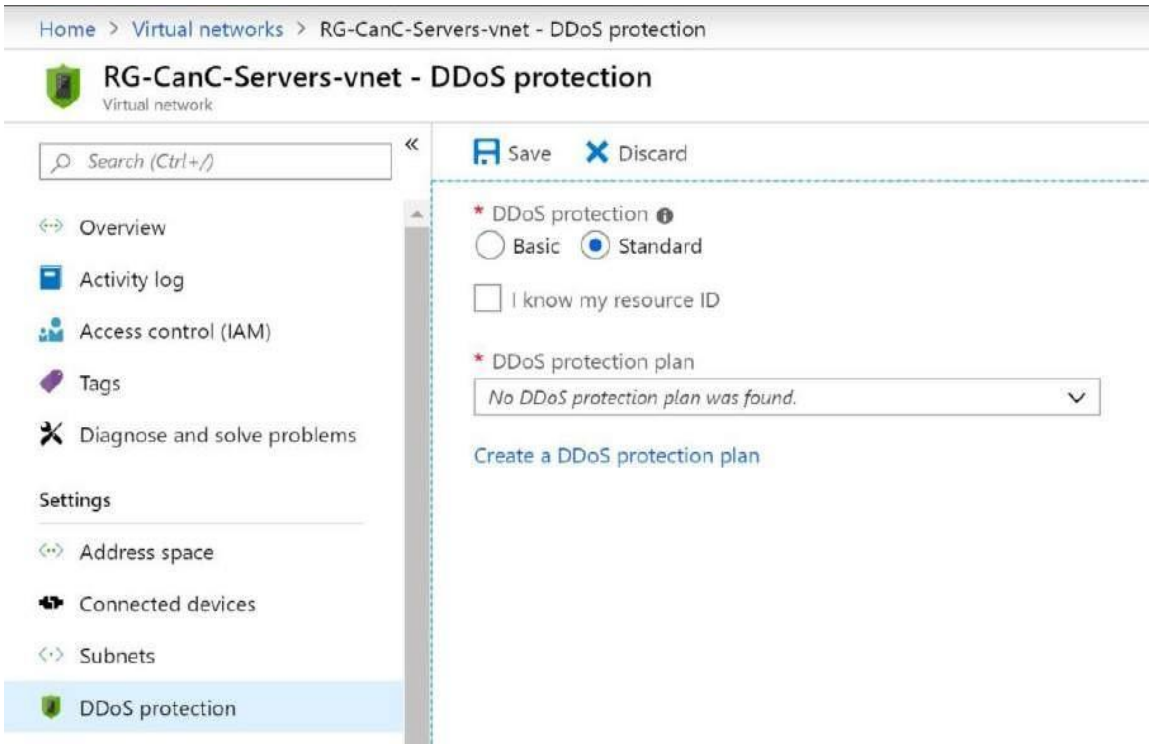


Gráfico 23: Interfaz principal del servicio de protección DDoS
Fuente: elaboración propia

En la imagen anterior se muestra la interfaz inicial de Azure DDoS *(Distributed Denial of Service*) que ofrece protección, supervisión y disminución automática de ataques de red que siempre estarán activas, mediante la limpieza del tráfico en el perímetro de la red de Azure.

Consejos para evitar un ataque DDoS

- Configurar *Routers* y *Firewalls,* que se encargan de: filtrar protocolos innecesarios, detienen IPs inválidas (Sistema Prevención de Intrusiones), incluso varios *firewalls* y *routers* proveen la opción de prevenir inundaciones (*floods*) en los protocolos TCP/UDP.

Se ejemplifica como configurar el *router* y firewalls:

1. Acceder al *router*, se tomará en cuenta la dirección IP de gestión, el nombre de usuario y la contraseña de acceso, mediante la consola cmd de *windows*.

Gráfico 24: Interfaz símbolo del sistema (cmd)

Fuente: elaboración propia

2. En el menú del *router* en la sección, virtual server la siguiente pantalla donde se ingresarán en el nombre del servicio de la aplicación, que se quiere cerrar, en la sección de protocolo en este caso sería TCP/UDP, en puerto interno y externo ingresar los de mayor vulnerabilidad, y si se desea configurar una IP interna y una de origen para seguridad adicional. Es recomendable realizar un *backup* de la configuración del *router*.

Gráfico 25: Interfaz del *router virtual server*

Fuente: elaboración propia

- Monitorear las conexiones TCP/UDP (*Transmission Control Protocol - User Datagram Protocol*), que se llevan a cabo en el servidor, como también se limitará las conexiones al servidor que converjan al mismo tiempo.

Se ejemplifica como monitorear los servicios de TCP/UDP en un *switch*:

1. Iniciar sesión en la web del *switch* y elegir seguridad y luego servicios TCP/UDP, con en la pantalla a continuación:

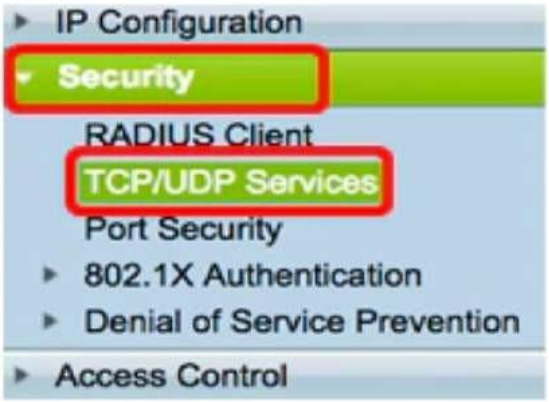


Gráfico 26: Interfaz del switch *sección seguridad*

Fuente: elaboración propia

2. En la siguiente tabla se muestra los servicios TCP donde se monitoreará los datos de servicios de acceso habilitados para observar si hay un establecimiento de conexión con internet confiable. Los más utilizados son:

- TCP — ofrece una conexión fiable entre hosts IPv4.
- TCP6: ofrece una conexión fiable entre los hosts IPv4 e IPv6.

TCP Service Table

Service Name	Type	Local IP Address	Local Port	Remote IP Address	Remote Port	State
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen
HTTP		10.10.100.106	80	10.10.100.105	54284	Time wait
HTTP		10.10.100.106	80	10.10.100.105	54352	Established
HTTP		All	80	All	0	Listen
HTTPS		All	443	All	0	Listen

Gráfico 27: Interfaz *switch* sección TCP *Service*

Fuente: elaboración propia

3. A continuación, se muestra los servicios UDP y monitorear los diferentes servicios de acceso habilitados actualmente para las conexiones UDP

UDP Service Table

Service Name	Type	Local IP Address	Local Port	Application Instance
	UDP	All	123	1
SNMP	UDP	All	161	1
	UDP6	All	546	1
Bonjour	UDP6	All	5353	1

Gráfico 28: Interfaz switch *sección UDP Service*

Fuente: elaboración propia

- Entrenar a los trabajadores de la organización para que estén preparados ante incidentes y ataques. Es importante acciones y planes para tener respuesta inmediata y acertada.

Tabla 5. Índices comunes en una organización.

Indicadores de Eventos	**Indicadores de Autenticidad del Usuario**
Constantes alertas de sistema de seguridad	Intentos fallidos del *Login*. Acceso autorizado
Caídas de los servidores	Compromiso del *Root*. Acceso autorizado
Constantes informes del software de antivirus	*Scanning* de puertos. Reconocimiento

Fuente: elaboración propia.

- Solicitar al Proveedor de Servicios de Internet (ISP), el bloqueo de tráfico para evitar que alcance a la organización.
- Los IDS/IPS (*intrusion-detection/prevention system*), estarán configurados adecuadamente por personal capacitado, de forma minuciosa, en lo posible se mantiene todas las herramientas actualizadas. Es importante llevar log de falsos positivos para reconfigurar las herramientas y mejorar su funcionamiento.

En la siguiente imagen se muestra el programa Suricata, software de pago, una herramienta IDS (Sistema de detección de intrusiones), que funciona como sistema de detección de intrusos, analiza los paquetes, solicitudes, peticiones, certificados en el tráfico de red.

Gráfico 29: Interfaz sistema detección de intrusiones

Fuente: (Alejandro, 2020)

Luego se observa uno de los *softwares* de pago más utilizados como herramienta IPS, *Botshield Interface* el cuál funciona como cortafuego tiene una alta capacidad de reacción ante incidentes, bloqueo automático frente a amenazas, disminución de falsas alarmas y optimización del rendimiento del tráfico.

Gráfico 30: Interfaz de usuario de *Botshield*

Fuente: (Services, 2020)

Protección contra *malware*

Para proteger el sistema es necesario contar con una protección Antivirus. Se empleará una protección antivirus y un *firewall* avanzado de amenazas (ATP), las ventajas de estos servicios son muchos, son más complejos como realizar bloqueos basados en geolocalización y reputación de IP (*Internet Protocol*), filtrar de forma inteligente direcciones IP de mala reputación para bloquearlas.

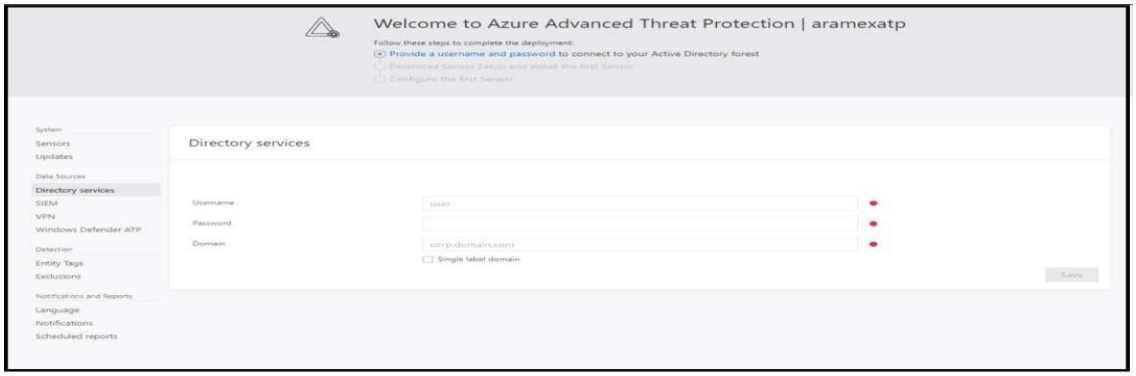


Gráfico 31: Portal de configuración de Azure

Fuente: (Microsoft, Microsoft Defender, 2020)

Algunas pautas para seguir son:

1. Eliminar la descarga de archivos de fuentes desconocidas o sospechosas.
2. Se evitará la instalación de programas o aplicaciones no autorizados
3. El equipo de seguridad elegirá un *software antimalware*/antivirus predeterminado para contrarrestar futuros ataques.
4. Evitar el uso compartido directo de discos con acceso de lectura y escritura.
5. Escanear siempre los medios extraíbles, (por ejemplo, discos flash USB, CDs, etc.) en busca de virus antes de usarlo.
6. El equipo de seguridad mantendrá un repositorio actualizado de solo lectura que contenga el *software antimalware*/antivirus predeterminado, sus definiciones de actualizaciones.
7. Se asegurará de que sus usuarios son conscientes de la amenaza y educarlos sobre cómo detectar y denunciar correos electrónicos sospechosos.

Gráfico 32: Virus WannaCry
Fuente: (Mejia, 2017)

En la imagen anterior se muestra *WannaCry*, que es uno de los virus de ataque informático de escala mundial más famosos.

2.2.4.2 Seguridad en entornos *cloud*.

Según (Rosero, 2012), la virtualización es un recurso lógico que es apoyado por servidores, dispositivos de almacenamiento y recursos físicos como memoria,

disco, CPU, adaptadores de red entre otros; y que son gestionados de forma dinámica, distribuidos a cada uno de los entornos o máquinas virtuales, que se configuren.

Los proveedores *de cloud computing* como Azure permiten utilizar estos recursos sin la necesidad de tener gran capacidad o recursos en hardware, se utiliza como un servicio de plataforma de acceso a la máquina virtual, esto es fácilmente visible en el entorno IAAS *(infrastructure as a service)*. (Gonzalez, Ballesteros, & Santamaria, 2015)

En este caso una vez configurada y tener lista la máquina virtual se tomará en cuenta el siguiente aspecto en cuanto a las medidas utilizadas en la seguridad:
Para restringir el acceso a una máquina virtual y que esta solo pueda ser accedida a través de RDP/SSH *(Remote Desktop Protocol – Secure Shell,* protocolos de conexión) una dirección o rango IP seguro los pasos a realizar son los siguientes:

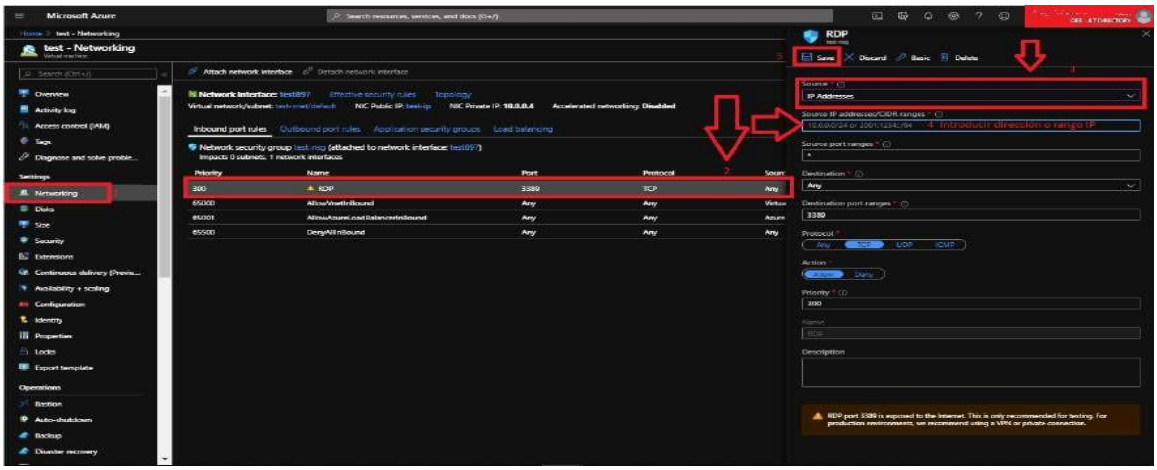


Gráfico 33: Interfaz Azure
Fuente: elaboración propia

Después de haber seleccionado la máquina virtual a la, que se le desea aplicar la restricción de seguridad se explica 5 pasos fundamentales para implementar el protocolo de seguridad.

1. Ir a la sección de red de la máquina virtual.
2. Seleccionar el protocolo, que se desea restringir (RDP / SSH).
3. En la sección Origen / Fuente -> Seleccionar IP *Address*
4. Introducir la dirección IP segura o el rango de IP
5. Guardar los cambios

2.2.4.3 Protección de datos en entornos *cloud*

Al tener la estación de trabajo en la plataforma y donde se encuentre alojada la web es recomendable asignar los permisos, de esa manera mitigar daños en el caso de que los datos del usuario sean comprometidos.

Según (Georgiou, 2017), expresa que la protección de datos comienza a otrogar privilegios a los usuarios y así evitar accesos innecesarios en las funciones, por lo tanto, no se usará una cuenta *root*/*admin*, si es suficiente una cuenta que posea permisos limitados para realizar las tareas requeridas. Una cuenta *root*/*admin* utilizará medios seguros como lo son conexiones cifradas SSH o IPSec (*Secure SHell*).

En el siguiente ejemplo se muestra como asignar permisos específicos a un usuario en una máquina virtual en Azure.

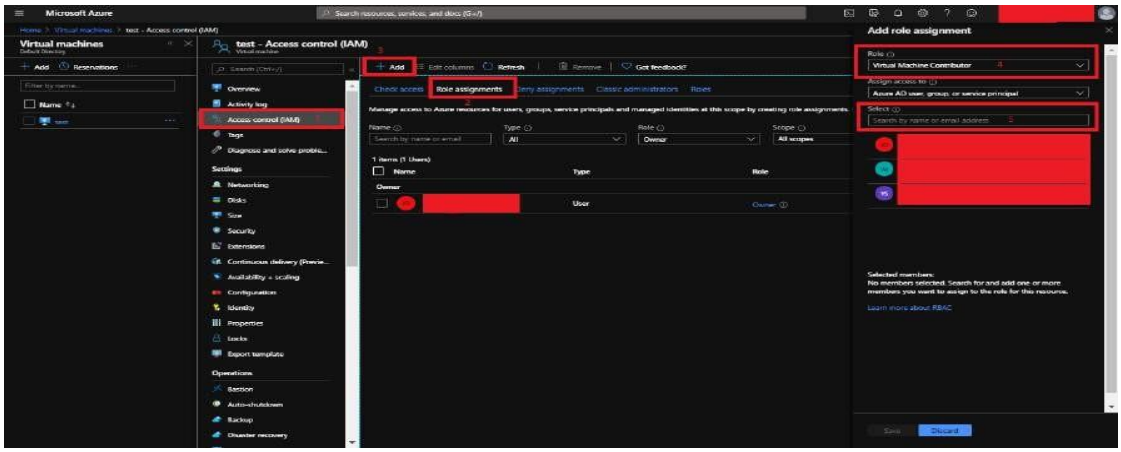


Gráfico 34: Interfaz Azure sección networking

Fuente: elaboración propia

Después de haber seleccionado la máquina virtual o recurso al, que se le desea asignar el permiso:

1- Seleccionar IAM (Administración identidad y acceso por sus siglas, que es la encargada de administrar el ingreso de los usuarios al sistema)
2- Asignación de rol (En la pestaña se muestra donde se registra a los usuarios que tienen permiso y acceso al sistema)
3- Añadir
4- Seleccionar el rol a asignar (se establece los parámetros de control del punto de acceso al sistema)
5- Seleccionar el usuario al, que se le desea asignar el rol (en esta parte el primer rol otorgado es el administrador de las cuentas de usuarios, es decir, permite añadir, eliminar o modificar las cuentas de usuarios)
6- Guardar.

Una vez creadas las cuentas es importante protegerlas se habilita capas de seguridad extra, en este ejemplo se observa cómo habilitar MFA *(multi- factor authentication*) desde el directorio activo de *Azure*.

El primer paso es seleccionar el directorio activo de *Azure* y luego usuarios.

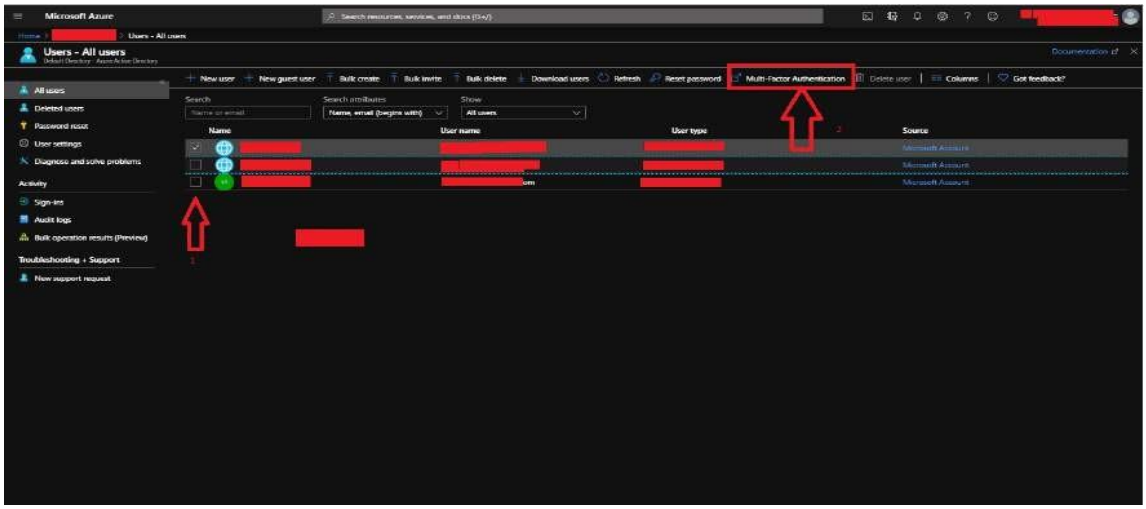


Gráfico 35: Interfaz Azure sección usuarios

Fuente: elaboración propia

1. Elegir el usuario a habilitar el MFA (que es el sistema de autenticación múltiple por sus siglas en inglés)
2. Seleccionar *multi-factor authentication,* en este caso se empleará desde contraseñas hasta generación códigos TOTP (Autenticación con contraseña de un solo uso por sus siglas en inglés). Una vez visto esto continuará en la siguiente pantalla:

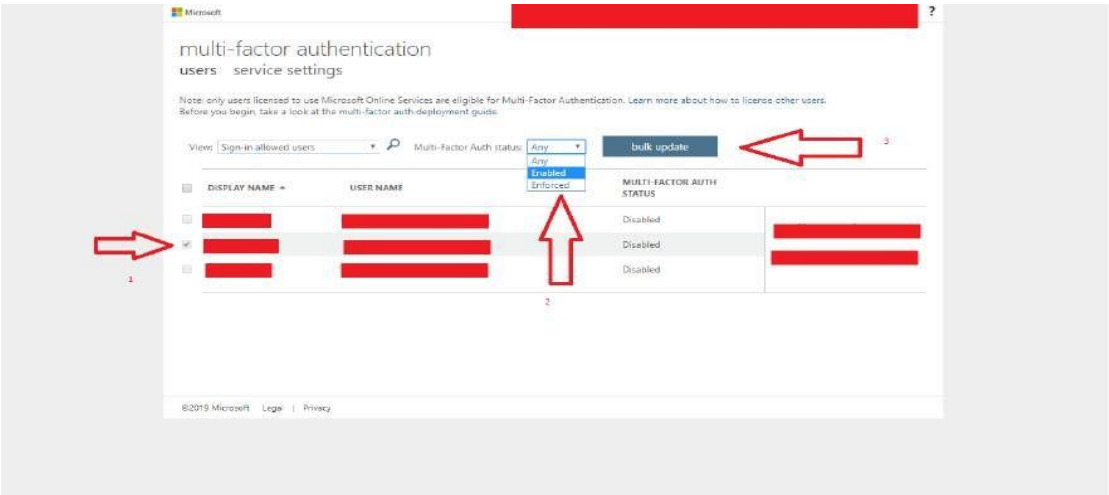


Gráfico 36: Interfaz Azure sección *networking* click *enable multifactor autentication*
Fuente: elaboración propia

- Seleccionar el usuario
- Habilitar el MFA para ese usuario.
- Actualizar la política

2.2.4.4 *Backup* y Recuperación de Datos

En esta sección se toma en cuenta el proveedor *Azure Backup* que una vez instalada la máquina virtual automáticamente se crea una copia de seguridad que luego lo identifica y lo transfiere a la sección *recovery services.*

Creación de un almacén de *Recovery Services*

En caso de crear una copia de seguridad de los datos se seguirá los siguientes

pasos:

1. Se selecciona todos los servicios

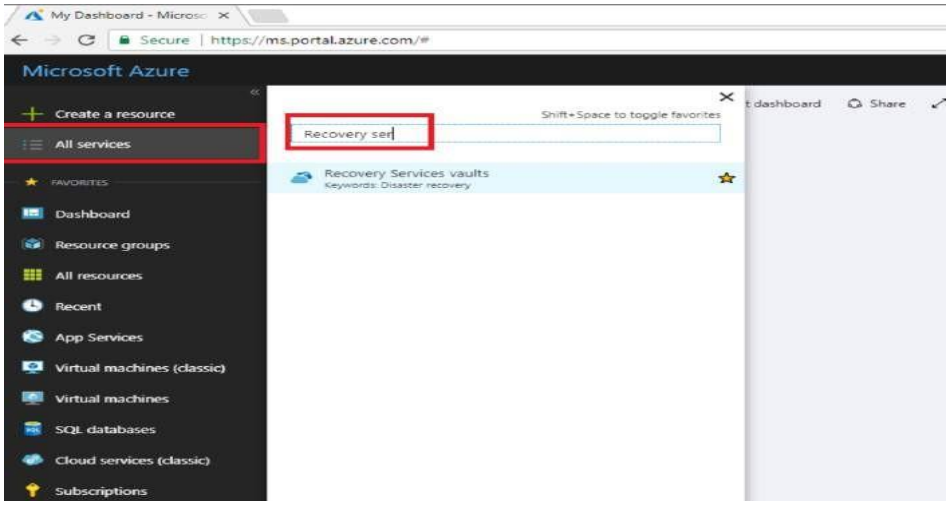


Gráfico 37: Interfaz Azure sección todos los servicios

Fuente: elaboración propia

2. En el menú de Almacenes se le da clic a agregar

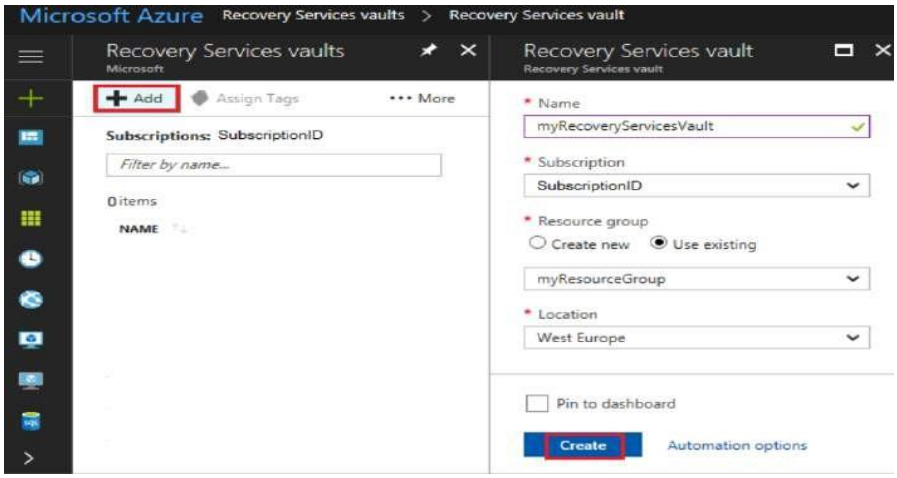


Gráfico 38: Interfaz Azure sección servicio

Fuente: elaboración propia

a. En el menú Almacén de *Recovery Services,* se escribe myRecoveryServicesVault en nombre. El id de suscripción actual aparecerá en suscripción. En grupo de recursos, se selecciona usar existente y se elige *myResourceGroup*. si no existe, se seleccionará crear nuevo. En el menú

desplegable ubicación, se elige el país. Y por último paso se crea el almacén de *Recovery Services.*

b. En la consola de *Recovery services*, se hará una copia de seguridad como respaldo

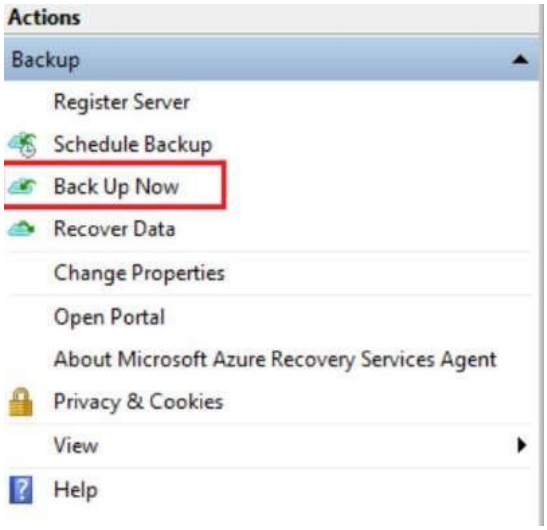


Gráfico 39: Interfaz Azure sección servicio copia de respaldo

Fuente: elaboración propia

2.2.4.5 Recomendaciones de uso y mantenimiento

Las recomendaciones generales en cuanto a la seguridad y autenticidad deberán tomarse en cuenta el modelo o entorno de prestación en la nube.

- Control de acceso, supervisión, detección y bloqueo de datos confidenciales mientras se está en uso, en movimiento y en reposo la plataforma.
- Emplear normativas de cifrado, IAM y MFA en cuentas de usuario, base de datos, administración y gestión del sistema
- Seguimiento y registro de actividad de cada usuario.
- Monitoreo continuamente de la red VPN
- Seguridad de los servicios obtenidos por los proveedores de *cloud*
- Realizar copias de seguridad de forma regular de los datos críticos y las configuraciones del sistema y almacenar los datos en un lugar seguro.
- Cambiar las contraseñas trimestralmente y que formen parte de la base de

datos de administración, ejemplo *Active Directory*.

- Al obtener sistemas nuevos deberán ingresarse con la gestión de contraseñas IAM en la base de datos global.
- Los usuarios autorizados manejarán el equipo de TI del proveedor, incluidos los dispositivos portátiles y los medios.
- El proveedor de *cloud* ejecutará una copia de seguridad diaria, semanal y mensual y la copia de seguridad mensual es un *backup* completo del sistema y la copia estará protegida mediante cifrado.
- Conservar mínimo tres generaciones de copias de seguridad

2.2.4.6 Términos y definiciones

- **Infraestructura:** Sistema, que se compone de recursos físicos y virtuales que admiten el flujo, el almacenamiento, el procesamiento y el análisis de datos. La infraestructura estará centralizada, o descentralizada.
- **IAAS (*Infrastructure as a Service*):** Provee como un servicio de los recursos de cómputo necesarios para la creación y configuración de la infraestructura de la empresa como son CPU, memoria *Ram*, cantidad y tipo de almacenamiento, dar flexibilidad y escalabilidad para crear servidores, máquinas virtuales. Estos alojan sistemas operativos, aplicaciones, etc.
- **IDS:** Es un sistema de detección de intrusos que revelan actividad sospechosa sobre un recurso informático.
- **IPS:** Son dispositivos encargados de revisar el tráfico de red, descarta o modifica los paquetes ante posibles ataques.
- **PAAS (*Platform as a Service*):** Proporciona facilidad para la ejecución y administración de aplicaciones, dar libertad al cliente de construir y administrar la infraestructura subyacente necesaria, pero tiene control sobre las aplicaciones desplegadas y las configuraciones de estas.
- **SaaS (*Software as a Service*):** Provee una aplicación que cubre una o varias tareas que la empresa desea realizar, se permite sacar de la ecuación todo el costo y peso que conlleva el armado y mantenimiento de

la infraestructura de hardware y software necesarios, al simplificar todo a sólo un modelo de suscripción.

- **Virtualización:** Es la creación de recursos tanto de software como de hardware de forma virtual o lógica, donde se crea una capa de abstracción independientemente de su estructura física y representa la base de diversos en la nube.
- **Azure:** Plataforma que ofrece servicios en la nube, su desarrollador es Microsoft. Se especializa en el almacenamiento y seguridad de base de datos, maneja los recursos y procesos, donde provee la virtualización de servicios, con Autoservicio bajo demanda, acceso a la red, pago por uso y otros servicios y ventajas.
- **ATP (*Advanced Threat Protection*):** Solución de seguridad basada en la nube que aprovecha las señales de *Active Directory* local para identificar, detectar e investigar amenazas avanzadas. En IAAS permite que los analistas encargados del nivel de seguridad atiendan ataques de protección de la infraestructura.
- **Firewall:** Elemento de seguridad de red que es hardware, software o ambos. Encargado de monitorear el tráfico de red entrante y saliente para decisiones sobre si bloquea o permite el paso del tráfico de información definido por un conjunto de reglas de seguridad.
- **Criptografía:** Es la creación de técnicas para el cifrado de datos. Se tiene como objetivo la confidencialidad de los mensajes. Una vez que los datos han pasado un proceso criptográfico, la información se encuentra cifrada. El criptoanálisis son los métodos para atacar el cifrado y obtener la información.
- **Biométricas:** Nace de bio (vida) y metría (medida), son métodos de reconocimiento, identificación y medición de personas con enfoca en su fisiología y características morfológicas únicas y diferenciadoras para fortalecer la seguridad al automatizar la captura y autenticación de parámetros biométricos.
- **RDP (*Remote Desktop Protocol*):** Es un protocolo propietario desarrollado

por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.

- **Plataforma:** Sistema que permite el funcionamiento y compatibilidad por la arquitectura, los sistemas operativos y el lenguaje de programación.
- **IAM (*Identity and Access Management*):** Sistema cuya tecnología se encarga de administrar el ingreso de los usuarios o individuos que forman parte de un colectivo, al identificar los datos de dichos usuarios, que pasan a ser parte del sistema y establece hasta qué punto tendrá acceso dentro de una compañía.
- ***Cloud computing*:** Servicio a través de Internet que proporciona recursos informáticos tales como infraestructura, plataforma y aplicaciones, sin que los usuarios tengan conocimiento y responsabilidad del funcionamiento de estos.
- **PKI (*Public key infrastructure*):** Garantiza la confidencialidad, autenticación, integridad de las transacciones electrónicas, se emite y derogar los certificados digitales, se sigue la política de seguridad pertinente, es un prestador de servicios de certificación, que lleva a cabo operaciones de criptográficas como el cifrado y la firma electrónica. (Toutchkov, 2019)
- **MFA (Autenticación de Factor Múltiple):** Gestionan la autenticación al seguir la directriz basada en la combinación de dos o más factores de autenticación: uno de ellos es el factor de posesión que es lo que el usuario posee y un factor inherente y único del usuario. Tradicionalmente reconocido como usuario/contraseña en alguna aplicación o sistema.
- **VPN (*Virtual Private Network*):** Tecnología de conexión encriptada a través de Internet desde un dispositivo a una red. La conexión cifrada ayuda a garantizar que los datos confidenciales se transmitan de forma remota con seguridad, evitado que la información enviada sea interceptada, modificada o robada. Es ampliamente utilizada en corporaciones.
- **Redes:** Sistema de dos o más computadoras que están vinculadas para compartir recursos, intercambiar archivos o permitir comunicaciones

electrónicas. Las computadoras en una red estarán conectadas a través de cables, líneas telefónicas, ondas de radio, satélites o haces de luz infrarroja.

- ***Private Key*:** También conocida como clave secreta, es una variable en la criptografía, que se utiliza con un algoritmo para cifrar y descifrar código. Las claves secretas solo se comparten con el generador de la llave, por lo que es muy seguro.
- ***Public Key*:** En criptografía, una clave pública es un valor numérico grande, que se utiliza para cifrar datos. La clave es generada por un programa de software o es proporcionada por un agente de confianza, designada a disposición de todo el mundo a través de un repositorio o directorio de acceso público.
- **SSH (*Secure Shell*):** Conjunto de utilidades y protocolos de red que ofrece una forma segura de acceder a un equipo ejecutar comandos y mover archivos de un equipo a otro. A través de una red, no segura, al proporcionar autenticación y comunicación cifrada de datos entre dos equipos a través de una red abierta, como Internet.
- ***Backup*:** Copia de los datos realizada para minimizar la pérdida de datos en caso de daños en los datos, ataques de malware, error humano. Una forma eficiente es que las copias de seguridad se realizan de forma regular para minimizar la pérdida de datos.
- **Códigos TOTP:** Contraseña de un solo uso, basada en el tiempo es un código de acceso temporal generado por un algoritmo que utiliza la hora actual del día como uno de sus factores de autenticación. Las contraseñas de un solo uso basadas en el tiempo se utilizan comúnmente para la autenticación de dos factores.
- **IPSec (*Internet Protocol Security*):** Conjunto de protocolos ampliamente utilizado para establecer el túnel VPN cuya función es asegurar las comunicaciones al ofrecer protocolos de capa superior con servicios de seguridad de red, incluido el control de acceso, la fuente de datos autenticación, cifrado de datos, etc.

2.2.5 Pruebas

En el capítulo III se documentará las pruebas de la siguiente manera:

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1 Evaluación general PYMES

Las normas ISO/IEC 27017 “Controles de Seguridad para servicios *Cloud*” detallan los controles importantes al momento de ofrecer un cumplimiento en el seguimiento de la calidad de las normas de autenticación.

- ✓ Protección y separación del entorno virtual del cliente.
- ✓ Configuración de una máquina virtual.
- ✓ Operaciones y procedimiento administrativos relacionados con el entorno *cloud*.
- ✓ Seguimiento de la actividad de clientes en la nube.
- ✓ Alineación del entorno de la red virtual y *cloud*.

El análisis presente se basa en la contestación de las preguntas básicas al planteamiento del problema del tema

¿Por qué se origina? El problema se origina porque las normas de autenticación se aplican en PYMES, y muchas de estas normas son necesarias, su problemática aborda distintas áreas de seguridad para las empresas, como lo es la seguridad en la información que protege en sí a los activos de la información en los negocios, así también como a su eficiencia en el trabajo.

¿Qué lo origina? Su origen es reciente gracias a la expansión de aplicaciones *Cloud Computing*, es necesario conocer el origen del *Cloud* como tal, su innovación constante ayuda a conocer las nuevas herramientas que salvaguardan la seguridad de la información en las empresas PYMES.

¿Cuándo se origina? Las normas de autenticación nacen con el problema creciente en la seguridad de la información, se requiere como tal integridad, confidencialidad y autenticación en el usuario.

Las PYMES de Ambato desconocen las medidas de seguridad y autenticidad de *cloud computing* como herramienta para sus empresas.

Se ha analizado en el presente trabajo la importancia del uso del *cloud computing* y así mismo demostrado los pasos, que se seguirán para el uso adecuado del registro, respaldo y mantenimiento de los datos de información.

Las normas de autenticación son necesarias, y mejoran en aspectos de seguridad informática, sistemas de la información y sobre todo cumplen con los estándares de calidad que una empresa (PYME) y como objetivo comprobar que las PYMES de Ambato desconocen las medidas de seguridad y autenticidad del *cloud computing*. El análisis denota los siguientes resultados:

- ✓ Los sistemas de *Cloud Computing* establecen soluciones a empresas pequeñas, medianas y grandes.
- ✓ Las normas de autenticación de *Cloud Computing* establecen un seguimiento de calidad en las PYMES basadas en normas internacionales ISO/IEC 27017 que brindan mayor seguridad y respaldo a la hora de administrar un sistema.
- ✓ En la presente investigación se demostró un amplio conocimiento en los entornos *Cloud Computing*.
- ✓ El *software* como servicio SaaS se demuestra que es el más utilizado a nivel empresarial, en comparación con los servicios IaaS y PaaS.
- ✓ El área administrativa de las PYMES conoce las ventajas que tienen los servicios de Cloud Computing en general.
- ✓ Se diagnóstica los resultados de la evaluación en base a las características de los sistemas utilizados, se conoce así sus ventajas.

- ✓ Según los datos de la encuesta en la investigación se demuestra que las PYMES en general tienen un presupuesto no mayor a los $5000,00 dólares anuales.

3.2 Cuadro comparativo de indicadores

Anteriormente mencionado se procede a realizar un cuadro comparativo de los indicadores que ofrece las ISO/IEC 27017 con los indicadores del proyecto, con el fin de sustentar el desarrollo del proyecto.

Tabla 6. Tabla comparativa

ISO/IEC 27017	**Guía Propuesta**	**Cumplimiento**
Quién es el responsable de lo que sucede entre el proveedor del servicio y el cliente		
La eliminación de activos sí un contrato se resuelve		
Protección y separación del entorno virtual del cliente	Protección y respaldos de información en entornos *cloud*	
Configuración de una máquina virtual	Configuración máquina virtual	
Operaciones y procedimiento administrativos relacionados con el entorno *cloud*	Sistemas de *Cloud Computing* establecen soluciones a empresas pequeñas, medianas y grandes.	
Seguimiento de la actividad de clientes en la nube	Vigilancia continua de la activad de los clientes en la nube	
Alineación del entorno de la red virtual y *cloud*	Vinculación entre entorno *cloud* y virtualización	

Fuente: elaboración propia

Los controles que ofrece la ISO/IEC 2017 y los controles de la guía propuesta, se llevó a cabo una tabla comparativa en la, cual, se toma en cuenta que, cinco de los controles de la guía propuesta se asemejen en su gran mayoría a los controles de la ISO/IEC 2017 por tanto la propuesta es viable para la aplicación en las PYMES de la ciudad de Ambato.

3.3 Validación técnica de IADOV

En el presente capítulo se analizan los resultados del proyecto en general, al llegar un término de conclusiones y recomendaciones, que se obtuvo en el proyecto.

Se realizó la técnica IADOV la, cual, permite validar la satisfacción de los usuarios finales con el producto propuesto, la misma que consta de cinco preguntas, tres cerradas y dos abiertas, da como resultado la complacencia del consumidor.

Tabla 7 Cuadro lógico IADOV

	P1) ¿Considera usted que la guía para implementación de seguridades en PYMES planteada satisface las necesidades para la Empresa?								
P3) ¿Cuál es su criterio sobre la guía para la implementación de normas de autenticación y seguridad en entornos *cloud* para PYMES?	NO			NO SÉ			SI		
	P2) ¿Utilizaría la guía propuesta?								
	SI	NO SÉ	NO	SI	NO SÉ	NO	SI	NO SÉ	NO
Me gusta mucho	1	2	6	2	2	6	6	6	6
Me gusta más de lo que me disgusta	2	2	3	2	3	3	6	3	6
Me da lo mismo	3	3	3	3	3	3	3	3	3
Me disgusta más de lo que me gusta	6	3	6	3	4	4	3	4	4
No me gusta	6	6	6	6	4	4	6	4	5
No sé qué decir	2	3	6	3	3	3	6	2	4

Fuente: elaboración propia.

El número proveniente de la relación de las tres preguntas expresa la escala de satisfacción del consumidor.

Índice de satisfacción individual (ISI).

- Clara complacencia
- Más complaciente que desagrado
- No definido
- Más desagrado que complaciente
- Claro desagrado
- Contradictorio

Participantes

A inicio del proyecto se obtuvo una muestra total de cincuenta personas a quienes se aplicaría encuestas, se tomó a los participantes y se aplicó la técnica IADOV, sin embargo, se obtuvo una participación de treinta y cuatro personas para realizar dicho procedimiento.

Análisis de resultados

El presente análisis está basado en las respuestas aplicadas al personal del área de TI las mismas se sometieron a la técnica de IADOV la, cual, permite validar la satisfacción de los usuarios finales, que se presenta a continuación.

Tabla 8: Respuestas a encuesta.

Personas	Columna	Fila	P1	P2	P3	ISI
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta más de lo que me disgusta	2	2	2	3
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	SI	Me gusta mucho	2	1	1	2

NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
SI	NO SÉ	Me gusta más de lo que me disgusta	3	2	2	3
NO SÉ	NOSE	Me gusta mucho	2	2	1	2
NO SÉ	SI	Me gusta mucho	2	1	1	2
NO SÉ	SI	Me gusta mucho	2	1	1	2
NO SÉ	NO SÉ	Me gusta más de lo que me disgusta	2	2	2	3
NOSE	NOSE	Me da lo mismo	2	2	3	3
NO SÉ	NO SÉ	Me gusta más de lo que me disgusta	2	2	2	3
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
SI	NO SÉ	Me gusta más de lo que me disgusta	3	2	2	3
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
NO SÉ	NO SÉ	Me gusta mucho	2	2	1	2
SI	NO SÉ	Me gusta mucho	3	2	1	6

Fuente: elaboración propia.

La imagen anterior demuestra el total de personas encuestadas, así como sus respuestas de tal manera, que se logra realizar la técnica propuesta, para obtener el valor final se realiza un procedimiento, que se mostrará más adelante.

Tabla 9: Procedimiento IADOV

	P1) ¿Considera usted que la guía para implementación de seguridades en PYMES planteada satisface las necesidades para la empresa?								
P3) ¿Cuál es su criterio sobre la guía para la implementación de normas de autenticación y seguridad en entornos cloud para PYMES?	SI			NO SÉ			NO		
	P2) ¿Utilizaría la guía propuesta?								
	SI	NO SÉ	NO	SI	NO SÉ	NO	SI	NO SÉ	NO
Me gusta mucho	1	2	6	2	2	6	6	6	6
Me gusta más de lo que me disgusta	2	2	3	2	3	3	6	3	6
Me da lo mismo	3	3	3	3	3	3	3	3	3
Me disgusta más de lo que me gusta	6	3	6	3	4	4	3	4	4
No me gusta	6	6	6	6	4	4	6	4	5
No sé qué decir	2	3	6	3	3	3	6	2	4

Fuente: elaboración propia.

Como indica la imagen es la valoración de la primera persona que respondió la encuesta enviada, además, la respuesta marcada con relleno color verde obscuro corresponde a las respuestas, así se procederá con todas las personas encuestadas para llegar a un resultado final que es la satisfacción del usuario con la guía propuesta.

El ISG tiene una escala en, cual, se posicionará el valor y sabrá la satisfacción el consumidor.

Tabla 10. Índice de satisfacción grupal (ISG)

Resultado	**Frecuencia**	**Escala**
Máxima complacencia	+1	A
Más complaciente que desagrado	0.5	B
No definido	0	C
Más desagrado que complaciente	-0.5	D
Máximo desagrado	-1	E

Fuente: elaboración propia.

Las respuestas obtenidas se aplicarán una fórmula, que se mostrará a continuación índice de satisfacción grupal (ISG). Se remplazará las incógnitas con los valores de la imagen para obtener el resultado.

$$ISG = \frac{A(+1) + B(+0.5) + C(0) + D(-0.5) + E(-1)}{N}$$

Tabla 11: Incógnitas

A	27
B	6
C	0
D	0
E	1

Fuente: elaboración propia.

$$ISG = \frac{3(+1) + 1(+0.5) + 0(0) + 0(-0.5) + 30(-1)}{34}$$

$$ISG = \frac{29}{34}$$

$$ISG = 0.85$$

El resultado obtenido la guía propuesta está en máxima complacía con un 0.85 de valor.

CONCLUSIONES

- Se indagó conceptos relacionados con el tema propuesto al considerar *cloud computing*, las pequeñas y medianas empresas. En la actualidad existe el avance tecnólogo el, cual, se aplica en la gran mayoría de empresas las, cuales, tienen entendimiento del concepto de computación en la nube, pero las PYMES al no tener presupuesto y falta de instrucción tiene miedo a la tecnología.

- Se realizó encuestas a los encargados del área de TI para obtener información de conocimientos de los entornos *cloud*, así como su aplicación. Se dio como resultado que la mayoría tenían entendimiento de *cloud computing,* sin embargo, no todos llegaban a comprender los beneficios que brinda este servicio, así como el temor al cambio, precio y falta de conocimiento de la implementación.

- Mediante la metodología cascada se realizó la guía propuesta al tomar en consideración varios puntos de esta, en lo, cual, se obtuvo un orden, que se seguirá para la implementación de normas de autenticación y seguridad para las PYMES en entornos *cloud*

- Para la validación se aplicó la técnica de IADOV para conocer el grado de satisfacción del usuario con respecto a la guía propuesta se logró un valor de 0.85 que significa que tiene clara satisfacción. Además, se realizó un cuadro comparativo entre la norma ISO/IEC 27017 e indicadores realizados en la guía propuesta donde se cumplió cinco sobre siete.

RECOMENDACIONES

- Continuar con el aprendizaje de las normas de autenticación y seguridad, así como las formas de vulnerar las mismas, de tal manera poder mitigar ataques en el futuro.

- Establecer procesos para el mejor manejo de información vulnerable de las distintas empresas a las, cuales, se puedan aplicar la guía, que se propuso en el tema investigación con el fin de mantener el uso debido de los archivos correspondientes a las distintas compañías, sociedades o industrias.

- Se recomienda a las empresas en general apoyarse a un manual de respaldo con base a las normas de autenticación, por todas las ventajas antes mencionadas y por todos los datos estadísticos (ver tabla 7), que el presente trabajo brinda de forma cuantificada y precisa. Así mismo se recomienda evaluar la necesidad de implementar una mejor seguridad de la información a través de normas de autenticación, estimar siempre costos y sobre todo calidad al momento de escoger un sistema o servicio Cloud Computing.

BIBLIOGRAFÍA

Academia.edu. (2009). academia.edu. Obtenido de academia.edu: Historia_de_la_seguridad_de_la_informacion

Alejandro. (04 de 2020). Protejer mi PC. Obtenido de https://protegermipc.net/2018/02/22/mejores-ids-opensource-deteccion-de-intrusiones/

Areba, J. (2001). Metodología del análisis estructurado de sistemas. Obtenido de https://books.google.com.ec/books?hl=es&lr=&id=PUqxsNVaQC8C&oi=fnd&pg=PA15&dq=Areba,+J.+(2001).+Metodolog%C3%ADa&ots=bLmzAAyzzD&sig=RI7sQlAoSzyvAgTgM0ON-2X2Of0#v=onepage&q=Areba%2C%20J.%20(2001).%20Metodolog%C3%ADa&f=false

Arenas, N. R. (2017). UNIVERSIDAD COMPLUTENSE DE MADRID. Obtenido de La contratación de servicios de cloud computing:.

ASEDESTO. (2019). asedesto. Obtenido de https://asedesto.com/Home.php

Bastar, S. G. (2012). Metodología de la Investigación. Obtenido de http://www.aliat.org.mx/BibliotecasDigitales/Axiologicas/Metodologia_de_la_investigacion.pdf

Blanchar, E. B., Portela, E. C., & Portela, N. C. (2015). Universidad de la Guajira. Obtenido de LA FUNCIÓN FINANCIERA EN LAS MICROS, PEQUEÑAS Y MEDIANAS EMPRESAS, DEL MUNICIPIO DE RIOHACHA: Dialnet-LaFuncionFinancieraEnLasMicrosPequenasYMedianasEmp-5200171%20(1).pdf

BSI. (18 de 07 de 2018). Norma ISO/IEC 27017 - Controles de Seguridad para Servicios Cloud. Obtenido de https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/

Bustamante, F. P. (24 de 7 de 2014). Universidad Santo Tómas . Obtenido de CLOUD COMPUTING COMO VENTAJA COMPETITIVA EN: http://www.laccei.org/LACCEI2014-Guayaquil/RefereedPapers/RP231.pdf

Centro Criptológico Nacional. (2017). Ministerio de hacienda y función pública. Obtenido de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

Chellapa, R. (17 de 04 de 2019). Holded. Obtenido de holded.com: https://www.holded.com/es/blog/historia-de-la-nube/

CLOUD SECURITY ALLIANCE. (2009). Guías de seguridad de áreas críticas en cloud computing V3.0. Obtenido de https://www.ismsforum.es/ficheros/descargas/guia-csa1354629608.pdf

Competencias e información especializadas en salud pública. (17 de 07 de 2018). Obtenido de Centro collaborador OMS de Québec para la promoción de la seguridad y prevención de traumatismos: https://www.inspq.qc.ca/es/competencias/seguridad-y-prevencion-de-traumatismos/centro-collaborador-oms-de-quebec-para-la-promocion-de-la-seguridad-y-prevencion-de-traumatismos/definicion-del-concepto-de-seguridad

Diaz, J. (13 de 07 de 2015). Negocios y Emprendimiento. Obtenido de Gestion de Procesos en mi PYME: https://www.negociosyemprendimiento.org/2015/07/gestion-por-procesos-en-mi-pyme.html

Gani, S. (2011). Cloud Computng & Securiy. Estados Unidos.

Georgiou, D. (2017). Security Policies for Cloud Computing. Rusia.

Gonzalez, J., Ballesteros, J., & Santamaria, F. (2015). Plataforma cloud computing como infraestructura tecnológica para laboratorios virtuales, remotos y adaptativos. Bogotá.

HEVIA M J, H. G. (2017). Herramientas útiles y métodos de búsqueda bibliográfica en PubMed: guía paso a paso para médicos no académicos. Revista Médica de Chile.

IBM. (24 de 06 de 2018). Autenticación de Usuarios. Obtenido de IBM Knowledge Center: https://www.ibm.com/support/knowledgecenter/es/SSANHD_7.6.0/com.ibm.mbs.doc/securgroup/c_authentication_users.html

Ionos. (07 de 05 de 2019). ionos. Obtenido de ionos.es: https://www.ionos.es/digitalguide/servidores/know-how/cloud-computing/

Krishnan, R. (2017). Security and Privacy in Cloud Computing. western Michigan University. Estados Unidos.

Logicbus. (18 de 7 de 2018). Obtenido de Cómo describir a una PyME: http://www.logicbus.com.mx/caracteristicas-pymes-tecnologicas.php

López, P., & Fachelli, S. (2 de 2015). METODOLOGÍA DE LA INVESTIGACIÓN SOCIAL CUANTITATIVA. Obtenido de https://ddd.uab.cat/pub/caplli/2016/163567/metinvsoccua_a2016_cap2-3.pdf

Maya, E. (2014). Métodos y Técnicas de Investigación. Obtenido de https://arquitectura.unam.mx/uploads/8/1/1/0/8110907/metodos_y_tecnicas.pdf

Mejia, J. (14 de 5 de 2017). SOLUCIÓN PARA EL VIRUS WANNA CRY: CONOZCA QUÉ ES Y CÓMO LIMPIAR EL MALWARE TIPO RANSOMWARE. Obtenido de https://www.juancmejia.com/temas-varios/solucion-para-el-virus-wanna-cry-conozca-que-es-y-como-limpiar-el-malware-tipo-ransomware/

Microsoft. (24 de 05 de 2005). Obtenido de https://technet.microsoft.com/es-ec/library/bb124839(v=exchg.65).aspx

Microsoft. (2020). Microsoft Defender. Obtenido de https://securitycenter.windows.com/

Ministerio de hacienda y administraciones públicas. (12 de 2014). GUÍA DE SEGURIDAD DE LAS TIC. Obtenido de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Seguridad y Privacidad de Información . Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G12_Seguridad_Nube.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2016). Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2016-2021. Obtenido de www.telecomunicaciones.gob.ec

Morales, A. (15 de 10 de 2015). ResearchGate. Obtenido de https://www.researchgate.net/profile/Aythami_Morales/publication/282858219_B

iometric_Student_Authentication_for_e-Learning_Platforms/links/561f8abb08ae93a5c9240bd2.pdf

Morejón, V. M., Acosta, M. d., Ávila, Ó. P., Cabrero, J. D., & Cabrera, H. M. (2014). MODELO DE NEGOCIO DE LAS MIPYME: UN. Obtenido de REVISTA INTERNACIONAL ADMINISTRACION & FINANZAS: ftp://ftp.repec.org/opt/ReDIF/RePEc/ibf/riafin/riaf-v7n3-2014/RIAF-V7N3-2014-3.pdf

ONTSI. (2012). Cloud Computing Retos y Oportunidades.

Orantes Jiménez , S. D., Aguillón Martínez, E., & Vázquez Álvarez , G. (2015). Computo en la Nube una opción para PYMES en Mexico. Obtenido de Instituto Politécnico Nacional, Centro de Investigación en Computación : http://www.iiisci.org/journal/CV$/risci/pdfs/CA565AE15.pdf

Portal, T. (17 de 12 de 2015). European Knowledge Center. Obtenido de Seguridad en la nube: ¿están sus datos protegidos?: https://www.ticportal.es/noticias/cloud-computing/seguridad-en-la-nube

Quintero, N. L., & Florez Fuente, A. S. (12 de 2014). Revista Mundo FESC. Obtenido de COMPUTACIÓN EN LA NUBE: Dialnet-ComputacionEnLaNube-5109245%20(1).pdf

R, K. (2017). Security and Privacy in Cloud Computing. western Michigan University. Estados Unidos.

Redondo, D. G. (30 de 11 de 2015). PUBLICATIC. Obtenido de ISO 27018: Cloud Computing: https://blogs.deusto.es/master-informatica/iso-27018-cloud-computing/

Reyna, J. E. (2009). Cloud Computing. Obtenido de http://campusv.uaem.mx/cicos/imagenes/memorias/7mocicos2009/Articulos/p11%20%20Cloud%20Computing.pdf

Richard Rojas, I. B. (2005). Ciclos de vida de Ingenieria del softare. Obtenido de https://www.academia.edu/8199293/Cascada-Modelo_V

Rosero, V. (2012). Estudio de tecnologías informáticas para asegurar la continuidad de servicios de sistemas computacionales mediante virtualización. Ecuador.

Sampieri. (2010). Metodología de la Invetihación . Obtenido de http://observatorio.epacartagena.gov.co/wp-content/uploads/2017/08/metodologia-de-la-investigacion-sexta-edicion.compressed.pdf

Sánchez, P. (14 de 6 de 2017). ESTUDIO ORGANIZACIONAL DEL. Obtenido de https://www.3ciencias.com/wp-content/uploads/2017/06/ART-1.pdf

Seguridad, F. d. (17 de 07 de 2018). Qué es la Seguridad . Obtenido de Foro de Seguridad: http://www.forodeseguridad.com/artic/discipl/4163.htm

Services, S. I. (2020). BOTSHIELD. Obtenido de http://www.botshield.de/en/info/

Torres, M., Paz, K., & Salazar, F. (2015). METODOS DE RECOLECCION DE DATOS PARA UNA. Obtenido de https://pdfs.semanticscholar.org/ba7a/d7cb67bf11712b324e90acef389b24a38e43.pdf?_ga=2.242005634.14765240.1590010063-1727444857.1590010063

Toutchkov, H. (2019). ¿Que es una PKI o infraestructura de clave pública? Obtenido de https://www.oodrive.es/blog/security/que-es-una-pki-o-infraestructura-de-clave-publica/

Trujillo, E. (2006). Diseño e implementación de una VPN en una empresa comercializadora utilizando IPSEC. Quito, Ecuador.

Valle, M. (2014). Análisis de métodos criptográficos para la gestión de firmas y certificados digitales dentro de un contexto de supervisión (SBS) para enfrentar los nuevos requerimientos de seguridad informatica. Quito, Ecuador.

VERIDOS. (2018). Identity Solutions . Obtenido de https://www.veridos.com/es/caracteristicas-de-seguridad

Zapata, I. (18 de 07 de 2018). Secura. Obtenido de Buscando el sistema de autenticación que mejor se adapta a la nube: http://www.redseguridad.com/especialidades-tic/cloud-y-data-center/buscando-el-sistema-de-autenticacion-que-mejor-se-adapta-a-la-nube

Zuluaga, S. (30 de 05 de 2015). elempresario. Obtenido de Estructura organizacional, clave del éxito para pymes: http://elempresario.mx/estructura-laboral/estructura-organizacional-clave-exito-pymes

ANEXOS

Anexo 1 Encuesta dirigida a departamentos de TI de las PYMES.

Título

Esta encuesta está dirigida a departamentos de TI de las PYMES.

Objetivo

Recopilar información del uso de las Tecnologías de Información y Comunicación (TIC), en relación con el *Cloud Computing* (CC) de las Pequeñas y Medianas Empresas (PYMES).

Instrucciones generales

•La encuesta a aplicar es de carácter investigativo, dirigida a gerentes, personal de la empresa y departamento de Tecnología de información (TI)
•Esta encuesta es un acercamiento de investigación educativa universitaria sobre aspectos importantes del uso de las TIC con relación a CC.

•Se agradece sus respuestas en el instrumento

•Se agradece colocar una X en el recuadro correspondiente

Cloud Computing

Datos de la empresa

Nombre o razón social de la empresa

Sector _____

Agricultura, Ganadería y Pesca	Información y Comunicación	Manufacturas	Suministro de Electricidad	Otras actividades de servicio
Construcción	Comercio	Transporte	Alojamiento	Administrativas
Actividades profesionales	Servicios	Enseñanza	Atención a la salud humana	Artes

P01.- ¿Conoce el concepto del *Cloud Computing* o Computación en nube?

P02.- La empresa contrata un servicio en la nube *Cloud Computing*

Pase a la P04

Si	No	No Contesta
Si	No	No

P03.- Describa tres motivos por las que no cuentan con un servicio de *Cloud Computing* (Fin de la encuesta)

……

……..……

……..……

P04.-La empresa en la que usted labora cuenta con alguno de estos servicios?

SaaS (Software como servicio)	
IaaS (Infraestructura como servicio)	
PaaS (Plataforma)	

P05.- Mencione algunos de los programas importantes que funcione dentro de la empresa, de acuerdo a la siguiente clasificación

Servidor Propio	**Servidor contratado**

P06.- Que áreas de la empresa cuenta con el servicio de *Cloud Computing*?

	Si	No	No contesta
Dirección/Gerencia			
Compras			
Talento Humano			
Producción			
Marketing			
Gestión de Riesgos			
Comercial/Ventas			
Administración			
Finanzas			
Contabilidad			
Tecnologías de información			

P07.- ¿Conoce las ventajas que tiene el servicio de

Cloud Computing **para su empresa?**

Si	No	No Contesta

P08.- ¿Cuáles son las principales ventajas que tiene la implementación de servicios en *Cloud Computing* para su empresa?

Alta disponibilidad		Seguridad	
Movilidad		Respaldo de información	
Ahorro de costos de infraestructura		Rápida implementación de aplicaciones	
Flexibilidad		Actualización automática de software	
Escalabilidad		Portabilidad	
Ahorro de costos de personal		Otros	

Cuales otros----------

P09.- Cuáles serían las principales desventajas que tiene la implementación de servicios de *Cloud Computing* en su empresa?

Problemas de ancho de banda		Mayores costos	
Depender de una conexión de internet		Problemas de confidencialidad	
Inseguridad		Falta de control de las operaciones	
Depender de un proveedor		Otros	

Cuales Otros

.....

P10.- Inversión anual en servicios en nube de su empresa

Menos de 5.000	
Entre 5.001 y 10.000	
Entre 10.001 y 25.000	
Más de 50.000	
No responde/Confidencial, Desconoce	

P11.- Percepción del nivel de madurez de la *Cloud Computing* de su empresa

Maduro	
En proceso de maduración	
Inmaduro	
No precisa	

Gracias por su colaboración

Anexo 2 Encuesta técnica IADOV

Título

Esta encuesta está dirigida a departamentos de TI de las PYMES.

Objetivo

Recopilar información sobre la satisfacción de la guía propuesta para las pequeñas y medianas empresas (PYMES).

Instrucciones generales

- La encuesta para aplicar es de carácter investigativo, dirigida al departamento de Tecnología de información (TI).
- Se agradece colocar una X en el recuadro correspondiente.
- Sus respuestas son totalmente anónimas
- Se agradece por su colaboración y tiempo.

P1 ¿Considera ud que la guía planeada satisface las necesidades para /con la empresa?

P2 ¿Utilizaría la guía propuesta?

P3 ¿Cuál es su criterio sobre la guía para la implementación de normas de autenticación y seguridad en entornos *cloud* para PYMES?

P4 ¿La guía es adaptable a la realidad de la organización?

P5 ¿Qué criterios creed ud que no cubre la guía?