UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

TEMA: “DISEÑO DE UNA ARQUITECTURA DE SEGURIDAD DE TI PARA CLOUD COMPUTING PARA UNA INSTITUCIÓN PÚBLICA DE LA PROVINCIA DE SANTA ELENA.”

AUTOR:

POZO ECHEVERRÍA EMILY JAZMÍN

MODALIDAD DE TITULACIÓN

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. WALTER OROZCO IGUASNIA

Santa Elena, Ecuador
Año 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez A., Mgtr.
DIRECTOR DE LA CARRERA

Ing. Walter Orozco I., Mgt.
TUTOR

Ing. Lídice Haz López, Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel S., Mgti.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por POZO ECHEVERRIA EMILY JAZMIN, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 2 días del mes de marzo del año 2023.

TUTOR

ING. WALTER OROZCO IGUASNIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Emily Jazmin Pozo Echeverria**

DECLARO QUE:

El trabajo de Titulación, "**Diseño de una arquitectura de seguridad de TI para cloud computing para una institución pública de la provincia de Santa Elena**", previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 2 días del mes de marzo del año 2023.

EL AUTOR

POZO ECHEVERRIA EMILY JAZMIN

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

En mi calidad de tutor del trabajo de titulación denominado "Diseño de una arquitectura de seguridad de ti para cloud computing para una institución pública de la provincia de santa elena", elaborado por el estudiante Pozo Echeverría Emily Jazmín, me permito declarar que una vez analizado en el sistema antiplagio COMPILATIO, luego de haber cumplido los requerimientos exigidos de valoración, el presente proyecto ejecutado, se encuentra con 2% de la valoración permitida, por consiguiente se procede a emitir el presente informe.


CERTIFICADO DE ANÁLISIS
magister

POZO_ECHEVERRIA_EMILY_Trab_Titulacion

2% Similitudes

3% Texto entre comillas
< 1% similitudes entre comillas
0% Idioma no reconocido

Nombre del documento: POZO_ECHEVERRIA_EMILY_Trab_Titulacion.docx
ID del documento: 957690458d81a663260b20792adc06cc5ce0d35e
Tamaño del documento original: 1,93 Mo

Depositante: WALTER ARMANDO OROZCO IGUASNIA
Fecha de depósito: 23/2/2023
Tipo de carga: interface
fecha de fin de análisis: 23/2/2023

Número de palabras: 12.918
Número de caracteres: 86.129

TUTOR

Ing. Walter Orozco Iguasnia

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

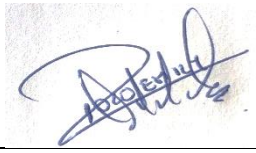
Yo, **Emily Jazmin Pozo Echeverria**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 2 días del mes de marzo del año 2023.

EL AUTOR



Pozo Echeverria Emily Jazmin

AGRADECIMIENTO

Agradezco a Dios por darme la fortaleza y permitirme llegar con éxito para culminar este proyecto investigativo. A mis abuelos que han sido como mis padres en todas las etapas de mi vida. A mi papá quien ha estado a mi lado brindándome su apoyo incondicional durante esta etapa. A mis amigos y compañeros que conocí durante este proceso, con quienes compartí conocimientos, supieron guiarme y apoyarme en el desarrollo académico. A los docentes que han sido guía para mi formación académica.

Emily Jamin Pozo Echeverria

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ANEXOS

RESUMEN

Actualmente, las instituciones públicas y privadas generan gran cantidad de datos ya sea como parte del proceso administrativo o del proceso de producción. El cuidado de los datos se convierte en una tarea básica, lo que exige la implementación no solo de infraestructura tecnológica sino también de procedimientos con el propósito de maximizar los niveles de seguridad. Cada día se evidencian las falencias de los mecanismos de protección de datos, lo que ubica a las instituciones en una situación de vulnerabilidad ante posibles ataques informáticos. Por medio de una de las metodologías de recolección de información aplicadas en la investigación se determina algunos de los problemas que se presentan en la infraestructura on - premise por el número de consultas en plataformas tanto web como de correo, en varias ocasiones existen sobrecargas causando interrupciones y fallas en las mismas, ocasionando retrasos en los trabajos del personal, de la misma manera el acceso no autorizado a información confidencial, falta de mantenimiento de los equipos, entre otros. Como solución se propuso el diseño de una arquitectura de seguridad de TI para cloud computing, en una de las instituciones de gobierno seccional, en base a las encuestas y entrevista para la recolección de información se reconocen los activos operativos, para la evaluación de la seguridad de la arquitectura actual. Se aplica el análisis de gestión de riesgos de los activos encontrados y por medio de la generación de matrices se determinan los vacíos de seguridad, amenazas y vulnerabilidades que se presentan en la actual infraestructura. A través del proceso de evaluación y análisis de riesgos se incluyen activos y medidas de seguridad adicionales para el diseño de la nueva arquitectura de seguridad. Finalmente, la arquitectura propuesta es simulada en la plataforma Docker ya que es una de las aplicaciones con características similares al migrar datos a la nube. La implementación de la arquitectura pretende minimizar el nivel de riesgo una vez implementada, además de aplicar estrategias y controles en base a las normativas ISO27001:2013 para el mantenimiento de un nivel bajo de los posibles riesgos presentados en cloud computing.

Palabras claves: análisis de riesgos, computación en la nube, controles ISO27001, Docker.

ABSTRACT

Currently, public and private institutions generate a large amount of data either as part of the administrative process or the production process. Data care becomes a basic task, which requires the implementation not only of technological infrastructure but also of procedures in order to maximize security levels. Every day the shortcomings of the data protection mechanisms are evident, which places the institutions in a situation of vulnerability before possible computer attacks. Through one of the information collection methodologies applied in the investigation, some of the problems that arise in the on-premise infrastructure are determined by the number of queries on both web and mail platforms, on several occasions there are overloads causing interruptions and failures in them, causing delays in the work of the staff, in the same way unauthorized access to confidential information, lack of equipment maintenance, among others. As a solution, the design of an IT security architecture for cloud computing was proposed, in one of the sectional government institutions, based on the surveys and interviews for the collection of information, the operational assets are recognized, for the evaluation of security. of the current architecture. The risk management analysis of the assets found is applied and through the generation of matrices the security gaps, threats and vulnerabilities that occur in the current infrastructure are determined. Through the risk assessment and analysis process, additional security assets and measures are included for the design of the new security architecture. Finally, the proposed architecture is simulated on the Docker platform since it is one of the applications with similar characteristics when migrating data to the cloud. The implementation of the architecture aims to minimize the level of risk once implemented, in addition to applying strategies and controls based on ISO27001:2013 regulations to maintain a low level of possible risks presented in cloud computing.

Keywords: risk analysis, cloud computing, ISO27001 controls, Docker.

INTRODUCCIÓN

En la actualidad la seguridad de la información se ha vuelto importante en las pymes debido al nivel de información que manejan, aun mas siendo una infraestructura on premise debido a que su implementación es poco óptima para la gestión de datos y procesos de administración, además que debe estar en constante mantenimiento para evitar interrupciones o perdida de información, por eso es circunstancial las medidas de seguridad necesarias para enfrentar eventualidades futuras ya que en la mayoría de veces ocurren de manera inesperada.

En el estudio de la institución pública como gobierno seccional existen varios riesgos tales como: la ausencia de procedimientos y controles sobre la gestión de seguridad de información, siendo una de las vulnerabilidades principales ante uno de los posibles riesgos de que los datos pasen a terceras personas. De cualquier manera, las instituciones corren el riesgo que sus datos sean vulnerados por la falta de métodos de protección de datos, errores causados por los mismos usuarios debido a la falta de capacitación y entrenamiento. Ante lo mencionado se propone el diseño de una infraestructura de seguridad informática para cloud computing para minimizar los riesgos y tener una mejor agilidad de los procesos y tareas administrativas durante la gestión de los empleadores mediante la aplicación de análisis de gestión de riesgos de la información.

Los trabajos relacionados a la propuesta uno de ellos consiste en; “Arquitectura de seguridad para la plataforma de computación en la nube” donde analiza la infraestructura en computación en la nube en la que proporciona un mejor acceso fluido a los servicios y aplicación que se ejecutan a nivel empresarial, el siguiente trabajo consiste en; “Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información” donde analiza los diferentes criterios de seguridad que son recomendados antes de hacer el contrato de servicio de cloud computing además de identificar el nivel de cumplimiento del mismo.

El trabajo de titulación está estructurado en dos capítulos;

Capítulo I, se describe la fundamentación compuesta por; los antecedentes que detalla los problemas presentados en el caso de estudio, la descripción del proyecto detalla las fases para la implementación de la propuesta, objetivos, justificación y la metodología MASI aplicadas en la propuesta. Capítulo II, se establecen los conceptos teóricos en el marco conceptual, las herramientas o recursos a utilizar más los componentes de la propuesta como son los requerimientos, otro apartado en este capítulo consiste en el diseño de la propuesta donde se describe las siguientes fases;

Primera fase el levantamiento de información consiste en considerar población y muestra no probabilística para la recolección de información, segunda fase, la evaluación de la seguridad del sistema actual, con los datos antes recolectados se realiza en análisis, evaluación y estimación de riesgos, tercera fase, diseño de la arquitectura del sistema de computación consiste en adicionar los nuevos servicios cloud computing que sean compatibles con la arquitectura actual de la organización, cuarta fase consiste en la simulación de la arquitectura de seguridad mediante la aplicación Docker y como última fase la evaluación de la nueva arquitectura de seguridad cloud computing, consiste en evaluar la arquitectura cloud computing por medio el análisis de gestión de riesgos, riesgos futuros que puedan surgir al migrar a la nube y aplicar estrategias para minimizar el número de riesgos.

CAPÍTULO I

1. Fundamentación

1.1. Antecedentes

Uno de los principales problemas que conlleva el empleo de una infraestructura On Premise en una institución es la falta de control sobre los datos. Mientras se usa herramientas locales, no se tiene ningún control sobre los datos, así, no se puede establecer un control oportuno sobre el acceso y uso adecuado de estos [1]. Otro aspecto que causa incertidumbre se centra en la falta de mantenimiento, dado que, el sistema se vuelve vulnerable a las amenazas de seguridad y problemas de rendimiento.

Se afirma que en las PYMES los errores comunes suceden al interior de las instituciones, por la poca valoración de los activos debido a la baja capacitación al personal de cada área. Algunas instituciones concuerdan que son altamente vulnerables a riesgos en seguridad de la información [2]. Desde este punto resalta la institución objeto de estudio, esta fue creada a raíz de la fundación de la provincia de Santa Elena. Está conformada por más de 70 empleados y su estructura la conforman 19 áreas dependiendo directamente del Ministerio del Interior. Dicha institución ha estado utilizando sus servicios On Promise, es decir, de manera local para sus necesidades de TI.

Mediante una observación estructurada se pudo determinar que la institución cuenta con una gran cantidad de equipos digitales, los mismos que están operativos en cada área, donde cada usuario tiene el acceso a las páginas locales y exteriores, evidenciándose una restricción leve sobre el acceso a otras páginas. Así, al no contar con un monitoreo y un registro adecuado, puede ser difícil detectar y rastrear la actividad maliciosa.

Con respecto a la seguridad de la red, los equipos están expuestos a cualquier riesgo debido al constante manejo de correos que están vinculados con las plataformas web, las mismas que son utilizadas para envíos de solicitudes entre áreas. Por ende, si la arquitectura local

no está protegida adecuadamente, las personas no autorizadas pueden obtener acceso físico a los sistemas y datos alojados dentro de la arquitectura, esto podría conducir a violaciones de datos u otra actividad maliciosa.

Sobre la situación de la institución, por medio de la entrevista realizada el usuario estratégico manifestó que no se cuenta con un servidor de dominio en el que se agilite la administración de las direcciones IP, no obstante, cuentan con el servidor local que le provee su ISP. Esto ocasiona una pérdida de tiempo al momento de hacer consultas de direcciones IP hacia el servidor local. Además, no existe una administración eficiente en cuanto qué páginas pueden ser visitadas por los usuarios de cada área, ya que el ISP es quien restringe el acceso en la institución. Un riesgo alineado a esto es que, las páginas, pueden estar sujetas a interrupciones o tiempo de inactividad debido a fallas de hardware o software. Esto puede ser un problema importante para las empresas que confían en que sus sistemas estén en funcionamiento en todo momento.

Se han revisado trabajos alineados a esta situación, donde, de una u otra manera, se aborda esta problemática mediante el empleo de arquitecturas de seguridad basadas en la nube, solventado así, los inconvenientes existentes de la arquitectura On Premise. A continuación, se analizan trabajos realizados en los siguientes ámbitos: mundial, regional y local.

Con respecto al ámbito mundial sobresale “Arquitectura de seguridad para la plataforma de computación en la nube” del Real Instituto de Tecnología de Suecia (KTH). Esta investigación se centró en el diseño de una arquitectura genérica y segura para las plataformas de computación en la nube, sin embargo, omite temas como tiempo de actividad de las operaciones, escalabilidad, e incluso, privacidad de los usuarios [3].

Un trabajo que resalta a nivel regional es “Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información”, desarrollado en la Universidad Católica de Colombia. Aquí se plantea solo un análisis de criterios de seguridad para generar recomendaciones al contratar e implementar

servicios de computación en la nube y no un diseño para evidenciar los aspectos importantes de la investigación [4].

A nivel local resalta “Análisis, Diseño e Implementación de Cloud Computing para una Red de Voz sobre IP” de la Universidad Politécnica Salesiana con sede en Cuenca [5].

En este trabajo se desplegó una nube privada para brindar el servicio de VoIP empleando Elastix como servidor y una instalación prototipo de OpenStack donde hubo inconvenientes acordes a la escalabilidad, limitando el procesamiento y almacenamiento de la información.

En conclusión, al analizar los trabajos anteriores, se evidencia que, existen limitaciones en el diseño de la arquitectura en torno a aspectos como seguridad y mantenimiento de la información, así como, el entendimiento, de parte de la organización o institución, sobre el ahorro de dinero en infraestructura de TI y costos de soporte. El propósito de este proyecto es desarrollar una arquitectura de seguridad para la computación en la nube que protegerá contra diversas amenazas. La arquitectura deberá tener en cuenta los diferentes tipos de implementaciones de computación en la nube (pública, privada e híbrida), así como los diferentes tipos de datos que a menudo se almacenan en la nube (por ejemplo, información personal, información financiera, etc.).

1.2. Descripción del proyecto

Debido a que se está evaluando la decisión de trasladar la arquitectura principal a la nube para proteger los datos gubernamentales y personales que la institución gestiona y de los que depende, aunque sea en genérico el caso de estudio al que se refiere es diseñar una arquitectura de seguridad que proteja estos datos de accesos no autorizados y usos indebidos. La arquitectura debe tener en cuenta los diversos riesgos asociados a la computación en nube, así como, adoptar las estrategias de prevención adecuadas.

El proyecto se desarrolla en cuatro fases, basadas en la metodología, Modelo de Arquitectura de Seguridad de la Información (MASI) [6]:

Primera fase. Levantamiento de Información.

Segunda fase. Evaluación de la seguridad del sistema actual.

Tercera fase. Diseño de la arquitectura de seguridad del sistema de computación.

Cuarta fase. Simulación de implementación de la arquitectura de seguridad.

1. **Levantamiento de información:** para esta fase se realiza las siguientes actividades.
   - Determinar la población entorno a instituciones públicas en la provincia de Santa Elena, siendo mi población los gobiernos seccionales (juntas parroquiales, municipio, prefectura).
   - Elaborar encuestas y entrevista para los dirigentes del departamento de TICs.
   - Determinar los servicios que lleva la institución como: sistemas web, sistemas de archivos, dispositivos compartidos en red, entre otros.
   - Analizar los resultados de la encuesta, determinando los aspectos físicos y lógicos de cada institución.

2. **Evaluación de la seguridad del sistema actual:**
   - Elaborar matriz para el análisis de riesgo con los activos que fueron encontrados en el levantamiento de información.
   - Determinar las brechas y los vacíos de seguridad que tiene la arquitectura.
   - Estudiar las amenazas, las vulnerabilidades, los ataques y los mecanismos de seguridad actuales.

3. **Diseño de la arquitectura de seguridad del sistema de computación:**
   - Comprender el funcionamiento de la arquitectura y los mecanismos de seguridad utilizados actualmente.
   - Elaborar matriz para el análisis de riesgo de los activos de computación en la nube.
   - Incluir medidas de seguridad adicionales, basadas en los resultados del estudio.
   - Analizar los posibles riesgos que se presenten al migrar los datos a la nube

4. **Simulación de implementación la arquitectura de seguridad**
   - Estudiar las nuevas tecnologías, las mejores prácticas para la simulación,
   - Realizar una simulación para la implementación de la arquitectura en este trabajo.
   - Proporcionar los recursos y servicios necesarios para las aplicaciones y servicios, así como cumplir con los requisitos de rendimiento y seguridad de la institución.
   - Implementar controles y estrategias para los riesgos presentados.

La arquitectura en la nube se diseñará para garantizar que el servicio esté altamente disponible, escalable y seguro, y, además, sea diseñada para minimizar el costo de ejecutar los servicios ejecutados dentro de la institución.

El diseño de una arquitectura de seguridad de TI para Cloud Computing se acopla a la línea de investigación de Tecnología y Sistema de la Información (TSI) en las organizaciones y en la sociedad, con el desarrollo del diseño de la arquitectura de seguridad de TI para una institución pública de la provincia de Santa Elena con el manejo de datos y amenazas de seguridad informática [7].

1.3. Objetivos del proyecto

1.3.1. Objetivo general

Desarrollar una arquitectura de seguridad informática para una institución pública de la provincia de Santa Elena mediante la aplicación de un enfoque administrativo de seguridad de la información.

1.3.2. Objetivos específicos

- Evaluar los riesgos de seguridad de las arquitecturas; on premise y cloud computing mediante la guía de la gestión de riesgo de seguridad de la información para establecer prioridades de seguridad en la institución pública.

- Diseñar una arquitectura de seguridad en la nube para la infraestructura de computación de la institución pública.
- Diseñar controles y procedimientos de seguridad para detectar y prevenir incidentes de seguridad a partir de las normas ISO27001.

1.4. Justificación

Los avances tecnológicos han cambiado drásticamente el funcionamiento de las empresas. En el pasado, las empresas almacenaban su información y datos importantes en servidores físicos u ordenadores. Sin embargo, esta ya no es la forma más segura de almacenar datos. La nube se ha convertido en el método de almacenamiento más popular para las empresas porque es más seguro y ofrece muchas otras ventajas [8].

La computación en la nube puede ayudar a las empresas a ser más ágiles y flexibles porque les permite aprovisionar e implementar rápidamente nuevas aplicaciones y servicios. Esto puede ayudarlos a responder más rápido a los cambios en el mercado o a las necesidades de sus clientes. La computación en la nube también puede ayudar a las empresas a reducir sus costos. Mediante el uso de servicios en la nube, las empresas pueden evitar la necesidad de invertir en hardware y software costosos. También pueden evitar la necesidad de contratar personal adicional para administrar estos recursos [9].

El diseño de una arquitectura basada en la nube para la institución pública a estudiar ofrece varias ventajas. Una de estas radica en el ahorro de espacio en los dispositivos, proporcionado copias de seguridad de sus datos. Así, la nube permite el acceso a los datos desde cualquier lugar y en cualquier momento sin ningún inconveniente. Para acceder a la nube, sólo se necesita un navegador web y una conexión a Internet, no es necesario descargar o instalar algún programa o software específico. Esta característica facilita a la institución a mantener relaciones comerciales y empresariales sin límites ni restricciones.

Al almacenar datos y aplicaciones en la nube, las empresas pueden permitir que los empleados accedan y compartan información desde cualquier ubicación. Por lo tanto, la computación en la nube permite a las organizaciones compartir recursos y experiencia con mayor facilidad, lo que lleva a una mayor colaboración y eficiencia. También permite a las organizaciones acceder a una gama más amplia de recursos y servicios, lo que puede impulsar la innovación y la competitividad.

Otro beneficio de la computación en la nube es la facilidad de acceso, siendo así, una gran ventaja para las empresas que quieren aprovechar la escalabilidad y la flexibilidad en sus procesos. Por esta razón, es importante diseñar e implementar una infraestructura de seguridad que proteja los activos físicos y lógicos de la empresa. Esta infraestructura de seguridad debe incluir medidas de seguridad tanto internas como externas. Internamente, las empresas deben implementar medidas de seguridad como cortafuegos y sistemas de detección de intrusos. Además, las empresas deben crear y aplicar políticas de seguridad estrictas. Externamente, las empresas deben hacer uso de servicios de seguridad como el cifrado y la autenticación de dos factores. Al aplicar estas medidas de seguridad, las empresas pueden ayudar a protegerse contra el acceso no autorizado, la pérdida de datos y las interrupciones del servicio.

El tema propuesto está enmarcado a los objetivos del Plan de Creación de Oportunidades 2021-2025, de manera específica se resalta:

Eje 2.- Eje social.
Objetivo 5.- Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [10].
Política 5.5.- Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [10].

1.5. Alcance del proyecto

El enfoque de este estudio es analizar y determinar los posibles riesgos a los que está expuesto la institución pública de Santa Elena y para migrar sus servicios a la nube se realiza

encuestas y entrevista como técnica de recolección de datos, además diseñar y proponer una arquitectura de seguridad más segura y simplificada para la institución, basada en el diseño y arquitectura actual.
A continuación, se describen las fases contempladas en la presente propuesta:

En la primera fase, se determina la población en relación con las instituciones públicas (gobiernos seccionales), se elaboran encuestas y una entrevista para el levantamiento de información, verificar en la parte operativa, los servicios que lleva la institución como sistemas web, sistemas de archivos, dispositivos compartidos en red, las características y sistema operativo de los servidores, paquetes y programas utilizados para el desarrollo y/o despliegue de estos.

Para analizar y determinar adecuadamente los posibles riesgos a los que se expone la institución pública al migrar sus servicios a la nube, así como para diseñar y proponer una arquitectura de seguridad más segura y simplificada, será necesario tener en cuenta y estudiar tanto los aspectos físicos como los lógicos. Para ello se incluirán aspectos implementados y probados en arquitecturas de seguridad de terceros, que servirán como ejemplo de funcionamiento e integración de los diferentes elementos que componen una arquitectura de seguridad completa y segura.

Segunda fase se realizará una revisión y evaluación de los activos, de los riesgos y de las consecuencias de las vulnerabilidades y amenazas a la seguridad en la organización. Esto incluirá un inventario de todos los activos, incluyendo hardware, software, datos y personal. Se identificarán y clasificarán todos los riesgos para determinar las consecuencias potenciales de cada vulnerabilidad y amenaza a la seguridad.

El análisis y estudio de la actual arquitectura de seguridad de la institución pública tendrá como objetivo comprender el funcionamiento de la arquitectura y los mecanismos de seguridad utilizados actualmente. Con base en esto, determinar las brechas y los vacíos de seguridad que tiene la arquitectura. Esto permitirá salvaguardar y garantizar la confidencialidad de la información de la Institución Pública (gobiernos seccionales).

La tercera fase de este proyecto consistirá en el diseño de una arquitectura de seguridad para la computación en nube. Esto incluirá la identificación de los riesgos de seguridad y las vulnerabilidades asociadas con el entorno de la nube, y el desarrollo de estrategias para prevenirlos, protegiendo los activos y los datos de la organización y que, al mismo tiempo, permita la flexibilidad y la escalabilidad, que son las ventajas de utilizar la computación en nube.
La arquitectura de la institución se utilizará como base para la arquitectura de seguridad del sistema de computación en nube. Esta será modificada para incluir medidas de seguridad adicionales, basadas en los resultados del estudio. Las modificaciones incluirán controles perimetrales mejorados, como un cortafuego, un sistema de detección de intrusos, un proxy, un proxy web, un equilibrador de carga, un servidor DNS y el traslado de los servicios web y el almacenamiento a la nube.

La cuarta y última fase de este proyecto consistirá en una simulación de implementación de la arquitectura propuesta, esta arquitectura de nube será capaz de manejar las cargas de trabajo de las aplicaciones y servicios dentro de la institución. No se añadirán más aplicaciones a los empleados de otras áreas que no sean las de sistemas, así mismos en tomar medidas como la gestión de vulnerabilidades y amenazas, así como en examinar el impacto de la seguridad del sistema.

También, se emplearán controles basados en metodologías de gestión de riesgos, donde se buscará establecer una estrategia de seguridad en la nube clara y completa que tenga en cuenta sus necesidades y objetivos específicos. Esto conllevará a evaluar los riesgos asociados con la nube para desarrollar un plan de prevención que permita abordarlos de forma adecuada.

1.6. Metodología

1.6.1. Metodología de la investigación

Para el desarrollo de esta propuesta tecnológica, se realizará una investigación exploratoria [11], con el fin de recopilar información de trabajos relacionados con el objetivo de realizar una infraestructura de seguridad informática en diferentes entidades, esto nos permitirá establecer comparativas que tengan una visión clara del alcance de cada uno y de la problemática a abordar.

Para conocer el proceso de diseño de infraestructura de seguridad informática en la institución y extraer información que nos permita ejecutar esta propuesta, se ejecutará el tipo de investigación diagnóstica [11], mediante la aplicación de las técnicas de entrevista y observación, esto nos ayudará a determinar los factores que contribuyen a la resolución de este objeto de estudio.

1.6.2. Población y muestra

La población ente de la propuesta la conforman los gobiernos seccionales que son ejercidos por los consejos provinciales, consejos municipales y las juntas parroquiales. Dentro de la provincia de Santa Elena comprende 3 consejos provinciales que conciernen a 3 consejos municipales y 7 juntas parroquiales tanto urbanas como rurales por lo tanto se tiene 10 instituciones públicas a nivel provincial. Se aplica el tipo de muestreo no probabilístico, mediante el muestreo por conveniencia simple se selecciona 5 de las instituciones como caso de estudio con características similares para el levantamiento de información.

1.6.3. Metodología de recolección de información

Para la recopilación de datos referentes al proceso en estudio se utilizarán técnicas de recolección de información cualitativas [12]. Se ejecutará la técnica de entrevista hacia el coordinador, usuario de nivel táctico responsable de TI (Anexo 2), donde se determinarán

la arquitectura de la seguridad de TI actual en la institución, así como, el funcionamiento y políticas establecidas para la protección de datos.

Además, se aplicará la técnica de observación dentro de la oficina de tecnologías de la información de la Institución, dónde se corrobora la información obtenida y se coordina los procesos del diseño (Anexo 1), de la misma manera se realiza encuestas para conocer las necesidades o problemas tecnológicos (Anexo 3).

1.6.4. Beneficiarios del proyecto

La solución tecnológica beneficiará directa e indirectamente a grupos que forman parte de la institución. Detallados mediante la siguiente tabla:

Tabla 1. Beneficiarios del proyecto

BENEFICIARIOS	
TIPO DE USUARIO	**USUARIOS**
U. Estratégico	Consejo municipal. Jefatura Política. Comisaría de Policía. Intendencia de Policía.
U. Técnico	Dpto. Administración financiera. Dpto. Asesoría jurídica. Dpto. secretaria general. Dpto. Planificación y gestión estratégica. Dpto. Comunicación social.

U. Operativo	Dpto. Tecnologías de la Información. Jefatura de área técnica.

1.6.5. Análisis de las técnicas de recolección de información

Análisis de entrevista realizada al usuario estratégico del área de TI de la institución pública, se realizó una entrevista con el objetivo de obtener información con el manejo de las tecnologías en la nube, información relacionada con la arquitectura de la red actual de la institución, sobre seguridad y políticas establecidas para la protección de datos.

En la encuesta realizada a los jefes de área de TI se pudo determinar que algunas de las instituciones no cuentan con un buen manejo de normativas o estrategias, políticas vigentes que no son aplicadas en su totalidad poniendo en riesgo la seguridad de datos con posibilidades de pérdidas de información, además de presentar algunos problemas en el área tecnológica entorno a la infraestructura on-premise. Aunque los empleados de rangos bajos estén en constante capacitación existen un porcentaje promedio de desconocimiento y practica sobre el manejo de la seguridad de la información, sobre la importancia de tomar ciertas medidas preventivas para minimizar el nivel de riesgo sobre los activos operativos dentro de la infraestructura de TI, ya que a diario las áreas circulan todo tipo de información para llevar a cabo determinada tarea ejecutiva.

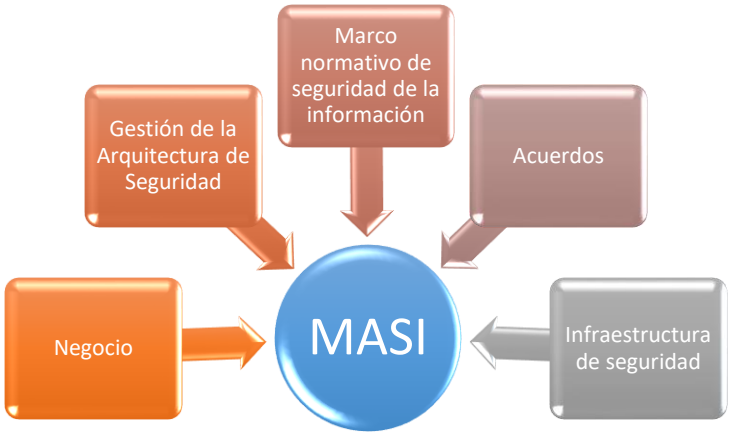
1.6.6. Variable

Nivel de cumplimiento y seguridad del servicio en el modelo cloud computing: Esta propuesta ofrece un diseño de una arquitectura de seguridad de TI en los servicios de computación en nube para cumplir este propósito se tiene como objeto la guía para la gestión de riesgo de seguridad de información que permitirá verificar el nivel de riesgo en la matriz general de riesgo a través del análisis entre la infraestructura On Promise y la infraestructura en Cloud Computing.

1.6.7. Metodología de desarrollo

La metodología utilizada en este proyecto es la metodología MASI (Figura 1), que es un enfoque integral de la seguridad informática que tiene en cuenta los diferentes aspectos de la seguridad, incluidos los aspectos técnicos, organizativos y humanos. Se eligió esta metodología porque se adapta bien a las necesidades de una institución pública de la provincia de Santa Elena, que tiene un presupuesto limitado y necesita un enfoque integral de la seguridad.

Figura 1. Metodología MASI



MASI [6], es una metodología para diseñar arquitecturas de seguridad informática. Se basa en el principio de seguridad por diseño, que aboga por la incorporación de consideraciones de seguridad en las primeras fases del proceso de desarrollo. La metodología MASI consta de cuatro pasos: (1) levantamiento de información, (2) evaluación de la seguridad del sistema actual, (3) Diseño de la arquitectura del sistema de computación, (4) simulación de implementación de la arquitectura de seguridad C.C. (5) evaluación de la seguridad de la arquitectura computación en la nube.

- **Levantamiento de Información:** En este paso, se obtendrán datos de los activos mediante las encuestas realizadas.
- **Evaluación de la seguridad del sistema actual**: En este paso, se identifican y se toman en cuenta los riesgos, e identificar las amenazas y vulnerabilidades.
- **Diseño de la arquitectura del sistema de computación:** En este paso, se diseñará la nueva arquitectura, en base a los datos recopilados anteriormente y considerando la seguridad de la información.
- **Simulación de implementación de la arquitectura de seguridad:** En este paso, se simulará la implementación de la arquitectura de seguridad Cloud Computing.
- **Evaluación de la seguridad de la arquitectura computación en la nube:** En este paso se identificarán los posibles riesgos e implantar estrategias o controles.

CAPITULO II

2. Propuesta

2.1. Marco Contextual.

2.1.1. Entidad Publica

Las entidades públicas como instituciones municipales, nacionales, educativas lideran y cumplen funciones administrativas ya que, por medio de planes estratégicos, planes de contingencia, programas, proyectos y demás recursos públicos permiten fomentar el desarrollo económico y social, fortaleciendo los cambios en las funciones gubernamentales. Además de conducir estrategias para la seguridad local en coordinación con otros organismos del estado [13].

2.2. Marco Conceptual

2.2.1. Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI consiste en el conjunto de políticas procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales. Actualmente las pymes como; estados, entidades bancarias, sociedades públicas y privadas conservan un gran porcentaje de datos e información, que son sistematizados en proceso manual o digital, el cual debe ser procesada de manera segura, por lo que se considera que las organizaciones aseguren y resguarden la información ante posibles riesgos que puedan surgir durante un proceso administrativo [14].

Por medio del SGSI se reduce o minimiza el riesgo de violación de datos ya que consiste en 3 principales características; confidencialidad, la afirmación no se pone a disposición ni se revela a individuos y entidades no autorizados, integridad, mantenimiento de la exactitud y completitud de la información y sus métodos de proceso, disponibilidad, acceso y

utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran [14].

Para la valoración y/o tratamiento del riesgo en el proceso de gestión de riesgo de la seguridad de la información puede ser iterativo, el enfoque iterativo provee un buen equilibrio en la reducción del tiempo requerido para identificar los controles, además garantizando que los riesgos de impacto alto se valoren de manera correcta. Para la gestión del riesgo de la seguridad de la información se realizan el siguiente proceso [15];

- Identificar los activos de información.
- Identificar las amenazas y las vulnerabilidades
- Identificar el riesgo.
- Analizar el riesgo.
- Determinar el nivel de estimación del riesgo.

2.2.2. Normas ISO 27001:2013

Las normas ISO son herramientas y disposiciones que se emplean en una organización para garantizar que los productos y/o servicios ofrecidos por dichas organizaciones cumplen con los requisitos de calidad del cliente y con los objetivos previstos. Las normas ISO 27001 ayuda a preservar la información, se ha demostrado que no es suficiente implantar controles y procedimientos de seguridad sin antes de haber un criterio establecido y sin considerar toda la información que se debe proteger. Además, aporta un Sistema de Gestión de la Seguridad de la Información [16]. La importancia de implementar las normas ISO 27001 es que permite a las empresas definir procesos de gestión de riesgos, para garantizar que la información este protegido, demostrando que es eficaz, mediante un proceso de gestión de seguridad de la información para determinar y revisar el análisis de los riesgos.

2.2.3. Computación en la Nube, Cloud Computing (CC)

Ofrece recursos de procesamiento como servicios por internet, elimina la necesidad de que las empresas obtengan o configuren recursos de más, permitiendo pagar solo por lo que usan. Es la evolución de un conjunto de tecnologías que afectan al enfoque a las empresas en cuanto a infraestructura de TIC, aquella tecnología que se puede utilizar cuando se necesite sin necesidad de instalación en infraestructura física. [1].

2.2.4. Arquitectura Cloud Computing

Nube pública. Es un servidor virtual fácil de implementar en una infraestructura on premise, de acuerdo a la carga de trabajo sus servidores automáticamente son escalables. Una característica importante es el modelo de pago por usar, implementación abierta y agilidad para compartición de recursos [17].

Nube privada. Los servidores y almacenamiento pueden ser agregados y escalados depende de la necesidad de la organización, una de las características es el costo fijo de implementación, el alto nivel de seguridad y hardware de uso [17].

Nube híbrida. Es la mezcla de ambas infraestructuras, dedicada y publica, puede ser una de las más dominantes puesto que posee la combinación de ambos modelos antes mencionados [17].

2.2.5. Modelos de Cloud Computing

Software como servicio, Software as a service (Saas). Se encuentra en la capa más alta en la que una aplicación se aloja como servicio para que los usuarios puedan acceder por medio de internet. La ventaja es cuando el software está alojado fuera del sitio el usuario no tiene que dar mantenimiento o soporte, además que se puede acceder a la misma aplicación con diferentes vistas [18].

Plataforma como servicio, Platform as a Service (PaaS). es la siguiente capa. Básicamente su objetivo es proporcionar un servicio de plataforma con lo necesario para

dar soporte al desarrollo de aplicaciones y servicios web, el usuario es el responsable de aprovisionar de la plataforma integral, por lo que no requiere mantenimiento de la infraestructura física y lógica [18].

Infraestructura como servicio (IaaS) corresponde a la capa baja, permite a los usuarios acceder a sus servicios como; el uso externo de servidores para base de datos, espacio en disco, evitando tener un servidor local e infraestructura de red física dentro de una organización [18].

2.2.6. Principales ventajas de Cloud Computing

Determinamos las ventajas de los servicios de computación en la nube frente al modelo On Premise [19].

Tabla 2. Ventajas de Cloud Computing

	On Premise	**Cloud Computing**
Costes	Invertir en equipos; hardware, software, además de copias de seguridad y actualizaciones del sistema.	Es rentable debido al modelo pay-per-use, quiere decir que se cancela depende de los recursos utilizados.
Mantenimiento	Los gastos los cubre la empresa debido a la infraestructura local como el centro de datos y servidores, depende del tamaño de la empresa es posible la contratación de un equipo de TI.	Los gastos antes mencionados (On Premise) recaen al proveedor de servicio de cloud computing.

Escalabilidad	Licencias adquiridas a largo plazo y con un nivel alto en costo.	Los recursos se pueden aprovisionar a los usuarios de manera elástica y liberar cuando ya no sean usados.

La aplicación de cloud computing comparado las alternativas de una adquisición de hardware y software como el método tradicional permite a las empresas reducir incidencias ya antes mencionadas en la (Tabla 2) de igual manera tiene sus pro y contra, mencionando: **Pro;** ahorro de inversiones para adquisiciones de infraestructura tecnológica, además de reducir costos para mantenimiento, actualizaciones de software rápida permitiendo acceder a la información y servicios desde cualquier lugar. La implementación es más rápida y con menos riesgos, ya que el pago es depende de la utilidad del servicio en la nube, en cuanto la escalabilidad que permite fortalecer a las organizaciones en los cambios que surgen en la demanda del mercado. **Contra;** la vulnerabilidad, debido que los proveedores de servicios en la nube son los que actualizan las medidas de seguridad informática, adicional que los servicios en la nube dependerán del servicio en línea [19].

2.2.7. Cloud DNS.

DNS permite almacenar direcciones IP y buscar por nombre ya que el mismo los asigna. Cloud DNS permite realizar los registros en el DNS y publicar las zonas sin necesidad de la carga de administrar los servidores y software DNS [20].

2.2.8. Cloud Proxy

Los datos que están almacenados localmente son transmitidos al servidor proxy, en el que cifra los datos antes de enviarlos por la red. Proxy maneja las operaciones criptográficas además de mantener las claves de manera interna o externa [21].

2.2.9. Cloud Firewall

Un cortafuego es la parte de una red informática que permite bloquear el acceso no autorizado y a la vez permite la comunicación autorizada. Firewall en la nube forman una barrera virtual ayudando a proteger la infraestructura local [22].

2.2.10. Load Balancer cloud

Balanceador de carga es un tipo de servicio que sirve de intermediario entre el workers y el tráfico de red, este permite distribuir el tráfico entre los nodos libres además atribuir una IP para dar acceso a los servicios [23].

2.2.11. El susbsistema de Windows para Linux, Windows Subsystem for Linux (WSL)

Para ejecutar un entorno Linux en un sistema operativo Windows, existe WSL que permite acceder al mismo tiempo. WSL permite a los desarrolladores ejecutar el entorno de GNU/Linux adicional las herramientas de línea de comandos y aplicaciones en el sistema operativo Windows, sin la necesidad de hacer alguna modificación o sobrecarga de una máquina virtual tradicional [24].

2.2.12. Docker

Es una plataforma de software donde permite crear, probar e implementar aplicaciones de manera eficaz, reduce el tiempo al usuario al momento de trabajar en configuraciones complejas. En cuanto a diferentes ventajas; asigna puertos, encargado de problemas que se presentan en el sistema de archivos y otras configuraciones, a la vez regularmente docker se actualiza con correcciones de errores y actualización de seguridad. Proporciona almacenamiento de software de manera estandarizada, una interfaz gráfica de usuario permitiendo administrar contenedores [25].

2.2.12.1. Contenedores Docker.

Los contenedores son formas de virtualizar, incluyen lo necesario para ejecutar cualquier cosa desde un microservicio a una aplicación de mayor tamaño, además de los ejecutables como; bibliotecas, herramientas de sistema, código y tiempo de ejecución [26].

2.2.12.2. Imágenes de Docker

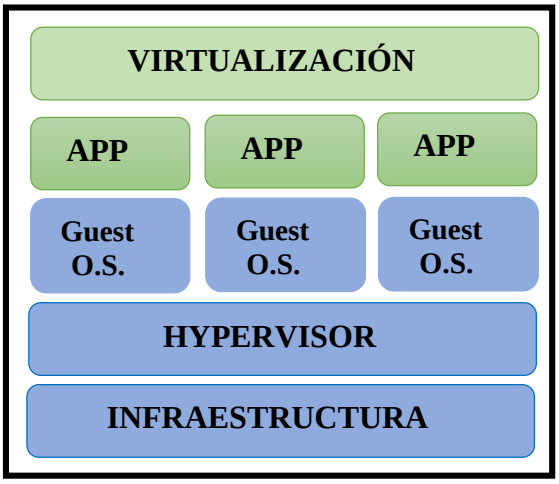
La imagen es una plantilla de solo lectura, una imagen contiene el código que se ejecutara. Tiene relación con los contenedores, ya que un contenedor es una imagen de Docker instanciada [27].

2.2.12.3. Volúmenes Docker

Ofrecen un almacenamiento persistente y gestionado por Docker, al momento de crear un volumen los datos se alojan en la maquina anfitriona. El volumen se monta como un directorio dentro del contenedor, ya que una de las ventajas que se pueden montar varios contenedores en un solo volumen con la posibilidad de compartir datos entre ellos [25].

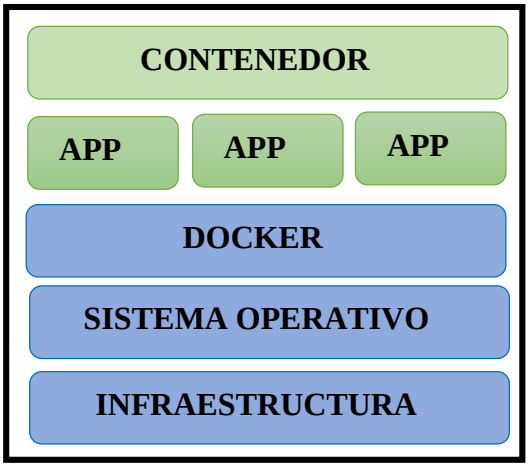
2.2.13. Diferencias Docker y Máquina Virtual

Figura 2. Capas de abstracción de una máquina virtual



Como se puede apreciar en la figura 2, la máquina virtual agrega más capas para la abstracción en la que baja el rendimiento, esto se debe a que se combina las dos para una mejor flexibilidad al ejecutar las aplicaciones [28].

Figura 3. Distribución de los contenedores sobre la plataforma Docker



En la figura 3, a diferencia de la máquina virtual, Docker usa las características del Kernel de Linux, para crear contenedores por encima del sistema operativo de esta manera automatiza el despliegue de las aplicaciones [28].

2.3. Marco Teórico

2.3.1. Importancia de políticas de seguridad informática de acuerdo con las ISO 27001 para pequeñas y medianas empresas del Ecuador

El articulo presenta lo importante que es el uso de las buenas prácticas informáticas por medio el uso de normas ISO 27001 en las PYMES, aplicando el uso de matriz de análisis de riesgos de TI para medir las vulnerabilidades informáticas. Recalca que es importante que las empresas realicen el análisis de las normas ISO27001, mediante la identificación de amenazas, riesgos, más la elaboración de políticas, de esta manera se podrán establecer las normas dando apoyo al diseño de políticas de seguridad informática, además garantizando la disponibilidad de la información dentro de la organización [29].

2.3.2. Análisis de las implicaciones de seguridad en la adopción del Cómputo en la nube para las PYMES

El artículo consiste en analizar los beneficios que tiene el uso del cómputo en la nube, analizar las condiciones y la relación que tiene con las PYMES. Durante la investigación determina que la computación en la nube influye a las organizaciones debido a nuevas necesidades operacionales que están asociadas con el gobierno de datos, política, seguridad y políticas en la sociedad. Además, determina que las PYMES muestran interés para conocer y buscar la posibilidad de aplicar la computación en la nube, debido a la preocupación sobre la seguridad de información que manejan, concientizando que les permite reducir costos, mejorar la flexibilidad y escalabilidad en adoptar sus datos a la nube [30].

2.3.3. Computación en la nube: infraestructura como servicio frente al modelo on premise

El trabajo investigativo muestra las ventajas, desventajas y los costos que se presentan ante la implementación de una infraestructura tradicional entre la implementación de una infraestructura de computación en la nube. Como resultado demuestra que la computación en la nube permite que los bienes o activos informáticos tradicionales se conviertan en un conjunto de recursos compartidos por medio de internet, considerando que diariamente a nivel gubernamental e institucional en varios ámbitos de la vida cotidiana se utilizan plataformas y servicios como principales recursos utilizados en grandes volúmenes de datos fortaleciendo el crecimiento de la computación en la nube [31].

2.4. Componentes de la Propuesta

2.4.1. Requerimientos

Objetivo Especifico	**Requerimiento del proyecto**
Evaluar los riesgos de seguridad de las arquitecturas; on premise y cloud computing mediante la guía de la gestión de riesgo de seguridad de la información para establecer prioridades de seguridad en la institución pública.	REQ01: Levantamiento de información mediante encuestas para identificar las características de infraestructuras de las instituciones.
	REQ02: Recolección de información sobre hardware, software e infraestructura interna del área de TIC.
	REQ03: Analizar los resultados de la encuesta para determinar los riesgos que existen actualmente en la infraestructura de la institución pública.
	REQ04: Evaluar los activos para determinar vulnerabilidades,

	amenazas y riesgos que presentan actualmente la organización.
	REQ05: Identificar los riesgos y determinar los vacíos de seguridad que presenta la actual arquitectura.
Diseñar una arquitectura de seguridad para la infraestructura de computación en la nube de la institución pública.	REQ06: Analizar la actual arquitectura de seguridad de la institución para comprender el funcionamiento y mecanismos de seguridad utilizados actualmente.
	REQ07: Diseñar la nueva arquitectura en la nube, modificando con nuevas medidas de seguridad.
	REQ08: Análisis de los activos cloud para determinar amenazas y vulnerabilidades futuras.
Diseñar controles y procedimientos de seguridad para detectar y prevenir incidentes de seguridad a partir de las normas ISO27001.	REQ09: Determinar los posibles riesgos de la arquitectura cloud computing.
	REQ10: Plantear controles y estrategias para disminuir los riesgos informáticos.

2.5. Diseño de la Propuesta

Fase 1. Levantamiento de Información.

Para concluir con la infraestructura se considera la información recolectada por medio de las encuestas que se toma como referencia a las instituciones públicas (gobiernos seccionales), además por medio de la entrevista se obtendrán datos como: sistemas de

archivos, ciertas características de dispositivos informáticos, sistemas web, programas de desarrollo, etc.

Fase 2. Evaluación de la seguridad del sistema actual.

Mediante la información recolectada se consideran todos los aspectos para la evaluación de la seguridad actual de la institución, para el análisis de gestión de riesgos se realiza la valoración de riesgo en la que consta de las siguientes actividades:

- Análisis del riesgo
    - Identificación del riesgo
    - Estimación del riesgo
- Evaluación del riesgo

Para el análisis del riesgo se identifica el riesgo en la que consta de las siguientes actividades:

- Identificación de los activos. Se consideran el sistema de información en la que consiste con los elementos de hardware, software, redes, personal, ubicación, estructura de la organización. además, se realiza una ponderación de activos (alto, medio o bajo). La valoración del impacto de un activo (VA) es el promedio entre los términos confidencialidad, integridad y disponibilidad (CID)

$$\boldsymbol{VA} = \frac{C+I+D}{3}$$

- Identificación de las amenazas. Se identifican las amenazas ya que tienden a causar daños a los activos.
- Identificación de vulnerabilidades. Se identifican las vulnerabilidades ya que estas pueden ser explotadas a causa de las amenazas.

Para la estimación del riesgo se identifican los riesgos, se analizan y se rigen bajo una escala de calificación (baja, media y alta), además de considerar los criterios de probabilidad de ocurrencia de amenazas, vulnerabilidades. El criterio de evaluación de riesgo según las normas ISO27001 se obtiene por medio de la probabilidad de ocurrencia de amenaza y vulnerabilidad y el valor de impacto del activo (CID)

Nivel de riesgo = VA(CID) * nivel de amenaza * nivel de vulnerabilidad

Nivel de riesgo	
1 - 3	**Bajo**
4 – 8	**Medio**
9 – 27	**Alto**

Figura 4. Nivel de riesgo

Para el tratamiento de riesgo se realizan decisiones enfrentando los riesgos existentes, considerando la reducción, aceptación, evitación o transferencia del riesgo.

Fase 3. Diseño de la arquitectura del sistema de computación

Para el diseño de la arquitectura se considera la arquitectura actual de la organización para hacer compatible con los nuevos servicios en la nube. Sobre el almacenamiento de datos se tiene el servidor de base de datos, para las reglas y normativas de entrada y salida de datos el servidor firewall, servidor proxy para el administrador siendo como punto de control de acceso de los usuarios a las aplicaciones web y recursos en la nube, servidor DNS para la administración y asignación de dominios, servidor web para las plataformas web de la institución, servidor VPN para monitoreo o configuración de los dispositivos on premise de la organización.

Fase 4. Simulación de implementación de la arquitectura de seguridad.

Se toma como referencia la aplicación Docker para la simulación ya que tiene algunas características similares que se encuentran en una plataforma en la nube, tales como; los contenedores, redes, volúmenes, e imágenes.

Fase 5. Evaluación de la seguridad de la arquitectura computación en la nube.

Se consideran la información existente actualmente, por lo tanto, retomando los activos de cloud computing en la infraestructura anterior, se procede aplicar la misma metodología de análisis de gestión de riesgo debido a las probabilidades de riesgos que pueden surgir al migrar a la nube.

Se tiene varias cualidades para identificar los vacíos de seguridad de la información; la información crítica, sensible y además de los riesgos.

Enlistamos los activos en la matriz del inventario de activos, para luego analizar los riesgos. Para identificar los riesgos se identifican los activos, en este caso los servidores en cloud computing, de la misma por medio de la valoración del activo, se determina el CID. Además de analizar las amenazas y vulnerabilidades de consideran la estimación de riesgo, por lo tanto, se consideran los siguientes riesgos:

El riesgo del cumplimiento normativos, determinar si la organización cuenta con algún documento donde especifique normativas que protejan la seguridad e integridad de los datos de la institución.

En caso de que no cuenten con estas normativas o no tengan conocimiento del mismo. Se procede al análisis de gestión de riesgo para culminar estableciendo normativas en base las ISO27001.

Evaluación del riesgo, se debe analizar los activos afectados, el nivel de probabilidad, nivel de riesgo. Luego considerar los riesgos técnicos, las que se encuentran en un ambiente cloud computing como son; intercepción de datos, perdida de datos, perdida de claves, virus malicioso, determinar la probabilidad que estos riesgos sucedan en caso de que sucedan pueden ocasionar algún impacto en la administración u operación de la institución.

Para el tratamiento de los riesgos, en base a las normas ISO27001 el riesgo puede ser mitigado, aceptado, o evitado considerando que el riesgo no puede ser descartado en su totalidad. Para ellos los riesgos deben ser analizados y controlados debido a las vulnerabilidades y amenazas que los afectan.

2.6. Resultados

Considerando el número de usuarios, el tamaño y la actividad de la empresa se determina el número de servidores y la dimensión de su instalación. Como metodología de recolección de información se realiza encuestas, la misma que está dividida en 4 secciones; información general, seguridad de TI, redes, software. Entonces por medio de la encuesta que se realiza al muestreo no probabilístico a las 5 instituciones públicas, como 1era sección de la encuesta; se comprueba el número de trabajadores, en la sección de seguridad de TI; en la 2da pregunta se determina que tres de las instituciones no cuentan con un documento oficial sobre las políticas de seguridad de información, la 4ta institución poseen el documento pero no son aplicados en su totalidad y 5ta institución si cuenta con un documento vigente, con respecto a la 3era pregunta sobre el análisis de gestión 4 de las instituciones no aplican el análisis de gestión y la 5ta institución aplica el análisis de gestión de seguridad de la información.

La 4ta pregunta consiste en determinar los principales problemas que tiene la empresa en las áreas de tecnología asociadas a la seguridad de información,

Tabla 3. Resultados de encuesta

	Institución A	**Institución B**	**Institución C**	**Institución D**	**Institución E**
Redes y cableado estructurado.	**X**	**X**	**X**	**X**	
Mantenimiento de plataforma web.	**X**	**X**	**X**	**X**	

Administración de servicios electrónicos.	**x**	**x**	**x**		**x**
Administración de firewall de seguridad.	No existe	No existe	No existe	Administrador ISP	Administrador ISP
Administración de base de datos	**x**	**x**	**x**	**x**	
Mantenimiento de los equipos TIC.	**x**	**x**	**x**		
Redes inalámbricas	**x**	**x**	**x**	**x**	**x**
Seguridad informática	**x**	**x**	**x**	**x**	**x**
Virtualización de servidores	No existe	No existe	No existe	No existe	No existe
Mantenimiento de dispositivos de redes: router, switch, etc.	**x**	**x**	**x**	**x**	

Se tiene como resultado de 5 de las instituciones responden que tiene problemas sobre: seguridad informática, de la misma manera no cuentan con virtualización de servidores, 4 de las instituciones tienen problemas en las redes y cableado, mantenimiento de plataformas web, baja administración de servidor de base de datos y mantenimiento de dispositivos de redes. 3 de las instituciones no cuentan con un servidor firewall de seguridad, de las 2 instituciones que posee un servidor firewall pero es administrado por su ISP, y la otra institución cuenta con el respectivo mantenimiento regular pero aun así tienen

problemas cuando todos los usuarios acceden a las plataformas digitales causan sobre carga de consultas en plataformas web y de gestión, también cuenta con 1 servidor firewall local por lo que están expuestos a posibles ataques cibernéticos.

En la sección de redes se obtiene los siguientes resultados; la 5ta pregunta que consiste en determinar las redes, servicios y topología de red. El tipo de red, 4 de las instituciones poseen red LAN, 1 de las instituciones trabaja con red LAN y MAN, en cuanto al tipo de servicio las 5 instituciones solo cuentan con IaaS que es otorgado por su ISP, en cuanto a topologías de red las 5 instituciones trabajan con topología estrella.

En la sección de software: como última pregunta consiste en conocer software de código abierto que posee la institución, las 5 instituciones trabajan con aplicaciones ofimáticas, cuentan con sistemas operativos W10 y linux, 3 de ellas aún utilizan W7, en cuanto a servidores web 4 de 5 instituciones no cuentan con servidor de correo, proxy, DNS y web, solo una institución posee servidor de correo local, y los servidores web y DNS lo mantiene bajo su ISP.

Fase 1. Levantamiento de Información.

Luego de obtener los resultados de las encuestas se pasa a realizar el inventario de activos, para identificar los activos de acuerdo a su valor, depende de aquello se determina o se asocia al riesgo. Para identificar los activos se realiza la siguiente matriz.

Tabla 4. Inventario de Activos

Nro. de Activo	Tipo de activo	Cantidad	Nombre de activo	Características
A1	Hardware	27	Equipo de escritorio	HP. Cpu Celeron 2.8GHz 4 Ram - 500Gb
A2	Hardware	2	Laptop	LG. Cpu Celeron 2.8GHz 4 Ram - 500Gb
A3	Hardware	7	Impresora	Epson L5290, Epson L375, Epson L310
A4	Sofware	1	Sistema de gestión documental	Sistema de Gestión Documental Quipux
A5	Hardware	1	UPS	UPS Forza
A6	Hardware	1	GPON	8 SFP
A7	Redes	7	Router WAN	TP-LINK TL-WR840N
A8	Redes	1	Cableado estructurado	Cable UTP CAT 6
A9	Redes	1	Switch Capa 3	Cisco Catalyst Administrable L3 24 puertos
A10	Redes	1	Switch Capa 2	Cisco Catalyst Administrable L2 48 puertos
A11	Redes	1	Switch No Administrable	Hikvision DS-3E0510P-E/M
A12	Hardware	2	Servidor	Intel Xeon, HDD 500GB, 8 RAM

Después de tomar en cuenta los activos que actualmente están operando en la institución se procede a la valoración de cada activo, depende del valor total que sume el CID (confidencialidad, integridad y disponibilidad) entre un rango de 1 - 3

Tabla 5. Valoración del Activo

Nombre de activo	Descripción de activo	C	I	D	Valoración del activo
Equipo de escritorio	Computadora personal para estación de trabajo.	3	3	3	3,00
Laptop	Computadora personal para estación de trabajo.	3	3	3	3,00
Impresora	Es un dispositivo que permite producir en formato físico un documento almacenado en un formato electrónico.	2	1	1	1,33
Sistema de gestión documental	Permite registro, control, flujo, organización y trazabilidad de los documentos digitales y/o físicos que se envían y reciben en la institución.	3	2	3	2,67
UPS	Dispositivo que proporciona energía en caso de fallo eléctrico.	3	3	3	3,00
GPON	Dispositivo que permite el acceso a internet desde un proveedor de servicios.	3	3	3	3,00
Router WAN	Dispositivo que permite la interconexión de ordenadores en red.	1	1	3	1,67
Cableado estructurado	Conjunto de cables, conectores, equipos para telecomunicaciones	3	3	3	3,00
Switch Capa 3	Dispositivo que permite el tráfico con la misma red o diferente.	3	3	3	3,00
Switch Capa 2	Dispositivo que permite el tráfico dentro de la misma red.	3	3	3	3,00
Switch No Administrable	Dispositivo que permite el tráfico dentro de la misma red.	3	3	3	3,00
Servidor	Servidor para proporcionar servicios a otros programas informáticos o a ordenadores.	3	2	1	2,00

Fase 2. Evaluación de la Seguridad del Sistema Actual.

Para evaluar la seguridad del sistema actual se toma cuenta la matriz de activos que se realizó anteriormente, y luego proceder a terminar el nivel de riesgo que presentan en la infraestructura actual de la organización.

Tabla 6. Amenazas y Vulnerabilidades

ANÁLISIS DE RIESGOS

Nro. de activo	**AMENAZA**	**VULNERABILIDAD**
	Descripción	**Descripción**
1	Infectación de Malware	Fallos de seguridad
	Formateo Intencional	Acceso indebido al equipo por parte de los usuarios.
2	Daño del equipo	Remplazo inadecuado de equipos viejos
	Divulgación de contraseñas	Inadecuada gestión de contraseñas
3	Fallo de los enlaces de comunicación.	Inadecuada gestión de red.
	Daño del equipo	Sensibilidad del equipo a la humedad, temperatura o contaminantes.
4	Pérdida de información.	Falta de políticas de administración de seguridad de la información.
	Daños en el software.	Daños en los equipos de cómputo.
5	Pérdida de información.	Falta de políticas de administración de seguridad de la información.
	Derechos de acceso al usuario.	Acceso indebido por parte de los usuarios.
6	Daños en el software.	Daños en los equipos de cómputo.
	Infectación de Malware	Fallos de seguridad
7	Sobrecarga	Acometida de cable en mal estado
	Incendio	Baterías de litio infladas
8	Ausencia de copias de seguridad	Pérdida de información
	Ausencia de soporte técnico	No se cuenta con personal experto.
9	Cortes eléctricos	Apagones
	Sobrecarga	Variaciones de voltaje
10	Cortes eléctricos	Falta de UPS, planta eléctrica, daño de equipos.
	Falla de hardware	Falta de Mantenimiento.
11	Ruptura de cable	Inadecuada seguridad del cableado
	Desgaste de los conectores	Falta de Mantenimiento.
12	Daño del equipo	Sensibilidad del equipo a los cambios de voltaje.
	Acceso a la red o al sistema de información por personas no autorizadas	Contraseñas predeterminadas no modificadas
13	Daño del equipo	Sensibilidad del equipo a la humedad, temperatura o contaminantes.
	Fallo de los enlaces de comunicación	Inadecuada gestión de red.
14	Daño del equipo	Sensibilidad del equipo a los cambios de voltaje.
	Fallo de los enlaces de comunicación	Inadecuada gestión de red.

Luego de determinar las vulnerabilidades y amenazas adicionalmente se calcula la evaluación de riesgo dependiendo los valores del CID y probabilidad (impacto y amenaza)

Tabla 7. Análisis de Riesgo

ANÁLISIS DE RIEGOS					
	EVALUACIÓN DE RIESGOS				
	Impacto	**Probabilidad**		**Cálculo de eval. de riesgo**	**Nivel de riesgo**
Descripción	**CID**	**Nivel de amenaza**	**Nivel de vulnerabilidad**		
Perdida por robo de información y control por el malware.	3,00	2	2	12,00	ALTO
Falta de control de acceso a los equipos de cómputo.	3,00	2	2	12,00	ALTO
Perdida de información.	3,00	1	1	3,00	BAJO
Divulgación de información.	3,00	1	1	3,00	BAJO
Errores de comunicación, servicios detenidos	1,33	2	1	2,67	BAJO
Falta de mantenimientos, daño por desgaste o defectos de fabricación.	1,33	2	1	2,67	BAJO
Si el equipo servidor tiene un fallo catastrófico es posible que se perdida información de orden institucional.	2,00	2	2	8,00	MEDIO
Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario.	2,00	2	2	8,00	MEDIO
Preparación del plan de backup.	2,67	1	1	2,67	BAJO
Controles de acceso.	2,67	1	1	2,67	BAJO
Fallas de programación que se presenten en software y herramientas de desarrollo.	1,33	2	2	5,33	MEDIO
Perdida por robo de información y control por el malware.	1,33	1	2	2,67	BAJO
Saltos de voltaje en los equipos de TI	3,00	2	2	12,00	ALTO
Explosión de la baterías y daño de equipos	3,00	2	2	12,00	ALTO
Falta de coordinación para producir copias de seguridad de los archivos existentes en forma periódica.	2,00	3	2	12,00	ALTO

No se cuenta con el personal experto para soporte de hardware.	2,00	3	3	18,00	ALTO
Falta de una planta eléctrica que podría causar daños a los equipos.	3,00	3	2	18,00	ALTO
Falta de mantenimientos, daño por desgaste o defectos de fabricación.	3,00	2	2	12,00	ALTO
Falta de una planta eléctrica que podría causar daños a los equipos.	1,67	1	1	1,67	BAJO
Falta de mantenimientos, daño por desgaste o defectos de fabricación.	1,67	1	1	1,67	BAJO
Errores de comunicación, servicios detenidos	3,00	2	2	12,00	ALTO
Errores de comunicación, servicios detenidos	3,00	1	2	6,00	MEDIO
Errores de comunicación, servicios detenidos	3,00	2	2	12,00	ALTO
Accesos no autorizados y perdidas de información	3,00	1	1	3,00	BAJO
Errores de comunicación, servicios detenidos	3,00	3	2	18,00	ALTO
Errores de comunicación y accesos no autorizados	3,00	1	1	3,00	BAJO
Errores de comunicación, servicios detenidos	3,00	2	2	12,00	ALTO
Errores de comunicación y accesos no autorizados	3,00	3	2	18,00	ALTO

Se determinan 24 riesgo, en cuanto al nivel de riesgo se obtienen como resultado 7 de nivel alto, 2 de nivel medio y 6 de nivel bajo.

Tabla 8. Resumen de los riesgos encontrados

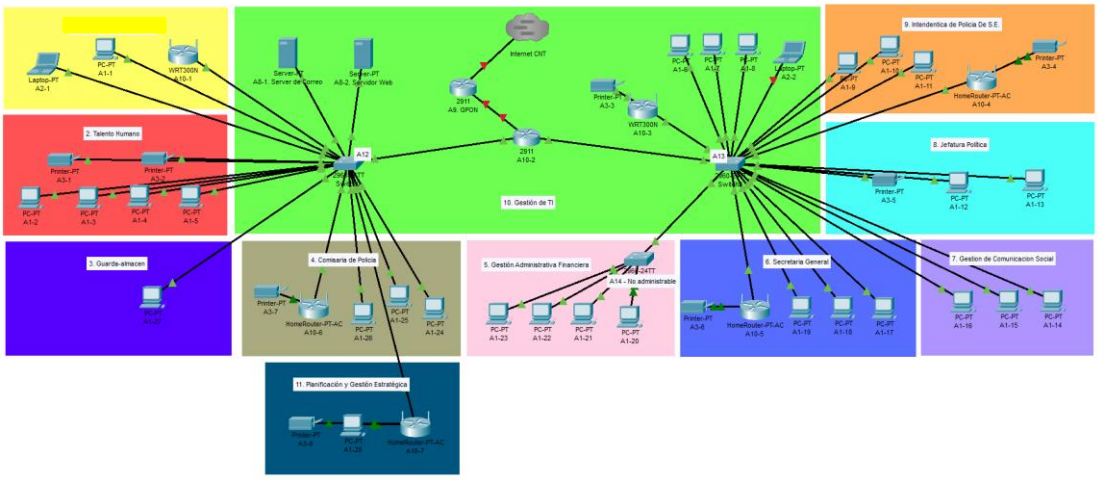
ANÁLISIS DE RIEGOS						
Riesgo		EVALUACIÓN DE RIESGOS				
		Impacto	Probabilidad		Cálculo de evaluación de riesgo	Nivel de riesgo
Código	Descripción	CID (Valoración del activo)	Nivel de amenaza	Nivel de vulnerabilidad		
R1	Perdida por robo de información y control por el malware.	3,00	2	2	12,00	ALTO
R2	Falta de control de acceso a los equipos de cómputo.	3,00	2	2	12,00	ALTO
R3	Perdida de información.	3,00	1	1	3,00	BAJO
R4	Divulgación de información.	3,00	1	1	3,00	BAJO

R7	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario.	1,33	2	2	5,33	MEDIO
R8	Preparación del plan de backup.	1,33	2	2	5,33	MEDIO
R9	Saltos de voltaje en los equipos de TI	2,67	1	1	2,67	BAJO
R10	Explosión de la baterías y daño de equipos	2,67	1	1	2,67	BAJO
R13	Falta de una planta eléctrica que podría causar daños a los equipos.	3,00	2	2	12,00	ALTO
R14	Falta de mantenimientos, daño por desgaste o defectos de fabricación.	3,00	2	2	12,00	ALTO
R16	Errores de comunicación, servicios detenidos	1,67	3	3	15,00	ALTO
R18	Accesos no autorizados y perdidas de información	3,00	2	2	12,00	ALTO
R20	Errores de comunicación y accesos no autorizados	3,00	1	1	3,00	BAJO
R23	Falta de coordinación para producir copias de seguridad de los archivos existentes en forma periódica.	3,00	2	2	12,00	ALTO
R24	No se cuenta con el personal experto para soporte de hardware.	3,00	1	1	3,00	BAJO

Fase 3. Diseño de la Arquitectura del Sistema de Computación.

Para el diseño de la arquitectura, se considera los aspectos analizados anteriormente en base a las encuestas realizadas, se tiene como resultado entre los datos más relevantes servidor de base de datos, servidor de correo, además que poseen servidores locales la protección de datos es escaza.

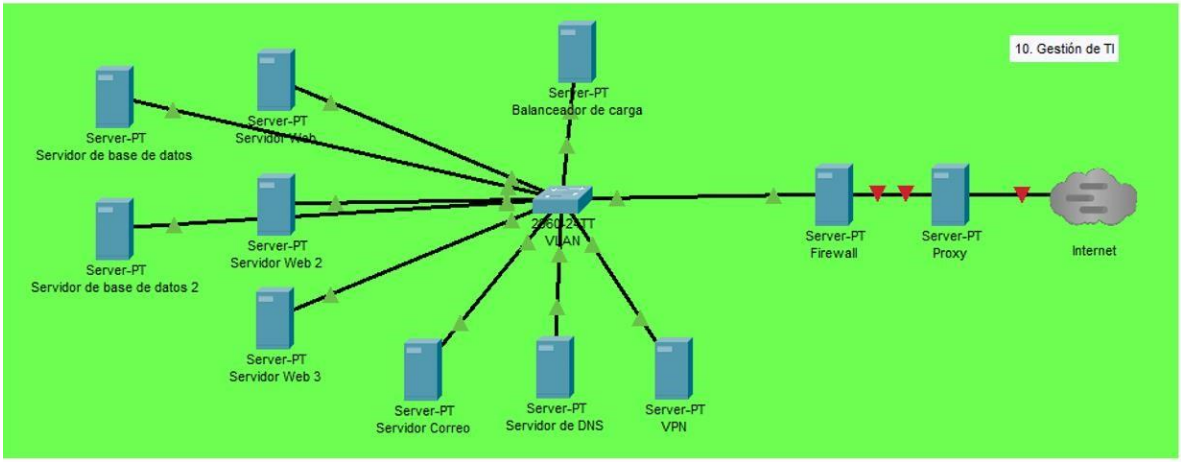
Figura 5. Infraestructura actual de la institución pública



El servidor proxy que servirá de puente, permitiendo la conexión indirecta con internet. Servidor firewall que servirá para la parte administrable del usuario principal, que le permitirá establecer reglas denegando el acceso no autorizado y no verificado a la conexión internet. Servidor de DNS para la traducción de direcciones IP de la red, servidor de VPN para permitir el acceso a configuraciones de los dispositivos de la red, 3 Servidor web, y 2 servidor de base de datos en conjunto con el balanceador de carga, permitiendo agilizar las

consultas o peticiones ya que normalmente las instituciones públicas administrativas hacen tareas como envío de datos, información, documentación es lo más concurrente entre áreas.

Figura 6. Infraestructura Cloud Computing



Fase 4. Simulación de la arquitectura de seguridad cloud computing.

Para simular el comportamiento en la nube de las maquinas en la nube, se hace de la tecnología de contenedores Docker, ya que este nos brinda muchas características similares que podemos encontrar en la nube. Tales como: contenedores, redes, volúmenes, y sus imágenes que nos proveen un "molde" de una máquina.

Requerimientos:

- Docker

1. Configurar los servicios para crear la infraestructura en Docker. (Servicios en cloud computing).
    a. Servidor Proxy
    b. Servidor Firewall
    c. Balanceador de Carga
    d. Servidor de DNS
    e. Servidor Web 1,2,3
    f. Servidor de Base de Datos 1,2

Los servidores web son una réplica de sí mismos, junto con su base de datos para poder hacer uso del balanceador de carga y mejorar la disponibilidad del servicio.

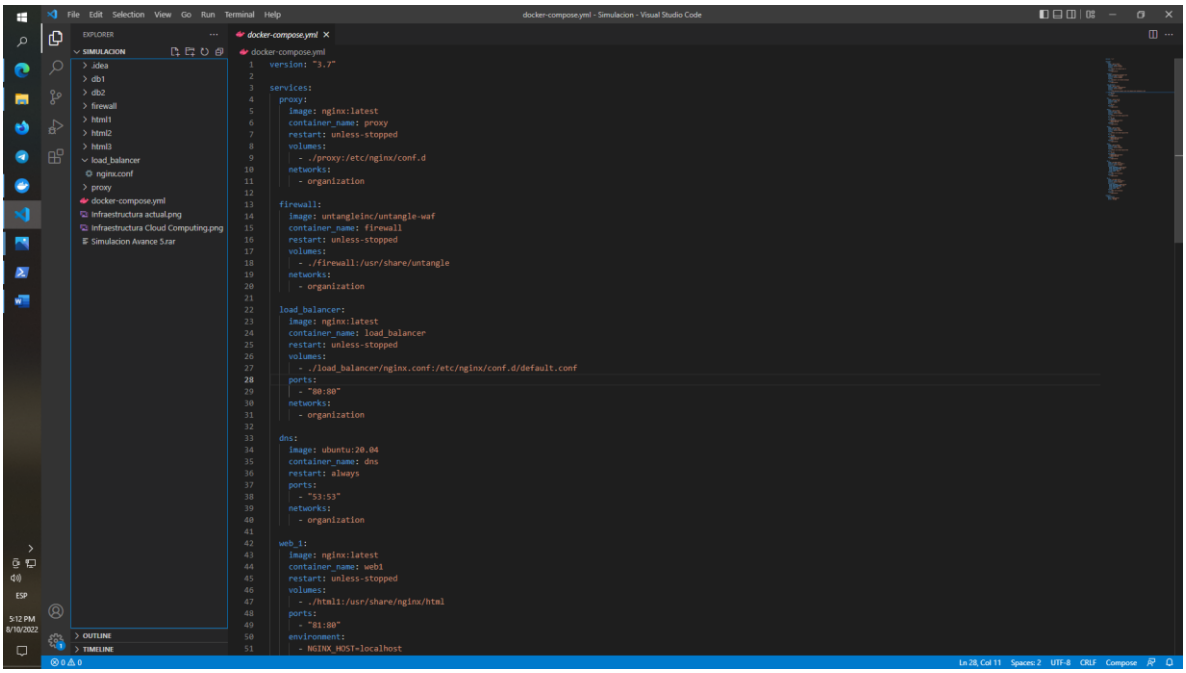


Figura 7. Configuraciones de los contenedores

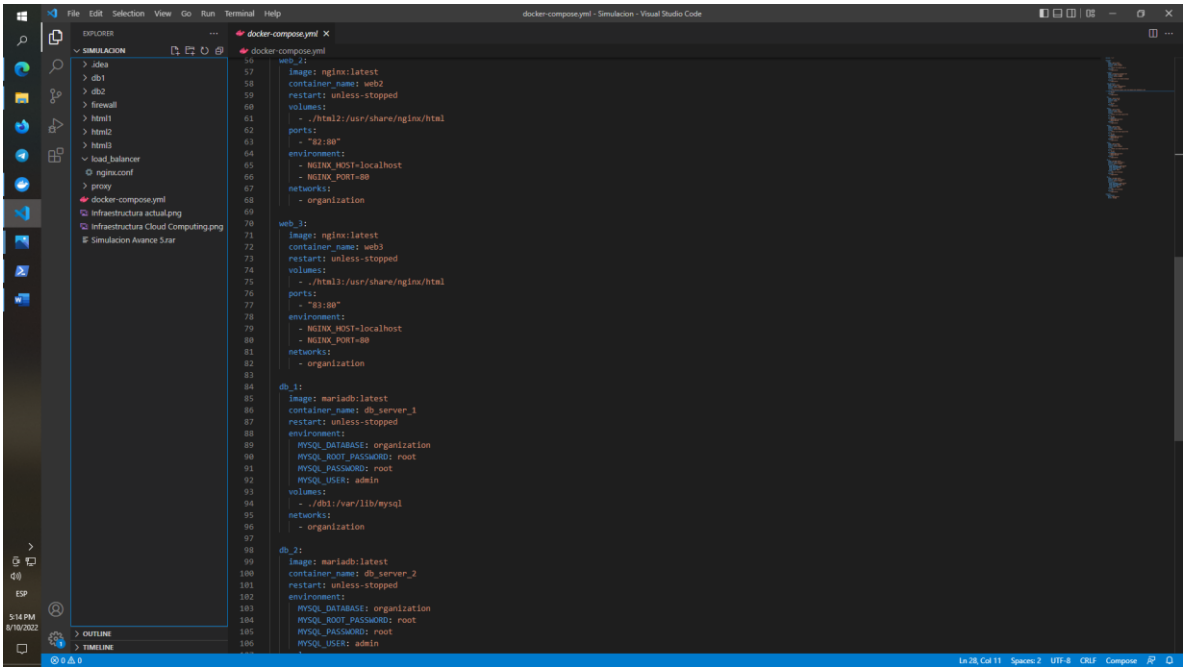


Figura 8. Características de los contenedores

En el archivo de configuración de Docker se escribe las características de los contenedores que se va a crear, la etiqueta “versión” se especifica la versión a utilizar del creador de contenedores de Docker, en los servicios se le asignan los nombres a los contenedores, especificamos el nombre del contenedor (container_name), se especifica la imagen a utilizar (image), la red en la que la vamos a usar (networks), los volúmenes que nos permiten compartir un directorio de la maquina host con el contenedor, y el parámetro “restart” que en caso de que ocurra una falla, se reinicie y lo intente nuevamente.

2. Levantamiento de la arquitectura en Docker

Para realizar el levantamiento de la simulación utilizamos el comando “docker-compose up -d”, la bandera “-d” nos ayuda a especificar en segundo plano.

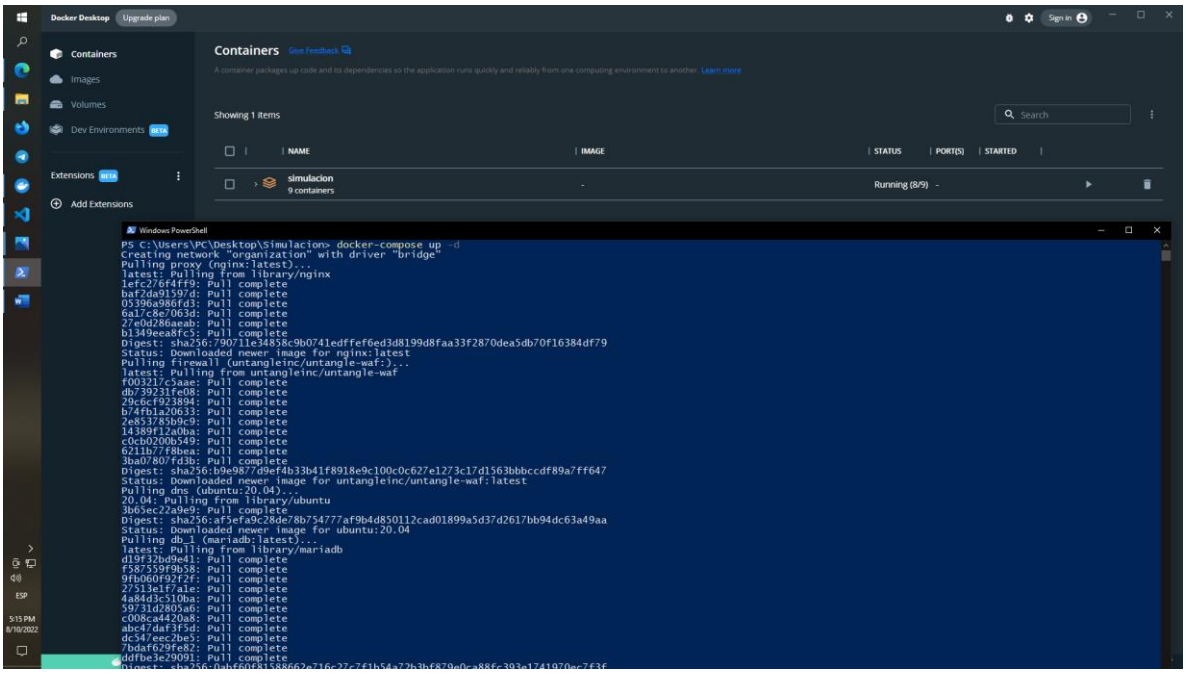


Figura 9. Levantamiento de la arquitectura en Docker

3. Listar los contenedores (servicios).

Por medio del comando “docker ps” obtenemos la información y el estado de las máquinas para verificar el estado de ejecución.

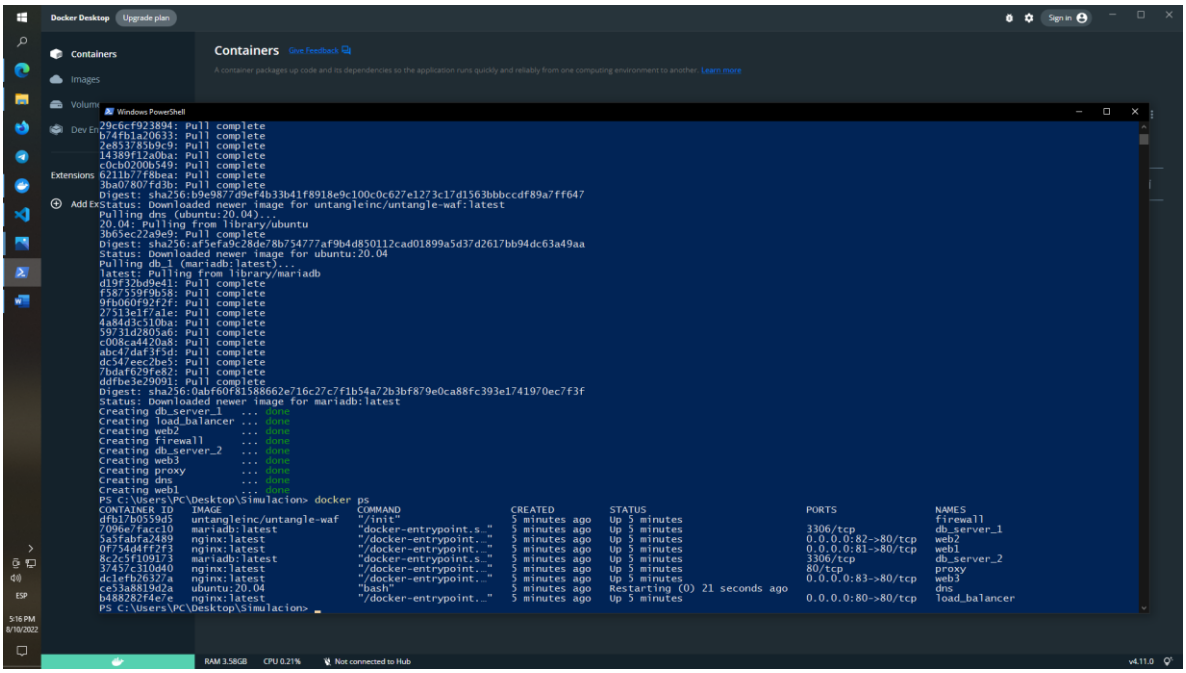


Figura 10. Listado de los contenedores en ejecución

4. Ingresamos a las maquinas a verificar la configuración en el sistema operativo (docker).
    a. Ingresar a uno de los servicios (servidor web) por medio del ID del contenedor, con el comando "*docker container exec -it 5a5fabfa2489 /bin/bash"*

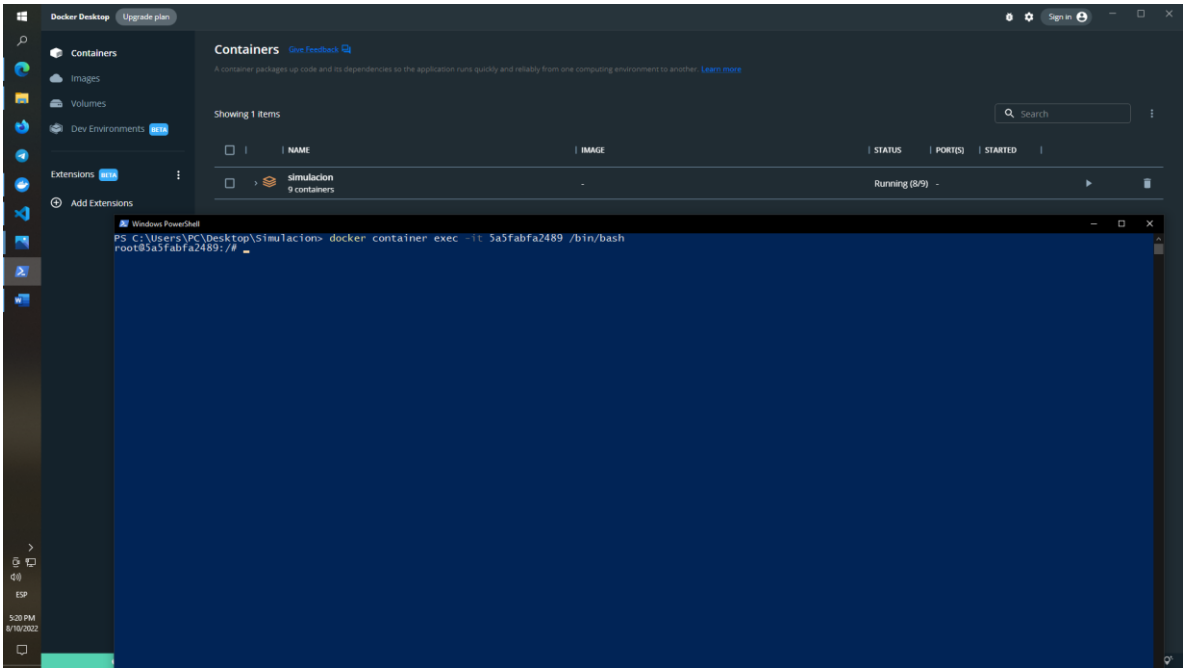


Figura 11. Comando para verificar las configuraciones en uno de los servicios (servidor web)

b. Entrar a configuraciones en el servidor web por medio de directorios con el comando *cd etc/nginx/*

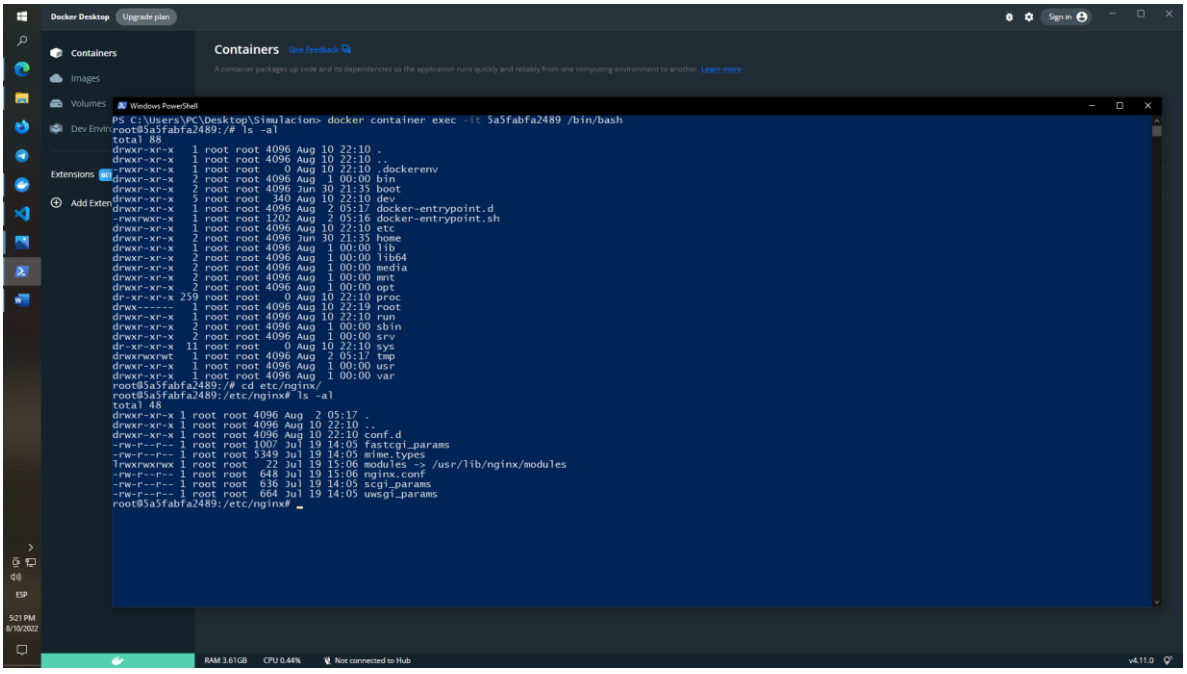


Figura 12. Configuraciones del servidor web

c. Entrar a la carpeta de configuraciones por el comando *cat default.conf*

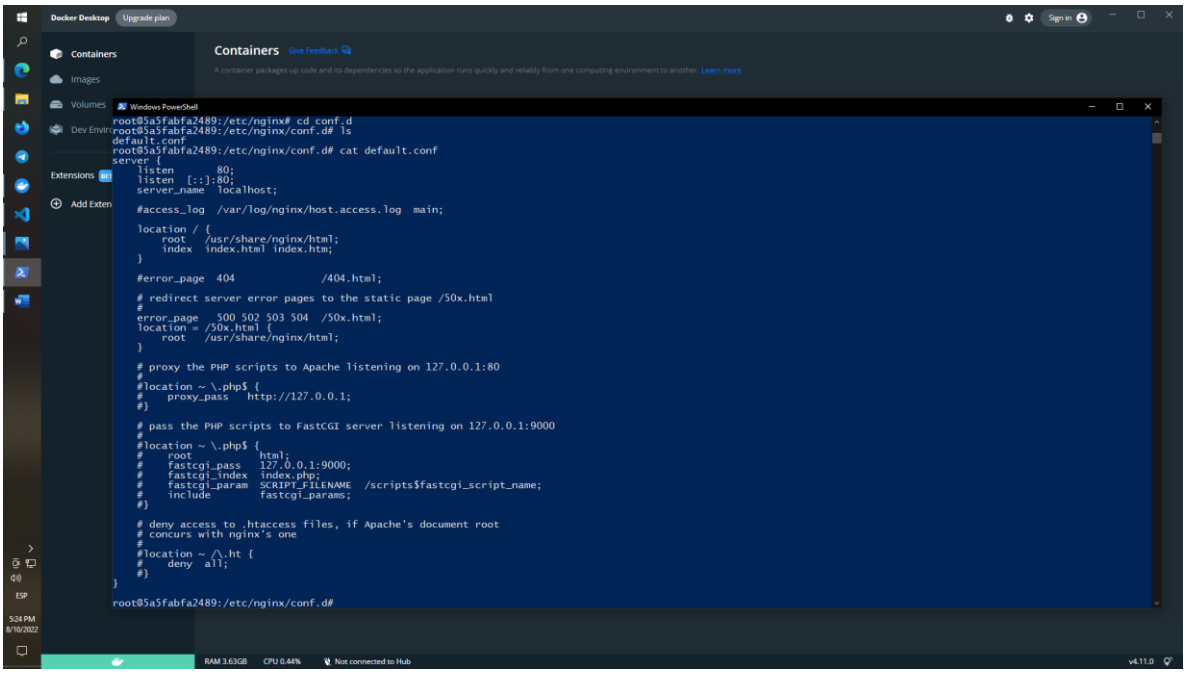


Figura 13. Configuraciones servidor web

Fase 5. Evaluación de la Seguridad de la Arquitectura, Computación en la Nube.

Con los nuevos activos de la misma manera se realiza un inventario y valoración de activos cloud computing, el análisis amenazas y vulnerabilidades para posibles riegos que pueden presentarse en la institución al migrar sus datos a la nube.

Tabla 9. Matriz de Activos Cloud Computing

	MATRIZ DE ACTIVOS	
Nombre de activo	**Descripción de activo**	**Ubicación**
Servidor de correo	Servidor para enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes.	Toda la organización
Servidor web	Es un sistema de gestión de contenido enfocado a la creación de cualquier tipo de página web.	Area de TIC´s
Servidor de base de datos	Es un sistema de gestión de bases de datos.	Cloud Computing
Servidor DNS	Es un servicio de Google Cloud Platform que ofrece alta disponibilidad, y baja latencia.	Cloud Computing
Servidor VPN	Es una herramienta de conectividad de código abierto.	Cloud Computing
Balanceador de carga	Es un servidor web de código abierto que, usado como servidor web, proxy inverso, cache de HTTP, y balanceador de carga.	Cloud Computing
Firewall	Es el servicio de firewall que ofrece Google Cloud Platform.	Cloud Computing
Proxy	Es un servicio que centraliza el acceso de los usuarios a las aplicaciones.	Cloud Computing

Tabla 10. Valoración de activos

Nombre de activo	Descripción de activo	C	I	D	Valoración del activo
Servidor de correo	Servidor para enviar, recibir y gestionar mensajes a través de las redes de transmisión de datos existentes.	2	1	3	2,00
Servidor web	Es un sistema de gestión de contenido enfocado a la creación de cualquier tipo de página web.	1	1	2	1,33
Servidor de base de datos	Es un sistema de gestión de bases de datos.	3	3	3	3,00
Servidor DNS	Es un servicio de cloud ofrece alta disponibilidad, y baja latencia.	3	3	3	3,00
Servidor VPN	Es una herramienta de conectividad de código abierto.	3	3	3	3,00
Balanceador de carga	Es un servidor web de código abierto que, usado como servidor web, proxy inverso, cache de HTTP, y balanceador de carga.	3	3	3	3,00
Firewall	Es el servicio de firewall que ofrece Cloud Platform.	3	3	3	3,00

Proxy	Es un servicio Cloud que centraliza el acceso de los usuarios a las aplicaciones.	3	3	3	3,00

Para el análisis de riesgo se enlista las posibles amenazas y vulnerabilidades, 2 amenazas y 2 vulnerabilidades por cada activo de cloud computing.

Tabla 11. Matriz de amenazas y vulnerabilidades de los activos cloud computing

Nro. de activo	Nombre de activo	AMENAZAS	VULNERABILIDAD	
		Descripción	**Descripción**	
		Ausencia de soporte técnico	No se cuenta con personal experto.	
13	Servidor de correo	Pérdida de información.	Falta de políticas de administración de seguridad de la información.	
		Daños en el software.	Daños en los equipos de cómputo.	
14	Servidor web	Daños en el software.	Daños en los equipos de cómputo.	
		Inafectación de Malware	Fallos de seguridad	
15	Servidor de base de datos	Borrado de datos	Acceso indebido al equipo por parte de los administradores.	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	
16	Servidor DNS	Secuestro de registros	Mala configuración del servicio y actualizaciones de seguridad	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	
17	Servidor VPN	Acceso de personal no autorizado	Mala gestión de credenciales de acceso	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	
18	Balanceador de carga	Comprometer el sistema back-end	Mala configuración del servicio y actualizaciones de seguridad	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	
19	Firewall	Acceso a áreas restringidas	Mala configuración del servicio y actualizaciones de seguridad	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	
20	Proxy	Envenamiento de proxies	Mala configuración del servicio y actualizaciones de seguridad	
		Divulgación de contraseñas	Inadecuada gestión de contraseñas	

Se visualiza el nivel de riesgo dependiendo del cálculo de evaluación de riesgo, en cuanto a la valoración (CID) y la probabilidad.

Tabla 12. Evaluación de riesgos

Riesgo		EVALUACIÓN DE RIESGOS				
		Impacto	Probabilidad		Cálculo de evaluación de riesgo	Nivel de riesgo
Código	Descripción	CID (Valoración del activo)	Nivel de amenaza	Nivel de vulnerabilidad		
R1	Si el equipo servidor tiene un fallo catastrófico es posible que se perdida información de orden institucional.	3,00	3	2	18,00	ALTO
R2	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario.	3,00	1	1	3,00	BAJO
R3	Fallas de programación que se presenten en software y herramientas de desarrollo.	3,00	2	2	12,00	ALTO
R4	Perdida por robo de información y control por el malware.	3,00	3	2	18,00	ALTO
R5	Borrado de información por parte de un tercero o malware	3,00	1	1	3,00	BAJO
R6	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO
R7	Redirección a servidores Phishing	3,00	2	1	6,00	MEDIO
R8	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO
R9	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario.	3,00	2	1	6,00	MEDIO
R10	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO
R11	Comprometer con un malware a los servicios detrás del LB	3,00	1	2	6,00	MEDIO
R12	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO
R13	Evadir las reglas impuestas por el firewall	3,00	1	2	6,00	MEDIO
R14	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO
R15	Redirección a servicios de terceros o phishing	3,00	2	1	6,00	MEDIO

R16	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO

En el resumen de la matriz de riesgos en cloud computing tenemos como resultado el total de 9 riesgos, en específico 3 de nivel alto, 2 de nivel medio y 4 de nivel bajo.

Tabla 13. Resumen de los riesgos identificados

ANÁLISIS DE RIEGOS						
Riesgo		EVALUACIÓN DE RIESGOS				
		Impacto	Probabilidad		Cálculo de evaluación de riesgo	Nivel de riesgo
Código	Descripción	CID (Valoración del activo)	Nivel de amenaza	Nivel de vulnerabilidad		
R1	Si el equipo servidor tiene un fallo catastrófico es posible que se perdida información de orden institucional.	3,00	3	2	18,00	ALTO
R2	Posible acceso indebido de terceros en los perfiles de los derechos de acceso del usuario.	3,00	1	1	3,00	BAJO
R3	Fallas de programación que se presenten en software y herramientas de desarrollo.	3,00	2	2	12,00	ALTO
R4	Perdida por robo de información y control por el malware.	3,00	3	2	18,00	ALTO
R5	Borrado de información por parte de un tercero o malware	3,00	1	1	3,00	BAJO
R6	Comprometer con un malware a los servicios detrás del LB	2,00	1	2	4,00	MEDIO
R7	Evadir las reglas impuestas por el firewall	1,33	1	2	2,67	BAJO
R8	Redirección a servicios de terceros o phising	3,00	2	1	6,00	MEDIO
R9	Revelación o pérdida de información.	3,00	1	1	3,00	BAJO

En cuanto los riesgos identificados se analizan que requieren estrategias y depende de los controles seleccionados bajo las normativas ISO27001 (Figura 14), se establecen controles a implementar para reducir, aceptar, evitar o trasferir el riesgo identificado.

CÓDIGO	DESCRIPCIÓN
A9.2.1	Registro y baja de usuario
A9.2.2	Provisión de acceso de usuario
A9.2.3	Gestión de privilegios de acceso
A9.4.1	Restricción del acceso a la información
A13.1.1	Controles de red
A13.1.2	Seguridad de los servicios de red
A13.1.3	Segregación en redes
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información
A14.2.2	Procedimiento de control de cambios en sistemas
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A14.2.4	Restricciones a los cambios en los paquetes de software
A14.2.5	Principios de ingeniería de sistemas seguros
A14.3.1	Protección de los datos de prueba
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información
A16.1.5	Respuesta a incidentes de seguridad de la información

Figura 14. Listado de anexos seleccionados en base las normas ISO27001:2013

Tabla 14. Controles propuestos para salvaguardar los datos

Controles propuestos	Controles ISO 27001:2013
Uso de reguladores de voltaje, Revisión de tendido eléctrico	A13.1.1 - A13.1.2 - A13.1.3
Configuración de Vlan's y troncales.	A13.1.1 - A13.1.2 - A13.1.3
Elegir medios de almacenamiento y establecer tiempos de respaldo.	A14.3.1

Establecer políticas de seguridad de la información, Restauración de contraseñas	A9.2.1 - A9.2.2 - A9.2.3 - A14.1.1 - A16.1.4 - A16.1.5
Realizar una evaluación de actualización de seguridad y adecuada configuración.	A14.2.2 - A14.2.3 - A14.2.4 - A14.2.5
Configuración de usuarios para el control de acceso a los equipos.	A9.4.1

Se puede identificar, luego de hacer el tratamiento de riesgo, en la que el nivel de riesgo pasa a un nivel bajo.

Tabla 15. Tratamiento de riesgos

TRATAMIENTO DE RIESGOS							
Método de tratamiento de riesgos	**Tipo de control**	**Controles a implementar**	**Nivel de amenaza**	**Nivel de vulnerabilidad**	**Cálculo de Evaluación de Riesgo con el control implementado**	**Nivel de riesgo con el control implementado**	**Riesgo residual**
Evitar, mitigar	Preventivo, Correctivo	A13.1.1 - A13.1.2 - A13.1.3	1	1	3,00	BAJO	Aceptable
Evitar, mitigar	Preventivo, Correctivo	A14.3.1	1	1	3,00	BAJO	Aceptable
Evitar, mitigar	Preventivo, Correctivo	A9.2.1 - A9.2.2 - A9.2.3 - A14.1.1 - A16.1.4 - A16.1.5	1	1	3,00	BAJO	Aceptable
Evitar, mitigar	Preventivo, Correctivo	A14.2.2 - A14.2.3 - A14.2.4 - A14.2.5	1	1	3,00	BAJO	Aceptable
Evitar, mitigar	Preventivo, Correctivo	A9.4.1	1	1	3,00	BAJO	Aceptable

CONCLUSIONES

- Por medio de la metodología para el levantamiento de información como las encuestas, se determinan características comunes y similares en varias de las instituciones de gobierno seccional, de esta manera se concluye una sola arquitectura de red para llevar a cabo la investigación. Mediante las mismas encuestas se pudo determinar que varias de las instituciones no cuentan con un documento de procedimientos y controles vigente para la seguridad de la información, con los resultados obtenidos se pudo comprobar varios de los vacíos de seguridad informática.

- Mediante el análisis de gestión de seguridad de información se logró comprobar los riesgos que se presentan actualmente en la institución, mediante el proceso del análisis de gestión de riesgos de seguridad, en la que se identifica y realiza la valoración de los activos operativos de la organización. Por medio de la matriz de amenazas y vulnerabilidades, la matriz de identificación de riesgos se logró priorizar los riesgos de nivel alto para la mejora de seguridad de datos e información en la infraestructura.

- Se identifican los activos y servicios que manejan actualmente en la organización mediante el levantamiento de información para que así, la nueva infraestructura sea compatible con los servicios que ofrece la nube, de esta manera se realiza el diseño de una nueva arquitectura de red para la institución con activos y servicios adicionales en cloud computing para mejorar la seguridad de TI.

- En base a las normativas establecidas en ISO27001: 2013 se aplican los controles siendo estrategia para mitigar los posibles riesgos de seguridad, procedimientos que permiten salvaguardar los incidentes de seguridad que cualquier institución presente durante sus procesos de administración y gestión.

RECOMENDACIONES

Al aplicar el mismo procedimiento de esta investigación e implementar en una determinada institución recomiendo el estudio y recolección de información actual de la institución debido a que los resultados pueden variar dependiendo el crecimiento de la infraestructura de red de la organización.

En base al documento actual recomiendo la modificación del diseño de la nueva arquitectura que sea acorde a las necesidades de la empresa o caso de estudio, de igual manera aplicar una metodología que permita la comparativa de varios de los proveedores de servicios en la nube, así obtener una mejor visión para la elección de este servicio cloud, que sea compatible y pueda cubrir los requerimientos actuales de la empresa.

A pesar de que se obtuvo buenos resultados luego del análisis de riesgos en base a las normativas ISO27001:2013, estudio que se realizó en la nueva infraestructura de seguridad en cloud computing, se recomienda aplicar nueva metodología para mejorar la identificación de amenazas y vulnerabilidades, además dar un mejor enfoque a los futuros vacíos de seguridad informática.

BIBLIOGRAFÍA

[1] G. S. Rodriguez, «Computacion en la nube,» *Lex,* vol. 17, nº 23, pp. 145-168, 2019.

[2] P. Sánchez Sánches, J. Garcia Gonzales, A. Triana y L. Perez Coronell, «Medida del nivel de seguridad informatica de las pymes en Colombia,» *Información Tecnológica,* vol. 32, nº 5, pp. 121-128, 2021.

[3] S. Dahal, «Security Architecture for Cloud Computing Platform,» 2012. [En línea]. Available: http://www.diva-portal.org/smash/get/diva2:582095/FULLTEXT01.pdf. [Último acceso: 25 Mayo 2022].

[4] L. E. Arcila Bonfante, «"Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información",» 2019. [En línea]. Available: https://repository.ucatolica.edu.co/bitstream/10983/23388/1/RECOMENDACIONES%20DE%20SEGURIDAD%20PARA%20LOS%20SERVICIOS%20DE%20COMPUTACION%20EN%20LA%20NUBE.pdf. [Último acceso: 25 Mayo 2022].

[5] A. M. Cornejo Orellana y C. F. Díaz Escalante, «"Análisis, Diseño e Implementación de Cloud Computing para una Red de Voz sobre IP",» Marzo 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/7921/1/UPS-CT004762.pdf. [Último acceso: 25 Mayo 2022].

[6] D. J. Parada, J. A. Calvo y A. Flórez, «Modelo de Arquitectura de Seguridad de la Información – MASI,» 2010. [En línea]. Available: https://www.iiis.org/CDs2010/CD2010CSC/CISCI_2010/PapersPdf/CA626FI.pdf. [Último acceso: Junio 2022].

[7] M. I. W. Torres, *Resolución RCF-FST-SO-09 No. 03-2021,* Santa Elena, 2022.

[8] C. F. Varela Pérez , J. E. Portella Cleves y L. Pallares, «Computación en la nube: Un nuevo paradigma en las tecnologías de la información y la comunicación,» *Redes de ingeniería,* vol. Especial, p. 138–146, 2017.

[9] I. Orozco y O. Jacobs, «LA NUEVA ERA DE LOS NEGOCIOS: COMPUTACIÓN EN LA NUBE,» *Télématique,* vol. 15, nº 2, pp. 172-191, 2016.

[10] Secretaría Nacional de Planificación, «Plan de Creación de Oportunidades 2021-2025 de Ecuador,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/es/planes/plan-de-creacion-de-oportunidades-2021-2025-de-ecuador. [Último acceso: 2022].

[11] N. Mohammad, Metodología de la investigación, Coyoacán Ciudad de México: Noriega Editorial, 2005.

[12] P. Bernal, La investigación en ciencias sociales, Bogotá: Universidad Piloto de Colombia, 2017.

[13] J. S. S. Zarate, «Informe de práctica empresarial Gobernación del meta - secretaría de competitividad y desarrollo económico,» Colombia, 2021.

[14] R. J. M. Guaman, «Analisis y diseño de un modelo para establecer un SGSI dentro de un ambiente CC.,» Babahoyo, 2022.

[15] «Ministerio de Telecomunicaciones y de la Sociedad de la Informacion,» Abril 2020. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf. [Último acceso: 5 Enero 2023].

[16] N. ISO, «NORMAS ISO,» [En línea]. Available: https://www.normas-iso.com/. [Último acceso: 5 Enero 2023].

[17] J. Guerra y F. Fermín, «Nube hibrida, tecnologia que combian lo mejor de Cloud Computing,» *Perspectivas, Revista de tecnología e información,* vol. 10, nº 11, pp. 50-55, 2017.

[18] O. A. Mejia, «Computacion en la nube,» Venezuela, 2011.

[19] M. P. Pollastri, «Cloud Computing en el Desarrollo de las PYMES,» *Revista Cientifica de Ciencias Económicas OIKONOMOS,* vol. 1, pp. 227-237, 2015.

[20] G. Cloud, «cloud DNS,» 1 Febrero 2023. [En línea]. Available: https://cloud.google.com/dns/docs/overview?hl=es-419#:~:text=Cloud%20DNS%20es%20un%20servicio,datos%2C%20y%20buscarlos%20por%20nombre.. [Último acceso: Enero 2023].

[21] G. D. MINTIC, «Seguridad en la nube,» 15 Mayo 2018. [En línea]. Available: https://gobiernodigital.mintic.gov.co/692/articles-150518_G12_Seguridad_Nube.pdf. [Último acceso: Enero 2023].

[22] CloudFlare, «CloudFlare,» Cloudflare, 2023. [En línea]. Available: https://www.cloudflare.com/es-es/learning/cloud/what-is-a-cloud-firewall/. [Último acceso: Enero 2023].

[23] G. A. Ernesto, «Despliegue de un cluster Kubernetes,» Universidad Politecnica de Valencia, Valencia, 2022.

[24] Microsoft, «Microsoft,» 12 Enero 2022. [En línea]. Available: https://learn.microsoft.com/es-es/windows/wsl/about.

[25] Docker, «Docker,» 2023. [En línea]. Available: https://docs.docker.com/desktop/. [Último acceso: Enero 2023].

[26] O. C. Infraestructure, «Oracle Cloud Infraestructure,» 2023. [En línea]. Available: https://www.oracle.com/mx/cloud/cloud-native/container-registry/what-is-docker/. [Último acceso: Enero 2023].

[27] A. W. Services, «Acloud Web Services,» Enero 2023. [En línea]. Available: https://aws.amazon.com/es/docker/#:~:text=Una%20imagen%20de%20Docker%20es,Docker%20instanciada%20(en%20ejecuci%C3%B3n)..

[28] D. Vallejos quiñones, «Seguridad de Contenedores Docker mediante Procesos de Hardening,» *Revista PGI. Investigación, Ciencia y Tecnología en Información,* nº 7, pp. 14-17, 2020.

[29] A. Llano Casa, M. Gaibor Gavilanez, C. Cruz Caiza y J. Cadena Moreano, «Importancia de políoticas de seguridad informática de acuerdo a las ISO27001

para PYMES del Ecuador,» *Revista ciencias de la ingenierira y aplicadas,* vol. 5, nº 2, Diciembre 2021.

[30] S. orantes, A. Zavala y G. Vazquez, «Analisis de las implicaciones de seguridad en la adopcion del computo en la nube para las PYMES,» *Sistemas, Cibernetica e Informatica,* vol. 13, nº 2, pp. 1-8, 2016.

[31] P. Muñoz Calderón y M. Zhindón Mora, «Computación en la nube: la infraestructura comno servicio frente al modelo On - Premise,» *Artículo de investigación Ciencias ténicas y aplicadas,* vol. 6, nº 4, pp. 1535-1549, Noviembre 2020.

ANEXOS

Anexo 1. Técnica de observación

GUIA DE ENTREVISTA SOBRE LA ARQUITECTURA DE SEGURIDAD DE TI DE LA INSTITUCION (GOBIERNO SECCIONAL)

Fecha: martes, 24 de mayo de 2022 **Hora: 15:30 pm**

Lugar: Prov. Santa Elena

Entrevistador: Emily Pozo Echeverria

Entrevistado: Usuario operativo

Introducción:

La presente entrevista tiene el propósito de obtener información relacionada a la arquitectura de la seguridad de TI actual en la institución, así como, el funcionamiento y políticas establecidas para la protección de datos.

Características:

Entrevista confidencial de 30 minutos.

Preguntas:

1. **¿Cómo se protege su institución contra los ataques cibernéticos**
2. **¿Qué políticas y procedimientos existen para prevenir violaciones de datos?**
3. **¿Cuál es la postura de su institución sobre el cifrado de datos?**
4. **¿Qué medidas existen para garantizar la seguridad física de la infraestructura de TI?**
5. **¿Cuáles son los procedimientos de la institución para el manejo de incidentes de seguridad de TI?**
6. **¿Cuáles son los procedimientos de la institución para administrar contraseñas u otra información confidencial?**
7. **¿Cuáles son los procedimientos de la institución para administrar las actualizaciones de software y hardware?**
8. **¿Cuáles son los procedimientos de la institución para administrar el acceso a sus sistemas de TI?**
9. **¿Cuáles son los procedimientos de la institución para monitorear la actividad en sus sistemas de TI?**
10. **¿Cómo se asegura la institución de que sus sistemas de TI sean seguros?**
11. **¿Qué procesos y procedimientos existen para evitar el acceso no autorizado a datos confidenciales?**
12. **¿Cómo responde la institución a las brechas de seguridad?**
13. **¿Qué programas de capacitación y concientización existen para educar al personal sobre los riesgos de seguridad de TI?**
14. **¿Qué planes de respuesta a incidentes existen en caso de un incidente de seguridad?**
15. **¿Qué opina sobre el cloud computing?**

Anexo 2. Formato de entrevista

Perspectivas de características de infraestructura de TI

Objetivo: Obtener información primaria para conocer la situación actual del uso de las tecnologías, características de infraestructura de TI.

Preguntas.

Información general

1. **¿En qué clasificación se encuentra la institución?,** en base a los siguientes criterios**:**
   - Microempresa: hasta 10 trabajadores.
   - Pequeña empresa: hasta 50 trabajadores.
   - Medianas empresas: 50 a 99 trabajadores.
   - Grandes empresas: más de 100 trabajadores.
     - Microempresa
     - Pequeña empresa
     - Mediana empresa
     - Grandes empresas

Seguridad TI

2. **¿Cuenta la institución un documento sobre las políticas de seguridad de información?**
   a. Si
   b. No.
3. **¿Han aplicado análisis de gestión de seguridad de la información?**
   a. Si
   b. No.
4. **¿Cuáles son los principales problemas que se tiene la empresa en el área de tecnología asociada a la seguridad de información?**
     - Redes y cableado estructurado.
     - Mantenimiento de plataforma web.
     - Administración de servicios electrónicos.
     - Administración de firewall de seguridad.
     - Administración de base de datos
     - Mantenimiento de los equipos TIC.
     - Administración de servidores.
     - Redes inalámbricas.
     - Mantenimiento de dispositivos de redes: router, switch, etc.
     - Seguridad informática.

Redes

5. **¿Cuál es el tipo de red, servicio y topología de red que posee en infraestructura de TI?**

a. Tipo de red
- LAN
- MAN
- WAN

b. Tipo de servicio
- Infraestructura como servicios
- Plataforma como servicios
- Software como servicios

c. Topología de red
- T. en estrella
- T. en bus
- T. en anillo
- T. en árbol
- T. de malla
- T. hibrida

Software.

6. **¿Cuáles de las siguientes tipologías de software de código abierto posee la institución?**

SOFTWARE		Si	No	Nombre
Sistema operativo	Linux			
	W7			
	W10			
Servidor	Correo			
	DNS			
	PROXY			
	Web			
Aplicaciones ofimáticas (M.Office)				
Sistema de Gestión				

Anexo 3. Formato de encuesta