



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
DEPARTAMENTO ACADÉMICO DE GRADUACIÓN**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERO EN TELEINFORMÁTICA**

**ÁREA
REDES INTELIGENTES**

**TEMA
“REPOTENCIACIÓN DE INFRAESTRUCTURA Y
SERVICIOS DE RED CON MEJORAS DE
SEGURIDAD ORIENTADO A LA NUBE”**

**AUTOR
BENAVIDES ALCIVAR VICENTE ALBERTO**

**DIRECTOR DEL TRABAJO
ING. TELECOMUNICACIONES PINOS GUERRA MARIO, MSI**

**2017-2018
GUAYAQUIL – ECUADOR**

DECLARACIÓN DE AUTORÍA

“La responsabilidad del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio Intelectual del mismo a la Facultad de Ingeniería Industrial de la Universidad de Guayaquil”

Benavides Alcivar Vicente Alberto

C.C. 0930672613

AGRADECIMIENTO

Le doy gracias a mi familia que me ha apoyado en este largo camino de estudio.

A mi madre, que fue mi pilar principal en todo este tiempo ya que sin su apoyo no hubiera podido cumplir esta meta.

A mi padre, que también me dio su apoyo incondicional.

A mi primo Manuel, que sin su ayuda en todo ese tiempo que estuve en la universidad no lo hubiera podido lograr.

A mi tutor de tesis, Ingeniero Mario Pinos quien me ayudó con su conocimiento y experiencia para desarrollar este proyecto.

DEDICATORIA

Dedico este proyecto de titulación a mis padres: Víctor Benavides y Adela Alcívar quienes fueron un ejemplo a seguir, también por el apoyo incondicional que ambos me brindaron en esta meta universitaria.

A mi familia, que me supieron ayudar en momentos difíciles.

A mis amigos quienes siempre estuvieron ahí ayudando y apoyando en superar las metas académicas .

ÍNDICE GENERAL

N°	Descripción	Pág.
	INTRODUCCIÓN	1

CAPÍTULO I EL PROBLEMA

N°	Descripción	Pág.
1.1	Planteamiento del problema	3
1.2	Formulación del problema	5
1.3	Sistematización del problema	5
1.4	Objetivos generales y específicos	6
1.4.1	Objetivo General	6
1.4.2	Objetivos Específicos	6
1.5	Justificación	7
1.6	Delimitación	8
1.7	Hipótesis o premisas de investigación	9
1.8	Operacionalización	9

CAPÍTULO II MARCO TEÓRICO

N°	Descripción	Pág.
2.1	Antecedentes de la investigación	11
2.2	Marco teórico	12
2.2.1	Equipos de redes de computadora	12
2.2.1.1	Router	12
2.2.1.2	Switch	13

N°	Descripción	Pág.
2.2.1.3	Servidores	14
2.2.1.4	Firewall	14
2.2.2	Protocolo	15
2.2.3	Modelo de referencia TCP/IP	15
2.2.3.1	Capa de acceso a la red	17
2.2.3.2	Capa de internet	17
2.2.3.3	Capa de transporte	17
2.2.3.4	Capa de aplicación	18
2.2.4	Protocolo IP	18
2.2.5	Computación en la nube	18
2.2.5.1	Tipos de computación en la nube	20
2.2.5.2	Beneficios de la computación en la nube	21
2.2.6	Microsoft Azure	23
2.2.7	Recuperación ante desastres	25
2.2.8	ISO 27031:2011	25
2.2.8.1	Sistemas de gestión IRBC	26
2.2.9	Diseño jerárquico de la red	28
2.3	Marco contextual	29
2.4	Marco conceptual	30
2.5	Marco legal	31

CAPÍTULO III

METODOLOGÍA

N°	Descripción	Pág.
3.1	Diseño de la investigación	33
3.2	Enfoque de la investigación	33
3.2.1	Investigación cualitativa	35
3.2.2	Investigación cuantitativa	35

N°	Descripción	Pág.
3.3	Tipo de Investigación	36
3.4	Población y Muestra	36
3.4.1	Determinación de tamaño de la muestra	36
3.4.2	Análisis de los resultados de las encuestas	37
3.5	Método de observación directa	43
3.6	Infraestructura actual de la red	43
3.7	Inventario de equipos	44
3.7.1	Servidores	45
3.7.2	Router	49
3.7.3	Switch	50
3.7.4	Firewall	52

CAPÍTULO IV

PROPUESTA DE LA INVESTIGACIÓN

N°	Descripción	Pág.
4.1	Plan para la repotenciación de la infraestructura como propuesta de mejora	53
4.2	Análisis de la infraestructura de red	54
4.3	Plan para la implementación	55
4.3.1	Fase 1: Diseño	55
4.3.2	Fase 2: Plan estratégico	56
4.3.2.1	Control de acceso a la red mediante el uso del Wifi	56
4.3.2.2	Segmentación de red entre usuarios y servidores	56
4.3.2.3	Repotenciación de los servidores	57
4.3.2.4	Cambios y actualizaciones en máquinas virtuales	57
4.3.2.5	Replicación de los servidores a Microsoft Azure	57
4.3.2.6	Configuración Azure	58
4.4	Control de acceso a la red mediante Wifi	58

N°	Descripción	Pág.
4.4.1	Instalación física	59
4.4.2	Configuraciones del Mikrotik	61
4.5	Segmentación de red entre usuarios y servidores	69
4.6	Repotenciación de la infraestructura y los servidores	73
4.6.1	Configuración de ruta estática en el Fortinet	74
4.6.2	Optimización de los servidores	76
4.7	Replicación de los servidores a la nube de Azure	79
4.7.1	Requisitos previos	79
4.7.1.1	Requisitos de compatibilidad de los Host	79
4.7.2	Acceso a URL específicas	81
4.7.3	Configuración en Azure	81
4.7.3.1	Creación de una red virtual en Azure	81
4.7.3.2	Cuenta de almacenamiento	83
4.7.4	Preparación de los Host Hyper-V	83
4.7.5	Preparación de los servidores VMM	84
4.7.6	Creación de almacén Recovery Service	85
4.7.7	Preparación de la infraestructura	85
4.7.8	Configuración del entorno de destino	87
4.7.9	Política de replicación	88
4.7.10	Habilitación de la replica	90
4.8	Simulacro de recuperación ante desastre	91
4.8.1	Pasos para la conmutación por error de prueba en una sola máquina virtual	92
4.9	Conclusiones	93
4.10	Recomendaciones	95

ÍNDICE DE TABLAS

N°	Descripción	Pág.
1	Operacionalización de variables	10
2	Diferencias de enfoques de investigación	35
3	Lista de variables	37
4	Actualización constante de equipos de cómputo	38
5	Control de acceso a la información de la empresa	39
6	Respaldos generados por la empresa	40
7	Mejoras en infraestructura de red	41
8	Mecanismos existentes en la empresa	42
9	Servidor Lenovo (1)	45
10	Servidor IBM (1)	45
11	Servidor IBM (2)	46
12	Servidor IBM (3)	46
13	Servidor IBM (4)	47
14	Servidor IBM (5)	47
15	Servidor IBM (6)	48
16	Servidor IBM (7)	48
17	Servidor IBM (8)	49
18	Router Cisco 1800 series	49
19	Switch HP V1910 – 24G	50
20	Switch 3COM Baseline 2824	50
21	Switch HP 1410 - 24G	51
22	Fortinet Fortigate 200D	52
23	Segmento de red de todas las sucursales	70
24	Rutas estáticas configuradas en el Fortinet	76
25	Componentes de arquitectura Hyper-V con VMM	79
26	URL habilitadas en los hosts	81

N°	Descripción	Pág.
27	Valores para agregar una red virtual en Azure	82
28	Compatibilidad de servidores con Hyper-V	83
29	Compatibilidad de servidores VMM	84

ÍNDICE DE FIGURAS

N°	Descripción	Pág.
1	Router	13
2	Switch	13
3	Servidores	14
4	Firewall	15
5	Modelo de referencia TCP/IP	16
6	Integration of IRBC and BCMS	27
7	Enfoques de investigación	34
8	Actualización constante de equipos de cómputo	38
9	Control de acceso a la información de la empresa	39
10	Respaldos generados por la empresa	40
11	Mejoras en infraestructura de red	41
12	Mecanismos existentes en la empresa	42
13	Esquema de red	44
14	Mikrotik instalado	59
15	Switch uso de Mikrotik	60
16	Interfaz de Winbox	62
17	Winbox – Address	63
18	Winbox – Address list	63
19	Winbox – Route list	64
20	Winbox – Dns settings	65
21	Winbox – Configuración de perfil	66
22	Winbox – Creación de usuario	67
23	Winbox – Creación de perfiles de usuario	68
24	Winbox – Lista de perfiles de usuarios	69
25	Antes del cambio de segmento IP	71
26	Después del cambio de segmento IP	72

N°	Descripción	Pág.
27	Conexión doble en la ciudad de Guayaquil	74
28	Configuración de ruta estática Fortinet	75
29	Corrección de la conexión en la ciudad de Guayaquil	76
30	Memoria RAM para servidores	77
31	Disco duro SAS	78
32	Esquema del proceso de Réplica	80
33	Creación de una nueva red virtual en azure	82
34	Ventana de creación de almacén Recovery Service	85
35	Ventana para agregar un nuevo servidor Recovery Site	86
36	Configuración del almacén	87
37	Asignación de Red	88
38	Creación de política de replicación	89
39	Configuración de propiedades de la máquina virtual a replicar	91

ÍNDICE DE ANEXOS

N°	Descripción	Pág.
1	Normas generales para las instituciones del sistema financiero	98
3	Preguntas de la encuesta	102

AUTOR: BENAVIDES ALCÍVAR VICENTE ALBERTO
TÍTULO: “REPOTENCIACIÓN DE INFRAESTRUCTURA Y
SERVICIOS DE RED CON MEJORAS DE SEGURIDAD
ORIENTADO A LA NUBE”
DIRECTOR: ING. TELEC. PINOS GUERRA MARIO, MSI.

RESUMEN

El presente trabajo de titulación tiene como objetivo el presentar una planificación de los cambios necesarios que se deben de realizar en la infraestructura y servicios de red de una empresa de seguros de la ciudad de Guayaquil, haciendo uso del enfoque cualitativo basado en el uso de herramientas como entrevistas y consultas dirigidas al departamento de TI y a sus trabajadores, para poder así obtener un esquema de la infraestructura de red actual y de las necesidades de esta empresa de seguros para poder analizar los cambios que se deben de realizar tanto a nivel físico como lógico de los dispositivos de red, adicionalmente se realiza una guía del proceso de repotenciación de los servidores, se propone cambios en las políticas de seguridad para el acceso de la red y se da recomendaciones a los trabajadores sobre el acceso a sus computadoras y evitar dejar expuesta información importante, también se hace uso de la metodología documental, explicando detalladamente los pasos a seguir en el proceso de cambio haciendo uso de la investigación científica y exploratoria, logrando con estos cambios planificados en la infraestructura y los servicios de red, realizar replicaciones de los servidores importantes de la compañía como respaldo en caso de ocurrir un desastre y de esta manera implementar la computación en la nube.

PALABRAS CLAVES: Repotenciación, Seguridad, Análisis, Red, Computación en la nube.

Benavides Alcívar Vicente Alberto
C.C.0930672613

Ing. Telecom. Pinos Guerra Mario, MSI.
Director del Trabajo

AUTHOR: BENAVIDES ALCIVAR VICENTE ALBERTO
TOPIC: "REPOTENCIATION OF INFRASTRUCTURE AND
NETWORK SERVICES WITH SECURITY
IMPROVEMENTS ORIENTED TO THE CLOUD "
DIRECTOR: ING. TELEC. PINOS GUERRA MARIO, MSI.

ABSTRACT

The objective of this work is to present a plan of the necessary changes that must be done in the infrastructure and network services of an insurance company in the city of Guayaquil, using a qualitative approach based on the use of tools such as interviews and consultations directed to the TI department and to its employees, in order to obtain the current network infrastructure diagram and the needs of this insurance company in order to analyze changes that must be done to the network devices, both at a physical level and at a logical one, in addition it is developed a guide on the repowering process of the servers, and it is proposed the security policies for the network access and there are some recommendations given to workers on access to their computers and so avoid exposing important information, also it is used the documentary methodology, explaining in detail the steps to follow in the changing process using scientific and exploratory research, achieving with these planned changes in the infrastructure and network services, replications of the important company servers done as a backup in the event of a disaster and in this way implementing cloud computing.

KEY WORDS: Repowering, Security, Analysis, Network, Cloud Computing.

Benavides Alcivar Vicente Alberto
C.C.0930672613

Ing. Telec. Pinos Guerra Mario, MSI.
Director of work

INTRODUCCIÓN

Desde la llegada del internet cambió la forma en la que las personas se comunicaban o realizaban trabajos colaborativos, también cambió mucho la forma en la se administraba mucha de la información por parte de las empresas.

De igual manera el hombre en su necesidad de facilitar las actividades diarias realizadas, trabaja arduamente en el desarrollo de nuevas tecnologías que son actualizadas de manera constante y que las empresas tienen que tomar a consideración ese hecho, ya que cada avance en la tecnología es una puerta más que se abre para una optimización en los procesos que se realizan en una institución.

Pero las empresas al no preocuparse por una actualización constante del medio donde se maneja la información importante, dejan abierta la posibilidad de que esa misma información se vea perjudicada por un mal manejo o por la manipulación de información que puede llevar a cabo cualquier otra persona ajena a la organización al poder ingresar a ella por la falta de actualización de los equipos de red.

También un aspecto importante a tomar en consideración es el tener un mecanismo de seguridad que vaya acorde a al cambio tecnológico constante al que nos vemos involucrados, los servicios en la nube nos ofrecen muchas ventajas que nos son de gran utilidad en la actual, el hecho de poder guardar información en su plataforma y poder acceder a ella en cualquier parte del mundo a cualquier hora.

La computación en la nube es un camino que trae un gran cambio en lo que se refiere a la administración de una red empresarial, ya que nos

brinda muchos beneficios en comparación al tener una infraestructura física como lo tiene normalmente cada empresa, la computación en la nube reduce mucho el costo que requiere el mantener servidores activos las 24 horas del día y nos ofrecen más seguridad ya que son menos propensos a fallar porque son servicios dedicados.

CAPÍTULO I

EL PROBLEMA

1.1 Planteamiento del problema

Las computadoras han tenido mucha importancia para el ser humano desde el momento en que fueron creadas y con el pasar del tiempo se han ido mejorando tanto en su funcionamiento como en la comodidad que le ofrece al hombre; todo esto ha sido uno de los grandes inventos que el ser humano ha forjado por la necesidad de mejorar sus condiciones de vida y realizar con facilidad y haciendo una simplificación de las dificultades o problemas de su vida diaria.

La información y la comunicación son dos de los temas estratégicos más importantes para el éxito de cada empresa.

Si bien hoy en día casi todas las organizaciones usan una cantidad sustancial de computadoras y herramientas de comunicación (como teléfono o fax), a menudo todavía están aisladas. Si bien los gerentes de hoy en día pueden usar aplicaciones como procesadores de texto u hojas de cálculo, no muchas de ellas usan herramientas informáticas para que entre departamentos se puedan conectar y compartir información.

Para superar estos obstáculos en un uso efectivo de la tecnología de la información, las redes de computadoras son necesarias. Son un nuevo tipo (podría llamarse paradigma) de organización de sistemas informáticos producidos por la necesidad de combinar computadoras y comunicaciones. Al mismo tiempo, son el medio para converger las dos áreas.

Las redes informáticas pueden eliminar las barreras que existen entre la información contenida en varios sistemas (no solo informáticos). Solo con la ayuda de las redes informáticas se puede construir un entorno de comunicación e información sin fronteras.

Desde la aparición del internet se ha considerado esta como una herramienta fundamental y de mucha importancia en cualquier ámbito de nuestras vidas, en la actualidad el internet es fundamental para la comunicación por vía electrónica ya que actualmente la mayor parte de las empresas en todo el mundo utiliza la Web para suministrar a sus clientes la información de la empresa, sus productos y los servicios que ofrece.

Pero, así como el internet es de suma importancia de la misma forma lo es el tener una buena estructura de red, la mayoría de las instituciones públicas y privadas que se localizan en la ciudad de Guayaquil tienen una estructura de red física la cual es de uso cotidiano de todos los empleadores de dichas instituciones.

Las estructuras de redes al pasar de los años han ido evolucionando acorde al avance de la tecnología o acorde a la necesidad de las instituciones que hacen uso de la misma, al día de hoy contar con una buena estructura de red en todos sus niveles es equivalente a contar con el servicio de energía eléctrica para nuestra institución, es decir, que son fundamentales para el desempeño de la propia organización.

Como tal, esta debe ser pensada como parte del núcleo de nuestra organización, debe de ser tratada más como una inversión y no como un gasto ya que nos ofrecen ventajas tales como:

- Mayor facilidad en la comunicación entre usuarios.
- Reducción en el presupuesto de software.
- Reducción en el presupuesto de hardware.

- Posibilidad de organizar grupos de trabajo.
- Mejorar la administración de los equipos.
- Mejora en la integridad de los datos.
- Mayor seguridad para acceder a la información.

Las redes de informática nos ayudan a simplificar nuestras tareas, pero debido a que no todas las organizaciones diseñan su infraestructura de red pensando en un crecimiento exponencial de la organización o incluso por no tener el conocimiento de las nuevas tecnologías (desarrolladas e implementadas después de varios años), esto ha ocasionado que algunas redes computacionales queden obsoletas con el tiempo por causa del deterioro o falta de actualización.

De la misma forma también se tienen los problemas de seguridad si no se ha actualizado la arquitectura de la red ya que las organizaciones pueden tener varias vulnerabilidades que pueden llegar al alcance de cualquier persona que tenga malas intenciones y que por estos descuidos pueda llegar a la información importante de la organización.

1.2 Formulación del problema

¿Cuáles son los mecanismos de repotenciación que se pueden aplicar a una infraestructura de red en una organización y como poder llevar dicha repotenciación a la nube como medio de contingencia?

1.3 Sistematización del problema

Hoy en día muchas de las organizaciones que existen en la ciudad de Guayaquil no se preocupan por realizar una actualización constante a los equipos de cómputo y a las redes que dicha organización usa diariamente, sin tomar en cuenta que el núcleo de la organización es la información que viaja por esas redes de un lugar a otro hasta cumplir un cometido. Por esta razón se tomará una empresa de seguros de la ciudad

de Guayaquil como ejemplo para hacer una repotenciación de la infraestructura y servicios de red para mantener la disponibilidad de la información.

En este trabajo de titulación se necesita dar respuestas a las siguientes interrogantes:

¿Cuál es la condición actual de la infraestructura de red dicha empresa de seguros?

¿Qué proceso se debe llevar a cabo para realizar una repotenciación de infraestructura y servicios de red?

¿Por qué debemos orientar esta repotenciación a la nube?

¿Cuáles son las mejoras de seguridad que se obtendrá realizando la repotenciación de la infraestructura y servicios de red de esta empresa de seguros?

1.4 Objetivos generales y específicos

1.4.1 Objetivo General

Re-diseñar la estructura y servicios de red de la empresa de seguros, proponiendo también una migración de los servidores fundamentales para el desempeño de la empresa a la nube Azure de Microsoft orientado a una posible actualización a futuro de los servicios basados en la nube.

1.4.2 Objetivos Específicos

- 1) Analizar el estado actual de la infraestructura de red de la empresa de seguros.

- 2) Identificar las configuraciones necesarias para la optimización de la red de la empresa de seguros.
- 3) Realizar una guía sobre el proceso de repotenciación y migración de la red a la nube de Microsoft.
- 4) Propuesta de un plan de mejora.

1.5 Justificación

Debido a que las redes de computación son tan importantes para una organización y son una parte fundamental para el desempeño de cada una de las actividades realizadas dentro de esa misma organización, las redes de computación es algo que siempre ha estado con nosotros de manera permanente.

Varias de las organizaciones de la ciudad de Guayaquil no diseñaron esas redes pensando en una crecimiento a futuro o incluso algunas solo se conformaron con que las conexiones de red estén en capacidad para trabajar y no se tomó a consideración un diseño óptimo para los diferentes segmentos de la red acorde a cada equipo que se va a conectar, si la vía donde viaja la información importante de la organización es la indicada para esto o incluso sin tener un control de quienes tienen acceso a ese medio.

Mantener los servidores separados del mismo rango ip que la LAN, tener una organización de jerarquías de equipos y permisos de cada uno, son unas de las tantas falencias que tienen muchas organizaciones en la ciudad de Guayaquil, falencias de las cuales se pueden aprovechar personas mal intencionadas y perjudicar a la empresa, ya que el núcleo de una organización es la información que ella maneja.

Debido al panorama descrito surge la idea de este proyecto en realizar un rediseño de la red con una repotenciación de los equipos de cómputo y ayudarnos con las nuevas tecnologías para crear una alternativa de actualización a futuro.

1.6 Delimitación

En el presente trabajo de titulación busca elaborar una guía instructiva para elegir la mejor opción que se puede emplear para realizar una repotenciación de la infraestructura y servicios de red de una empresa de seguros de la ciudad de Guayaquil acorde a la infraestructura que posee actualmente.

Se indicará en el instructivo como realizar una reorganización de las redes que dispone la organización para llevar un control de todos los segmentos de red que hace uso tanto en Guayaquil como en las otras sucursales (Quito, Cuenca).

También en el instructivo se indicará como hacer una reorganización de las redes de la empresa con una mentalidad a futuro utilizando el servicio de la nube de Microsoft que nos ofrece beneficios tales como:

- 1) Reducción de costes ya que la nube evita la compra de hardware y un importante ahorro en consumo energético
- 2) Flexibilidad en obtener más recursos de los que normalmente se necesita según la necesidad de cada momento.
- 3) Disponibilidad ya que las máquinas virtuales están basadas en infraestructuras de alta redundancia permitiendo que trabajen continuamente.

- 4) Seguridad en la información debido a que Microsoft cumple con altas normativas de seguridad que son aplicadas a sus datacenters.

El propósito de este proyecto es documentar el proceso que se debe llevar a cabo para el mejoramiento de la infraestructura y servicios de red de una organización y dando una guía sobre cómo llevar este mejoramiento a la nube en el futuro, ya que el avance de la tecnología nunca se detiene.

En el instructivo se indicará también como podemos usar una copia de respaldo sincronizada como un método de seguridad si el centro de cómputo de la organización llegará a tener algún fallo grave y no pueda operar por un tiempo determinado, ya que se puede activar las máquinas virtuales en la nube de Azure re direccionar el tráfico de la red y seguir realizando las actividades diarias.

1.7 Hipótesis o premisas de investigación

En este proyecto se va ofrecer un plan de mejoras en la infraestructura y servicios de red que tiene una empresa de seguros, que adicionalmente se podrá usar esa mejora para hacer una copia sincronizada de dicha red a la nube Azure de Microsoft mejorando así el rendimiento de la red, ofreciendo más seguridad en la información que se maneja diariamente con la información de la empresa y mantener un respaldo que caso de algún desastre poder seguir realizando las actividades de forma normal con la ayuda de la nube hasta que se pueda reestablecer el centro de cómputo sin pérdida de datos.

1.8 Operacionalización

A continuación, se realiza una descripción del cuadro de operacionalización:

TABLA N° 1
OPERACIONALIZACIÓN DE VARIABLES

Variables	Tipo de variable	Definición	Dimensión	Indicadores
Fuga de información	Dependiente	Robo y manipulación de datos por terceras personas	Integridad y Disponibilidad de los datos	- Tracking en tiempo real - Verificar los logs
Pérdida de conexión		Perder la conectividad con los servidores o con computadoras que cumplen una actividad específica	Disponibilidad en los servicios que brinda la organización	- Logs de los equipos cuando los puertos se apagan
Carencia de sistemas de redundancia y repotenciación de la infraestructura	Independiente	Asegurar la disponibilidad de los sistemas	Asegurar el manejo de la información de manera permanente	- Valoración de la antigüedad de la red

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes de la investigación

En las últimas décadas el avance de la tecnología nos ha sorprendido cada vez más, el hecho de que un año tengamos un dispositivo tecnológico y que años más tarde tengamos ese mismo dispositivo 2 o 3 veces más potente que el que solíamos tener, nos muestra como el hombre en su necesidad de simplificar las actividades diarias sigue desarrollando tecnología arduamente y que debemos de mantenernos actualizados para tener un óptimo desempeño en nuestras actividades.

Lo mismo aplica para las redes de informática, ya que estas nos ayudan a simplificar el manejo de información dentro de la misma organización e incluso reducir tiempo y costos si se tiene una organización con varias sucursales en el país, porque al contar con una red de informática se puede trabajar con la misma información en varios lugares del país al mismo tiempo, se optimiza el tiempo en el que le tomaría a un gerente viajar a una reunión importante a una sucursal ya que lo podría realizar desde su propia oficina haciendo uso del internet.

La inseguridad en el manejo de la información es algo que preocupa constantemente a muchas de las organizaciones de la ciudad de Guayaquil, principalmente por el hecho de tener un centro de cómputo ubicado en una de las localidades principales de la empresa y que todo el tráfico de red pasa por ella antes de salir al internet, eso da a entender que ese centro de cómputo es una parte fundamental para el desarrollo de las

actividades diarias y que debe tener un mantenimiento constante para su correcto funcionamiento.

Pero lamentablemente varias de las organizaciones no van realizando los cambios pertinentes a su red de manera constante y se quedan con la tecnología que tienen en ese momento hasta que les deje de funcionar, esto impide que las organizaciones se puedan adaptar a nuevas tecnologías o nuevos servicios que se pueden emplear a nuestras actividades diarias facilitando aún más su desarrollo.

Debido a los antecedentes mencionados anteriormente se llega a la necesidad de hacer una repotenciación en los equipos de la red de informática de las organizaciones, mejorar las características de los servidores que lo requieran, y hacer los cambios necesarios para poder orientar ese centro de cómputo a la nube de Microsoft para usarlo como método de contingencia en caso de algún problema.

2.2 Marco teórico

2.2.1 Equipos de redes de computadoras

2.2.1.1 Router

Un enrutador conecta redes en función a su conocimiento actual de la red a la que está conectado, un enrutador actúa como despachador ya que decide de qué forma enviar cada paquete de información. Un enrutador se encuentra en cualquier puerta de enlace (donde una red se encuentra con otra), incluido cada punto de presencia en Internet. (Alencar, 2012)

FIGURA N°1
ROUTER

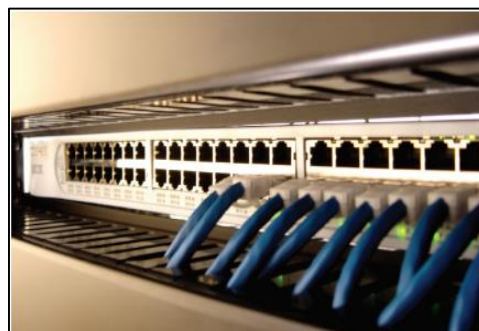


Fuente: Fundamentos de Redes de Computadores
Elaborado por: (Alencar, 2012)

2.2.1.2 Switch

Un switch es un dispositivo que analiza los datos entrantes desde cualquiera de los múltiples puertos de entrada al puerto de salida específico que llevará los datos hacia su destino previsto. En la red telefónica tradicional con switch de circuitos, uno o más switch se utilizan para establecer una conexión o circuito dedicado, aunque temporal para un intercambio entre dos o más partes. (Alencar, 2012)

FIGURA N°2
SWITCH

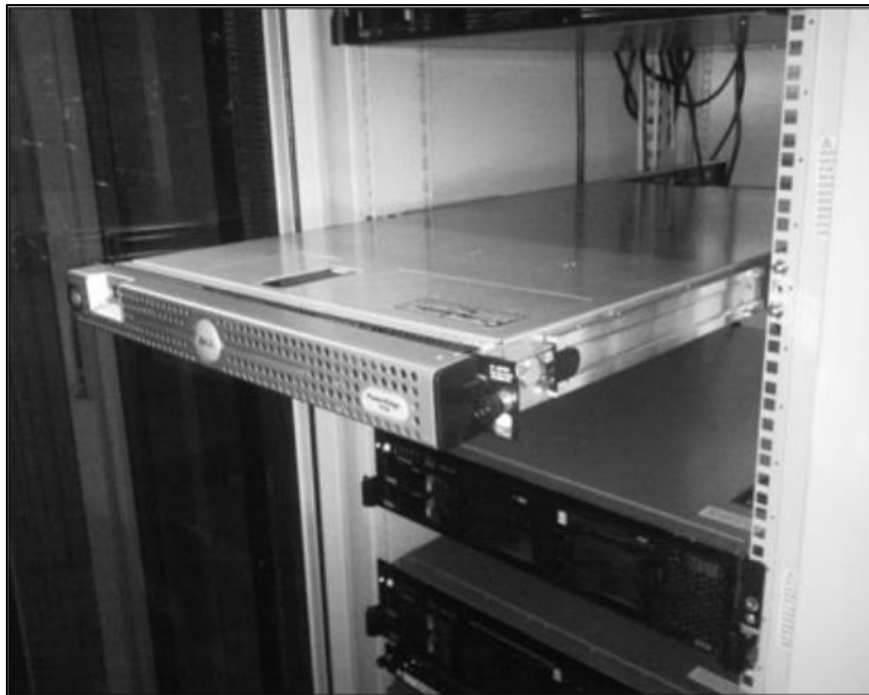


Fuente: Fundamentos de Redes de Computadores
Elaborado por: (Alencar, 2012)

2.2.1.3 Servidores

Un servidor es una computadora diseñada para procesar solicitudes y entregar datos a otras computadoras (clientes) a través de una red local o internet. Aunque cualquier computadora con software especial puede funcionar como servidor, el uso más común de la palabra hace referencia a las máquinas muy grandes y de gran potencia que funcionan como bombas que empujan y extraen datos a través de Internet. (Enzo Augusto, 2011)

FIGURA N°3
SERVIDOR



Fuente: Administrador de servidores
Elaborado por: (Enzo Augusto, 2011)

2.2.1.4 Firewall

Un firewall actúa como una barrera entre una red confiable y una red que no es de confianza. Un firewall controla el acceso a los recursos de una red a través de un modelo de control positivo. Esto significa que el único

tráfico permitido en la red se define en la política del firewall; todo el otro tráfico es denegado. (Cisco, 2017)

FIGURA N°4
FIREWALL



Fuente: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html
Elaborado por: Cisco

2.2.2 Protocolo

Conocido a veces como un método de acceso, un protocolo es un estándar usado para definir un método de intercambio de datos a través de una red informática, como red de área local, Internet, Intranet, etc. Cada protocolo tiene su propio método de cómo se formatean los datos cuando enviado y qué hacer con él una vez recibido, cómo se comprimen esos datos, o cómo comprobar si hay errores en los datos. (Tanenbaum & Wetherall, 2012)

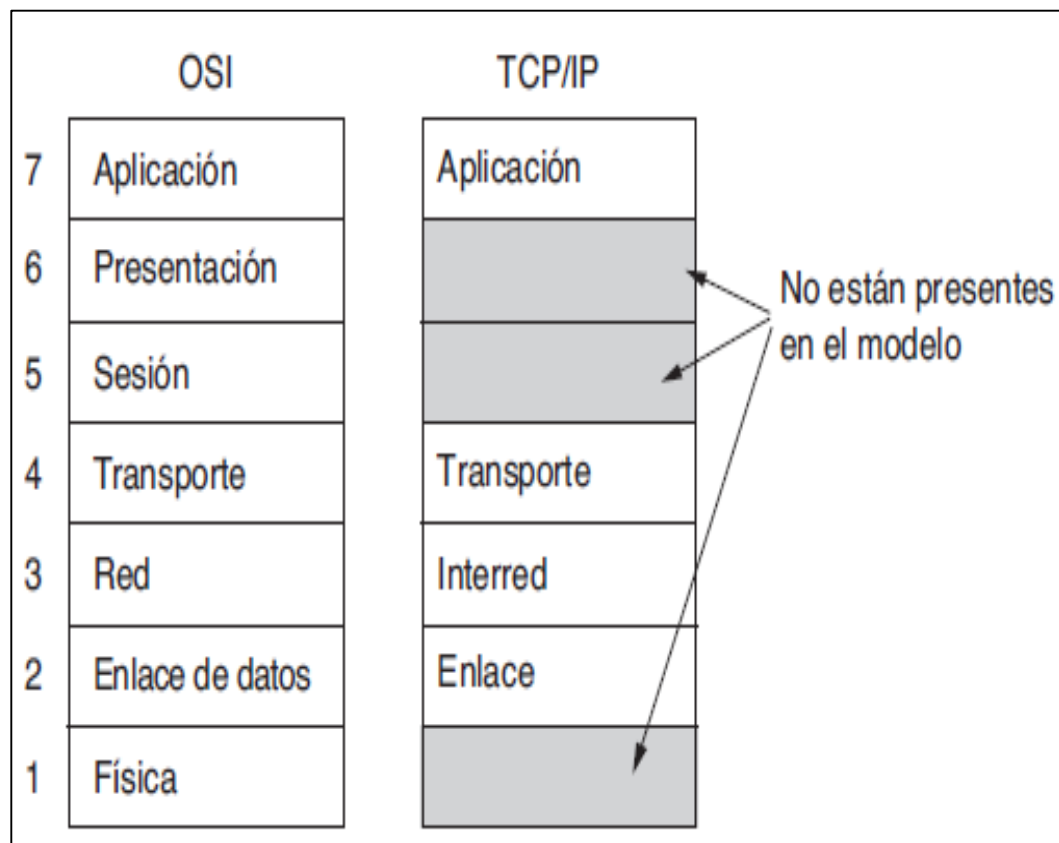
2.2.3 Modelo de referencia TCP/IP

El conjunto de protocolos Protocolo de control de transmisión / Protocolo de Internet (TCP / IP) es el motor para Internet y redes en todo el mundo. Su simplicidad y poder ha llevado a que se convierta en el protocolo de red único de elección en el mundo de hoy. TCP / IP es un conjunto de

protocolos desarrollados para permitir que las computadoras cooperantes compartan recursos a través de la red.

Este modelo fue desarrollado y utilizado inicialmente por ARPANET (Advanced Research Project Agency Network). ARPANET fue una comunidad de investigadores patrocinados por el departamento de defensa de los EE. UU. Define un conjunto de reglas para permitir que las computadoras se comuniquen a través de una red, especificando cómo se deben empaquetar, direccionar, enviar, enrutar y entregar los datos al destino correcto. La especificación define protocolos para diferentes tipos de comunicación entre computadoras y proporciona un marco para estándares más detallados. (Tanenbaum & Wetherall, 2012)

FIGURA N°5
MODELO DE REFERENCIA TCP/IP



Fuente: redes de computadoras
Elaborado por: (Tanenbaum & Wetherall, 2012)

2.2.3.1 Capa de enlace de red

La capa de interfaz de red, también llamada capa de enlace o la capa de enlace de datos o Host a capa de red, es la interfaz con el hardware de red real. Esta interfaz puede proporcionar o no una entrega confiable, y puede estar orientada a paquetes o secuencias.

De hecho, TCP / IP no especifica ningún protocolo aquí, pero puede usar casi cualquier interfaz de red disponible, lo que ilustra la flexibilidad de la capa IP. (Tanenbaum & Wetherall, 2012)

2.2.3.2 Capa de Internet

Es la segunda capa del modelo TCP / IP de cuatro capas. La posición de la capa de Internet se encuentra entre la capa de acceso a la red y la capa de transporte. Los datos del paquete de capa de Internet guardan en paquetes de datos conocidos como datagramas IP, que contienen información de dirección de origen y destino (dirección lógica o dirección IP) que se utiliza para reenviar los datagramas entre los hosts y las redes. La capa de Internet también es responsable del enrutamiento de los datagramas de IP. (Tanenbaum & Wetherall, 2012)

2.2.3.3 Capa de transporte

La capa de transporte proporciona la transferencia de datos de extremo a extremo entregando datos desde una aplicación a su par remoto. Múltiples aplicaciones pueden ser soportadas simultáneamente. El protocolo de capa de transporte más utilizado es el Protocolo de control de transmisión (TCP), que proporciona entrega confiable de datos orientada a conexión, supresión de datos duplicados, control de congestión y control de flujo. (Tanenbaum & Wetherall, 2012)

2.2.3.4 Capa de aplicación

La capa de aplicación es provista por el programa que usa TCP / IP para la comunicación. Una aplicación es un proceso de usuario que coopera con otro proceso generalmente en un host diferente (también hay un beneficio para la comunicación de la aplicación dentro de un solo host). Entre los ejemplos de aplicaciones se incluyen Telnet y el Protocolo de transferencia de archivos (FTP). (Tanenbaum & Wetherall, 2012)

2.2.4 Protocolo IP

Abreviatura de la dirección del Protocolo de Internet, una dirección IP o IP es un número que se usa para indicar la ubicación de una computadora u otro dispositivo en una red que usa TCP / IP. Estas direcciones son similares a las de una casa, lo que permite que los datos lleguen al destino apropiado en una red e Internet.

IP especifica el formato de los paquetes, también llamados datagramas, y el esquema de direccionamiento. La mayoría de las redes combinan IP con un protocolo de nivel superior llamado Transmission Control Protocol (TCP), que establece una conexión virtual entre un destino y una fuente.

La IP en sí misma es algo así como el sistema postal. Le permite abordar un paquete y soltarlo en el sistema, pero no hay un vínculo directo entre usted y el destinatario. TCP / IP, por otro lado, establece una conexión entre dos hosts para que puedan enviar mensajes de ida y vuelta durante un período de tiempo. (Forouzan, 2011)

2.2.5 Computación en la nube

Internet está cambiando la forma en que hacemos negocios e interactuamos como sociedad. Tradicionalmente, el hardware y el software

están completamente contenidos en la computadora de un usuario. Esto significa que accede a sus datos y programas exclusivamente dentro de su propia computadora.

La computación en la nube permite acceder a los datos y programas fuera de su propio entorno informático. En lugar de almacenar los datos y software en su computadora personal o servidor, se almacena en 'la nube'. Esto podría incluir aplicaciones, bases de datos, correo electrónico y servicios de archivos.

Una analogía común para describir la computación en la nube es alquilar versus comprar. Básicamente, se alquila capacidad (espacio de servidor o acceso a software) de un proveedor de servicios en la nube y se conecta a través de Internet. En lugar de comprar sus propios requisitos de TI, se alquila un proveedor de servicios, pagando solo por los recursos que usa (Thomas, Zaigham, & Ricardo, 2013).

La computación en la nube tiene 4 modelos en términos de diferentes opciones de acceso y seguridad. Antes de mover sus datos a la nube, deberá considerar qué modelo funciona mejor para su negocio y las necesidades de datos.

Nube privada: Una nube privada es donde los servicios y la infraestructura son mantenidos y gestionados el administrador de TI o un tercero. Esta opción reduce los posibles riesgos de seguridad y control, y le servirá si sus datos y aplicaciones son una parte central de su negocio y necesita un mayor grado de seguridad o requisitos de datos confidenciales.

Nube comunitaria: es una nube de la comunidad donde varias organizaciones comparten el acceso a una nube privada, con consideraciones de seguridad similares. Por ejemplo, una serie de

franquicias tienen sus propias nubes públicas, pero están alojadas de forma remota en un entorno privado.

Nube pública: Una nube pública es donde los servicios se almacenan fuera del sitio y se accede a través de Internet. El almacenamiento lo gestiona una organización externa como Google o Microsoft. Este servicio ofrece el mayor nivel de flexibilidad y ahorro de costos; sin embargo, es más vulnerable que las nubes privadas.

Nube híbrida: Un modelo de nube híbrida aprovecha las ventajas de los servicios de nube públicas y privadas. Al difundir sus opciones a través de diferentes modelos de nube, obtiene los beneficios de cada modelo.

Por ejemplo, podría usar una nube pública para que sus correos electrónicos ahorren en grandes costos de almacenamiento, mientras mantiene sus datos altamente confidenciales seguros y protegidos detrás de su firewall en una nube privada.

2.2.5.1 Tipos de computación en la nube

Hay 3 tipos principales de modelos de servicios de computación en la nube disponibles, comúnmente conocidos como:

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

Software as a Service (SaaS): es la forma más común de computación en la nube para pequeñas empresas. Puede acceder a aplicaciones de software alojadas en Internet utilizando un navegador, en lugar de aplicaciones tradicionales almacenadas en su propia PC o

servidor. El host de la aplicación de software es responsable de controlar y mantener la aplicación, incluidas las actualizaciones y configuraciones de software. Usted, como usuario, tiene un control limitado sobre la aplicación y la configuración.

Un ejemplo típico de un SaaS es un servicio de correo basado en la web o un sistema de gestión de relaciones con el cliente.

Infrastructure as a Service (IaaS): Por lo general, IaaS significa comprar o alquilar la energía de su computadora y el espacio en disco de un proveedor de servicios externo. Esta opción le permite acceder a través de una red privada o a través de Internet. El proveedor del servicio mantiene el hardware físico de la computadora, incluido el procesamiento de la CPU, la memoria, el almacenamiento de datos y la conectividad de la red. Los ejemplos de IaaS incluyen Amazon EC2, Rackspace y Windows Azure.

Platform as a Service (PaaS): se puede describir como un cruce de ambos, SaaS e IaaS. Básicamente alquila el hardware, los sistemas operativos, el almacenamiento y la capacidad de red que proporciona IaaS, así como los servidores de software y los entornos de aplicaciones. PaaS le ofrece más control sobre los aspectos técnicos de su configuración informática y la capacidad de personalizar para satisfacer sus necesidades.

2.2.5.2 Beneficios de la computación en la nube

La computación en la nube brinda muchos beneficios para las empresas. Estos servicios dan una gran comodidad para administrar su negocio en cualquier lugar y en cualquier momento que se desee gracias a que este servicio nos da la capacidad de tener nuestra oficina virtual donde podemos administrar los recursos de nuestros servicios de red en la nube.

Menos problemas operativos: la computación en la nube puede parecer complicada, pero en realidad tiene menos problemas que otras

infraestructuras. Dado que la nube se ejecuta en sus propios servidores a través de una empresa cuyo único trabajo es hacer que la nube sea funcional y libre de errores, por lo general es mucho más confiable que su propio servidor en la ubicación física.

De hecho, en el momento en que surge un pequeño error, la compañía que ejecuta su red en la nube probablemente ya está buscando una solución. Si este fuera su servidor remoto, tendría que presentar un reclamo con soporte técnico y hacer que el departamento envíe a alguien para que lo revise.

Ahorra de dinero: una de las mejores partes de la nube es que realmente se ahorra dinero a largo plazo. Si no tiene que contratar un equipo de soporte técnico para solucionar los problemas del servidor, bueno, eso ya tiene beneficios en el bolsillo.

Además, la computación en la nube es escalable. Los servidores tradicionales requieren actualizaciones costosas que cuestan mucho por adelantado. Si su empresa no se expande tanto como esperaba, ese es el dinero que ha desperdiciado. Los proveedores de servicios en la nube generalmente le permiten escalar hacia arriba y hacia abajo sin problemas.

La nube requiere menos capital: una de las principales ventajas de la computación en nube es que requiere menos costos de inicio que un servidor regular y local. Simplemente paga por la cantidad de almacenamiento que necesita por mes. Dado que el trabajo de su servicio de computación en la nube es actualizar su sistema con parches nuevos, esto sucede automáticamente. No tiene que gastar dinero en actualizaciones de hardware sofisticadas y lentas. Obtiene puramente lo que necesita, cuando lo necesita.

La nube tiene una mejor seguridad: la computación en la nube ofrece más seguridad que los servidores locales. Nunca tendrá que

preocuparse por perder datos críticos y aplicaciones comerciales debido a un desastre natural o un colapso total de la computadora. Algunos proveedores de servicios en la nube incluso respaldan datos en servidores remotos adicionales, por lo que la pérdida de datos simplemente no ocurrirá. Los proveedores de nube también realizan auditorías de seguridad más regulares de lo que probablemente haría en su servidor local. Esto lo hace hermético y su información confidencial se mantiene en secreto.

2.2.6 Microsoft azure

Microsoft Azure, anteriormente conocida como Windows Azure, es la plataforma de computación en la nube pública de Microsoft. Proporciona una gama de servicios en la nube, incluidos los de cómputo, análisis, almacenamiento y redes. Los usuarios pueden seleccionar y elegir entre estos servicios para desarrollar y escalar nuevas aplicaciones, o ejecutar aplicaciones existentes, en la nube pública. (Microsoft, 2017)

Microsoft categoriza los servicios de Azure en 11 tipos de productos principales:

- a) Computación: Microsoft en este tipo de servicio nos ofrece el poder tener acceso a máquinas virtuales, contenedores de almacenamientos de bases de datos, un nivel de procesamiento por niveles de lotes y el poder hacer uso de las aplicaciones desde cualquier lugar remotamente
- b) Web y dispositivos móviles: estos servicios respaldan el desarrollo y la implementación de aplicaciones web y móviles, y también ofrecen funciones para la administración, notificación e informes de la API.
- c) Almacenamiento de datos: esta categoría incluye las ofertas de Base de datos como servicio para SQL y NoSQL, así como el almacenamiento en la nube no estructurado y en caché.

- d) **Análisis:** estos servicios brindan análisis y almacenamiento distribuidos, así como análisis en tiempo real, análisis de big data, lagos de datos, aprendizaje automático y almacenamiento de datos.
- e) **Redes:** este grupo incluye redes virtuales, conexiones y gateways dedicados, así como también servicios para el manejo del tráfico, balanceo de carga y alojamiento de sistemas de nombres de dominio (DNS).
- f) **Medios y red de entrega de contenido (CDN):** estos servicios incluyen la transmisión a demanda, la codificación y la reproducción e indexación de medios.
- g) **Integración híbrida:** estos son servicios para copia de seguridad del servidor, recuperación del sitio y conexión de nubes privadas y públicas.
- h) **Identity and access management (IAM):** estas ofertas garantizan que solo los usuarios autorizados puedan emplear los servicios de Azure y ayudar a proteger las claves de cifrado y otra información confidencial.
- i) **Internet de las cosas (IoT):** estos servicios ayudan a los usuarios a capturar, monitorear y analizar datos de la IoT desde sensores y otros dispositivos.
- j) **Desarrollo:** estos servicios ayudan a los desarrolladores de aplicaciones a compartir código, probar aplicaciones y rastrear problemas potenciales. Azure admite una variedad de lenguajes de programación de aplicaciones, incluidos JavaScript, Python, .NET y Node.js.

- k) Administración y seguridad: estos productos ayudan a los administradores en la nube a administrar su implementación de Azure, programar y ejecutar trabajos, y crear automatización. Este grupo de productos también incluye capacidades para identificar y responder a amenazas de seguridad en la nube.

2.2.7 Recuperación ante desastres

La recuperación ante desastres es un área de planificación de seguridad que tiene como objetivo proteger a una organización de los efectos de eventos negativos significativos. Esto permite a una organización mantener o reanudar rápidamente funciones de misión crítica después de un desastre.

Un desastre puede ser cualquier cosa que ponga en riesgo las operaciones de una organización, desde un ciberataque hasta fallas en los equipos o desastres naturales. El objetivo de la recuperación ante desastres es que una empresa continúe operando lo más cerca posible de lo normal. (Snedaker, 2013)

2.2.8 ISO 27031:2011

El estándar abarca todos los eventos e incidentes (no solo relacionados con la seguridad de la información) que podrían tener un impacto en la infraestructura y los sistemas de TIC. Por lo tanto, amplía las prácticas de manejo y gestión de incidentes de seguridad de la información, planificación y servicios de preparación de TIC.

La disponibilidad de las TIC debería, por supuesto, reducir el impacto (es decir, el alcance, la duración y / o las consecuencias) de los incidentes de seguridad de la información en la organización.

La norma incorpora el enfoque cíclico PDCA, que extiende el proceso de planificación de la continuidad del negocio convencional para tener más en cuenta las TIC. Incorpora 'métodos de evaluación de escenarios de falla' como FMEA (Modalidades de falla y análisis de efectos), con un enfoque en la identificación de 'eventos desencadenantes' que podrían precipitar incidentes más o menos graves. (Jon & Trey, 2014)

ISO 27031 introduce un enfoque de sistemas de gestión para abordar las TIC en apoyo de un sistema de gestión de continuidad empresarial más amplio, como se describe en ISO 22301. ISO 27031 describe un sistema de gestión para la disponibilidad de TIC para la continuidad del negocio (IRBC).

Un IRBC es un sistema de gestión centrado en la recuperación de desastres de TI. IRBC utiliza el mismo modelo de Planificar-Hacer-Verificar-Actuar (PDCA) que el sistema de gestión de la continuidad del negocio descrito en ISO 22301. El objetivo de IRBC es implementar estrategias que reduzcan el riesgo de interrupción de los servicios TIC, así como responder y recuperarse de una interrupción.

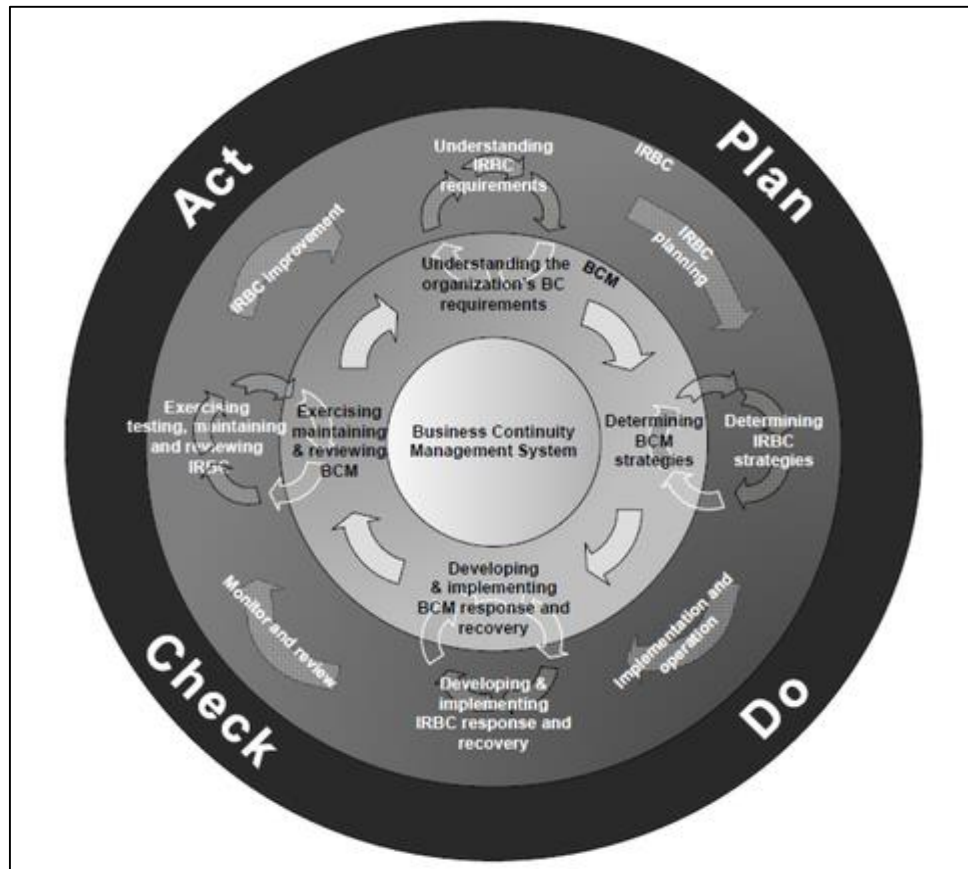
Los profesionales de la continuidad empresarial y de TI encontrarán muy familiar el uso del modelo PDCA, pero con los cambios necesarios para respaldar la capacidad de recuperación de las TIC en función de los requisitos y expectativas del negocio.

2.2.8.1 Sistemas de gestión IRBC

ISO 27031 utiliza el mismo sistema de gestión de PDCA básico utilizado en ISO 22301, pero lo adapta para adaptarse a la naturaleza técnica de IRBC. Además de los cambios técnicos en PDCA, ISO 27031 también se basa en las conclusiones del Análisis de Impacto Empresarial (BIA), desarrolladas y aprobadas como parte de un BCMS más amplio para

una organización. Para IRBC, el sistema de gestión de PDCA se desglosa de la siguiente manera:

FIGURA N°6
Integration of IRBC and BCMS



Fuente: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en>
Elaborado por: ISO/IEC 2011

Plan: la fase Plan crea y actualiza la estructura de gobierno para el sistema general de gestión IRBC. Los productos clave de la fase del Plan son una política de IRBC que aborda adecuadamente la continuidad de las tecnologías de información y comunicación y las opciones de estrategia que la organización puede implementar para cumplir con los requisitos del negocio.

Do: esta fase se centra en realizar actividades e implementar soluciones que permitan a la organización monitorear, responder y

recuperarse de una interrupción en los servicios de TIC. Los productos clave para la fase Do son la implementación de estrategias, la generación de planes y la ejecución de actividades de capacitación y sensibilización para promover la continuidad de los servicios de TIC.

Check: la fase de verificación incluye la revisión y evaluación del rendimiento del sistema de gestión IRBC. Los principales resultados de la fase de verificación incluyen el monitoreo continuo de las tecnologías de información y comunicación para las interrupciones y los niveles de rendimiento, así como revisiones periódicas de la capacidad de respuesta y recuperación de las TIC.

Act: esta fase le brinda a la administración la oportunidad de revisar el desempeño del esfuerzo de IRBC así como dirigir la implementación de acciones correctivas que mejorarán el desempeño del sistema de gestión y / o reducirán el riesgo de futuras interrupciones en los servicios de TIC.

2.2.9 Diseño jerárquico de la red

Para cumplir con los objetivos comerciales y técnicos de un cliente para un diseño de red corporativa, es posible que deba recomendar una topología de red que consta de muchos componentes interrelacionados. Esta tarea es más fácil si puede "dividir y conquistar" el trabajo y desarrollar el diseño en capas.

Los expertos en diseño de redes han desarrollado el modelo de diseño de red jerárquico para ayudarlo a desarrollar una topología en capas discretas. Cada capa se puede enfocar en funciones específicas, lo que le permite elegir los sistemas y características correctos para la capa. Por ejemplo, los enrutadores WAN de alta velocidad pueden transportar tráfico a través de la red troncal WAN empresarial, los enrutadores de velocidad media pueden conectar edificios en cada campus y los conmutadores pueden conectar dispositivos y servidores de usuario dentro de los edificios.

Existen 3 capas en las jerarquías de red:

- 1) **Capa de acceso:** En el modelo jerárquico de Cisco, también es conocido como el modelo de interconexión jerárquico, la capa de acceso es responsable de proporcionar a los dispositivos del usuario final una conexión a los recursos de la red.
- 2) **Capa de distribución:** La capa de distribución es una de las capas más significativas entre las tres (núcleo, acceso, distribución), ya que agrega los datos recibidos desde la red de la capa de acceso antes de transmitir a la capa central.
- 3) **Capa de núcleo:** Las redes con capa de núcleo generalmente tienen una topología de malla que proporciona conexiones de cualquier tipo entre dispositivos en la red. Muchos proveedores de servicios tendrían sus propias redes centrales que están interconectadas. Algunas grandes empresas tienen su propia red núcleo, que generalmente están conectadas a las redes públicas.

2.3 Marco contextual

En el desarrollo de este proyecto de titulación sobre el tema de la repotenciación de servicios y servicios de red con mejoras de seguridad orientado a la nube, se realizó una investigación en una empresa de seguros de la ciudad de Guayaquil, donde en una conversación con el administrador del centro de cómputo de dicha organización se indicó que carece de un plan estratégico de mejoras de su centro de cómputo orientado a la nube.

También se pudo identificar que el motivo era porque los equipos con los que estaban trabajando no cumplían un requerimiento mínimo para permitir el acceso y el desarrollo de su red empresarial junto con la nube, ya que parte de las mejoras que se sugiere en este trabajo de titulación es

el que aparte de las mejoras de la propia red, se pueda trabajar con copias de seguridad en la nube Azure de Microsoft para poder utilizarse en caso de alguna emergencia.

2.4 Marco conceptual

Este trabajo de titulación se desarrolla a partir de la necesidad de asegurar la conectividad y la información que maneja las organizaciones del ecuador, muchas de las empresas de la ciudad de Guayaquil no cumplen con una constante actualización de los equipos, en este trabajo de titulación se toma como referencia una compañía de seguros en esta compañía de seguros de la ciudad de Guayaquil se pudo constatar este inconveniente y de ahí nace la necesidad de repotenciar los equipos de cómputo que le ofrece la red a esta empresa.

Otro aspecto que también se involucra en este trabajo de titulación es la reorganización de las redes que manejan las empresas ya que mantenerlos en diferentes tipos de redes dentro de la misma compañía, limita a que los demás departamentos tengan acceso a información que no es de su labor diaria, y tener un control de la red ayuda a que se pueda llevar a cabo mecanismos de seguridad para mantener integridad de la información.

Por estas razones se realiza un plan de mejoras a infraestructura y servicios de red en esta empresa de seguros mejorando la seguridad de la información que se maneja en dicha organización, ya que al contar con una correcta organización se puede llevar un control constante al acceso de los datos.

También, se tomó a consideración el desarrollo tecnológico constante y se incorpora a este trabajo de titulación el poder llevar esos cambios a la nube Azure de Microsoft como mecanismo de seguridad adicional ya que, al ser una copia en tiempo real de la red de esta empresa de seguros, en

caso de algún desastre se puede activar esta red de la nube permitiendo así el llevar a cabo las actividades diarias hasta la recuperación de la red física

2.5 Marco legal

Normas generales para las instituciones del sistema financiero - superintendencia de bancos y seguros

2.5.1 Sección II.- Factores del riesgo operativo

2.5.1.1 Artículo 4

Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí:

4.3.- Las normas que nos provee la superintendencia de bancos y seguros en su artículo 4.3 nos habla sobre el control que deben de llevar las empresas que usan la tecnología de la información y asegurar el buen manejo de la misma, así también como su procesamiento y almacenamiento para que siempre esté disponible de manera oportuna.

Este articulo también nos indica las consideraciones que debemos de tomar en la gestión de riesgos operativos, así como también los procedimientos y metodologías que deben de asegurar las empresas que están siendo controladas por el inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014.

4.4.- nos indica los eventos externos que pueden ser perjudiciales para las actividades de la continuidad de la empresa, tanto como pueden ser problemas con los servicios públicos, desastres naturales y actos que

van contra la integridad de las instituciones, pudiendo estas alterar el desarrollo financiero de la empresa y a su vez la razón de tener un plan de contingencia.

2.5.2 Sección IV.- Continuidad del negocio

2.5.2.1 ARTÍCULO 15

Este artículo nos indica sobre el control que se debe de llevar en la continuidad de negocios, el garantizar que una empresa pueda operar de forma continua y reducir las pérdidas en caso de algún desastre que pueda impedir el funcionamiento del negocio. Esto se lo indica en el artículo sustituido con la resolución No. JB-2014-3066 de 2 de septiembre del 2014, a su vez las instituciones deben de tomar como referencia la ISO 22301 para decidir las políticas de seguridad que se van a tomar.

CAPITULO III

METODOLOGÍA

La elaboración de este capítulo tiene como finalidad, brindar una explicación detallada de cada uno de los pasos que se realizaron para llevar a cabo el desarrollo de este proyecto. Documentando cada uno de los procedimientos que fueron utilizados para de esta forma dar una solución al problema planteado inicialmente.

3.1 Diseño de la investigación

Durante la elaboración de este Trabajo de Titulación se hizo uso de diversas metodologías y técnicas de investigación, las cuales ayudaron a conseguir los objetivos planteados anteriormente.

Por lo que se adoptaron algunas metodologías existentes para el uso de este proyecto como las siguientes: bibliográfica o documental, experimental, analítico, deductivo; de la misma manera se emplearon herramientas como la encuestas y entrevistas para poder analizar e interpretar los datos de forma estadística.

3.2 Enfoque de la investigación

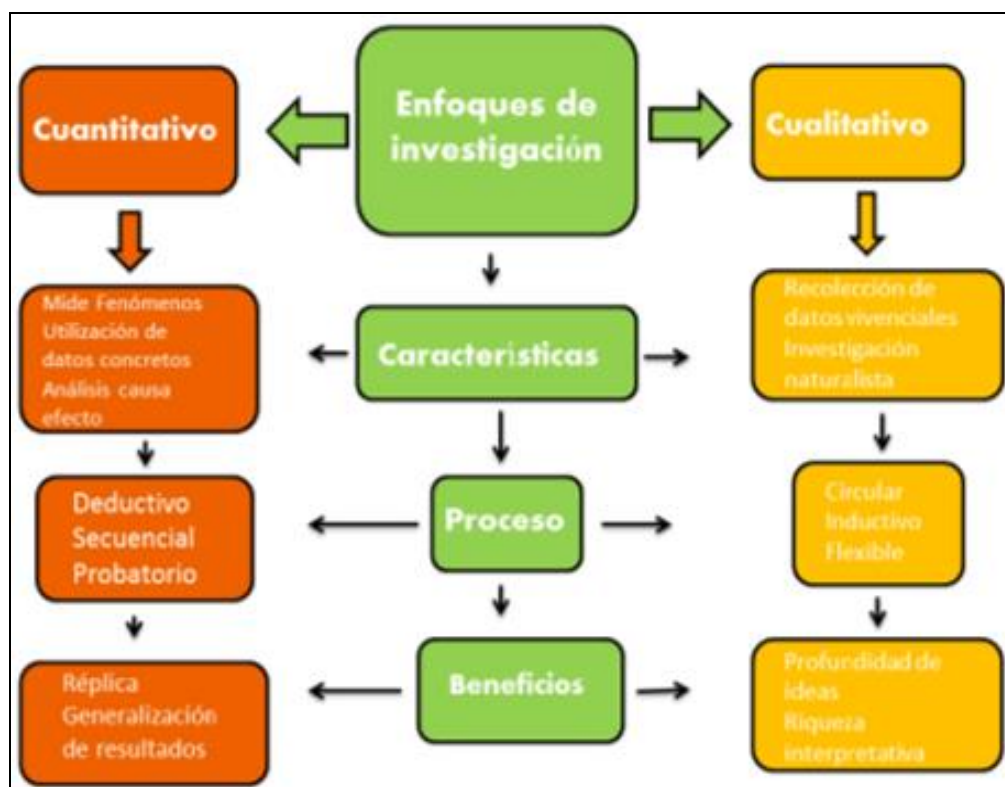
El enfoque de investigación es un plan y procedimiento que consiste en los pasos de suposiciones generales al método detallado de recopilación, análisis e interpretación de datos. Por lo tanto, en función de la naturaleza del problema de investigación que se aborda.

Los enfoques para el análisis de datos son de dos tipos:

- Inductivo
- Deductivo

La información cualitativa requiere un enfoque inductivo de análisis. Por otro lado, los datos cuantitativos usan un enfoque deductivo. En el tipo mixto de datos, se utilizan enfoques de análisis tanto inductivos como deductivos. Sin embargo, debe haber cierta coherencia entre los métodos, la metodología y el análisis. Esto es importante para demostrar la lógica. Por lo tanto, para que la investigación sea creíble para el lector, la investigación debe conducir a los hallazgos de la investigación. (Grinnell & Unrau, 2005)

FIGURA N°7
ENFOQUES DE INVESTIGACIÓN



Fuente: <http://normasapa.net/tesis-enfoque-cuantitativo-cualitativo/>
Elaborado por: Normas APA

3.2.1 Investigación cualitativa

Pone gran énfasis en los métodos utilizados para recopilar o generar datos. Sin embargo, pone menos énfasis en las técnicas analíticas para la interpretación de datos. Además, el enfoque inductivo utiliza principalmente la lectura detallada de datos secundarios para derivar conceptos, temas y modelos. Por lo tanto, es ampliamente utilizado para analizar datos cualitativos. (Trochim, 2002)

3.2.2 Investigación cuantitativa

La investigación cuantitativa a menudo se traduce en el uso del análisis estadístico para establecer la conexión entre lo que se sabe y lo que se puede aprender mediante la investigación. En consecuencia, el análisis de datos con estrategias cuantitativas requiere una comprensión de las relaciones entre variables, ya sea por estadística descriptiva o inferencial. La estadística descriptiva ayuda a sacar conclusiones sobre las poblaciones y a estimar los parámetros. (Trochim, 2002)

TABLA N°2
DIFERENCIAS DE ENFOQUES DE INVESTIGACIÓN

CUANTITATIVA	CUALITATIVA
Medición permanente y controlada	Observación naturista sin control
Objetiva	Subjetiva
Inferencia más allá de los datos	Inferencia de sus datos
Confirmatoria, inferencial, deductiva	Exploratoria, inductiva y descriptiva
Orientada al resultado	Orientada al proceso

Fuente: investigación directa

Elaborado por: Benavides Alcivar Vicente

3.3 Tipo de Investigación

- 1) **Científica.** - Mediante este tipo de investigación podemos conocer cuáles son las soluciones y mejoras que se pueden dar a la red de la empresa de seguros que estamos utilizando como referencia para aplicar este proyecto de tesis
- 2) **Exploratoria o de campo.** - Nos permite conocer cuál es el estado actual de la infraestructura de esta empresa de seguros, también el reunir información necesaria para ejecutar un análisis y obtener conclusiones

3.4 Población y Muestra

La población es el universo que es afectado por la problemática estudiada. Es el grupo completo seleccionado que cumple con las características que nuestro tema requiere.

La muestra es una selección representativa del universo, puede ser entre un 30 o 20 % de la población y debe ser escogida con criterios estadísticos.

3.4.1 Determinación del tamaño de la muestra

Utilizaremos la siguiente ecuación para determinar el tamaño de la muestra, ya que disponemos del dato del tamaño de la población:

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

TABLA N°3
LISTA DE VARIABLES

n	Es el tamaño de la muestra a calcular,
Z	Es el valor obtenido de la tabla normal estándar que depende del grado de confianza.
σ	Representa la desviación estándar de la población.
N	Es el tamaño de la población.
e	Refleja el límite del error muestra, es aceptado en el intervalo de 1% al 10%

Fuente: Investigación directa

Elaborado por: Benavides Alcivar Vicente Alberto

En este proyecto de titulación el tamaño de la población es:

$$N = 80$$

El valor de la desviación estándar de la población es desconocido, por lo que asumiremos un valor constante de 0.5 que se usa generalmente.

$$\sigma = 0.5$$

El grado de confianza establecido será del 95%

$$Z_{0.05} = 1.64$$

El error muestral definido será del 10% es decir 0.1

$$e = 0.10$$

Reemplazando los valores en la ecuación:

$$n = \frac{1.64^2 \times 0.5^2 \times 80}{0.1^2 \times (80 - 1) + 1.64^2 \times 0.5^2}$$

Resolviendo la operación:

$$n = 36.78$$

$$n \approx 37$$

3.4.2 Análisis de los resultados de las encuestas

Debido a que la población es un número pequeño se decidió hacer la encuesta a las 80 personas que forman parte de la empresa de seguros en la cual se está realizando este proyecto de titulación.

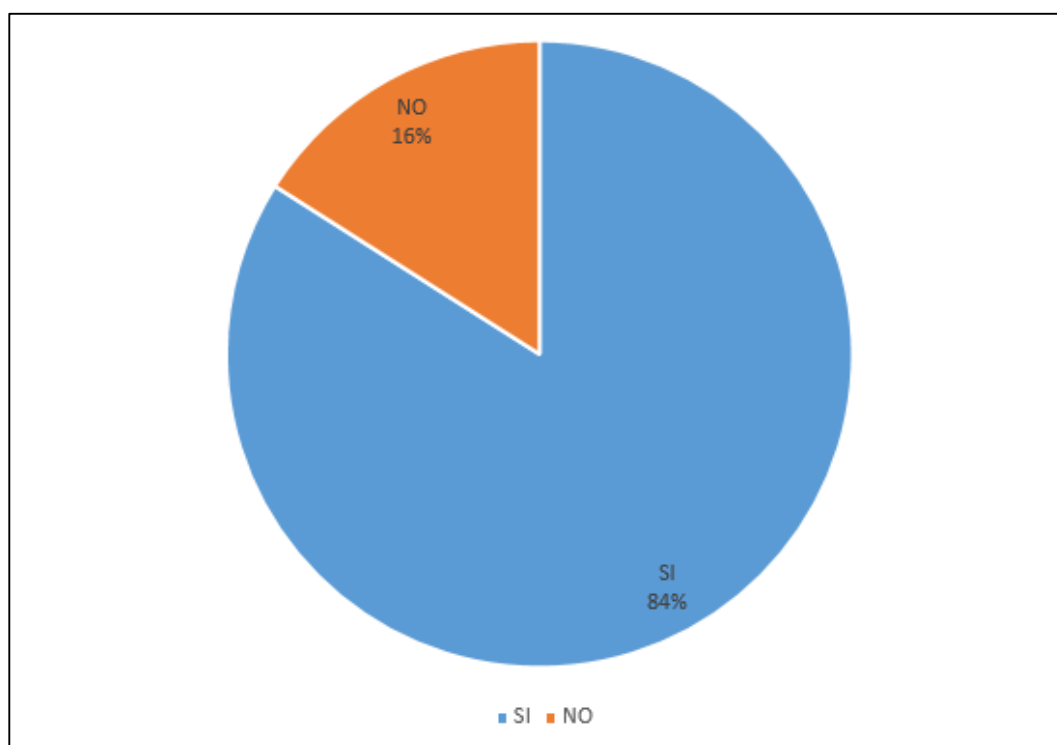
¿Cree usted que es necesario tener una actualización constante de los equipos de cómputo?

TABLA N°4
ACTUALIZACIÓN CONSTANTE DE EQUIPOS DE CÓMPUTO

Descripción	Frecuencia	%
Si	67	84%
No	13	16%
TOTAL	80	100%

Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°8
ACTUALIZACIÓN CONSTANTE DE EQUIPOS DE CÓMPUTO



Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

Análisis: De una muestra de 80 de los encuestados que equivalen al 100% se obtuvo los siguientes porcentajes un 84% de los encuestados están de acuerdo con el tener una actualización constante de los equipos de cómputo, un 16% indicaron que el proceso de actualización en algunas ocasiones daña lo que está funcionando bien en ese momento.

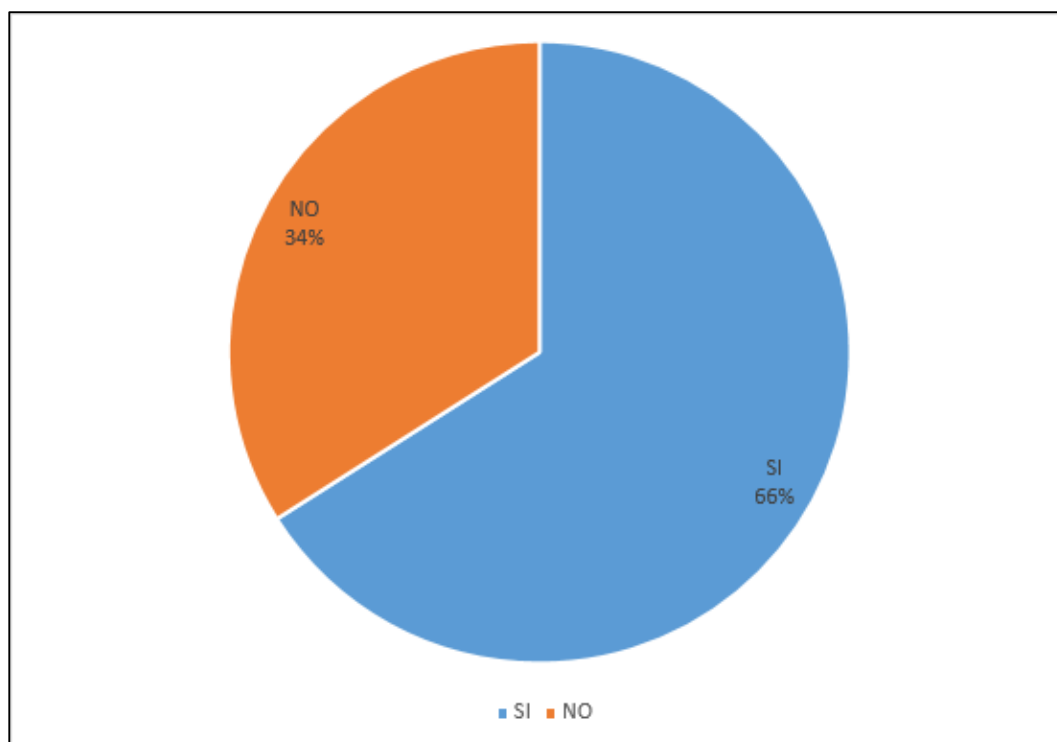
¿Cree usted que se debe llevar un control de las personas que puedan acceder a la información de la compañía?

TABLA N°5
CONTROL DE ACCESO A LA INFORMACION DE LA EMPRESA

Descripción	Frecuencia	%
Si	53	66%
No	27	34%
TOTAL	80	100%

Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°9
CONTROL DE ACCESO A LA INFORMACION DE LA EMPRESA



Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

Análisis: De una muestra de 80 de los encuestados que equivalen al 100% se obtuvo los siguientes porcentajes un 66% de los encuestados están de acuerdo con llevar un control de las personas que puedan acceder a la información, un 34% indicaron que todos deberían de tener acceso a la información para agilizar el trabajo.

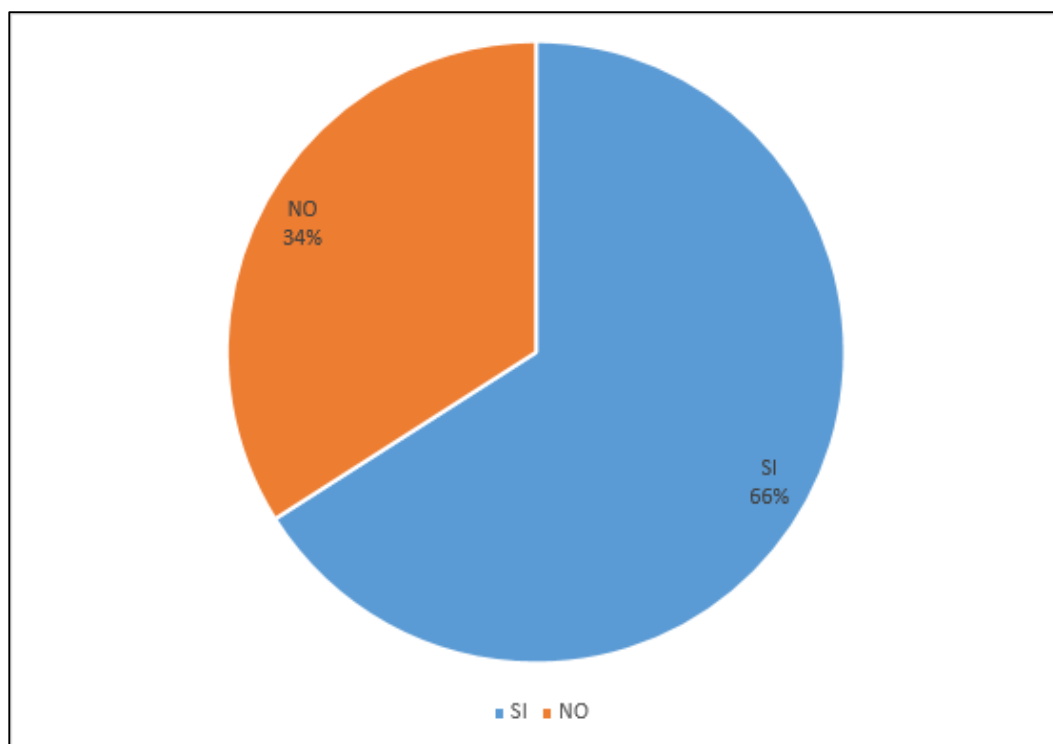
¿Cree usted que es suficiente los respaldos generados por la empresa?

TABLA N°6
RESPALDOS GENERADOS POR LA EMPRESA

Descripción	Frecuencia	%
Si	53	66%
No	27	34%
TOTAL	80	100%

Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°10
RESPALDOS GENERADOS POR LA EMPRESA



Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

Análisis: De una muestra de 80 de los encuestados que equivalen al 100% se obtuvo los siguientes porcentajes un 66% de los encuestados están de acuerdo proceso de respaldo actual, un 34% indicaron que en algunas ocasiones parte de su información se vio afectada y perdida en el proceso.

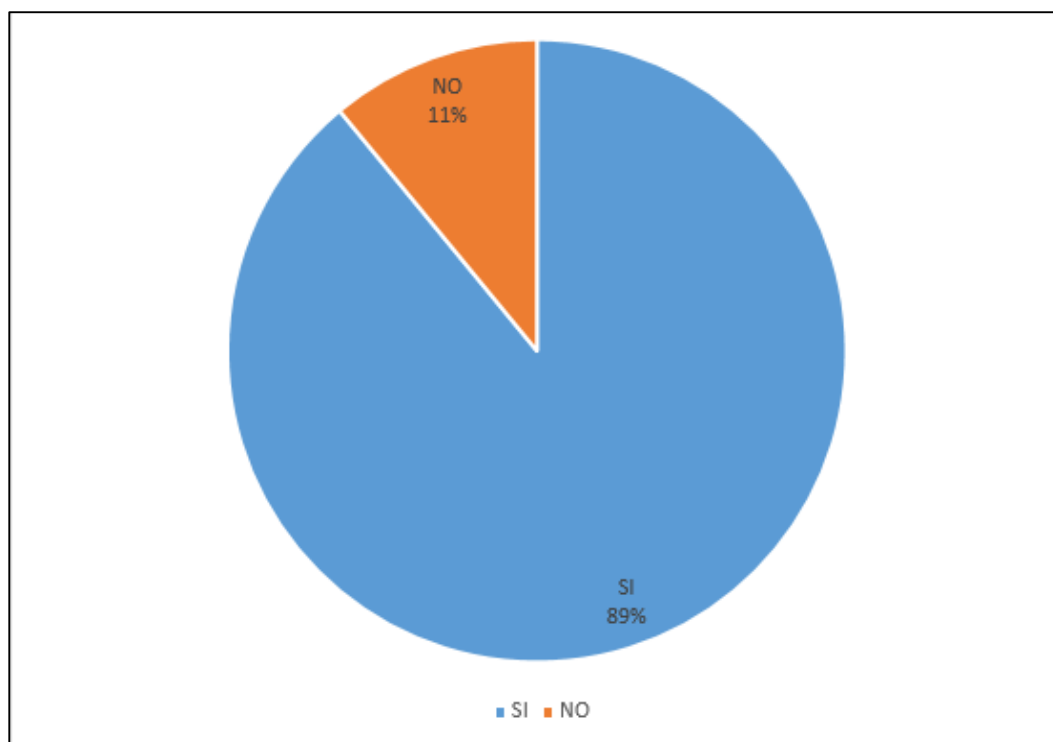
¿Cree usted que se necesita mejorar a nivel de infraestructura de red para que los procesos sean rápidos?

TABLA N°7
MEJORAS EN INFRAESTRUCTURA DE RED

Descripción	Frecuencia	%
Si	71	89%
No	9	11%
TOTAL	80	100%

Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°11
MEJORAS EN INFRAESTRUCTURA DE RED



Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

Análisis: De una muestra de 80 de los encuestados que equivalen al 100% se obtuvo los siguientes porcentajes un 89% de los encuestados están de acuerdo con mejorar la infraestructura de la red, un 11% indicaron que este tiempo de cambios no les iba a permitir laborar con normalidad.

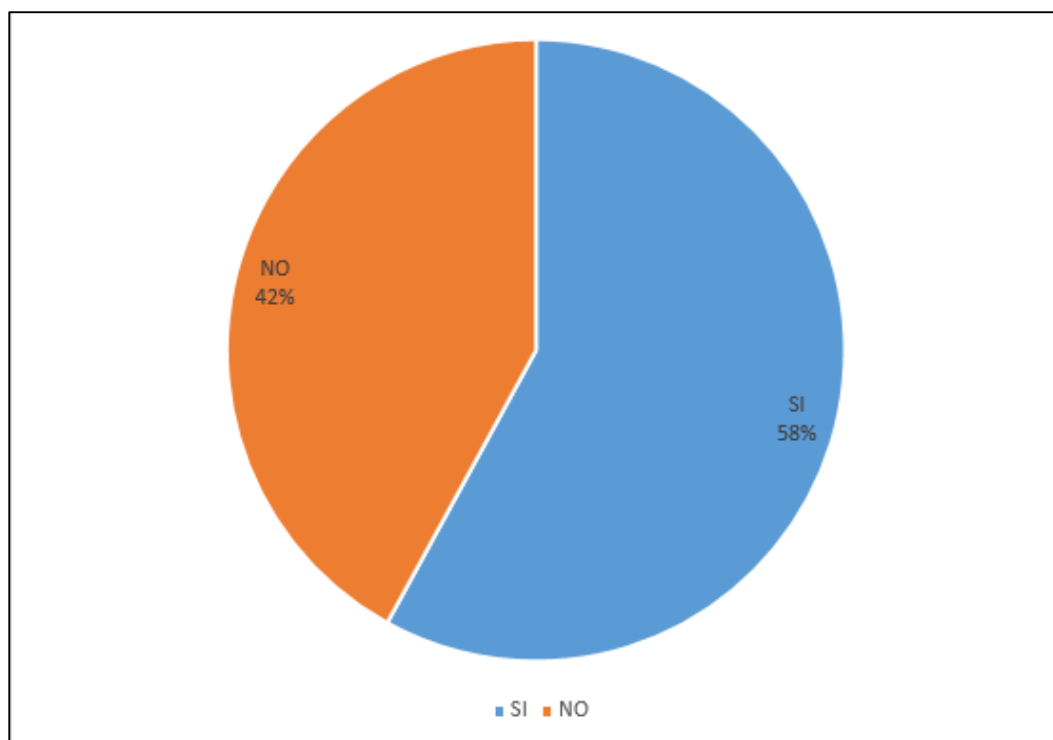
¿Cree usted que los mecanismos existentes en la empresa son suficiente para que la empresa siga trabajando en caso de desastre?

TABLA N°8
MECANISMOS EXISTENTES EN LA EMPRESA

Descripción	Frecuencia	%
Si	46	58%
No	34	42%
TOTAL	80	100%

Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°12
MECANISMOS EXISTENTES EN LA EMPRESA



Fuente: Encuesta realizada durante el Trabajo de Titulación
Elaborado por: Benavides Alcivar Vicente Alberto

Análisis: De una muestra de 80 de los encuestados que equivalen al 100% se obtuvo los siguientes porcentajes un 58% de los encuestados están de acuerdo con los mecanismos existentes, un 42% indicaron que sería recomendable implementar nuevos mecanismos en caso de un desastre.

3.5 Método de observación directa

La observación directa, también conocida como estudio observacional, es un método de recopilación de información evaluativa que al evaluar se observa al sujeto en su entorno habitual sin alterar ese entorno. La observación directa se usa cuando el objetivo es evaluar un proceso, evento o situación de conducta en curso; o cuando hay resultados físicos que se pueden ver fácilmente.

La observación directa puede ser abierta, cuando el sujeto y las personas en el ambiente conocen el propósito de la observación, o encubierto, cuando el sujeto y los individuos en el ambiente no conocen el propósito de la observación.

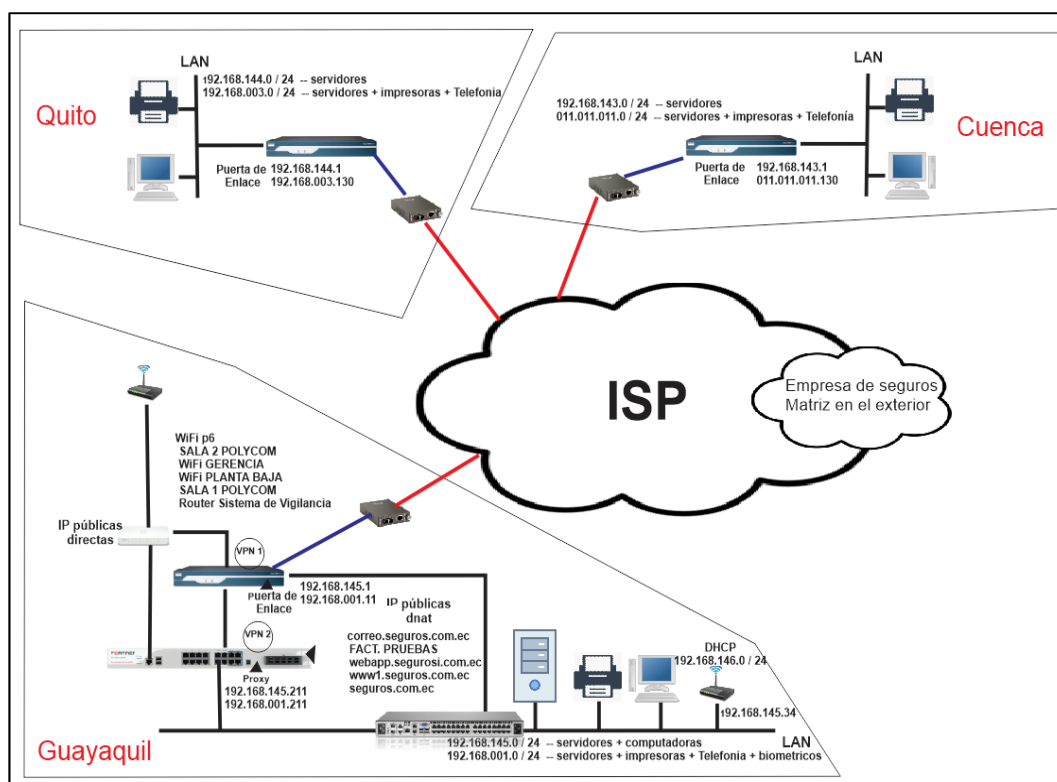
En este proyecto de titulación se utilizó la observación directa abierta para poder identificar cual es el estado actual de la infraestructura de la red y definir cuál es el procedimiento que se va a seguir para mejorarlo.

3.6 Infraestructura actual de la red

Haciendo uso de la investigación directa se realizó una verificación de cuál era la infraestructura de red actual de esta empresa de seguros, se identificó que esta empresa tiene conexión con sus sucursales en Quito y Cuenca mediante el uso de una red privada que le proporcionó Telconet, esto quiere decir que todo tráfico de esas sucursales viaja desde esas ciudades a la ciudad de Guayaquil para ser procesada y poder salir al internet.

Dentro de los equipos que usa esta empresa de seguros el más importante a tomar a consideración es el Fortinet que también lo provee Telconet, ya que este es el que está brindando el servicio de servidor Proxy y de Firewall en el esquema de red.

FIGURA Nº13
ESQUEMA DE RED



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

A su vez se puede observar que esta empresa mantiene una conexión permanente con su matriz Ubicada en el exterior la cual acceden mediante la WAN y con configuraciones DNS, el administrador de red indicó que toda la infraestructura que mantienen ahora fue evolucionando a pasar el tiempo, algunos equipos se han mantenido en la misma ubicación mientras otros han sido modificados dependiendo a la necesidad en ese momento


3.7 Inventario de equipos

A continuación, se detalla la información de los equipos que conforman la infraestructura de red de la empresa de seguros la cual se está utilizando en este proyecto de titulación como referencia:

3.7.1 Servidores

A continuación, se detallan los servidores y equipos de red encontrados en la investigación directa que se realizó a la empresa de seguros.


TABLA N°9
SERVIDOR LENOVO (1)

	
Modelo	X36050MS – 546 – AC1
Procesador	Xeon Octa Core 2.6 GHz
Procesadores virtuales	16
RAM	32 GB
Disco Duro	2x1TB SAS RAID1 + 3x1TB SAS RAID5
Sistema Operativo	Windows Server 2012 R2
Host	Hiper V

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°10
SERVIDOR IBM (1)

	
Modelo	X36050M4 – 7915 – AC1
Procesador	Xeon SIX Core 2.3 GHz
Procesadores virtuales	12
RAM	32 GB
Disco Duro	2x1TB SAS RAID1 + 3x1TB SAS RAID5
Sistema Operativo	Windows Server 2012 R2
Host	Hiper V

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°11
SERVIDOR IBM (2)



Modelo	X36050M4 – 7945 – AC1
Procesador	Xeon Quad Core 2.4 GHz
Procesadores virtuales	8
RAM	12 GB
Disco Duro	5x500GB SATA RAID 5
Sistema Operativo	SLES 11 SP1
Host	XEN

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°12
SERVIDOR IBM (3)



Modelo	X3250M4 – 2583 – EBU
Procesador	Xeon Quad Core 2.4 GHz
Procesadores virtuales	4
RAM	12 GB
Disco Duro	2x1TB SATA RAID 1
Sistema Operativo	IMSVA
Host	STAND ALONE

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°13
SERVIDOR IBM (4)



Modelo	X36050M4 – 7945 – AC1
Procesador	Xeon Quad Core 2.4 GHz
Procesadores virtuales	8
RAM	16 GB
Disco Duro	4x1TB SATA RAID 5
Sistema Operativo	SLES 11 SP2
Host	XEN

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°14
SERVIDOR IBM (5)



Modelo	X36050M4 – 7945 – AC1
Procesador	Xeon SIX Core 2.4 GHz
Procesadores virtuales	12
RAM	8 GB
Disco Duro	3x1TB SAS RAID 5
Sistema Operativo	Windows Server 2012 R2
Host	Hiper V

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°15
SERVIDOR IBM (6)



Modelo	X36050M4 – 7915 – AC1
Procesador	Xeon SIX Core 2.3 GHz
Procesadores virtuales	12
RAM	16 GB
Disco Duro	4x1TB SAS RAID 5
Sistema Operativo	Windows Server 2012 R2
Host	Hiper V

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°16
SERVIDOR IBM (7)




Modelo	X36050M4 – 7915 – AC1
Procesador	Xeon SIX Core 2.3 GHz
Procesadores virtuales	12
RAM	16 GB
Disco Duro	4x1TB SAS RAID 5
Sistema Operativo	Windows Server 2012 R2
Host	Hiper V

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°17
SERVIDOR IBM

	
Modelo	X36050M3 – 7945 – AC1
Procesador	Xeon Quad Core 2.4 GHz
Procesadores virtuales	8
RAM	16 GB
Disco Duro	4x500GB SAS RAID 5
Sistema Operativo	Citrix Xen Server 5.6
Host	

Fuente: Observación directa

Elaborado por: Benavides Alcivar Vicente Alberto

3.7.2 Router

TABLA N°18
ROUTER CISCO 1800 SERIES

	
Características	Puerto DSL WAN
	Puertos 10/100 FE WAN
	Switch Gestionado de 8-Puertos
	ISDN BRI Dial Backup
	802.11a/b/g Wireless Model
	Puertos de Consola y Auxiliares

Fuente: <http://www.abox.com/productos.asp?pid=597>

Elaborado por: Benavides Alcivar Vicente Alberto

3.7.3 Switch

TABLA N°19
SWITCH HP V1910 -24G

	
Procesador	ARM a 333 MHz
Puertos	-24 puertos RJ-45 10/100/1000 -4 puertos SFP de 1000 Mbps -100BASE-TX, IEEE 802.3ab -Admite un máximo de 24 puertos 10/100/1000 de detección automática más 4 puertos SFP 1000BASE-X, o una combinación de los mismos
Memoria	128 MB
Velocidad	hasta 41.7 millones de pps
Administración	-IMC - Intelligent Management Center -Interfaz de línea de comandos limitada -Navegador Web -Administrador de SNMP

Fuente: <https://pcel.com/Hewlett-PackardV1910-24G-97966>

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°20
SWITCH 3COM BASELINE 2824

	
Tipo de dispositivo	Conmutador - 24 puertos
Subtipo	Sobremesa - 1U
Puertos	24 x 10/100/1000
Tamaño de tabla de dirección MAC	8K de entradas

Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x
------------------------	---

Fuente: <https://www.almacen-informatico.com/producto.asp?fb=3COM&pr=baseline-switch-2824-3CBLUG24-ME&id=53942>

Elaborado por: Benavides Alcivar Vicente Alberto

TABLA N°21
SWITCH HP 1410 24G


	
Puerto	22 puertos 10/100/1000 de detección automática (IEEE 802.3 tipo 10BASE-T, IEEE 802.3u tipo 100BASE-TX, IEEE 802.3ab tipo 1000BASE-T), tipo de soporte: MDIX automático, dúplex: 10BASE-T/100BASE-TX: medio o completo; 1000BASE-T: sólo completo; 2 puertos de doble función, cada puerto se puede utilizar como puerto RJ-45 10/100/1000 (IEEE 802.3 tipo 10Base-T; IEEE 802.3u tipo 100Base-TX; IEEE 802.3ab 1000Base-T Gigabit Ethernet) o como ranura mini-GBIC abierta (para usar con transceptores mini-GBIC)
Memoria	512 KB de memoria flash, tamaño de búfer de paquetes: 512 KB
Normas y Protocolos	Prioridad IEEE 802.1p; IEEE 802.3ab 1000BASE-T; IEEE 802.3i 10BASE-T; IEEE 802.3u 100BASE-X
Velocidad	Hasta 35.7 millones de pps (paquetes de 64 bytes)

Fuente: <https://pcel.com/Hewlett-Packard-HP-1410-24G-86775>

Elaborado por: Benavides Alcivar Vicente Albert

3.7.4 Firewall

TABLA N°22
FORTINET FORTIGATE 200D

	
Características	Puerto de gestión USB
	Puerto de gestión
	Puerto de consola
	Puerto USB
	2 x 10/100/1000 WAN Interfaces
	16 x 10/100/1000 Interfaces internas
	2 x GbE SFP DMZ Interfaces
	10/100/1000 interfaces WAN (RJ45) 2
	10/100/1000 Interfaces internas (RJ45) 16
	GbE SFP DMZ Interfaces 2
	USB (cliente / servidor) 1/1
	Console (RJ45) 1
	Almacenamiento local 16GB
	3 Gbps salida a través del Firewall
	1.3 Gbps rendimiento VPN
	1,400,000 sesiones concurrentes
	77,000 nuevas sesiones/segundo

Fuente: <https://www.znet.com.ar/blog/2017/06/fortinet-200d-fortigate-200d/>

Elaborado por: Benavides Alcivar Vicente Alberto

CAPITULO IV

PROPUESTA DE LA INVESTIGACIÓN

4.1 Plan para la repotenciación de la infraestructura como propuesta de mejora

El objetivo principal de este proyecto de titulación es poder realizar un análisis del estado de la infraestructura de red de una empresa de seguros de la ciudad de Guayaquil y que acorde a los resultados se pueda realizar esta mejora en su red.

Mediante el uso de la observación directa se pudo realizar un esquema de red en donde se puede verificar cual es el estado actual de la red y cuáles son los puntos que se necesita corregir para que la infraestructura tenga la fluidez necesaria y poder adaptarse al uso de nuevas tecnologías en serán indispensable en un tiempo determinado.

Es necesario tomar en consideración en este plan que cada cambio que se va a realizar en la infraestructura de la red debe ser compatible con el uso de la nube, debido a que la nube de Microsoft Azure forma parte del plan de seguridad el cual puede ser utilizado en caso de desastre.

Por lo tanto, se debe de realizar una organización de los segmentos de red asignados a cada grupo de trabajo de esta empresa de seguros, realizar cambios en varios servidores para lograr la compatibilidad con Microsoft Azure, realizar una configuración que permita la conexión entre la red física y la red virtual para poder obtener el grado de seguridad necesario en el manejo de la información y sobretodo el poder acceder a ella en cualquier momento.

4.2 Análisis de la infraestructura de red

En el análisis de la infraestructura que realizamos en este proyecto de titulación se puede observar el estado actual de las conexiones entre las diferentes sucursales del país y la matriz de esta empresa de seguros que está ubicada en el exterior.

Esta empresa de seguros para poder conectarse con sus diversas sucursales lo hace mediante redes privadas que es un servicio que presta el ISP y para conectarse con matriz lo hace mediante el uso de VPN la cual según el esquema de red están configuradas en el router de la ciudad de Guayaquil, todo el tráfico de red de las ciudades de Quito y Cuenca viajan a través de las redes privadas a la ciudad de Guayaquil para finalmente salir al internet, como dato adicional, ninguna de las sucursales tiene salida directa al Internet a excepción de Guayaquil.

También se pudo observar en el esquema de red que existe una conexión directa entre el Router y Switch y otra que va desde el Router al Firewall llegando después al Switch, esto debido a una migración realizada hace tiempo atrás y no se realizó la configuración respectiva a la red, dejando por separada la ruta donde viajan los datos de la empresa y la ruta donde viajan los datos de Internet.

El problema que ocasiona el tener esa configuración es que la red de datos viaja directamente por el Router sin pasar por el firewall y los datos de internet si viajan a través del firewall/proxy, pero debido a la conexión doble muchas veces se presentan perdidas al momento de realizar un tipo de conexión entre datos e internet, ya que los paquetes no encuentran la ruta correcta para poder transportarse, aparte de que la red de datos no cuenta con la protección del firewall.

Otro problema que se pudo identificar fue el hecho de que en la ciudad de Guayaquil las computadoras de los usuarios y los servidores de

la empresa están dentro del mismo segmento de red 192.168.145.0/24, cuando por políticas de seguridad y de organización en la red, los equipos de cómputo de los usuarios y los servidores deben de estar ubicados en un segmento diferente de la red.

Por estas razones se debe realizar estas correcciones en la infraestructura de red de esta empresa de seguros, ya que mejorará la seguridad de la información y sobretodo se llevará un control de quienes tienen permitido ingresar a dicha información. Adicionalmente se recomienda el uso de un hotspot para la administración Wifi, ya que realizando el esquema de red se identificó que no se lleva un control de las personas que acceden al Wifi.

4.3 Plan para la implementación

Para poder realizar la implementación de este plan es necesario tener muchos factores a consideración que nos permitirán optimizar los recursos de la red para sacarle el mayor beneficio posible, tanto como la reorganización de la red, cambios en servidores y configuraciones para que se puede crear el respaldo en la nube de Azure

4.3.1 Fase 1: Diseño

Análisis de la situación actual: se trata de verificar el área donde se va a realizar los cambios, reconocer el tipo de conexión que tiene la empresa de seguros y como está estructurada, ya que esta información será de suma importancia para identificar cuáles son los correctivos necesarios a implementar.

Análisis de los equipos de red: se trata sobre identificar cuáles son los equipos de red y de computación que dispone la empresa de seguros, cuáles son las características y los recursos que poseen para poder determinar si la potencia actual que disponen es la necesaria para poder

realizar los cambios que se plantean con este proyecto de titulación, y también poder verificar si el diseño actual en el que está estructurada la red es la más óptima para un buen desempeño del manejo de datos.

Análisis del nivel de seguridad actual de los datos: se debe verificar que el trato que se le da a la información de la empresa es la más segura posible, ya que los datos es la parte fundamental de toda compañía. Hay que realizar una verificación con el esquema de red si existe un mal diseño de la red que deja expuesta una vulnerabilidad la cual puede ser identificada por un atacante y poder tener acceso no autorizado a los datos

4.3.2 Fase 2: Plan estratégico

4.3.2.1 Control de acceso a la red mediante el uso de Wifi

Es necesario aplicar un control en el acceso a la red mediante el uso del Wifi y para ellos se hará uso de un Hotspot WLAN que nos permitirá controlar quien puede ingresar a la red, ya que de este modo solo podrán ingresar con autorización previa o con usuarios predefinidos para cada persona según las labores a desempeñar en la compañía.

4.3.2.2 Segmentación de red entre usuarios y servidores

Se debe separar las IP de los usuarios y los servidores de la ciudad de Guayaquil según el esquema de red que pudimos realizar con la investigación directa, para este propósito se deberá consultar con la matriz en el exterior para la asignación de un rango de IP exclusivo para la LAN de la ciudad de Guayaquil y realizar las configuraciones necesarias a cada usuario.

4.3.2.3 Repotenciación de los servidores

En el análisis de los equipos de red realizado anteriormente se pudo identificar que existe servidores los cuales no tienen los suficientes

recursos para poder administrar nuevos servidores que son parte de los cambios que se plantea en este proyecto, a su vez también se debe de realizar la repotenciación de los servidores y equipos de red como un paso que se debe llevar antes de realizar una migración a la nube Azure de Microsoft.

4.3.2.4 Cambios y actualizaciones en máquinas virtuales

Es importante también tomar en consideración los cambios que se deben de realizar en las máquinas virtuales que contienen los servicios activos de la empresa, se debe de agrupar un mismo tipo de máquinas virtuales en un mismo servidor, como por ejemplo que en un servidor este ubicado todas las máquinas virtuales que contienen usos relacionados al ambiente web, para así llevar un control y una organización de dichas máquinas virtuales.

Por otro lado, es necesaria una actualización a los sistemas operativos de las máquinas virtuales que contienen los servidores, ya que en la investigación que se pudo realizar existen varias máquinas virtuales que tienen servicios activos en base a un sistema operativo Windows 7, Windows8. Esos sistemas operativos no son diseñados para la administración de procesos a nivel empresarial por lo cual el necesario realizar estos cambios.

4.3.2.5 Replicación de los servidores a Microsoft Azure

Para poder realizar una copia de seguridad a la nube de Azure se debe realizar una réplica exacta de los servidores fundamentales para el desarrollo de las actividades de la empresa, se plantea una guía del proceso que se debe de realizar para realizar dicha replicación de una manera organizada sin perjudicar el desarrollo de las actividades del resto de trabajadores de esta empresa de seguros.

4.3.2.6 Configuración Azure

Se debe realizar la configuración para que los servidores subidos a la nube de Azure puedan tener una actualización automática de los nuevos datos que se ingresan diariamente en la empresa, realizar también las respectivas configuraciones para que esas virtualizaciones en la nube de Azure se puedan conectar tanto con las sucursales de Quito y Cuenca, así como también que tenga la conectividad con la matriz en el exterior.

4.4 Control de acceso a la red mediante Wifi

Debido a que el acceso mediante el uso del wifi es la forma más común de poder infiltrarse en una red, suele ser uno de los puntos débiles en lo que se respecta a seguridad en una red empresarial, tanto por el hecho de que se puede acceder a los recursos de la compañía como también el que puedan saturar la red haciendo uso de un gran ancho de banda que esta de forma predeterminada designada para el uso de ciertos procesos llegando así a poder ralentizar el flujo de trabajo.

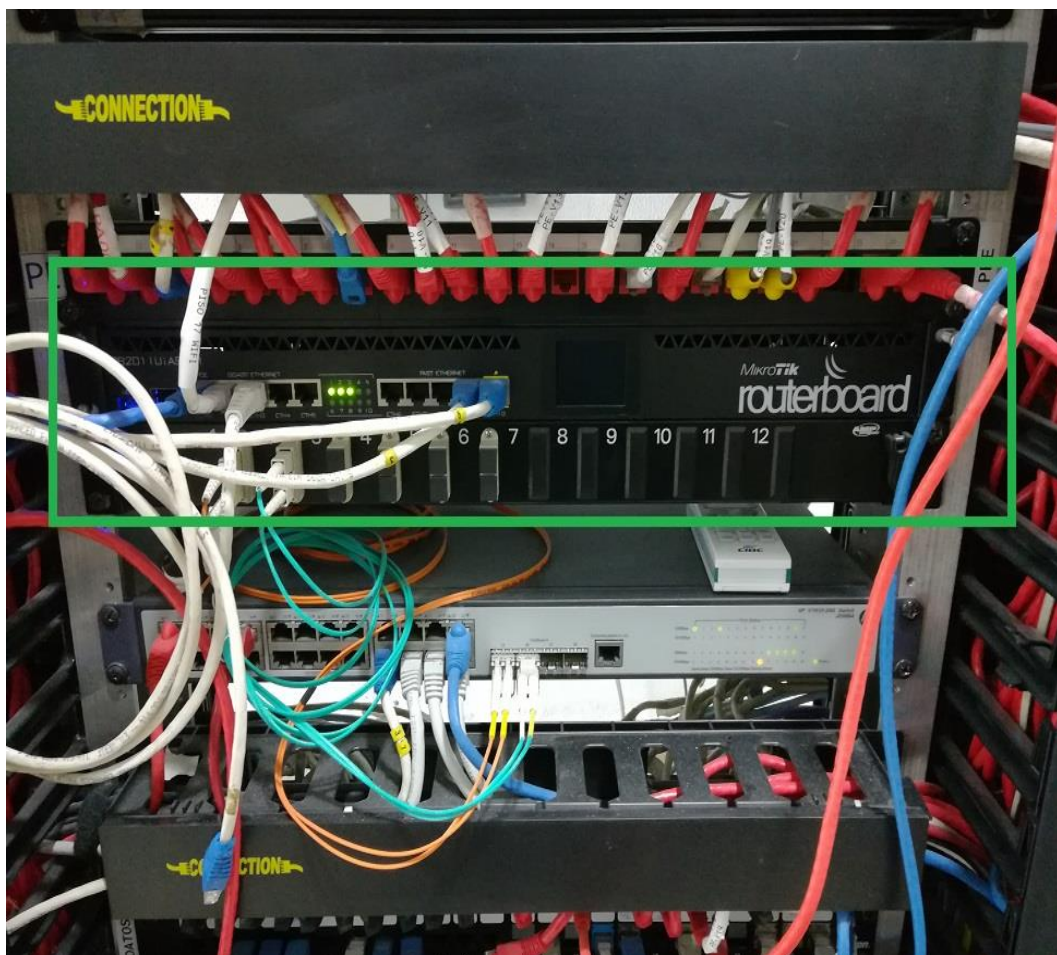
En el desarrollo de este proyecto de titulación mediante el uso de una investigación directa se pudo identificar que existía una conexión libre al wifi en todas las áreas, sin ningún tipo de control ni ningún tipo de limitación en cuanto al ancho de banda que pueden hacer uso, se debe de realizar un cambio en este modo de acceso wifi como parte de cambios en políticas de seguridad que propone la propuesta de mejora de este proyecto de titulación.

Tomando dicha información como parte de inicio se realizó una propuesta al administrador del área de TI de la empresa de seguros en que se debe implementar el uso de un hotspot wifi, en lo que el administrador de TI pudo indicar que disponían ya de un equipo Hotpost wifi de marca Mikrotik el cual nunca se le dio ningún uso y el administrador indico que se puede realizar la implementación con dicho dispositivo

4.4.1 Instalación física

Se realizó la instalación física del equipo Mikrotik en el centro de cómputo realizando la compartición de la red mediante la conexión de un cable ethernet el cual ya tenía designado un control de acceso referente a los recursos que puede acceder en la compañía.

FIGURA N°14
MIKROTIK INSTALADO



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Y en el otro extremo mediante cable ethernet se hizo la instalación de varios switches wifi en lugares estratégicos donde mediante el uso de la observación se pudieron identificar, como también para tener la mayor cobertura posible dentro de las instalaciones de esta empresa de seguros.

FIGURA N°15
SWITCH USO DE MIKROTIK



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

4.4.2 Configuraciones del Mikrotik

Para poder realizar la configuración del mikrotik se puede ingresar de 2 diferentes formas

- a) Ingresando desde una computadora mediante el uso del navegador web nos dirigimos a la dirección IP del mikrotik
- b) Ingresando mediante el uso de una aplicación portable WinBox con pocos requerimientos de recursos, que mediante el uso de un direccionamiento IP puede ingresar y mostrar la interfaz con mucha más estabilidad y fluidez.

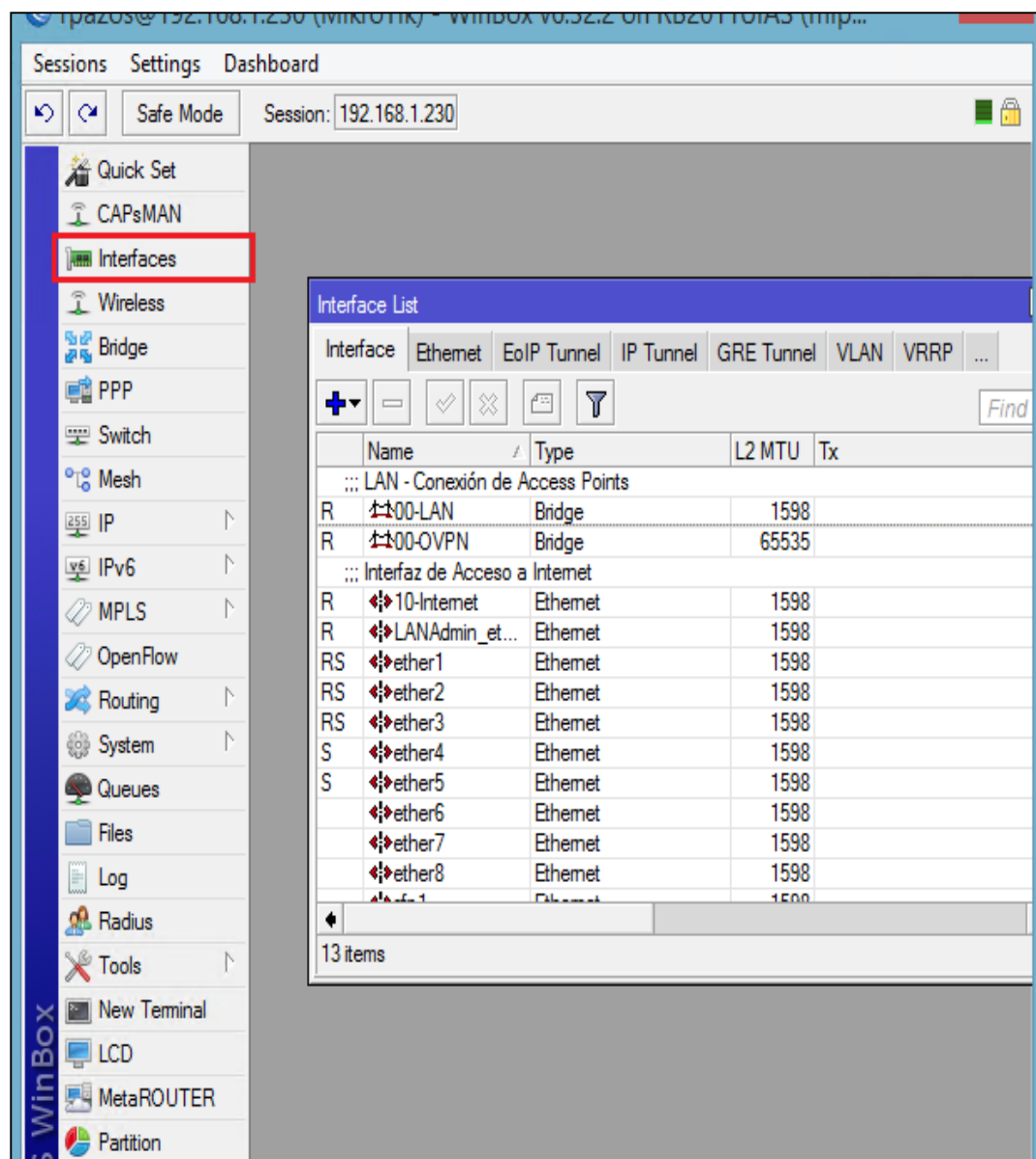
En este caso nosotros haremos uso de Winbox para realizar la administración del hotspot.

Winbox es un programa en versión portable el cual nos permite realizar un acceso rápido desde el servidor donde lo tenemos configurado, este programa toma la misma interfaz web que nos mostraría el Mikrotik si ingresáramos mediante el navegador web.

La dirección IP que se le asigna a este dispositivo es 192.168.1.230/24, la primera vez que se realiza el ingreso se realiza solo con el usuario admin y sin necesidad de ingresar una contraseña, luego de eso nos mostrará la interfaz principal.

Debemos abrir la opción de “interfaces” que se encuentra en la barra lateral izquierda, una vez abierta la ventana de interfaces renombrar los puertos conectados del dispositivo Mikrotik.

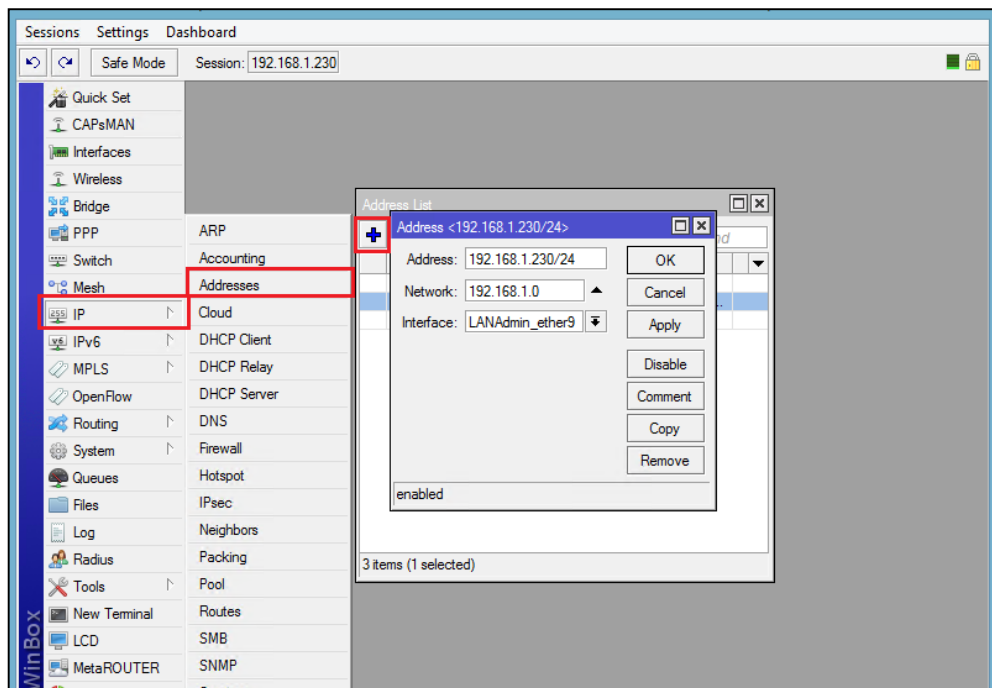
FIGURA N°16
WINBOX - INTERFAZ



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

En la barra lateral izquierda ingresar a IP>ADDRESSES y luego al botón de “+” para agregar las direcciones que necesitamos según los requerimientos de red.

FIGURA N°17
WINBOX - ADDRESS



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

En este caso ingresamos 3, las cuales tienen los siguientes usos:

- 181.198.39.58: acceso a privilegios de internet
- 192.168.1.230: LAN diseñada para usos administrativos
- 192.168.88.1: segmentos de red ofrecido a los usuarios del mikrotik

FIGURA N°18
WINBOX - ADDRESS LIST

Address	Network	Interface
181.198.39.58...	181.198.39.56	10-Internet
192.168.1.230...	192.168.1.0	LANAdmin_eth...
192.168.88.1/...	192.168.88.0	00-LAN

3 items (1 selected)

Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Ingresa en la barra lateral izquierda a IP>ROUTES para agregar la configuración de la navegación de internet que provee el dispositivo Mikrotik

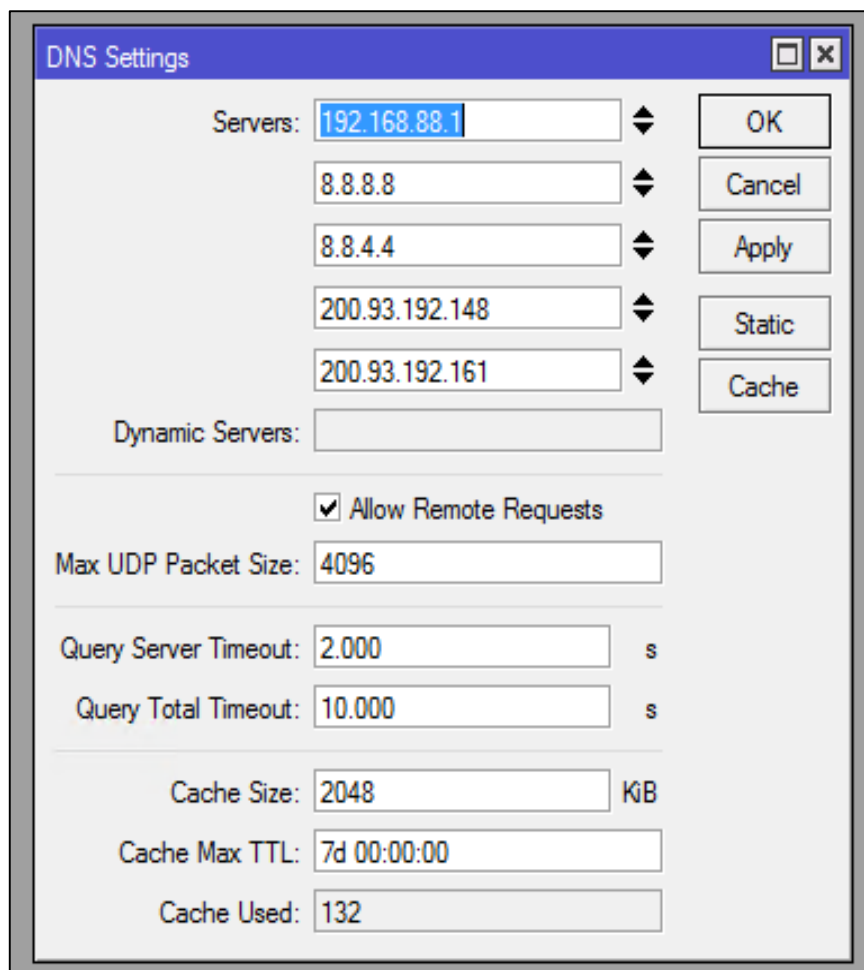
FIGURA N°19
WINBOX - ROUTE LIST

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

Para configurar los DNS debemos ingresar en la barra lateral izquierda a IP>DNS y en el cuadro agregar la información del server 192.168.88.1 que es la red que se está dejando de forma predeterminada para los usuarios del hotspot y en los siguientes recuadros ingresar 2 DNS de google y 2 DNS propios de la compañía.

FIGURA N°20
CONFIGURACIÓN DNS



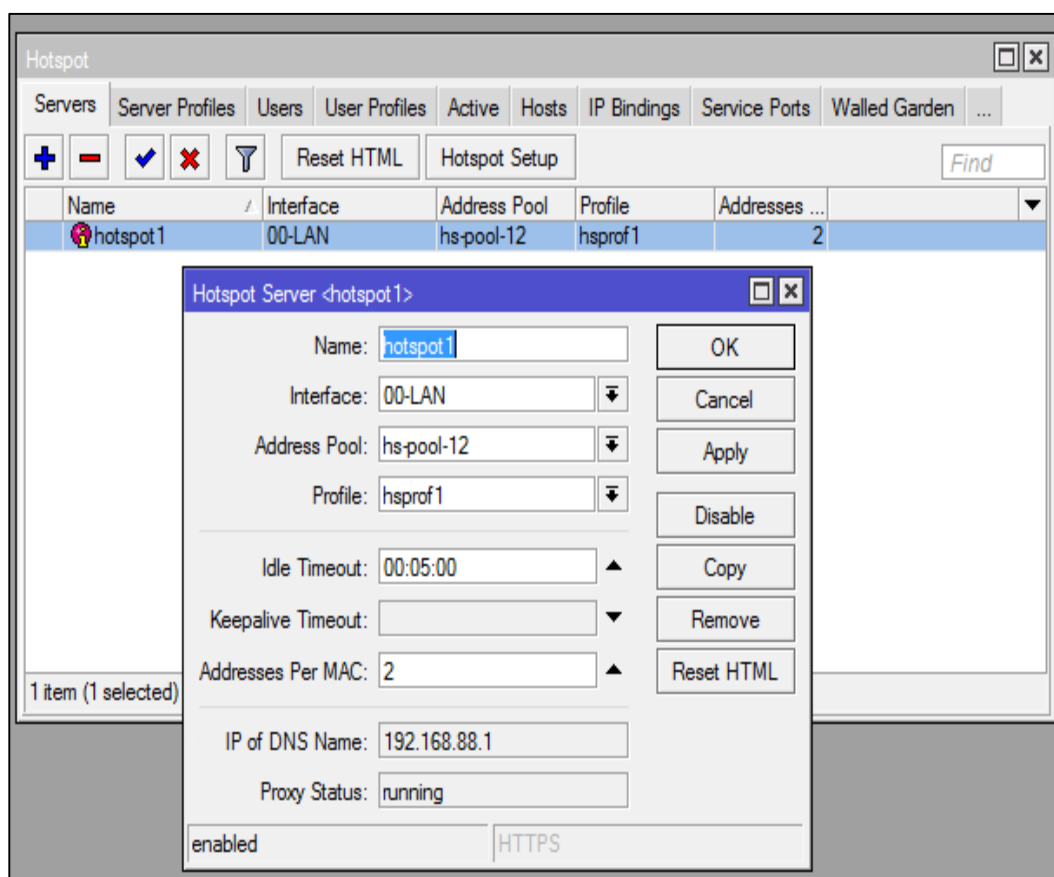
Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Para crear el DHCP SERVER tenemos 2 alternativas, la primera sería crear manualmente el servidor dhcp y la segunda sería crear directamente el perfil de hotspot que este a su vez crea el servidor dhcp de manera automática.

En este caso elegimos la segunda alternativa y creamos directamente un perfil de hotspot abriendo la ventana desde la barra lateral izquierda IP>Hotspot

FUENTE N°21

CREACIÓN DE PERFIL



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

Para la creación de un usuario, debemos ingresar en la misma ventana de hotspot la sección Users y agregar pulsando el botón “+” en donde debemos ingresar el nombre de usuario y la contraseña la cual le tenemos que proveer a la persona que necesita hacer uso del internet en el hotspot.

El administrador de la red podrá decidir el nombre de usuario y la contraseña dependiendo de la necesidad del momento, pero siempre llevando un orden en los nombres de usuario para llevar un control, en este caso se propuso que siempre los nombres de usuario sea la primera letra del nombre seguido por el apellido.

FIGURA N°22
CREACIÓN DE USUARIO

Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente

Con la configuración que se ha realizado hasta ahora ya el usuario “vbenavides” puede hacer uso del hotspot pero no tiene limitaciones del ancho de banda que puede usar

En la misma ventana de hotspot que teníamos abierta anteriormente ir a la sección User Profile y con el botón “+” agregamos un nuevo perfil En donde se debe llenar las opciones de la siguiente forma:

- **Name:** el nombre del perfil de usuario
- **Address Pool:** se deja en none ya que se realizó una configuración dhcp automática
- **Keepalive Timeout:** es el tiempo en el que se va a caducar la sesión cada 24 horas
- **Status Autorefresh:** el tiempo en el que se va a refrescar la información de ese usuario en el panel de administración del dispositivo Mikrotik

- **Shared Users:** es el número de conexiones permitidas por el mismo usuario
- **Rate Limit (rx/tx):** es la velocidad de internet asignada al perfil siendo rx la velocidad de subida y tx la velocidad de bajada

FIGURA N°23
CREACION DE PERFIL DE USUARIO

Hotspot User Profile <usuarios>

General Queue Advertise Scripts

Name: usuarios

Address Pool: none

Session Timeout:

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (p/tx): 512k/512k

☒ Add MAC Cookie

MAC Cookie Timeout: 3d 00:00:00

Address List:

Incoming Filter:

Outgoing Filter:

Incoming Packet Mark:

Outgoing Packet Mark:

Open Status Page: always

☒ Transparent Proxy

OK Cancel Apply Copy Remove

default

Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Los perfiles de usuario quedarían de la siguiente manera según los perfiles necesarios para cada tipo de usuario que hace uso del Wifi de la empresa de seguros

FIGURA N°24
LISTA DE PEFILES DE USUARIOS

Name	Session Time...	Idle Timeout	Shared Users	Rate Limit (rx/tx)
Brokers		none		1 512k/512k
Cientes		none		1 512k/512k
auditor		none		1 512k/512k
cobradores		none		1 1M/1M
* default		none		1
ejecutivos		none		2 1M/1M
usuarios		none		1 512k/512k

7 items (1 selected)

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

A su vez como políticas de manejo para el acceso al Wifi se establecieron las siguientes políticas:

- a) Cada empleado de la compañía que desee realizar uso del Wifi debe de realizar la respectiva solicitud al personal del departamento de TI
- b) Para Usuarios externos a la compañía se dispone de usuarios predefinidos entregados a la recepcionista de la compañía en sobres sellados, los cuales para que sea disponible la conexión debe notificar al departamento de TI para la activación

4.5 Segmentación de red entre usuarios y servidores

Como se pudo observar en el esquema de red que se mostró en los puntos anteriores la ciudad de Guayaquil tiene un error en su segmentación de red, ya que comparte el mismo segmento de red con los servidores 192.168.145.0/24.

TABLA N°23
SEGMENTO DE RED DE TODAS LAS SUCURSALES

Ubicación	Segmento de red
Guayaquil	192.168.145.0/24
	192.168.1.0/24
Quito	192.168.144.0/24
	192.168.3.0/24
Cuenca	192.168.143.0/24
	11.11.11.0/24

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

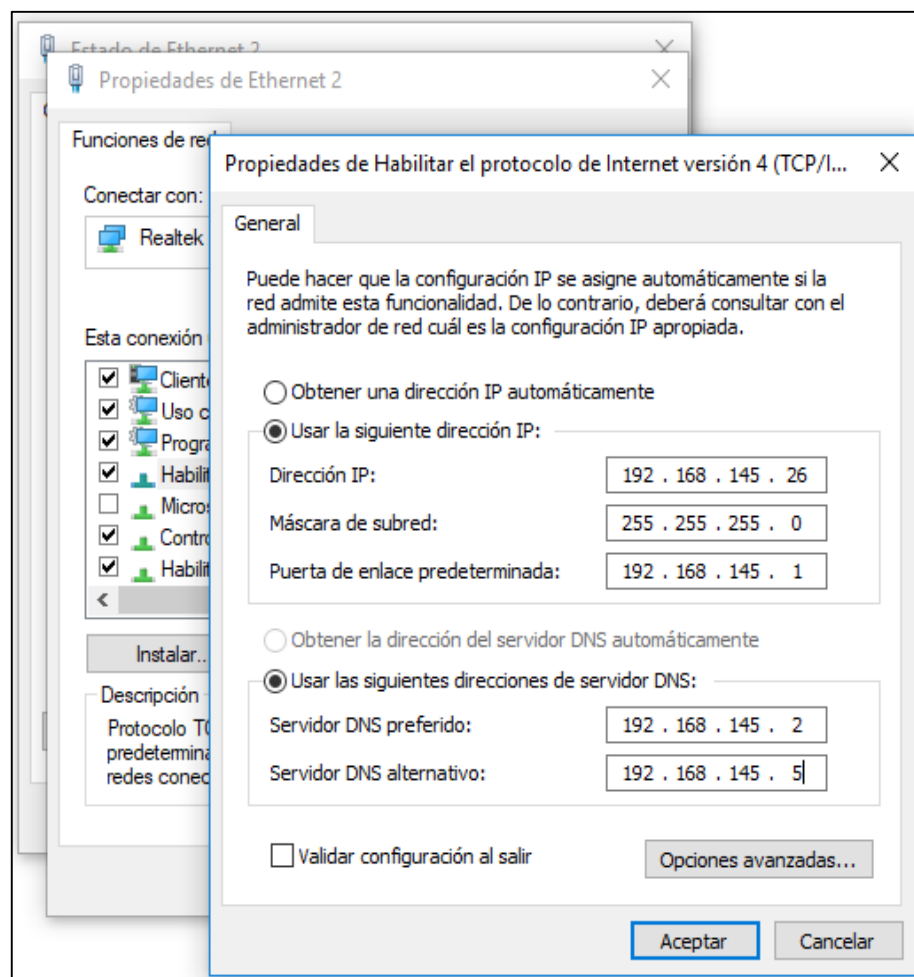
Uno de los problemas que se pudo encontrar en esta segmentación de red en la ciudad de Guayaquil es que según como se refleja en el esquema la red el segmento 192.168.145.0/24 esta compartido entre usuarios y servidores de la compañía, esto es un problema en la seguridad de la infraestructura, ya que al estar mezclado los usuarios y los servidores que son parte importante para el desempeño de la compañía dejan una brecha en la cual pueden ser atacados por personas con intenciones maliciosas.

Tomando a consideración que al estar mezclado los usuarios y los servidores se planificó una solución junto con el administrador del departamento de TI en separar a los usuarios de los servidores, es decir, dejarles un segmento de red solo para los usuarios de la compañía en la ciudad de Guayaquil mientras los servidores se mantienen en el segmento 192.168.145.0/24, el hecho de no realizar esta separación de usuarios y servidores daban la posibilidad de que cualquier persona ajena a la compañía se pudiera conectar a un punto de red libre y realizar un ataque.

Debido a que esta empresa de seguros es Internacional se conecta a la matriz en el exterior mediante el uso de una VPN, por lo cual la matriz es la que le da los segmentos disponibles para su uso en Ecuador, ya que ellos en exterior llevan un registro de todo el acceso de las sucursales mediante una gran segmentación de IP por países.

De este modo fue que se estableció que el nuevo segmento de red designado para los usuarios en la ciudad de Guayaquil será el 192.168.147.0/24, el cual no tiene ningún otro dispositivo importante conectado en esa red que pueda ser vulnerable al ataque.

FIGURA N°25
ANTES DEL CAMBIO DE SEGMENTO IP



Fuente: Investigación Directa

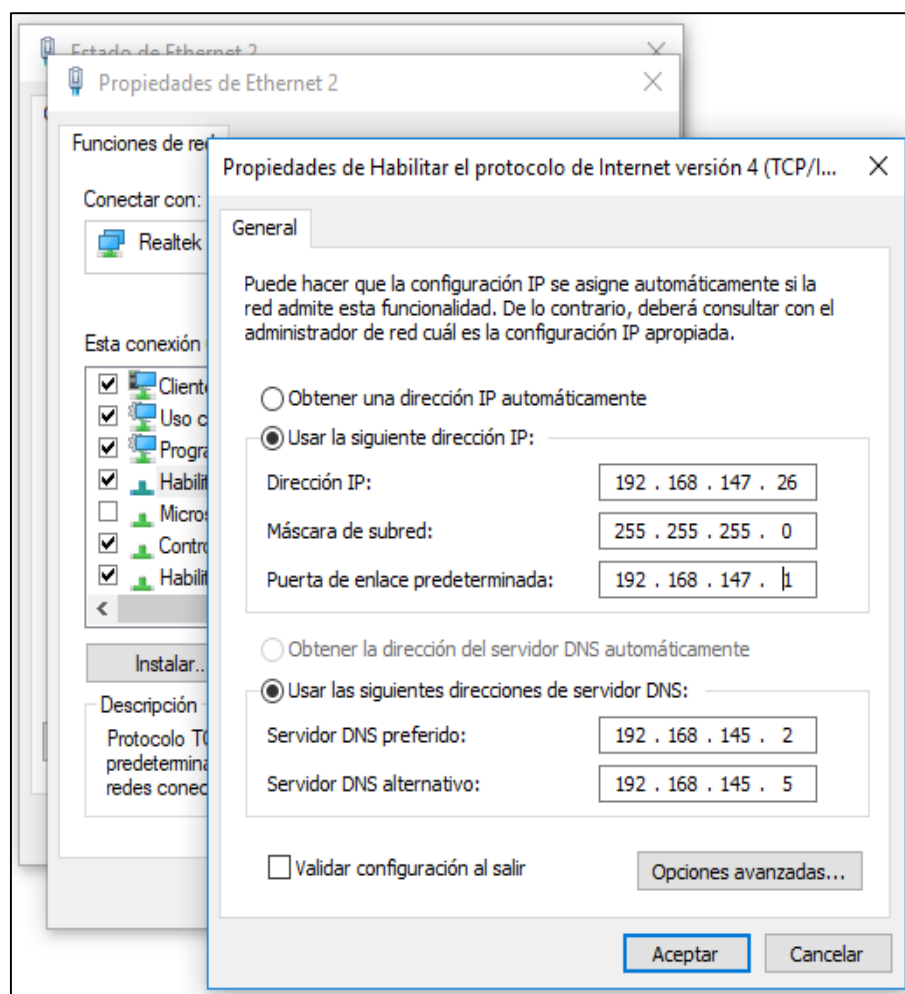
Elaborado por: Benavides Alcivar Vicente Alberto

Por otra al realizar el esquema de red se pudo identificar que las ciudades de Quito y Cuenca no tienen este inconveniente, estas ciudades si tienen una correcta segmentación de red entre las computadoras y servidores, tomando esto a consideración y luego de ya definir cuál será el nuevo segmento de red a implementarse se procede con la configuración

manual de todos los usuarios de la ciudad de Guayaquil, cambiándoles el segmento 192.168.145.0/24 por 192.168.147.0/24.

Como recomendación se propuso también el aprovechar la situación de que se realizará una configuración en cada computadora de todos los usuarios de la compañía en la ciudad de Guayaquil para darles unas recomendaciones que deben de tomar a consideración sobre el uso de la computadora y no dejar expuesta el acceso a ella cuando se mueven de sus puestos.

FIGURA N°26
DESPUÉS DEL CAMBIO DE SEGMENTO IP



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

4.6 Repotenciación de la infraestructura y los servicios

Una buena infraestructura de red en una compañía trae beneficios a corto y a largo plazo, ya que proporciona un buen manejo de la información en la actualidad y si está estructurado de manera correcta a futuro se podrá poder hacer una escalabilidad con el crecimiento de la infraestructura, debido a que si no se tiene una buena estructura resulta difícil implementar nuevos equipos o nueva tecnología que serían de beneficio para la empresa.

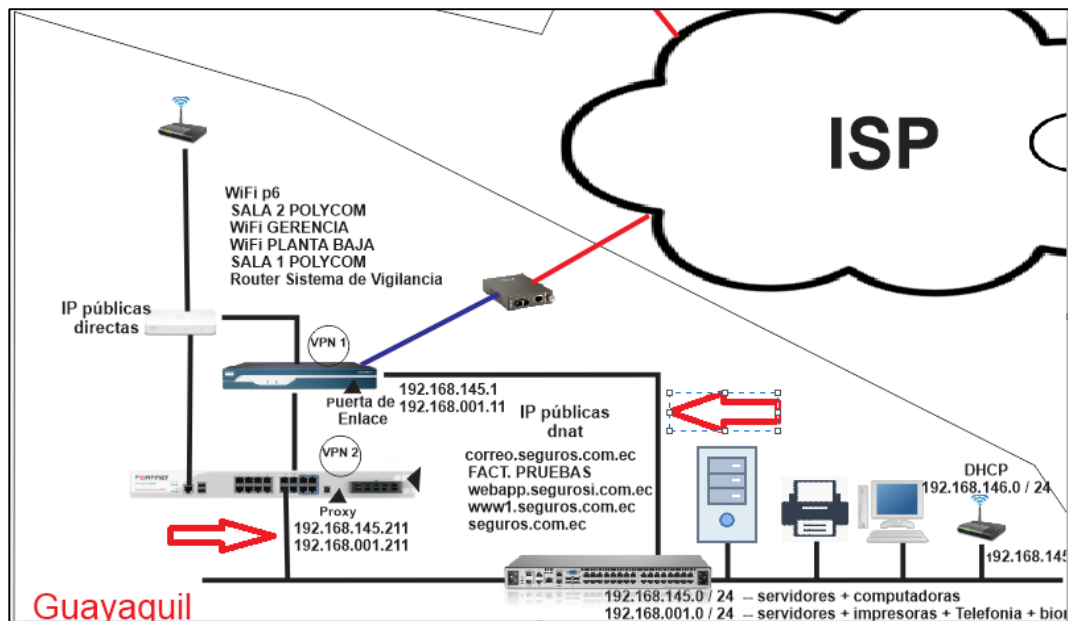
Un problema que se pudo identificar en esta infraestructura es que esta empresa de seguros tiene una conexión doble entre el router y el firewall (Fortinet) hacia la LAN, en esta infraestructura se maneja 2 tipos de canales de comunicación.

Canal de datos: por este medio viaja toda la información relacionada a procesos internos ingreso de producción y procesos de pólizas

Canal de internet: por este medio viaja toda la información que tiene algún proceso relacionado o que involucra alguna conexión a internet

En la infraestructura de la LAN de la ciudad de Guayaquil se identificó que todas las computadoras tienen configurada como puerta de enlace el router ya que es su salida a otras redes o hacia el internet, pero en este caso el Fortinet está brindando los servicios de Firewall y de Proxy por lo que para que cada computadora pueda tener una conexión por internet deben de pasar por el Fortinet que es el servidor Proxy y después al Router.

FIGURA N°27
CONEXIÓN DOBLE EN LA CIUDAD DE GUAYAQUIL



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

El problema radica en que al existir esta conexión doble en varias ocasiones hay problemas al momento de realizar la comunicación entre servicios, ya que los datos están divididos entre el camino que recorren para llegar a su destino, la solución que se propone en este proyecto de titulación y como parte de la mejora en la infraestructura de la red es dejar dicha conexión que de manera obligatoria pase por el firewall y que no exista una conexión directa entre el router y el switch como se mostró en la figura anterior

Tomando esto a consideración se procede a realizar el cambio en la conexión y se quita la que sale del switch al router y se le conecta al puerto f0/4 de equipo Fortinet eliminando así la conexión directa del router con el switch.

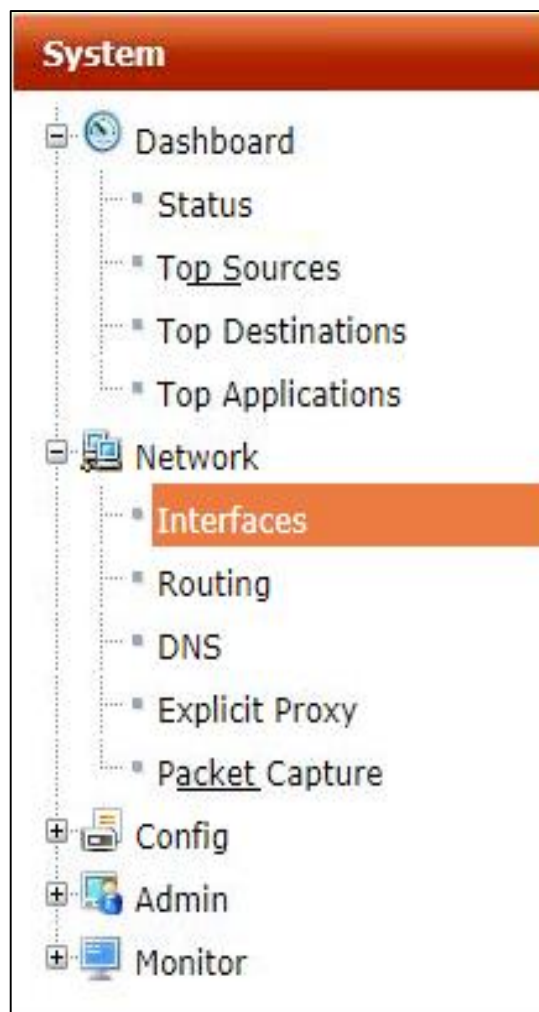
4.6.1 Configuración de ruta estática en el Fortinet

Para poder configurar una ruta estática en el Fortinet debemos ingresar al panel de control que en este caso sería la IP

192.168.145.211/24, la cual solo está configurada para recibir conexión de la computadora del administrador de TI y del subgerente de TI.

Una vez ya ingresado a la página de las configuraciones del Fortinet nos debemos dirigir en la barra lateral izquierda a la opción Network > Interface donde podremos agregar la nueva ruta estática y así poder dar conexión del canal de datos entre el switch y el router con el Fortinet como intermediario.

FIGURA N°28
CONFIGURACIÓN DE RUTA ESTÁTICA FORTINET



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

Agregamos las rutas las siguientes rutas estáticas

TABLA N°24
RUTAS ESTÁTICAS CONFIGURADAS EN EL FORTINET

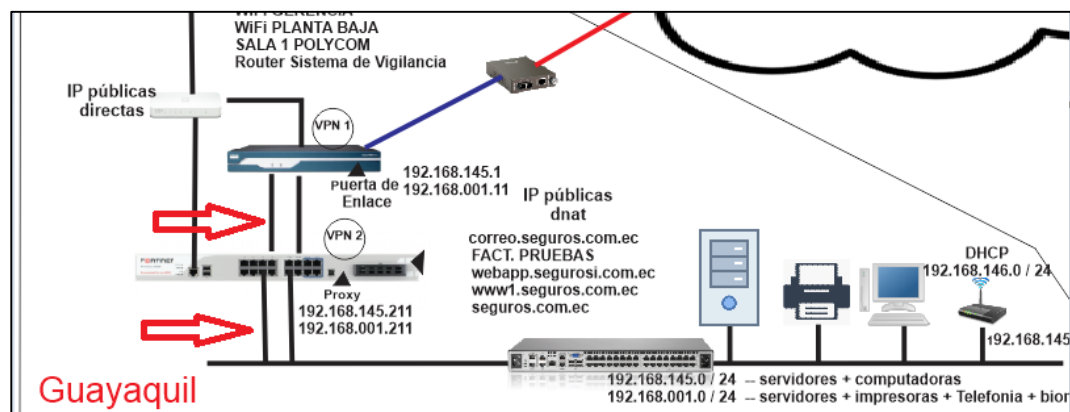
Red a la que queremos llegar	Mascara	Puerta de enlace
192.168.145.0	255.255.255.0	192.168.145.1
192.168.1.0	255.255.255.0	192.168.1.11
192.168.147.0	255.255.255.0	192.168.147.1

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

Realizada esta configuración en el Fortinet la infraestructura de red ya quedaría de manera más estable ya que todo el tráfico de red pasa por el mismo canal y todo trafico llevaría su control por parte del Fortinet, luego de haber realizado estos cambios el esquema de red nos quedaría de esta forma como muestra la siguiente figura.

FIGURA N°29
CORRECCIÓN DE LA CONEXIÓN EN LA CIUDAD DE GUAYAQUIL



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

4.6.2 Optimización de los servidores

Los servidores son parte fundamental para el desarrollo de las actividades que se realizan en una empresa, son los encargados de brindar los diferentes servicios que se les pueda agregar de una manera continua las 24 horas le día y todos los días del año, pero el hecho de que sean dispositivos diseñados para mantener un uso constante no quiere decir que

una vez adquiridos seguirán trabajando de igual manera el resto de su vida útil.

Se debe mantener las condiciones óptimas para que puedan cumplir su función tanto en el espacio designados para ellos como también su sistema eléctrico y la refrigeración, por otra parte, lo que no hay que descuidar es el mantenimiento que se le debe de dar y las respectivas actualizaciones, ya sea actualizaciones en software como en hardware.

Realizando la investigación de los dispositivos de cómputo y red que dispone esta empresa de seguros se pudo identificar que si se provee el respectivo mantenimiento en software a los servidores con una actualización constante de los programas que son necesarios para ellos, pero también se pudo identificar que varios de estos servidores estaban trabajando a toda su capacidad con las mismas características de fábrica.

FIGURA N°30

MEMORIA RAM PARA SERVIDORES



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Tomando a consideración que varios de esos servidores tienen servicios fundamentales para la empresa y necesitan tener una fluidez para no ralentizar el proceso de producción diaria, se tomó la iniciativa de aumentar las características de esos equipos y realizar una reorganización en las máquinas virtuales que no se encontraban en un orden según sus servicios como por ejemplo los servidores de las aplicaciones web donde

la página web estaban en otro servidor diferente al de los aplicativos web y a la intranet de la compañía.

El motivo por el cual se optó a agruparlos según el proceso que realizan es para darle prioridad de rendimiento a esos servidores específicos, tanto el aumentarle las memorias RAM como el aumentar las capacidades de disco duro para que tengan una mayor fluidez al momento de recibir mucha demanda de servicios, por otro lado se encontró una máquina virtual sobre aplicativos web que usa Xampp para brindar servicios web, el problema respecto a esto es que el sistema operativo en el que está ubicado dicho servicio es un Windows 8 y no una versión de Windows server como podría ser la versión de Windows Server 2012 R2 que está instalado en los demás servidores.

FIGURA N°31
DISCO DURO SAS



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Debido a esos inconvenientes con los servidores y a esa máquina virtual se procedió a hacer la adquisición de 2 módulos de memoria RAM de 8GB cada uno para el servidor de producción GEHIPERV04 – WINDOWS SERVER HOST4 pasando de tener 8gb de RAM a tener 24GB de RAM, al servidor de página web y servidor de archivos GEHIPERV3 – WINDOWS SERVER HOST3 se le agregó 3 módulos de memoria RAM de

8GB y 4 discos duro SAS de 1TB de almacenamiento pasando de tener 16GB de RAM a tener 40GB de RAM y de 2TB de disco duro a tener 6 TB de disco duro.

4.7 Replicación de los servidores a la nube de Azure

La nube Azure de Microsoft tiene una gran herramienta que nos ayuda en el proceso de replica que se realiza de un servidor local a la nube de Azure, a continuación, se detallan los pasos a seguir para poder realizar esta replica como mecanismo de seguridad en caso de un desastre.

4.7.1 Requisitos previos

4.7.1.1 Requisitos de compatibilidad de los Host

La siguiente tabla muestra de manera general todos los componentes que se ven involucrados en la replicación a azura cuando se tiene una arquitectura de Hyper-V administradas en VMM

TABLA N°25
COMPONENTES DE ARQUITECTURA HYPER-V CON VMM

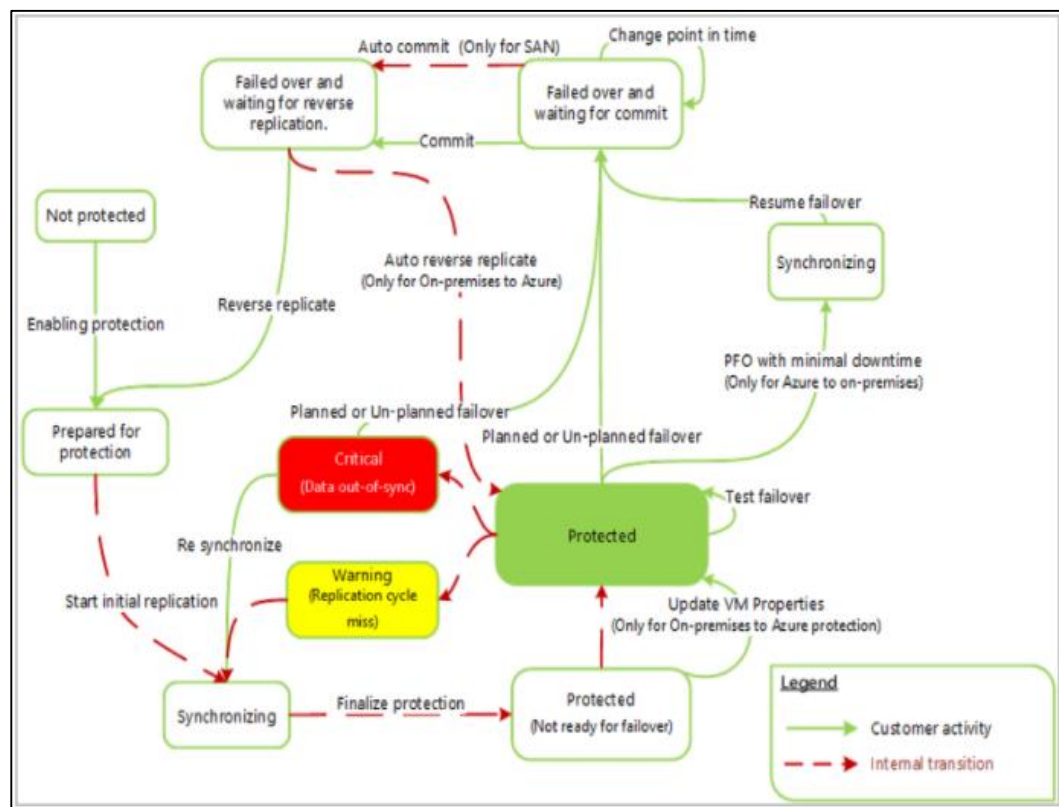
Componentes	Requisito	Detalles
Las tablas de Azure	Suscripción de Azure, cuenta de Azure Storage y red de Azure	Los datos de las máquinas virtuales replicadas en Azure se almacenan en la cuenta de almacenamiento
Servidor VMM	Servidores VMM que contienen varias nubes con hosts Hyper-V	Consiste en realizar una instalación de Site Recovery en el servidor VMM para que pueda realizar las resplicas registrando en el almacen de Recovery Service
Host de Hyper-V	Uno o más hosts o clústeres de Hyper-V	Se realiza la instalación de Recovery Service en

	administrados por VMM.	cada miembro del cluster o host.
Máquinas virtuales de Hyper-V	Una o varias máquinas virtuales en ejecución Hyper-V	No es necesario realizar ninguna instalación en las máquinas virtuales
Redes	Configuración realizada en el servidor VMM el cual contiene redes lógicas y de máquinas virtuales	Las redes de máquinas virtuales se asignan a redes virtuales de Azure. Cuando se realiza una conmutación por error es agregada a la red de Azure las máquinas virtuales en lugar de las que tenía asignada previamente

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

FIGURA N°32
ESQUEMA DEL PROCESO DE REPLICA

Fuente: <https://docs.microsoft.com/es-es/azure/site-recovery/concepts-hyper-v-to-azure-architecture>

Elaborado por: Microsoft Azure

4.7.2 Acceso a URL específicas.

Para poder hacer uso de este servicio que nos ofrece la nube Azure de Microsoft debemos de realizar una comprobación en todos los hosts que se disponga del acceso a las siguientes URL nombradas a continuación:

TABLA N°26
URL HABILITADAS EN LOS HOSTS

URL	DETALLE
.accesscontrol.windows.net	Utilizada para los controles de acceso y administración de identidades
https://login.microsoftonline.com	Acceso y administración de identidades AAD
*.backup.windowsazure.com	Transferencia de datos de replica
*.blob.core.windows.net	Acceso a cuentas de almacenamiento de datos
*.hypervrecoverymanager.windowsazure.com	Operaciones de administración de replica
time.nist.gov time.windows.com	Comprobación de la sincronización

Fuente: <https://docs.microsoft.com/es-es/azure/site-recovery/tutorial-hyper-v-to-azure>

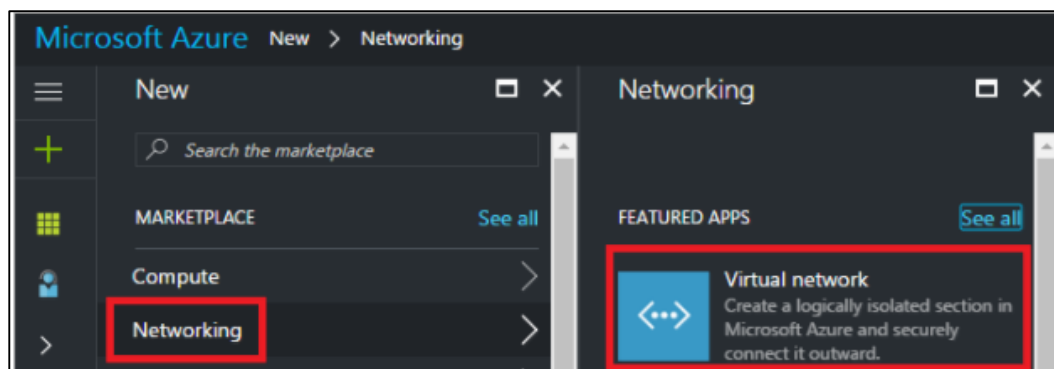
Elaborado por: Benavides Alcivar Vicente Alberto

4.7.3 Configuración en Azure

4.7.3.1 Creación de una red virtual en Azure

Para realizar la creación de una red virtual en Azure primero debemos ingresar a la página de Azure y seleccionar en el panel de la parte izquierda la opción “Nuevo”, luego hacer clic en “Redes” y después el “Red Virtual”

FIGURA N°33
CREACIÓN DE UNA NUEVA RED VIRTUAL EN AZURE



Fuente: Investigación Directa
 Elaborado por: Benavides Alcivar Vicente Alberto

Luego en la hoja de la creación de la “Red Virtual” se debe dejar seleccionado “Resource Manager” como modelo de implementación y se procede a darle clic al botón de “crear”

A continuación, se muestra una tabla donde se hace referencia a los valores que deben ser agregados en la hoja de creación de la red virtual

TABLA N°27
VALORES PARA AGREGAR UNA RED VIRTUAL EN AZURE

Configuración	Detalles
Name	Se debe escribir el nombre único para el nombre de recursos
Espacio de direcciones	Se especifica el espacio de direcciones que se desee en la notación
Nombre de la subred	Se debe escribir el nombre que va a ser designado para la subred que debe ser un nombre único para evitar conflicto con otras subredes
Intervalo de direcciones de subred	Se especifica el espacio de direcciones designadas a la red virtual
Grupos de recursos	Se debe registrar un nombre para grupo de recursos el cual debe ser único y no repetirse
Ubicación	se selecciona la ubicación de la región más cercana a la ubicación de la empresa

Fuente: Investigación Directa
 Elaborado por: Benavides Alcivar Vicente Alberto

4.7.3.2 Cuenta de almacenamiento

En la nube Azure de Microsoft disponen de 2 tipos de cuentas de almacenamiento:

- Cuenta de almacenamiento de uso general
- Cuenta de almacenamiento de Blob Storage

Cuenta de almacenamiento de uso general: son el tipo de cuenta que de una forma general nos permite el acceso a discos de máquinas virtuales, tablas, diferentes tipos de archivos, el beneficio de este tipo de cuenta es que nos provee de un nivel de rendimiento de almacenamiento estándar un buen precio regular.

Cuenta de almacenamiento Blob Storage: este tipo de cuenta de almacenamiento es especializado, ya que nos permite el manejar datos como blobs por su forma de guardar los datos de forma no estructurada a diferencia de la cuenta de almacenamiento de uso general, la cuenta de almacenamiento de Blob como gran beneficio nos provee un nivel de acceso frecuente y acceso esporádico, pero en ambos casos nos permite el almacenar datos a un costo mucho menor.

4.7.4 Preparación de los host HYPER-V

A continuación, se muestra la tabla de compatibilidad de los host Hyper-V

TABLA N°28
COMPATIBILIDAD DE SERVIDORES CON HYPER-V

Implementación	Soporte Técnico
Servidor de máquina virtual de VMware o Físico	vCenter 6.5, 6.0 o 5.5
Hyper-V(con Virtual Machine Manager)	System Center Virtual Machine Manager 2016 y System Center Virtual Machine Manager 2012 R2

Servidor de máquina virtual de VMware o físico	vSphere 6.5, 6.0 y 5.5
Hyper-V (con o sin Virtual Machine Manager)	Windows Server 2016 y Windows Server 2012 R2 con las actualizaciones más recientes. Si se usa SCVMM, los hosts de Windows Server 2016 debe administrarlos SCVMM 2016.

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

4.7.5 Preparación de los servidores VMM

A continuación, se muestra la tabla de compatibilidad de los servidores VMM

TABLA N°29
COMPATIBILIDAD DE SERVIDORES VMM

Implementación	Soporte Técnico
Servidor de máquina virtual de VMware o físico	vCenter 6.5, 6.0 o 5.5
Hyper-V (con Virtual Machine Manager)	System Center Virtual Machine Manager 2016 y System Center Virtual Machine Manager 2012 R2
Servidor de máquina virtual de VMware o físico	vSphere 6.5, 6.0 y 5.5
Hyper-V (con o sin Virtual Machine Manager)	Windows Server 2016 y Windows Server 2012 R2 con las actualizaciones más recientes. Si se usa SCVMM, los hosts de Windows Server 2016 debe administrarlos SCVMM 2016.

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

4.7.6 Creación de almacén Recovery Service

Para poder realizar la creación del almacén Recovery Service de Azure el cual vamos a utilizar para la replicación de las máquinas virtuales demos acceder al panel de control de Azure, dirigirnos a “Nuevo > Supervisión y administración > Backup y Site Recovery”

En el recuadro que nos aparece llenaremos el campo de “Name” con el nombre que le queremos asignar a la recuperación y en el recuadro

“Create a new resource group” seleccionaremos un nombre para el grupo de maquina virtuales las cuales vamos a replicar

FIGURA N°34
VENTANA DE CREACIÓN DE ALMACÉN RECOVERY SERVICE

Recovery Services vault
Recovery Services vault - PREVIEW

* Name
ContosoVault ✓

* Subscription
ASR Canary Test Subscription 1 >

* Create a new resource group
ContosoRG ✓
[Select existing](#)

* Location
East US >

☒ Pin to dashboard

Create

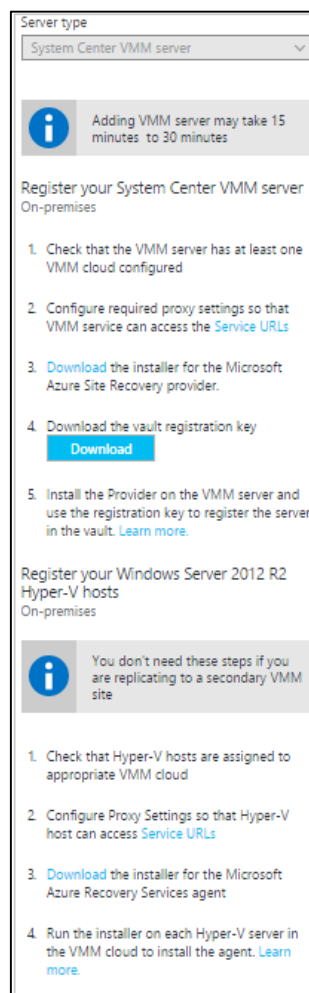
Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

4.7.7 Preparación de la infraestructura

La preparación de la infraestructura se refiere a preparar el entorno de origen, es decir nuestras máquinas virtuales las cuales van a ser replicadas a la nube de Azure, para ello en nuestra página de Azure nos dirigimos a la opción de “Preparar Origen” y le damos clic al botón “+VMM” para poder agregar un nuevo servidor

Se mostrará la siguiente ventana en donde debemos darle clic a la opción número 3 de la ventana donde dice “Download” y se realizara la descarga de un archivo con el nombre de “AzureSiteRecovery.exe”

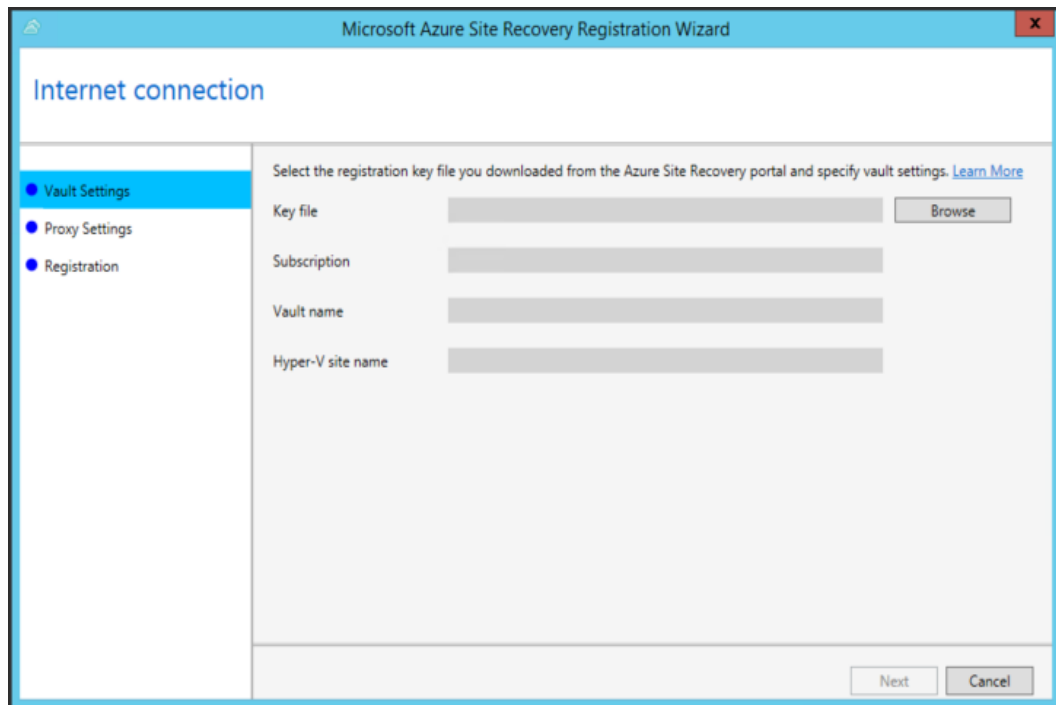
FIGURA N°35
VENTANA PARA AGREGAR UN NUEVO SERVIDOR RECOVERY SITE



Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Ese archivo descargado de ser ejecutado en el host donde tenemos las máquinas virtuales y luego de instalarlo nos aparecerá una ventana que nos pide un archivo de “Key” el cual se descarga en el paso número 4 que se muestra en la figura anterior en el cuadro celeste que dice “Download”.

FIGURA N°36
CONFIGURACIÓN DEL ALMACÉN



Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

En la configuración del Proxy se debe especificar la configuración que usa el Host físico actual para conectarse a internet

En la parte de Cifrado de datos se puede especificar el cifrado de los datos que Azure va a recibir por nuestra parte, se emite un certificado que es necesario para descifrar los datos más adelante

4.7.8 Configuración del entorno de destino

En esta parte se realiza la comprobación de los recursos de destino, para ellos debemos de hacer clic en “Preparar infraestructura > Destino”, después de llenar los espacios con la información solicitada como es el tipo

de suscripción y el modelo de implementación que se quiere usar en Azure para la conmutación por error debemos realizar la configuración de la red

Para realizar la asignación de la red debemos dar clic a la siguiente opción “Infraestructura de Site Recovery > Asignaciones de red > Asignación de red > + asignación de red”

Se debe asignar como destino Azure al momento de agregar la asignación de red

FIGURA N°37
ASIGNACIÓN DE RED

* Source System Center VMM	* Target
CP-L2B18-X64-48.dratest.nttest.microsoft... ▼	Azure ▼
	* Subscription
	ASR Canary Test Subscription 1 ▼
	* Post-failover deployment model
	Resource Manager ▼
* Source network	* Target network
VSwitch_VLan ▼	VNetworkV2-1 ▼
Network type No isolation	Subnet default 10.0.0.0/24
Subnet No subnets are configured.	
Network ID e056827b-0d94-41bc-9631-d972e3395541	

Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

4.7.9 Política de replicación

Realizar la creación de la directiva de replicación es la configuración que se le da a la réplica de cómo quiere que se ejecute, ya que esto nos

permite seguir un cronograma de replicaciones en caso de que no lo pudiéramos hacer de manera instantánea.

FIGURA N°38
CREACIÓN DE POLÍTICA DE REPLICACIÓN

Create and associate policy
ContosoVault

* Name ⓘ
ContosoReplicationPolicy x

Source type ⓘ
Hyper-V v

Target type ⓘ
Azure v

Copy frequency ⓘ
15 Minutes v

* Recovery point retention in hours ⓘ
2

* App-consistent snapshot frequency in hours ⓘ
1

Initial replication start time ⓘ
Immediately v

Encrypt data stored on azure ⓘ
On Off

Associated VMM cloud ⓘ
Sales_Application

Advanced VMM settings (Optional) ⓘ
Azure subscription users >

Fuente: Investigación Directa
Elaborado por: Benavides Alcivar Vicente Alberto

Para ingresar a la configuración de la política de replicación debemos hacer clic en “Preparar Infraestructura > Configuración de la replicación > +Crear y asociar”.

En Retención de punto de recuperación, se especifica el tiempo máximo en horas que se puede realizar una retención en el proceso de replica

En Frecuencia de instantánea coherente con la aplicación, se especifica en los puntos de restauración el numero en horas con la que se realizan instantáneas de las máquinas virtuales

Se debe especificar la hora de inicio de la replicación y si se desea o no el cifrar los datos que se van replicando

4.7.10 Habilitación de la replica

Una vez ya realizada las configuraciones entre las máquinas virtuales y el servicio de Azure podemos empezar con el proceso de replica que demorará dependiendo de la conexión a internet que tenga el Host.

Debemos ingresar a Replicar la aplicación > Origen, donde se nos mostrará unos recuadros donde se debe ingresar en Origen el sitio donde tenemos la máquina virtual Hyper-V y en Destino se seleccionad la conexión con Azure, ya que ahí es donde se van a almacenar las replicaciones que se van a realizar.

Finalmente seleccionamos la característica de la máquina virtual que vamos a replicar en la ventana de configuración de propiedades y se procede a realizar el proceso de réplica, podemos hacer un seguimiento de cómo va el proceso ingresando al apartado de Recover Service en nuestro portal de Azure o verificando en la barra de notificaciones de la pantalla principal.

FIGURA N°39

CONFIGURACIÓN DE PROPIEDADES DE LA MAQUINA VIRTUAL A REPLICAR

NAME	OS TYPE	OS DISK	DISKS TO REPLICATE	TARGET NAME
Defaults	Select	Need to select per VM.	Need to select per VM.	Fix per VM
NANO SERVER	Windows	NANO-01	NANO-01 [4.00 GB]	NANOSERVER

Fuente: Investigación Directa

Elaborado por: Benavides Alcivar Vicente Alberto

4.8 Simulacro de Recuperación ante Desastre

La configuración para la recuperación ante desastre como se la explicó en la sección anterior se lo define en la política de replicación, dicha configuración es la que Azure toma a consideración para realizar la replicación de las computadoras que pueden ser utilizadas en un caso de desastre.

Antes de proceder con un simulacro debemos realizar las siguientes verificaciones respecto a la máquina virtual para cumplir con los requerimientos de Azure.

1. Realizar una verificación en “Elementos Replicados” al cual podremos acceder entrando a “Elementos Protegidos” desde el Panel de Control de Azure.
2. En el panel de “Elemento Replicado” podremos realizar una verificación del estado de la máquina virtual, tanto en el estado de mantenimiento como los puntos de restauración que se han ido almacenando periódicamente según lo programado en las políticas de replicación.

3. En la opción “Proceso y red” se puede realizar modificaciones sobre la máquina virtual que se está replicando actualmente, cambios como el grupo de recursos, el tamaño del destino y la configuración de disco administrados.
4. En la parte de **Discos** se puede ver los datos sobre el sistema operativo que dispone la máquina virtual y la información de los discos de datos

4.8.1 Pasos para la conmutación por error de prueba en una sola máquina virtual

En el mismo panel de control de “Elementos replicados” debemos de realizar los siguientes pasos:

1. Ir a Configuración > Elementos replicados, dirigirse a la parte de VM y seleccionar +Probar conmutación por error
2. Se debe de seleccionar un punto para la restauración que pueda ser utilizado en la conmutación por error:
 - a. **Procesado más recientemente:** este procesa el último punto de restauración que fue procesado por el servicio Site Recovery,
 - b. **Más reciente coherente** realiza la conmutación por error en todas las VM con la diferencia de que se realiza de una restauración con la verificación de que cada proceso se finalizó correctamente y se continua a partir de todos los procesos finalizados
 - c. **Personalizado:** se muestran varias alternativas para la recuperación que el usuario podrá elegir a su conveniencia

3. Seleccionar “Probar conmutación por error” y asignar la red que Azure va a usar como destino para conectarse con las máquinas virtuales en la conmutación por error
4. Dar clic en “Aceptar” para dar inicio a la conmutación por error, para poder realizar un seguimiento del progreso de la conmutación se debe dirigir a la máquina virtual y en las propiedades saldrá la información.
5. Cuando se finaliza la conmutación por error se mostrará la máquina virtual en el portal de Azure con el tamaño adecuado y conectado a la red correspondiente en modo de ejecución.
6. Cuando se desee borrar la máquina virtual creada en la prueba se selecciona la máquina y se le da a la opción de “Limpiar conmutación por error de prueba”

4.9 Conclusiones

En este proyecto de titulación se pudo realizar un plan de mejora orientado a una empresa de seguros de la ciudad de Guayaquil, en donde se hizo una investigación sobre la infraestructura de red y los servicios que mantenía para poder así a partir de esa investigación realizada brindar una solución aplicable para la mejora de los procesos que se realizan diariamente.

Mediante el uso de la observación directa se pudo comprobar cual era el estado actual de los equipos de red que maneja esta empresa de seguros, tanto el hardware como el software que poseen dichos dispositivos y los equipos que se disponían como backup para poder implementarlos en este proyecto para la mejora de la propuesta y verificar mediante el uso de las encuestas cuales eran algunas de las necesidades que se necesitaba cumplir.

En lo referente a las mejoras de seguridad en la red se realizó una segmentación de red adicional para los usuarios de la ciudad de Guayaquil, ya que existía un segmento compartido entre usuarios y servidores que son de gran importancia para la empresa, realizando esta separación en la red se pudo evitar que los usuarios realicen algún ingreso sin autorización a los servidores de la empresa y perjudicar los procesos que se llevan a cabo.

Como mecanismo de seguridad en el acceso Wifi se implementó el uso de un dispositivo Mikrotik que realiza la función de un hotspot el cual la compañía ya lo disponía pero no se estaba utilizando, se crearon políticas para la creación de usuarios que pueden acceder al Wifi de la compañía y con perfiles específicos para cada tipo de usuario ya que en varias ocasiones se presentaba el inconveniente que personas ajenas a la empresa o incluso los mismos usuarios de la misma con el acceso sin control al wifi consumiendo mucho ancho de banda provocando lentitud en el procesos importantes de producción.

También se realizó una verificación de los recursos que disponían los servidores de la compañía, en el cual se pudo identificar que dichos servidores estaban realizando su trabajo con limitaciones de recursos e impidiendo que puedan trabajar con fluidez y poder reducir tiempos de respuesta en las peticiones que reciben diariamente, por lo cual se realizó una actualización en los recursos de los servidores y también una organización de las máquinas virtuales en los servidores según su función (esta empresa dispone de 9 servidores).

Debido a un problema que se pudo identificar al momento de realizar el esquema de red se realizó una corrección en las conexiones que existían para el canal de datos y para el canal de internet, un problema el cual ocasionaba intermitencia en algunas ocasiones y que era necesario para poder realizar la réplica de los servidores en la nube Azure de Microsoft.

Para poder realizar las réplicas de los servidores fundamentales de la compañía a la nube de Azure se realizó una petición al proveedor de Internet para subir el ancho de banda en la velocidad subida de manera temporal debido al gran volumen de información que debe ser replicada, la replicación en Azure consiste en la creación de la cuenta donde se debe llevar a cabo unos pasos a seguir que se encuentran detallados en el capítulo 4 de este proyecto de titulación y también el cómo poder realizar un simulacro de la recuperación de ellos en caso de un desastre.

4.10 Recomendaciones

Se recomienda hacer una organización en el etiquetado de los cables y la identificación de que maquina virtuales tiene cada servidor ya que al momento de realizar las verificaciones varias de las etiquetas se encontraban erróneas debido a que no se actualizaron al momento de realizar un cambio.

Es necesario una capacitación en el equipo Fortinet al personal del área de TI para poder tener menos dependencia del ISP que realiza la gestión de dicho dispositivo firewall, ya que en la investigación se pudo identificar que existen configuraciones las cuales pueden realizar el propio departamento de TI que por falta de capacitación no las pueden realizar de manera correcta.

Se recomienda hacer un rediseño de las políticas de seguridad que se manejan en esta empresa de seguros para poder llevar un control en el acceso a los datos importantes de la compañía, brindar charlas constantes a los trabajadores para que puedan adoptar las medidas de seguridad que se debe de tener al momento de manejar una computadora y que tengan el conocimiento de los datos que pueden ser perjudicados por un descuido.

Es importante tomar en consideración los beneficios que está trayendo el cambio tecnológico referente a las arquitecturas de red en las empresas, debido a que la computación en la nube ofrece muchos beneficios en comparación al mantener equipos físicos en cada empresa, ya que brinda la posibilidad de un escalamiento según la necesidad de la empresa sin la necesidad de hacer una gran inversión en la adquisición de nuevos equipos que necesitan un mantenimiento constante.

ANEXOS

ANEXO Nº1

NORMAS GENERALES PARA LAS INSTITUCIONES DEL SISTEMA FINANCIERO

SUPERINTENDENCIA DE BANCOS Y SEGUROS

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

4.3 Tecnología de la información. - Las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones. (reformado con resolución No. JB- 2014-3066 de 2 de septiembre del 2014) Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir políticas, procesos, procedimientos y metodologías que aseguren una adecuada planificación y administración de la tecnología de la información. (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014) Dichas políticas, procesos, procedimientos y metodologías se referirán a: (inciso reformado con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

4.4 Eventos externos. - En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 15.- Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

Para el efecto, las instituciones del sistema financiero deben establecer un proceso de administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 o el que lo sustituya, y considerar al menos lo siguiente:

15.1 La definición de objetivos, políticas, estrategias, procedimientos, metodología, planes y presupuesto para la administración de la continuidad;

15.2 Un comité de continuidad del negocio que esté conformado como mínimo por los siguientes miembros: el funcionario responsable de la unidad de riesgos, quien lo preside, el funcionario responsable de la administración de la continuidad, quien hará las veces de secretario, el funcionario responsable del área de tecnología de la información, el funcionario responsable del área de talento humano, el auditor interno, solo con voz, y el máximo representante de cada una de las áreas involucradas en el proceso de administración de la continuidad.

El comité de continuidad del negocio debe sesionar mínimo con la mitad más uno de sus integrantes, al menos una vez cada trimestre, y sus decisiones serán tomadas por mayoría absoluta de votos. El presidente del comité tendrá voto dirimente. El comité de continuidad del negocio debe dejar evidencia de las decisiones adoptadas, las cuales deben ser conocidas y aprobadas por el comité de administración integral de riesgos.

El comité de continuidad del negocio debe tener al menos las siguientes responsabilidades:

15.2.1. Monitorear la implementación del plan y asegurar el alineamiento de éste con la metodología; y, velar por una administración de la continuidad del negocio competente;

15.2.2. Proponer cambios, actualizaciones y mejoras al plan;

15.2.3. Revisar el presupuesto del plan y ponerlo en conocimiento del comité de administración integral de riesgos;

15.2.4. Dar seguimiento a las potenciales amenazas que pudieran derivar en una interrupción de la continuidad de las operaciones y coordinar las acciones preventivas; y,

15.2.5. Realizar un seguimiento a las medidas adoptadas en caso de presentarse una interrupción de la continuidad de las operaciones;

15.3 Análisis de impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros.

El análisis de impacto debe ser revisado periódicamente y actualizado cuando existan cambios en la organización o en su entorno, que puedan afectar sus resultados;

15.4 Análisis que identifique los principales escenarios de riesgos, incluyendo las fallas en la tecnología de la información, tomando en cuenta

el impacto y la probabilidad de que sucedan. Para ello, debe seguirse una metodología consistente con aquella utilizada para la evaluación de los demás riesgos;

15.5 Evaluación y selección de estrategias de continuidad por proceso que permitan mantener la continuidad de los procesos que soportan los principales productos y servicios, dentro del tiempo objetivo de recuperación definido para cada proceso, mismas que deben tomar en cuenta, al menos lo siguiente: la seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de procesamiento e información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso;

15.6 Realización de pruebas del plan de continuidad del negocio que permitan comprobar su efectividad y realizar los ajustes necesarios, cuando existan cambios que afecten la aplicabilidad del plan o al menos una (1) vez al año;

15.7 Procedimientos de difusión, comunicación, entrenamiento y concienciación del plan y su cumplimiento; e,

15.8 Incorporación del proceso de administración de la continuidad del negocio al proceso de administración integral de riesgos, que garantice la actualización y mejora continua del plan de continuidad del negocio.

ARTÍCULO 16.- El plan de continuidad del negocio debe contener al menos los procedimientos operativos, tecnológicos, de emergencias y comunicaciones para cada proceso crítico y para cada escenario cubierto, los cuales deben considerar, según corresponda, como mínimo lo siguiente. (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014)

16.1 Escenarios de riesgos y procesos críticos cubiertos y alertas de los escenarios y procesos críticos no cubiertos por el plan;

16.2 Roles y responsabilidades de las personas encargadas de ejecutar cada actividad;

16.3 Criterios de invocación y activación del plan;

16.4 Responsable de su actualización;

16.5 Acciones y procedimientos a ejecutar antes, durante y después de ocurrido el incidente que ponga en peligro la operatividad de la institución, priorizando la seguridad del personal;

16.6 Tiempos máximos de interrupción y de recuperación de cada proceso;

16.7 Acciones y procedimientos a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas o para el restablecimiento de los procesos críticos de manera urgente;

16.8 Información vital y cómo acceder a ella (incluye información de clientes, contratos, pólizas de seguro, manuales técnicos y de operación, entre otros);

16.9 Comunicaciones con el personal involucrado, sus familiares y contactos de emergencia, para lo cual debe contar con la información para contactarlos oportunamente (direcciones, teléfonos, correos electrónicos, entre otros);

16.10 Interacción con los medios de comunicación;

16.11 Comunicación con los grupos de interés;

16.12 Establecimiento de un centro de comando (considerar al menos un sitio principal, y uno alternativo); y,

16.13 Ante eventos de desastre en el centro principal de procesamiento, los procedimientos de restauración en una ubicación remota de los servicios de tecnología de la información deben estar dentro de los parámetros establecidos en el plan, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. La ubicación remota no debe estar expuesta a los mismos riesgos del sitio principal.

ANEXO N°2

Preguntas de la encuesta

- 1. ¿Cree usted que es necesario tener una actualización constante de los equipos de cómputo?**
 - Si
 - No

- 2. ¿Cree usted que se debe llevar un control de las personas que puedan acceder a la información de la compañía?**
 - Si
 - No

- 3. ¿Cree usted que es suficiente los respaldos generados por la empresa?**
 - Si
 - No

- 4. ¿Cree usted que se necesita mejorar a nivel de infraestructura de red para que los procesos sean rápidos?**
 - Si
 - No

- 5. ¿Cree usted que los mecanismos existentes en la empresa son suficiente para que la empresa siga trabajando en caso de desastre?**
 - Si
 - No

BIBLIOGRAFÍA

Alencar, M. A. (2012). Libro. Fundamentos de las redes de computadoras. Componentes Generales de <https://www.uv.mx/personal/artulopez/files/2012/09/08-Fun-y-Tec-de-Redes-de-C.pdf>. Pág 18 de PDF.

Barot, G. (2015). Libro. Hadoop Backup and Recovery solutions. Backup Design Philosophy de https://indico.cern.ch/event/532157/contributions/2167584/attachments/1275002/1891182/Backup_and_Recovery_for_Hadoop.pdf. Pág 7 de PDF.

BEZET-TORRES, J., & BONNET, N. (2016). Libro. Windows server 2016 infraestructura de red. Recursos Informáticos de <https://www.ediciones-eni.com/libro/windows-server-2016-infraestructura-de-red-9782409012242>. Pág 179 de PDF.

Cisco. (2017). Art. ¿Qué es un Firewall?. Tipos de Firewall. de https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html.

Enzo Augusto, M. (2011). Art. Políticas de seguridad. Administrador de servidores. de <https://clasesdeseguridadinformatica.files.wordpress.com/2014/03/administrador-de-servidores.pdf>. Pág 76 de PDF.

Forouzan, B. A. (2011). Libro. Network Layer. TCP/IP Protocol Suite. de https://vaibhav2501.files.wordpress.com/2012/02/tcp_ip-protocol-suite-4th-ed-b-forouzan-mcgraw-hill-2010-bbs.pdf. Pág 93 de PDF.

Grinnell, R. M., & Unrau, Y. (2005). Art. Learning Objectives. Social Work Research and Evaluation: Quantitative and Qualitative Approaches. New York: Cengage Learning. de <https://fsw.ucalgary.ca/files/fsw/sowk-355-f15.pdf>. Pág 2 de PDF.

Huidobro, J. M. (2014). Libro. Tecnologías de las redes. Telecomunicaciones. Tecnologías, Redes y Servicios. 2da Edición. de <https://downloadflix.com/download/book/keyword.html?aff.id=9217>. Pág 56 de PDF.

Jon, B., & Trey, M. (2014). Art. BCP Trends & Considerations. Business Continuity and Disaster Recovery. de http://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/11-13-14-audit/business-continuity.pdf. Pág 14 de PDF.

Microsoft (2017). Art. Conmutación por error y conmutación por recuperación de las máquinas virtuales de Azure entre regiones de Azure. de <https://docs.microsoft.com/es-es/azure/site-recovery/azure-to-azure-tutorial-failover-failback>.

Snedaker, S. (2013). Art. From an IT perspective, what should we be thinking about?. Business Continuity and Disaster Recovery Planning for IT Professionals. de <http://www.contractpackaging.org/files/public/businesscontinuitybird-quatro.pdf>. Pág 10 PDF.

Tanenbaum, A. S., & Wetherall, D. J. (2012). Libro. Establecimiento de una conexión TCP. Redes de computadoras Pearson Educación. de https://bibliotecavirtualapure.files.wordpress.com/2015/06/redes_de_computadoras-freelibros-org.pdf. Pág 481 de PDF.

Thomas, E., Zaigham, M., & Ricardo, P. (2013). Libro. Fundamental Cloud Architectures. Cloud Computing: Concepts, Technology & Architecture. de

<http://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/0133387526.pdf>. Pág 255 de PDF.

