PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

"SEDE ESMERALDAS"

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO:

DISEÑO DE UN PROTOTIPO CON UNA ARQUITECTURA DE RED SEGURA EN LA PUCESE.

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

LINEA DE INVESTIGACIÓN: Redes y Comunicación

AUTORA:

CINDY JOHANNA CHOEZ CALDERÓN

ASESOR:

MGT. GUSTAVO CHANGO

Esmeraldas, ABRIL 2019

Tesis de grado aprobada luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERÍA DE SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Título: Diseño de un prototipo con una arquitectura de red segura en la PUCESE.

Autora: CINDY JOHANNA CHOEZ CALDERÓN

Mgt. Gustavo Chango Sailema **f.**_____

Asesor

Mgt. Juan Casierra Cavada **f.**_____

Lector #1

Mgt. Marc Grob

Lector #2 **f.**_____

Mgt. Xavier Quiñonez Kú

Director de Escuela **f.**_____

Ing. Maritza Demera Mejía **f.**_____

Secretaria General PUCESE

ESMERALDAS, ABRIL 2019.

DECLARACIÓN DE AUENTICIDAD Y RESPONSABILIDAD

Yo, **CINDY JOHANNA CHOEZ CALDERÓN,** portadora de la cédula de identidad No. **0803584762,** confirmo que los resultados obtenidos en la investigación que presento como tesis de grado, previo a la obtención del título de **"Ingeniero de Sistemas y Computación"** son absolutamente originales, auténticos y personales.

De tal manera, declaro que todo el contenido incluyendo, los resultados, conclusiones, parte legal, académicos que se desglosan en mi investigación de tesis son y serán de mi exclusiva responsabilidad legal y académica.

CINDY JOHANNA CHOEZ CALDERON

CI: 080358476-2

CERTIFICACIÓN

Mgt. Gustavo Chango docente investigador de la PUCESE, certifica que:

La investigación realizada por **CINDY JOHANNA CHOEZ CALDERÓN** bajo el título "Diseño de un prototipo con una arquitectura de red segura en la PUCESE." reúne los requisitos de calidad, originalidad y presentación, además de haber sido incorporadas al documento final, las sugerencias dadas; en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, abril del 2019.

Mgt. Gustavo Chango

Asesor

DEDICATORIA

El presente trabajo de investigación se lo dedico a Dios, por haberme permitido cumplir con una de mis metas, por ser mi guiador e impulsador a cada momento, por darme las fuerzas para alcanzar cada uno de mis objetivos.

A mi papá Walter Choez por ser mi apoyo emocional y económicamente, por ser el mejor padre que Dios me pudo dar, por todo su cariño y afecto que me brinda en todo momento.

A mi mamá Mónica Calderón por ser mi guiadora, quien me apoya y me da ánimos, por ser una madre incondicional y haberme enseñado buenos valores, por confiar en mí.

A mis hermanas Jessenia y Vanessa, a mi hermano Jonathan gracias por poner su granito de arena, gracias a toda mi familia por su apoyo nunca los defraudare.

A mis amigos del aula, con quien compartí muchos ratos agradables y únicos, los llevare en mi corazón.

Johanna Choez

AGRADECIMIENTO

Agradezco infinitamente a Dios por ser mi guiador y darme la oportunidad de haber cumplido con esta meta.

A mi familia por ser mi pilar de apoyo a lo largo de este camino por los sacrificios que hicieron por mí, por sus ánimos, por su apoyo incondicional.

Mi agradecimiento infinito a mi asesor Mgt. Gustavo Chango por su tiempo y apoyarme en todo momento a mis lectores Mgt. Juan Casierra y Mgt. Marc Grob, gracias por sus observaciones y guía en la elaboración y culminación de mi tesis.

Mi agradecimiento especial a mi papa y hermana por apoyarme a lograr mi sueño.

Johanna Choez

RESUMEN

La presente investigación fue desarrollada con el objetivo de analizar las arquitecturas propuestas por CSIRT bajo el contexto de redes seguras y con ello presentar un prototipo para la PUCE-Esmeraldas con el propósito de mejorar la seguridad de sus redes. Para el levantamiento de información se realizó un estudio cualitativo exploratorio, que se basó en recolectar bases teóricas, antecedentes, consto de una entrevista y análisis de los datos de la infraestructura de la red.

Para obtener la información de la infraestructura se realizó una entrevista al jefe del departamento de sistemas de esta manera, se obtuvo la identificación de las posibles amenazas y dificultades. Luego se procedió analizar las arquitecturas de las bases teóricas donde se concluyó que la institución debería optar por tener una Red Segura según la propuesta de CSIRT.

El ambiente de prueba se realizó dentro de la institución PUCESE es totalmente operativo y funcional, se levantó una red con un router, se instaló el firewall Pfsense en un CPU con el sistema operativo CentOS, se le añadió 2 tarjetas de red adicional para simular las redes LAN, WAN, DMZ. La implementación de esta arquitectura ayudaría a la seguridad, confiabilidad y estabilidad aplicando las diferentes reglas de NAT, la separación DMZ, V'LANS, VPN, QOS.

Una vez concluida la investigación se pudo comprobar que contar con una buena Arquitectura de Red ayuda a que las empresas o instituciones tengan una mayor seguridad en sus redes y por lo tanto tenga mayor confiabilidad en sus datos.

Palabras Claves: Arquitecturas, Red, Seguridad, CSIRT.

ABSTRACT

This research was developed with the aim of analyzing the architectures proposed by CSIRT under the context of secure networks and with it present a prototype for the PUCE-Esmeraldas in order to improve the security of their networks. An exploratory qualitative study was carried out to collect information, which was based on collecting theoretical bases, antecedents, an interview and analysis of the network infrastructure data.

In order to obtain information on the infrastructure, an interview was conducted with the head of the systems department in order to identify possible threats and difficulties. Then we proceeded to analyze the architectures of the theoretical bases where it was concluded that the institution should choose to have a Secure Network according to the CSIRT proposal.

The test environment was performed within the institution PUCESE is fully operational and functional, a network was built with a router, the Pfsense firewall was installed in a CPU with the CentOS operating system, 2 additional network cards were added to simulate LAN, WAN, DMZ networks. The implementation of this architecture would help security, reliability and stability by applying the different rules of NAT, DMZ separation, V'LANS, VPN, QOS.

Once the investigation was concluded, it was proved that having a good Network Architecture helps companies or institutions to have a greater security in their networks and therefore have greater reliability in their data.

Keywords: Architecture, Network, Security, CSIRT.

ÍNDICE DE CONTENIDOS

TRIBUNAL DE GRADUACIÓN i
DECLARACIÓN DE AUENTICIDAD Y RESPONSABILIDAD ii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN vi
ABSTRACT vii
ÍNDICE DE CONTENIDOS viii
ÍNDICE DE ILUSTRACIONES x
ÍNDICE DE TABLAS xi
ÍNDICE DE ANEXOS xi
GLOSARIO DE TÉRMINOS xii
INTRODUCCIÓN 1
Presentación del tema 1
Planteamiento del Problema 1
Justificación 2
Objetivos 3
Objetivo General: 3
Objetivos Específicos: 3
CAPÍTULO I: MARCO TEÓRICO 4
1.1. Bases teórico-científicas 4
1.1.1. Redes LAN 4
1.1.2. Seguridades para Redes. 4
1.1.2.2. Zona DMZ (Zona Desmilitarizada) 7
1.1.3. Balanceo de Cargas. 10
1.1.4. QOS “Calidad de Servicios” 10
1.1.5. Hardening 11
1.1.6. Arquitectura de Redes 12
1.2. Antecedentes 20
1.3. Marco Legal 24

CAPITULO II: MATERIALES Y MÉTODOS 25
2.1. Área de Estudio 25
2.2. Tipo de Estudio 25
2.3. Métodos 25
2.4. Técnicas e instrumentos 26
2.5. Análisis de Datos 26
CAPÍTULO III: RESULTADOS 28
3.1. Análisis de la Infraestructura de Red de la Institución 28
3.2. Análisis General de la Infraestructura de la institución 28
3.3. Propuesta 29
3.3.1. Análisis e interpretación del prototipo de Arquitectura de Red 29
3.3.2. Características de la solución de la Red Segura 30
3.3.3. Descripción General 31
3.3.4. Ambiente de prueba para la propuesta 32
3.4. Criterio General 38
CAPÍTULO IV: DISCUSIÓN 39
CAPÍTULO V: CONCLUSIONES 40
CAPÍTULO VI: RECOMENDACIONES 41
REFERENCIAS 42
ANEXOS 44

ÍNDICE DE ILUSTRACIONES

Ilustración 1. Tipo de Red LAN. 4
Ilustración 2. Diseño Red Básica Segura 13
Ilustración 3. Diseño de Red Segura Redundante. 14
Ilustración 4. Diseño Red Segura Segmentada y Redundante 16
Ilustración 5. Diseño Red Básica Segura Separada de la Organización 18
Ilustración 6. Arquitectura Básica de la Red. 21
Ilustración 7. Topología de Prueba 23
Ilustración 8. Infraestructura de la PUCESE. 28
Ilustración 9. Modelo de Arquitectura de Red Segura propuesta por CSIRT 30
Ilustración 10. Propuesta de la Infraestructura. 31
Ilustración 11. Ambiente de Prueba de Arquitectura de Red. 32
Ilustración 12. Ingreso al Servidor PfSense. 33
Ilustración 13. Interfaz / WAN. 33
Ilustración 14. Interfaz / Configuración WAN 34
Ilustración 15. Interfaz / LAN 34
Ilustración 16. Interfaz / Configuración LAN 35
Ilustración 17. Interfaz / DMZ 35
Ilustración 18. Interfaz /Configuración DMZ 36
Ilustración 19. Interfaces (LAN, WAN, DMZ) 36
Ilustración 20. Reglas de LAN. 37
Ilustración 21. Reglas DMZ 37
Ilustración 22. Probar acceso a Internet 38

ÍNDICE DE TABLAS

Tabla 1. Tabla Comparativa OPNsense y Pfsense 6
Tabla 2. Parámetros de QOS. 11
Tabla 3. Calidad QOS 11
Tabla 4. Características Red Básica Segura 14
Tabla 5. Características Red Básica Segura Redundante 15
Tabla 6. Características Red Básica Segura Segmentada y Redundante. 17
Tabla 7. Características Red Básica Segura separada por la organización 19
Tabla 8. Cuadro comparativo de los tipos de Arquitecturas propuestas por CSIRT. 19
Tabla 9. Definiciones, abreviaturas 30
Tabla 10. Características del Ambiente de Pruebas. 32

ÍNDICE DE ANEXOS

Anexo 1.Entrevista al jefe del departamento de TIC'S de la PUCESE. 44
Anexo 2. Código para configuración Hardening. 46

GLOSARIO DE TÉRMINOS

CSRIT: Equipo de Respuestas ante Incidencias de Seguridad Informáticas.

LAN: Red de área local.

VPN: Red privada virtual.

VLAN: Red de área local virtual.

DMZ: Zona Desmilitarizada.

QOS: Calidad de servicios.

INTRODUCCIÓN

Presentación del tema

La presente investigación se centra en el análisis y diseño de un prototipo con una infraestructura tecnológica basándose en una arquitectura y diseño de redes, proponiendo un prototipo en la PUCE Esmeraldas, que le permita a la institución contar con una red segura para toda su infraestructura.

Se debe mencionar que las características principales de una arquitectura segura para una empresa o institución se basan en la infraestructura, seguridad, confiablidad, estabilidad, disponibilidad y velocidad de la red.

Para analizar esta problemática fue necesario definir los requerimientos principales para previamente elegir la arquitectura a proponer para la institución.

Planteamiento del Problema

Es muy común en una empresa o institución encontrar inconvenientes en la infraestructura de sus redes, la Pontificia Universidad Católica del Ecuador "Sede Esmeraldas" ha intentado mejorar la Arquitectura de sus redes, el balanceo de cargas y la seguridad de acceso a sus servidores. Sin embargo, en los últimos años se ha incrementado varios equipos de alta tecnología para el departamento de redes y así poder solventar la problemática, pero no se ha podido implementar una infraestructura basada en una arquitectura segura que conlleve todos los requerimientos de seguridad, confiabilidad, rendimiento y esto ha llevado a consecuencias negativas para la gestión de servicios (autoridades, docentes y estudiantes), el no disponer de red segura, confiable que se adapte los requerimientos institucionales.

Según estudios realizados en el informe Anual de la seguridad de Cisco en el año 2016 que resumen errores en actualizaciones sobre vectores y métodos de ataques web, vulnerabilidades, amenazas, el masivo crecimiento el uso de cifrado y riesgos de seguridad en donde un (91,3%) utiliza DNS para llevar a cabo sus campañas maliciosas, a consecuencia de ello las empresas o instituciones se ven afectadas directamente por el robo de información y también otro problema de suma importancia es la pésima

distribución de cargas de datos dentro de sus redes y la falta de firewalls que impiden tener una red que cumpla con todos los requisitos de seguridad y rendimiento de sus redes.

Para ello fue preciso levantar información cualitativa respecto al tipo de arquitectura de redes informáticas necesarios para un buen funcionamiento de los equipos tecnológicos dentro de la institución.

Por esto resulta importante implementar una arquitectura de red básica segura según las recomendaciones de CSIRT, que contenga una arquitectura de red optima, además que tenga firewalls de seguridad para el acceso a la infraestructura, zona desmilitarizada (DMZ). Para que una arquitectura de redes sea optima, rápida y eficaz debe tener una regla de balanceo de carga de datos en cuanto no se esté utilizando en fragmento nada de los datos pasen automáticamente estos datos a el otro fragmento.

Justificación

La presente investigación tuvo como objetivo la propuesta de un prototipo de una arquitectura de red segura según las recomendaciones de CSIRT, la utilización de VPN, firewalls de seguridad y balanceo de cargas.

En una empresa o institución una de las características fundamentales con la que debe contar es con una infraestructura de red segura con VPN, por ello es importante investigar, definir y plantear una arquitectura de red que permita tener una red segura.

Partiendo de esta idea, a través de esta investigación se diseñó una arquitectura de red, que permita que los empleados de la institución puedan tener acceso desde sus hogares a la red privada de su trabajo, además de ello obtener una red con balanceo de cargas, que contengan todas las seguridades de firewalls.

Diseñando este prototipo de arquitectura de red segura permitirá a la institución tener mejor servicio mediante la segmentación de la red, estudiantes y personal satisfechos, además de ello contará con una seguridad en la información interna de la institución que se encuentra alojada en los servidores. Esta arquitectura de red tendrá como beneficiarios directos a los docentes, estudiantes y administrativos de la PUCESE.

Objetivos

Objetivo General:

- Diseñar un prototipo con una infraestructura de Red Segura para la PUCESE.

Objetivos Específicos:

- Comparar los diferentes tipos de Arquitecturas de Redes Seguras propuestas por CSIRT.
- Identificar que Infraestructura de Red tiene la PUCESE.
- Proponer la infraestructura seleccionada a la Pontificia Universidad Católica Del Ecuador Sede Esmeraldas.

CAPÍTULO I: MARCO TEÓRICO

1.1. Bases teórico-científicas

1.1.1. Redes LAN

Local Área Network son redes que se conectan en un área pequeña, se pueden conectar redes entre sí permitiendo que los usuarios envíen y reciban archivos[1].

Estas son redes de áreas locales que conectan computadoras de una zona relativamente pequeña, las redes LAN se limita a un área especial relativamente pequeña no muy extensa, tales como puede ser un hogar o una organización. Estas redes se pueden conectar entre ellas a través de líneas telefónicas, ondas de radio, satélites, fibra óptica entre otras. Las estaciones de trabajo y los ordenadores personales en oficinas normalmente están conectados en una red LAN, lo que permite que los usuarios envíen o reciban archivos y compartan el acceso a los archivos y a los datos[2].

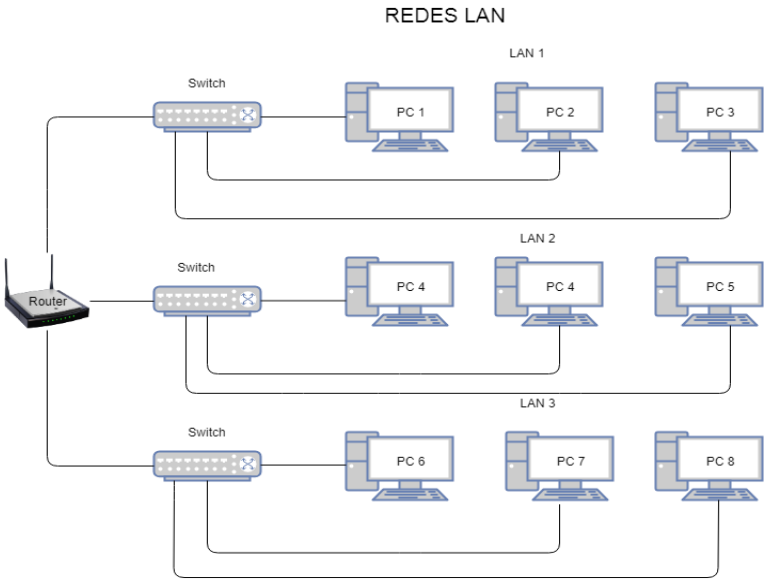


Ilustración 1. Tipo de Red LAN.

1.1.2. Seguridades para Redes.

1.1.2.1. Firewalls

Son aplicaciones o dispositivos diseñados para bloquear comunicaciones no autorizadas y permitiendo a los que si están autorizados para realizar las configuraciones, para ello se deben seguir normas o reglas, mediante este mecanismo se puede tener una seguridad alta en la infraestructura de la red[3].

Los firewalls se encuentra en la puerta de enlace entre las dos redes por general una red privada y una pública, se puede tener varios firewalls en una red privada de esta manera se tiene una mayor seguridad en la red, existen varios tipos de filtrados como son, filtro de direcciones, los cortafuegos pueden filtrar paquetes en función de su origen, destino o número de puerto[4].

Se pueden clasificar de acuerdo con el tipo de información que filtran. Puede ser un ruteador comercial con capacidad de filtración de paquetes. En este caso el firewall examina el encabezado de los paquetes que van hacia afuera o vienen entrando a la red privada. Las reglas de este firewall permiten dejar pasar el paquete o descartarlo. Las reglas se fijan en función de las direcciones, protocolos en la capa superior, y puertos, básicamente. Otro tipo de firewall se conoce como proxy a nivel circuito. Este firewall establece una conexión a nivel IP, entre un cliente en una interfaz y un DMZ Red Internet servidor en otra interfaz, no analiza los protocolos de la capa superior; la conexión segura es conocida como circuito. Se le considera proxy, pues es el intermediario entre el cliente y el servidor[5].

Dentro de los firewalls se pueden permitir o denegar el acceso a ciertos tráficos de la red entre ellos están el: Ping, DNS, HTTP, HTTPS, entre otros a esto se lo denomina protocolo de filtrados, se debe tomar em cuenta que los firewalls dan seguridad dentro de la red rechazando acceso de redes no autorizadas, pero no pueden dar seguridad al mal uso de las redes de los empleados de una institución o empresa.

Existen diferentes tipos de plataformas de firewalls de código abierto entre los más usados por las empresas están OPNsense y Pfsense

PfSense es una plataforma FreeBSD personalizada y gratuita, distribución adaptada para ser utilizada como cortafuegos y como enrutador a través del sitio web. Además de ser potente y flexible. Incluye una larga lista de características y un sistema de administración de paquetes que le permite instalar características adicionales[6].

OPNsense es una plataforma de enrutamiento y cortafuegos basada en FreeBSD de código abierto. OPNsense está diseñado para ser fácil de usar y fácil de construir para reemplazar a pfSense. Es rico en características y ofrece características gratuitas que cuestan a los competidores, tienen actualizaciones de seguridad semanales para combatir cualquier amenaza emergente[6].

Tabla 1. *Tabla Comparativa OPNsense y Pfsense [7].*

Tabla Comparativa

Características	**OPNsense®**	**pfSense®**
Cortafuegos	Inspección de estado	Inspección de estado
Fecha de Creación	2015	2004
Interfaz gráfica basada en web	Bootstrap basado en Phalcon PHP Framework	* De 2.3 migrado a Bootstrap
Asistente de configuración de instalación	Sí	Sí
Panel configurable	Sí	Sí
Compatibilidad con IPv4 e IPv6	Sí	Sí
Punto de acceso inalámbrico	Sí	Sí
Soporte de cliente inalámbrico	Sí	Sí
Configurar y filtrar / aislar múltiples	-	Sí
Interfaces (LAN] DMZ] etc.)	Sí	Sí
Conformación de tráfico	Sí	Sí
Controles de la tabla de estado	Sí	Sí
NAT	Sí	Sí
Redundancia / Alta disponibilidad	Sí	Sí
Soporte Multi-WAN	Sí	Sí
Equilibrio de carga de entrada del servidor	Sí (configuración del servidor virtual)	Sí
Utilidades de diagnóstico de red	Vea abajo	Vea abajo
[silbido]	Sí	Sí
[traceroute]	Sí	Sí
[pruebas de puerto a través de la GUI]	Sí	más con paquetes] como nmap
VPN		
[IPsec (incluyendo NAT de fase 2)]	Sí	Sí
[OpenVPN]	Sí	Sí
[L2TP]	Sí (plugin de tramite)	Si (paquete de tramite)
[PPPoE]	Sí (plugin de tramite)	Si (paquete de tramite)
[PPTP]	Sí (Non considerata sicura)	No (Tolta perché non sicura)
Gráficos RRD	No (Salud del sistema)	Sí
Gráficos de tráfico de interfaz en tiempo real	Sí	Sí
DNS Dinámico	Sí	Sí
Portal cautivo	Sí	Sí
Servidor y relé DHCP (IPv4 e IPv6)	Sí	Sí
Acceso a la línea de comandos	Sí	Sí
Activación de la LAN	Sí	Sí

Construido en la captura de paquetes / sniffer	Sí	Sí
Copia de seguridad y restaurar la configuración fw	Sí	Sí
Editar archivos a través de la web GUI	Sí	Sí
Interfaces virtuales para:		
[VLAN]	Sí	Sí
[LAGG / LACP]	Si no	Sí Sí
[GIF]	Sí	Sí
[GRE]	Sí	Sí
[PPPoE / PPTP / L2TP / PPP WANs]	Si si SI SI	Si si SI SI
[QinQ] y puentes]	Sí	Sí
Caching DNS Forwarder / Resolver	Sí	Sí
Se puede ejecutar en muchos entornos de virtualización.	Sí	Sí
Servidor proxy	Sí	usando paquetes
IPS	Sí	SNORT (PAQUETE EXTRA)
IDS	Sí	SNORT (PAQUETE EXTRA)
Actualización de seguridad	Si semanal	Sí, con la versión de corrección de parche
Software de raid	Sí apoyado extraoficialmente	Sí totalmente compatible

La presente tabla identifica las características de OPNsense y Pfsense como se puede observar los dos firewalls tienen las mismas funciones la única diferencia radica en que Pfsense se creó desde el 2004 y por tanto tiene más documentación en la web, pero los dos brindan seguridad y confiabilidad en las redes.

Entre los firewalls pagados están **Palo Alto** es un competidor sólido para todas las empresas, especialmente cuando las evaluaciones dan más peso a la característica y calidad de gestión que al precio, **Forcepoint** ha demostrado constantemente una buena calidad de las características, inteligencia y la capacidad de tunelizar el tráfico web a la nube, **Fortinet** es un buen candidato para la lista final de todos los firewalls empresariales, especialmente cuando la relación precio/rendimiento es alta en la evaluación[8].

1.1.2.2. Zona DMZ (Zona Desmilitarizada)

Este es el proceso de establecer un segmento de red semi segura que es divida en una red externa y una interna que permite que estas conexiones sean permitidas[9].

La zona desmilitarizada sirven para asegurar la separación de la red de la empresa, esta es la separación entre el nivel de seguridad 0 a 3 y el nivel 4 a 5. Esta separación es necesaria según estándar IACS (Industrial Automation and Control System) y las mejores prácticas para aprovechar la disponibilidad y la seguridad que se consideran requisitos críticos para el giro de negocio de la empresa[10].

Los DMZ tienen unas características esenciales que se deben tomar en cuenta para su implementación:

- Todo usuario antes de acceder a los servicios dentro de red previamente debe identificarse.
- Brindan soporte y seguridad en la administración de la red.
- Realizan un análisis y control del flujo de tráfico que hay en las redes.
- Realizan una inspección de los paquetes con estado y detección.

Los DMZ se implementan en la infraestructura de la red con el fin de brindar seguridad dentro de la red LAN obteniendo con ello que un usuario que este fuera de la red puedan ingresar solo cuando esta red este protegido por los firewalls con los que cuenta la red básica segura. Para la implementación se debe tener equipos específicos para la conexión de los servidores DMZ. Estos tienen dos categorizaciones:

- Servicios Tradicionales. – Estos son exclusivos para los servidores que intercambian información delicada de los clientes.
- Servicios No Tradicionales. - Aquí se encuentran los servidores que brindan un servicio dirigido para el internet.

Propósitos de los DMZ

Tienen como propósito brindar una red confiable en donde se pueden configurar para mejorar la seguridad de la red se utilizan para pruebas o entornos de laboratorio o para redes de invitados. En cuanto a la seguridad, una DMZ se considera una red semi-confiable porque no es totalmente abierto ya que habrá seguridad de red y recursos. Dejar una DMZ abierta es solo pidiendo problemas. Una DMZ puede albergar varios recursos diferentes que los usuarios públicos y usuario de red confiable tendrá acceso a. Estos pueden incluir web, correo electrónico, FTP, DNS, VoIP, VPN y servidores Proxy. En realidad, todo se reduce a qué servicios quiere colocar una organización en esta área basada en la seguridad. Dicho esto, una DMZ también se puede usar para separar recursos específicos o sistemas dentro de la red confiable. Entonces, ¿por qué uno necesita una DMZ? Una DMZ se convierte en barrera de primera línea entre el mundo exterior y sus recursos vitales. éste es uno de componentes es la configuración de un principio de defensa en profundidad mediante la separación de lo externo del interno. Por supuesto, uno también necesita entender que la separación entra en riesgo en actuación. El tráfico

ahora tiene que moverse a través de múltiples componentes como firewalls. El nivel de degradación depende del diseño de la DMZ[9].

1.1.2.3. VLAN´S

Facilitan la administración y configuración dentro de la infraestructura de la institución, permiten que los cambios que se realizan en un dispositivo se propaguen automáticamente a todos los demás Switches conectados al mismo dominio.

Ventajas de utilizar VLAN:

- Seguridad: Los grupos de trabajo que tengan datos sensibles se separaran del resto de la red, y con ello disminuir la posibilidad de ocurran violaciones de la información confidencial.
- Mejor rendimiento: Divide la red en múltiples grupos lógicos de trabajo, esto ayuda a reducir el tráfico innecesario incrementando el rendimiento de esta.
- Migración: El cambio de los dispositivos a la nueva arquitectura es facilitada por la división de la red en las VLAN.
- Administración: Esto facilita al personal de TI

1.1.2.4. VPN

Red Privada Virtual es una tecnología que permite la extensión de una red pública como Internet a un espacio de red local[11]. Son una tecnología o herramienta utilizada para conectar una o más computadoras a una red privada de una empresa o institución con el fin de que los trabajadores tengan acceso a esta red desde sus hogares.

Al implementar VPN, existen cuatro aspectos fundamentales: el costo, desempeño, confianza y seguridad que es uno de los aspectos más relevantes, no importa que tan barata, rápida y confiable sea una red, sino tiene una seguridad adecuada ya que los riegos serían más que los beneficios que esta brinde. Los VPN ofrecen encriptación y encapsulación de datos de manera que hace que viajen codificados y a través de un túnel[12].

Tipos de VPN

A continuación, se detallarán tres tipos de VPN (Host a Host, Host a Red, Red a Red):

- **VPN Host a Host**

Este tipo de red se la implementa cuando se desea conectar oficinas remotas desde una Sede a la oficina Central de la organización, las VPN tiene un vínculo a internet

permanente, que acepta conexiones vía internet proveniente de los sitios y establece un túnel, los servidores de las sucursales se conectan a internet utilizando los servicios de su proveedor local de Internet[12].

- **VPN de Host a Red (Roadwarrier)**

También denominadas Red Privada Virtual de Marcación (Virtual Prívate Dial-up Network).Este tipo de VPN consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos ya sea desde sus domicilios o cualquier parte del mundo que estos se encuentren, utilizando el internet como vinculo de acceso, una vez que sean autenticados tienen un nivel de acceso similar al que tienen en la red local de la empresa[12].

- **VPN de Red a Red**

Este esquema es el menos difundido, pero es uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar internet como medio de conexión, emplea la misma red LAN de la empresa, además de ellos sirve para aislar zonas de servicios de la red interna[12].

1.1.3. Balanceo de Cargas.

En informática el balanceo de carga se refiere a la técnica usada para compartir el trabajo que se va a realizar en diferentes procesos con varios computadores, discos duros y otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles. El balanceo de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella[13].

1.1.4. QOS "Calidad de Servicios"

La seguridad QOS mide la confiabilidad y mecanismos de seguridad implementados, colabora en la autenticación de los principales servicios, se puede implementar la autorización para que ciertas personas tenga acceso a dicho servicio, confiabilidad, responsabilidad, trazabilidad[14].

Parámetros de la Calidad de Servicios

Tabla 2. *Parámetros de QOS[15].*

Parámetros de Calidad de Servicios	
Rendimiento	Indica cuantos datos son transmitidos por la red.
Retardo	Indica el tiempo que dura en transmitirse un bit enviado desde su origen hasta su destino.
Variación de retardo de transmisión	Es la variación percibida entre dos retardos continuos durante el procesamiento de datos y transmisión
Perdida de paquetes o fiabilidad	Indica que paquetes transmitidos de extremo a extremo no alcanzan su destino
Ancho de banda	El transporte de información a través de un canal de comunicación

Toda Calidad de servicios debe contar con los 5 parámetros establecidos (Rendimiento, Retardo, Variación de retardo de transmisión, Perdida de paquetes o fiabilidad, Ancho de banda) que indican el tiempo de entrada y llegada de la información de los datos.

Tabla 3. *Calidad QOS [16].*

Calidad de Servicios	
Funciones QOS	Soportar el Ancho de banda dedicado. Mejora de las características de pérdida. Cómo evitar y administrar la congestión de la red. Formar el tráfico de la red. Configuración de prioridades de tráfico en la red.

En la tabla anterior se mencionan las funciones que realizan los QOS entre la función más importante que realizan es administrar la red para evitar congestiones en la misma.

1.1.5. Hardening

Es el proceso de asegurar un sistema por medio de la reducción de vulnerabilidades aquí se evalúan servicios, software y accesos innecesarios dentro de la red. Todo empresa tiene información confidencial que debería estar estrictamente protegido y asegurado usando técnicas, normas y documentación necesaria basada en seguridades de la información[17].

1.1.6. Arquitectura de Redes

Es el diseño de una red de comunicaciones, que se encargan de especificar los componentes físicos en una red, su configuración y funcionalidad de sus procedimientos[3].

Estas arquitecturas se encargan de elaborar un plan para desarrollar e implementar una red siguiendo unos protocolos para luego interconectarlas entre sí. Las redes deben admitir una amplia variedad de aplicaciones y servicios, como así también funcionar con diferentes tipos de infraestructuras físicas. El término arquitectura de red, en este contexto, se refiere a las tecnologías que admiten la infraestructura y a los servicios y protocolos programados que pueden trasladar los mensajes en toda esa infraestructura. Debido a que el Internet evoluciona, al igual que las redes en general, descubrimos que existen cuatro características básicas que la arquitectura subyacente necesita para cumplir con las expectativas de los usuarios: tolerancia a fallas, escalabilidad, calidad del servicio y seguridad[18].

Segmentación de Redes

Dentro de una red básica segura debe de estar implementada una segmentación que separe las redes en subredes y con ello incrementar el número de pc que van a estar conectados a la red, aumentado con ello la rapidez y el rendimiento del internet. La Segmentación es la opción más segura de contar con dos redes diferentes físicamente separadas para las tareas de respaldo y recuperación de información, para ellos es necesario contar con más de una tarjeta NIC en cada computador y en los servidores a utilizar[19].

CSIRT "Equipo de respuesta a incidentes de seguridad de la información"[20].

A continuación, se estudiarán cuatro tipos de arquitecturas y diseño de redes según lo propone CSIRT de las cuales se analizará cada una de ella y se verificará cual será la mejor arquitectura según los requerimientos de la institución para poder ser implementada en la misma:

1.1.6.1. Arquitectura de Red Básica Segura

Una red básica segura parte de un modelo de arquitectura de red separada por zonas, se recomienda dividir la red en el número de segmentos de red necesarios para poder diferenciar y dotar de las medidas de seguridad y control de tráfico apropiados para cada uno de ellos. Esta separación es un concepto efectivo y esencial en la planificación de

cualquier arquitectura de red e igualmente aplicable en Sistemas de Control Industrial. Este tipo de diseño, unido a controles de flujo de datos adecuados entre los dominios definidos, minimizará el daño producido por el posible compromiso de un dispositivo de un dominio determinado[21].

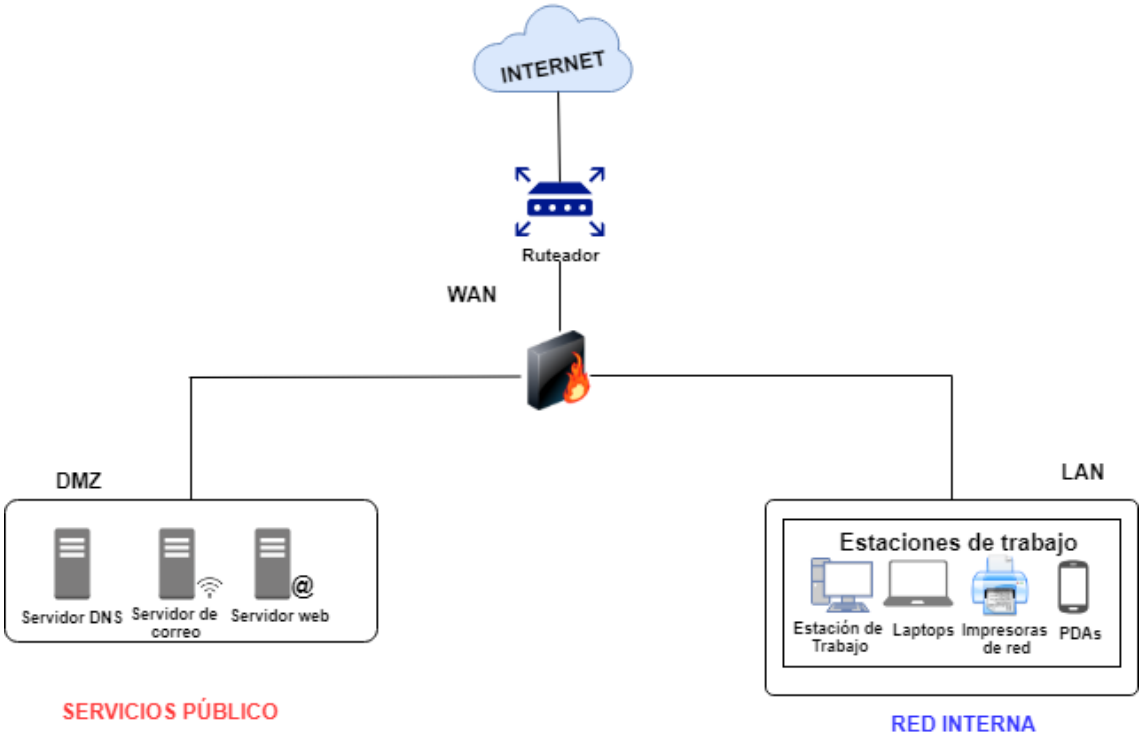


Ilustración 2. *Diseño Red Básica Segura* [22].

En la ilustración anterior puede observarse, la arquitectura de una red básica segura en donde está el internet de cualquier proveedor que tenga la institución o empresa, un router y a continuación de esta tiene un firewall de seguridad que está en la división de dos segmentos el de la parte derecha están la red LAN de todas las estaciones de trabajo (PC, Impresoras, Celulares, Laptops) y del lado izquierdo se encuentran los servidores como (Servidor DNS Servidor de correo y Servidor Web).

Tabla 4. *Características Red Básica Segura* [22]**.**

Red Básica Segura	
Detalles	**Descripción**
Características	• Esquema para brindar reactivos • No posee redundancia de servidores • Cuenta con dos segmentos básicos de red administrados por un firewall
Software	• Tiene acceso a internet mínimo de 2Mbps • Se puede utilizar cualquier software libre

En la Tabla 4. Se detallan las características principales que debe tener una Red Básica Segura que debería estar separada en dos segmentos protegida por un firewall según CSIRT.

1.1.6.2. Arquitectura de Red Segura Redundante

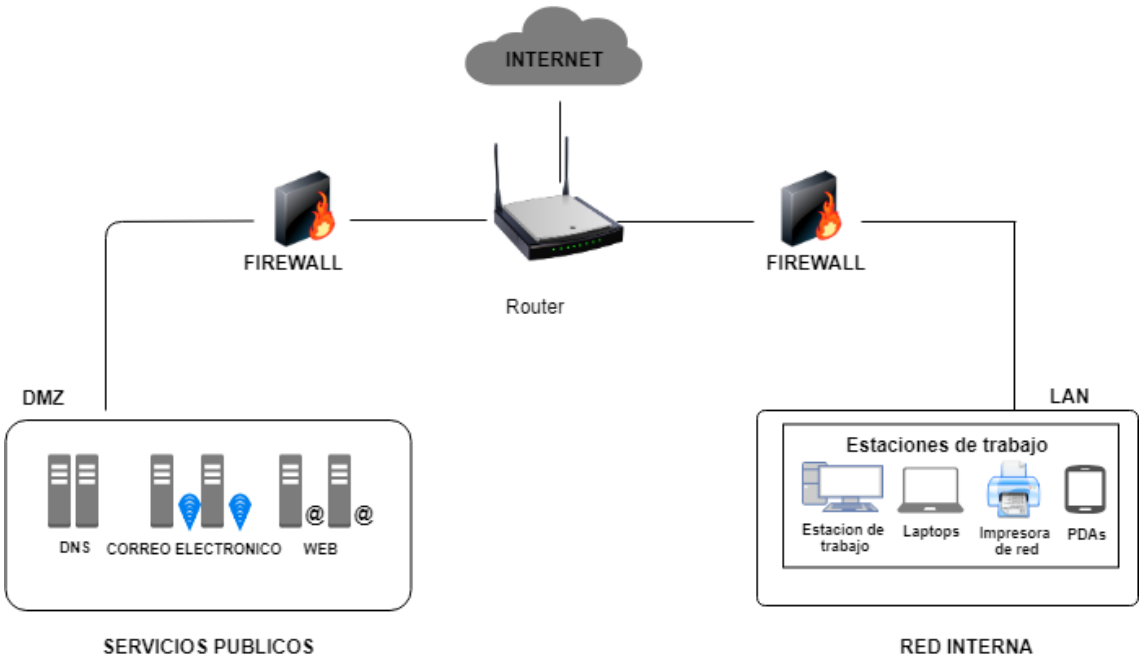


Ilustración 3. *Diseño de Red Segura Redundante*[22].

En la ilustración anterior puede observarse, la conexión de una red segura redundante que está divida en dos segmentos, el primer segmento de la parte derecha cuenta con un firewall y la red interna donde se encuentra las estaciones de trabajo (PC, Impresoras, etc.) y los servidores (Base de datos, Dominio, Aplicaciones entre otros) y en la parte

izquierda tiene firewall de seguridad para bloquear conexiones no autorizadas a la red, tiene un DMZ (DNS, Correos, WEB)

Las redes Segura Redundante tienen las siguientes características que se detallan en la siguiente tabla:

Tabla 5. *Características Red Básica Segura Redundante*[22]**.**

Red Básica Segura Redundante

Detalles	**Descripción**
Características	• Esquema para brindar reactivos • Tiene redundancia de servidores • Tiene dos Firewalls
Software	• Cuenta con dos segmentos básicos de red regulados por un firewall • Tiene acceso a internet mínimo de 2Mbps • Se puede utilizar cualquier software libre

En la Tabla 5. Se detallan las características principales, que debe tener una Red Básica Segura Redundante que se caracteriza por estar separada en dos segmente protegida por dos firewalls según CSIRT.

1.1.6.3. Arquitectura de Red Segura Segmentada y Redundante

Las redes seguras segmentadas se separaron de manera lógica los servicios, tanto como base de datos, aplicativos y usuarios, considerando en distintos segmentos cada uno de estos servicios, obteniendo una mejor administración y una rápida detección de posibles problemas sin comprometer toda la red, como es el caso en una red plana, la distribución de los servicios. Esta red tiene mayor fortaleza en la redundancia y la alta disponibilidad[23].

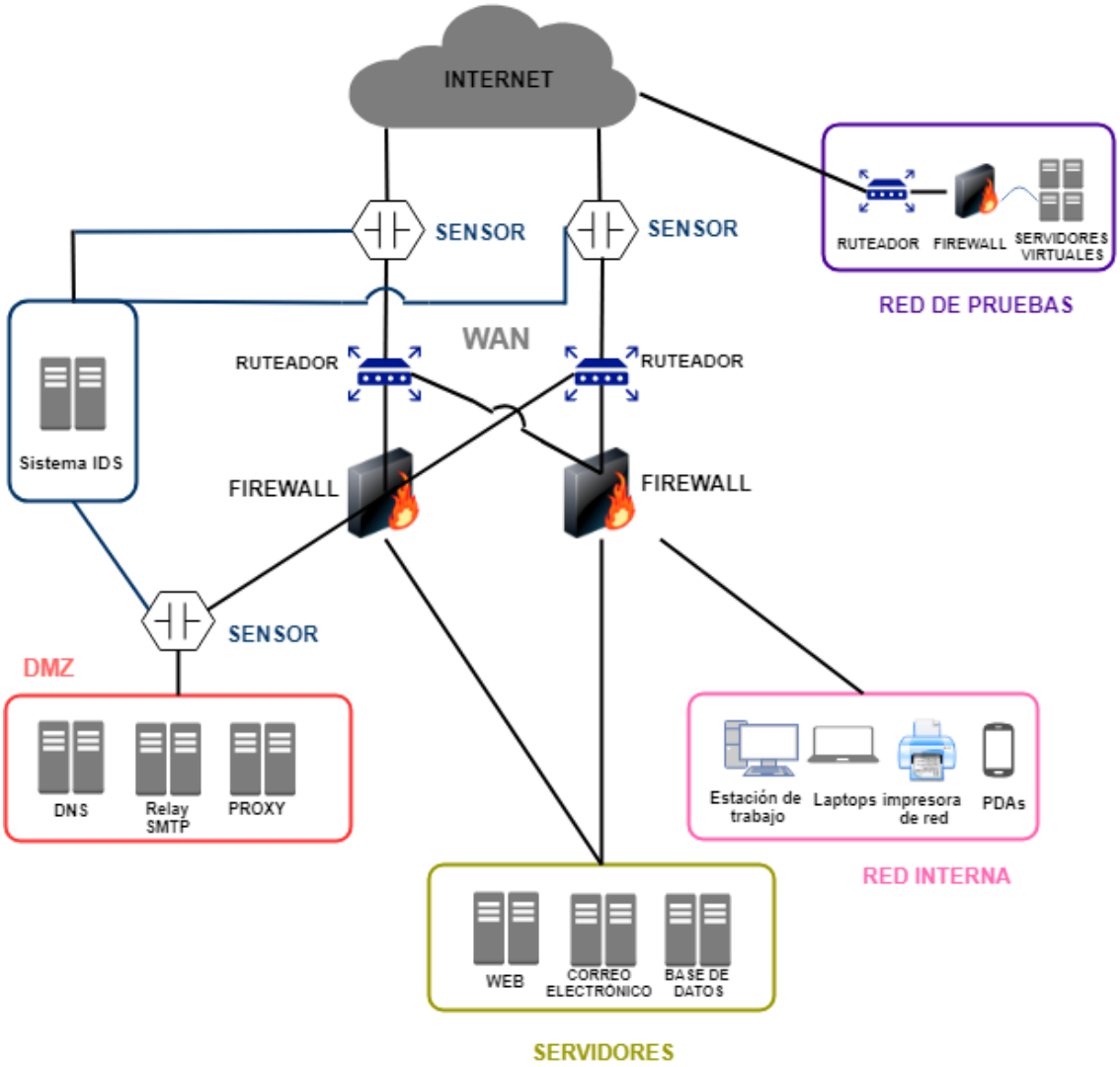


Ilustración 4. *Diseño Red Segura Segmentada y Redundante* [22].

En la ilustración anterior puede observarse, una Red segura segmentada y redundante que está compuesta por el internet de cualquier proveedor que tenga una institución, está separada en 5 segmentos el primero es una red de pruebas cuenta con un router seguido de un firewall que contiene servidores virtuales para las pruebas , luego viene los 4 segmentos que están compuestos por dos sensores, dos firewalls, hay un segmento de los sistemas IDS, otro de los DMZ (DNS, PROXY, SMTP) , los servidores(WEB, Correo, y la base de datos) y el ultimo segmentos es la red interna de la institución (PC, Laptops, Impresoras, Celulares).

Tabla 6. *Características Red Básica Segura Segmentada y Redundante*[22]**.**

Red Básica Segura Segmentada y Redundante

Detalles	**Descripción**
Características	• Esquema para brindar reactivos y proactivos. • Posee sensores y servidor con un Sistema Detección de Intrusos (IDS) • Tiene redundancia en sus servidores • Tiene dos Firewalls • Tiene enlaces redundantes a Internet • Alta disponibilidad en sus servicios • Cuenta con tres segmentos de Red para los servicios de la Organización.
Características para ser implementada en un Laboratorio	• Tiene acceso entre segmentos regulados para varios firewalls. • Acceso al internet • Enlace principal de 8 Mbps • Enlace secundario para pruebas a 2 Mbps
Software	• Se puede utilizar cualquier software libre

En la Tabla 6. Se muestran las características principales, que debe tener un Arquitectura de un Red Segura Segmentada y Redundante que se caracteriza por estar separada en tres segmentos protegida por dos firewalls.

1.1.6.4. Arquitectura de Red Segura Segmentada separada de la Organización

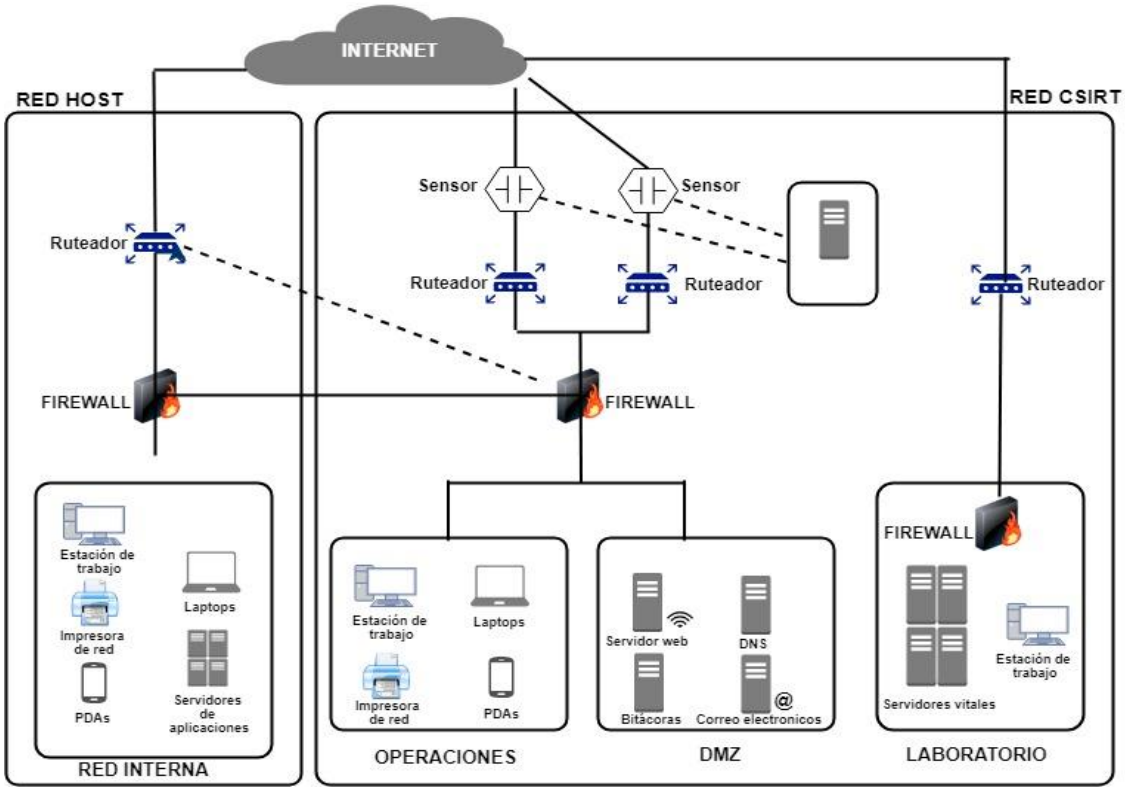


Ilustración 5. *Diseño Red Básica Segura Separada de la Organización* [22]

En la ilustración anterior puede observarse, una Red básica segura separada de la Organización que cuenta con el internet de cualquier proveedor con que cuente la institución está dividida en dos red la primera es de Host tiene un router un firewall y una red interna que está compuesta por (PC, Impresoras, Laptops, Celulares, Servidores de aplicaciones) la segunda red de CSIRT tiene dos sensores, tres router, y dos firewall, tiene tres segmentos el primero de operaciones(Pc, Laptops, Impresoras, Celulares), la segunda de los DMZ(Servidor web, DNZ, Bitácoras, Correos) y la tercera compuesta por el Laboratorio(Servidores Virtuales, Firewall, PC).

Tabla 7. *Características Red Básica Segura separada por la organización*[22]**.**

Red Básica Segura Segmentada separada por la organización

Detalles	**Descripción**
Características	• Esquema para brindar servicios reactivos y proactivos • Tiene 3 Firewalls • Separación física de red CSIRT y de la organización
Características para ser implementada en un Laboratorio	• Enlaces para el acceso al Internet redundantes para la red CSIRT • Tiene servidores y sensores con sistema de Detección de Intrusos • Red aislada para pruebas en el laboratorio • Cuenta con tres redes diferentes • Segura en el acceso interno regulado por los firewalls • Acceso a internet: Enlace de la Organización 2 Mbps, Enlace de redundancias CSIRT 4 Mbps, Enlaces para la red del laboratorio 2 Mbps
Software	• Se puede utilizar cualquier software libre

En la Tabla 7. Se muestran las características principales, que debe tener un Arquitectura de un Red Segura Segmentada separada por la organización que es la red más segura y por las características que tiene su implementación es de un alto costo está compuesta por tres firewalls y separa física de la red y otra la organización.

Tabla 8. *Cuadro comparativo de los tipos de Arquitecturas propuestas por CSIRT.*

	Ventajas	**Desventajas**
Arquitectura de Red Segura	Brinda Reactivos Fácil de Implementar Bajo costo de implementación	No posee redundancia de Servidores
Arquitectura de Red Segura Redundante	Brinda Reactivos Tiene Redundancia en sus servidores Bajo costo de implementación Fácil de Implementar	No posee proactivos
Arquitectura de Red Segura Segmentada y Redundante	Brinda Reactivos y proactivos Tiene Redundancia en sus servidores Tiene sistema de detección de intrusos Alta disponibilidad en sus servicios	Costo Alto de Implementación Dificulta en la implementación

Arquitectura de Red Segura Segmentada separada de la Organización	Brinda Reactivos y proactivos Tiene Redundancia en sus servidores Tiene sistema de detección de intrusos Alta disponibilidad en sus servicios Separación CSIRT y de la organización	Costo Alto de Implementación Dificultad en la implementación

En la Tabla 8. Se muestran un cuadro comparativo de los tipos de Arquitecturas propuestas por CSIRT la más segura es la Arquitectura de Red Segura Segmentada separada por la organización, pero es de alto costo, si una empresa o institución no cuenta con los recursos debería tener implementa la Red Segura que brinda una seguridad comprobada a un bajo costo de implementación.

1.2. Antecedentes

Las empresas e instituciones deben actualizarse a medida que la tecnología avanza, específicamente los departamentos de Tecnología de la Información. TI son el conjunto de tecnologías que permiten la manipulación de datos, producción, acceso de la comunicación telecomunicación de la información presentada del análisis [24].

La institución actualmente se está actualizando con una infraestructura de red segura para tener un respaldo de la virtualización de las redes, un firewall que brinde las seguridades que requiere un la laboratorio o departamento de TICS y con ello reducir las vulnerabilidades que se puedan presentar.

Según la propuesta de redes seguras por CSIRT dice que se debería tener una infraestructura segura con red privada virtual, para poder reducir las vulnerabilidades con una zona desmilitarizada (DMZ) y con ella controlar la seguridad de la misma.

Para el desarrollo de esta investigación, fue necesario identificar, analizar y revisar trabajos realizados anteriormente, de tal modo exista suficiente fundamento teórico que se pueda tomar a consideración en el desarrollo de esta investigación.

En la investigación sobre “Modelo de Seguridad de la Información” en el que uno de sus objetivos de la evaluación de riegos es garantizar la supervivencia de la organización, minimizando las pérdidas de información y, sobre todo, garantizando el riesgo mínimo en cada elemento de red o software que se emplee para su protección [3]. Para ello se debe hacer el análisis de riesgos para identificar las vulnerabilidades del sistema, en qué riesgos se está incurriendo y cómo mitigarlos[25].

La metodología utilizada por los investigadores es de tipo analítica, ya que analizaron e identificaron los riesgos en cómo evitar o reducir los peligros asociados con la seguridad de la información. Para ello, evaluaron cuidadosa de todos los factores internos y externos que intervienen o afectan los servicios de la organización. Para tener un conocimiento de lo que se debe asegurar y tomar la mejor decisión en las herramientas, metodologías, o prácticas a utilizar, es importante hacer una evaluación consiente y profunda del riesgo. Lo primero es identificar los riesgos, es decir, recopilar todos los activos informáticos de la organización y seleccionar cuáles son los elementos críticos que pueden ser afectados por algún riesgo, la probabilidad de que ocurra y los costos que involucran. Luego, se identifican todas las amenazas informáticas, tanto internas como externas. Al momento de hacer el análisis de riesgos, se toman las amenazas y se analizan con cada uno de los activos que se tiene; esto se evalúa por medio de una calificación de riesgos y con base en lo que afecta, el costo involucrado y el tiempo que se requiere para corregirlo. Posteriormente, se identifican los mecanismos para tratar los riesgos en cuanto a cómo reducirlos, evitarlos, mitigarlos o transferirlos. Estos mecanismos se implementan en diseños de seguridad, funcionalidades, políticas, configuraciones, monitoreo y seguimientos periódicos. El modelo propuesto de seguridad es la base para implantar una arquitectura de seguridad eficiente, invirtiendo en lo que se necesita y logrando así un retorno de la inversión a corto plazo. Para la implementación del modelo de seguridad se deben seguir los siguientes pasos: 1. Identificar y analizar los riesgos 2. Definir las políticas de seguridad 3. Diseñar la arquitectura de red [25].

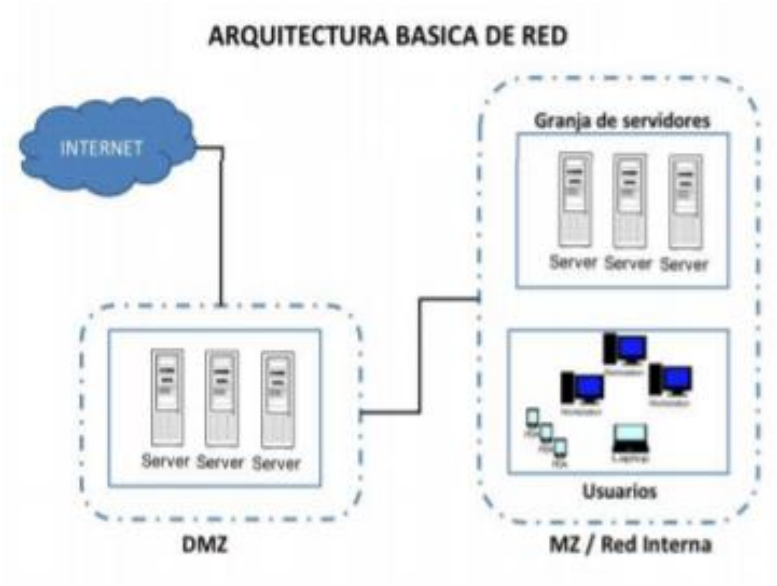


Ilustración 6. *Arquitectura Básica de la Red*[25].

En la ilustración anterior puede observarse, la solución de una arquitectura de red implementada en la investigación "Modelo de seguridad de la información", separando por segmentos la red.

La investigación "Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia" su objetivo principal de su investigación fue el análisis de seguridad de redes WLAN en la ciudad de Tunja Boyacá Colombia mediante muestra aleatorias, esta investigación se realizó se utilizaron las técnicas Warchalking y Wardriving en donde analizaron 150 puntos de red en los que arrojo los siguientes resultados el 44% de las redes eran de hogares, el 36% pertenecían a centro comerciales e instituciones y un 20% no se pudieron analizar por su SSID, se analizó la encriptación WEP en donde se utilizó un vector de inicialización para establecer los valores de la llave de seguridad estos tienen una característica de estabilidad y estos permanecen en las laves lo que posibilidad que el sistema sea vulnerable el tiempo promedio en encontrar esta llave es de 4 minutos por lo cual no es seguro la posibilidad de robo de información es alto. En cambio, con una encriptación WPA para capturar una clave dura aproximadamente 6 horas como resultado final de la investigación se dieron ciertas pautas para la seguridad en las empresas entre una de ella es ocultar el SSID en la configuración del router del wifi así se evitara atacantes, solo se podrán conectar los que conocen de la red, otra práctica de seguridad es configurar el router para que solo acepte conexiones confiables en los dispositivos previamente registrada su MAC, también es recomendable utilizar contraseñas fáciles de usar pero difíciles de adivinar debe ser una contraseña conformada por números, letras, caracteres especiales. Para las empresas o instituciones es recomendable seguir una administración basada en la ISO 27000 que proponen practicas certificadas en la administración de la red[26].

En la investigación "Análisis de los Sistemas de Ataque y Protección en redes inalámbricas WIFI, bajo el Sistema Operativo Linux", se plantearon como objetivo el diseños de una red inalámbrica WIFI con sistemas de detección de intrusos Snort y Kismel, para ello utilizaron una metodología exploratoria, para la solución de esto utilizaron Snort que es un sistema de detección y prevención de intrusos en la red y Kimet es un detector de redes inalámbricas para el proceso de la evaluación pusieron en marcha los sistemas a evaluar, se realizaron pruebas, recolección y clasificación de datos. Con objeto de las pruebas se colocaron los siguientes equipos: Se coloca un equipo con sistema operativo Ubuntu 12.0.4; con Snort y Kismet instalados según indicaciones de sus páginas

web oficiales, se conecta una tarjeta D-Link DWA125 A3 para las pruebas con Kismet y para Snort se coloca un switch(configurado port mirroring) entre el FortiAP y el switch de acceso, debido a que al ejecutarse sobre la tarjeta inalámbrica en modo monitor, no se podía decodificar el tráfico generado; DLT IEEE802.11 127[27].

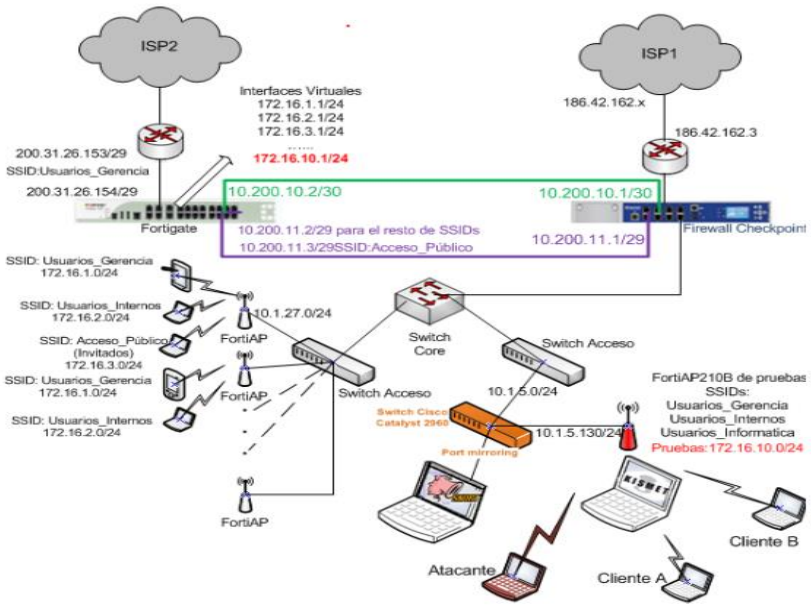


Ilustración 7. *Topología de Prueba* [27].

En la ilustración anterior puede observarse, la Arquitectura estructurada para las pruebas de la investigación.

Según los resultados obtenidos luego de los ataques se dieron como recomendaciones tener un antivirus y firewall instalados y actualizados, tener contraseña en los equipos, en el router configurar las políticas de seguridad de acceso, en WPA+TKIP una clave mínima de 10 a 15 caracteres, implementar un filtrado de MAC.

Esta investigación hace pruebas de seguridad de la red utiliza una arquitectura segura con firewalls utiliza software libre Ubuntu por lo que hace referencia a la investigación que se está realizando.

1.3. Marco Legal

En la presente investigación, debido a la relación que se estable en el concepto de software libre e Internet; se rige bajo las disposiciones del Código Orgánico de la economía social de los conocimientos, creatividad e innovación del Ecuador emitida en el año 2016 por la asamblea nacional.

Según el artículo 211 de la sección VII de las limitaciones y excepciones a los derechos patrimoniales párrafo segundo el factor 24 menciona La referencia o enlace de sitios en línea, u otras actividades lícitas similares, así como la reproducción y almacenamiento necesarios para el proceso de funcionamiento de un motor de búsqueda de la Internet siempre y cuando esto no implique violación de contenidos protegidos.

Según el artículo 142 de la sección V apartado segundo de las tecnologías libres y formatos abiertos Tecnologías libres manifiesta "Se entiende por tecnologías libres al software de código abierto, los estándares abiertos, los contenidos libres y el hardware libre. Los tres primeros son considerados como Tecnologías Digitales Libres. Se entiende por software de código abierto al software en cuya licencia el titular garantiza al usuario el acceso al código fuente y lo faculta a usar dicho software con cualquier propósito. Especialmente otorga a los usuarios, entre otras, las siguientes libertades esenciales: La libertad de ejecutar el software para cualquier propósito; La libertad de estudiar cómo funciona el software, y modificarlo para adaptarlo a cualquier necesidad. El acceso al código fuente es una condición imprescindible para ello; La libertad de redistribuir copias; y, La libertad de distribuir copias de sus versiones modificadas a terceros[28]."

CAPITULO II: MATERIALES Y MÉTODOS

2.1. Área de Estudio

La Pontificia Universidad Católica del Ecuador – Esmeraldas, se encuentra ubica en la calle Espejo subiendo a Santa Cruz en el centro de la ciudad Esmeraldas. Forma parte de una de las mejores universidades acreditadas por la SENESCYT. Los beneficiarios directos son: personal administrativo, docentes y estudiantes de la universidad.

2.2. Tipo de Estudio

En el presente proyecto de investigación se realizó un análisis y propuesta de una infraestructura tecnológica basándose en un tipo de arquitectura previamente seleccionada planteando un prototipo de diseño de redes en un laboratorio.

Por su amplio campo es una investigación exploratoria cualitativa, ya que se va a hacer un análisis del problema mediante una investigación del tipo de redes que tiene la institución. La Investigación Exploratoria cualitativa se realiza cuando se tiene como objetivo analizar, investigar, examinar, comprobar un tema o problema poco estudiado[29]. Para la obtención de información utilizaremos la encuesta y la entrevista.

También se determinó una investigación narrativa descriptiva por la recolección de información a través de la técnica de observación y la entrevista.

2.3. Métodos

Para la presente investigación se emplearon los métodos analíticos, deductivos y bibliográficos los cuales se los especificara a continuación:

Método Analítico: Este método de investigación consiste en analizar y estudiar por separado cada parte de un objeto o elemento de un todo, para conocer su naturaleza, efecto y comportamiento.

- La forma clásica de entender el método analítico ha sido la de un procedimiento que descompone un todo en sus elementos más básicos y, por tanto, que va de lo general (lo compuesto) a lo especifico (lo simple), también se lo puede definir como un camino que parte de los fenómenos para llegar a las leyes, es decir, de los efectos a las causas[30].

Este método se utilizó para especificar los problemas en la infraestructura de la arquitectura de redes con la que cuenta la Pontificia Universidad Católica del Ecuador Esmeraldas, para de esta manera establecer los problemas y las necesidades de la implementación de una buena arquitectura para mejorar, la seguridad de las redes y la rapidez de esta, con mínimos errores.

Método Deductivo: Este método ayudo a deducir conclusiones lógicas a través de procesos que van de los principios generales a los hechos específicos.

Este método se lo utilizara para evaluar la infraestructura que posee la universidad acorde a los requerimientos que se obtengan luego del análisis de esta investigación.

Método Bibliográfico: Este método permitió obtener información directa y objetiva del problema que se va a investigar, en donde se podrá evidenciar los inconvenientes con el que cuenta la PUCESE en cuanto a la seguridad de sus redes, analizando proyectos realizados previamente en relación con lo que se va a analizar.

2.4. Técnicas e instrumentos

Entrevista: En esta investigación se utilizó la técnica de la entrevista que se la realizo directamente al jefe del departamento de redes de la Pontificia Universidad Católica del Ecuador "Sede Esmeraldas", con el objetivo de obtener información del tipo de arquitectura que tiene la institución y recolectar requerimientos.

Para la creación de la entrevista se recurrió a proyectos ya realizados relacionados con el tema, los mismos que ayudaron con la recopilación de los datos, algunas preguntas fueron modificadas por intereses propios del tema de investigación.

Técnica Observación Científica: En esta investigación se aplicó la técnica de la Observación Científica para comparar las diferentes Arquitecturas de Redes propuestos por CSIRT y poder hacer una comparación de estas para escoger la mejor arquitectura que se adapte a todos los requerimientos de las PUCESE.

Especificación de requerimientos según CSIRT: Se pudo obtener descripción completa del comportamiento de la red y los requerimientos para que una red sea segura.

2.5. Análisis de Datos

La información tomada para el desarrollo de esta investigación se obtuvo a través del análisis de las arquitecturas de seguridad propuestas por CSIRT, la información obtenida

por medio de la entrevista al jefe del departamento de sistemas y obtención de información del jefe del departamento de redes con el fin de conocer que tiene actualmente la infraestructura de la institución, herramientas con las que trabajan.

CAPÍTULO III: RESULTADOS

3.1. Análisis de la Infraestructura de Red de la Institución

Con los resultados obtenidos por medio de la entrevista al jefe del departamento de sistemas y previamente analizados los diferentes tipos de arquitecturas expuestos en el marco teórico, se ha logrado examinar la infraestructura que actualmente tiene la universidad y se ha evidenciado que no tienen las suficientes seguridades en su infraestructura, recientemente están implementando el firewalls pero aún no está en funcionamiento, se ha venido trabajando con seguridades por medio del Mikrotik. .

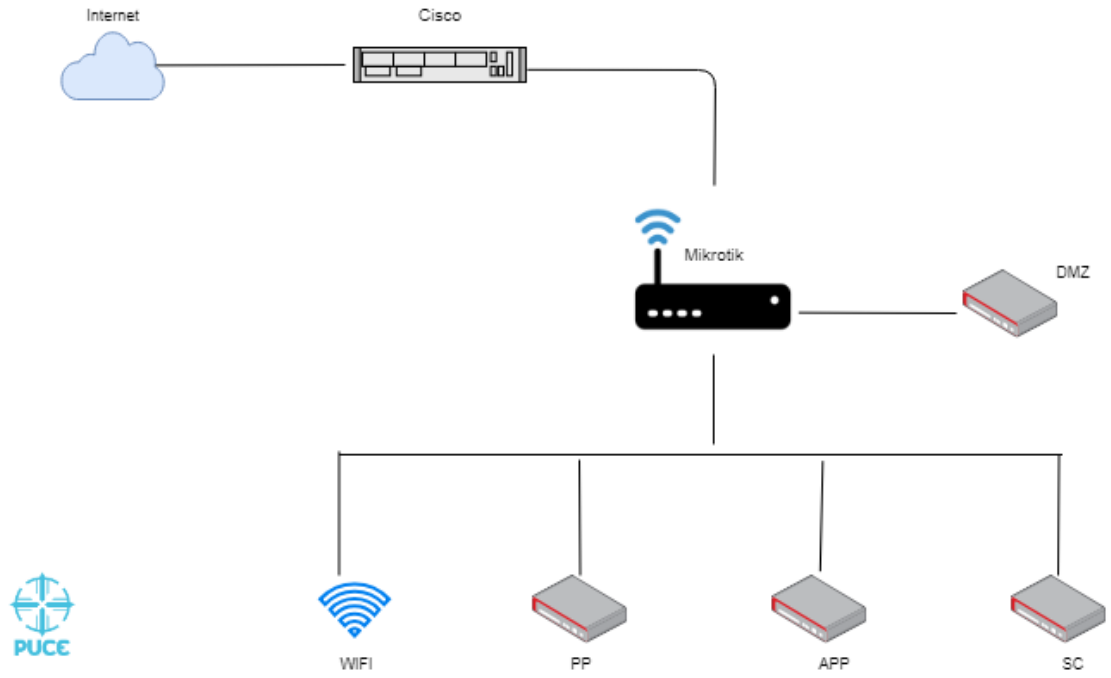


Ilustración 8. *Infraestructura de la PUCESE.*

En la ilustración anterior puede observarse, la infraestructura de la PUCESE en donde tiene el proveedor del internet que se dirige a un Switches CISCO, cuentan con roter Mikrotik, la red está dividida en dos segmentos una DMZ y una red interna en donde se encuentra el (WIFI,PP,APP,SC).

3.2. Análisis General de la Infraestructura de la institución

La arquitectura de red de la institución actualmente está separada en dos segmentos DMZ una interna y una externa donde se encuentran todos los servicios que brindan, cuenta con un sistema de antivirus que está en cada punto final es pagado, seguridades en los

servidores (configuración) por medio de contenedores, está aislado es libre por la utilización de Docker, cuentan con Mikrotik es el ruteador principal y el firewall que está incluido en el paquete de Mikrotik.

El jefe del departamento de sistemas afirma que la red no necesita balanceo de carga pues actualmente solo cuentan con un solo proveedor de internet.

Para el ingreso a los servidores se tienen unas configuraciones, pero no se las tiene aseguradas con VPN para la encriptación, se está utilizando el sistema operativo base (proxy, citrix) para acceder a los servidores, físicamente tienen 7 servidores.

Actualmente no tienen seguridades dependiendo del rol en que se esté trabajando, el acceso a servidores solo como administrador con su seguridad, pero el acceso a las aplicaciones sí se encuentra restringido para los estudiantes.

3.3. Propuesta

3.3.1. Análisis e interpretación del prototipo de Arquitectura de Red

Esta problemática conlleva a proponer la Arquitectura de Red Segura propuesta por CSIRT por motivos que se detallaran a continuación:

RED SEGURA es una solución para obtener una arquitectura sin que sus servidores tengan redundancia, que toda su red este administrada y segura con los firewalls.

En la arquitectura incluye tanto como seguridad del servidor donde está los firewalls (reglas Nat), seguridad en la información, balanceo de carga de red, claves públicas y privadas.

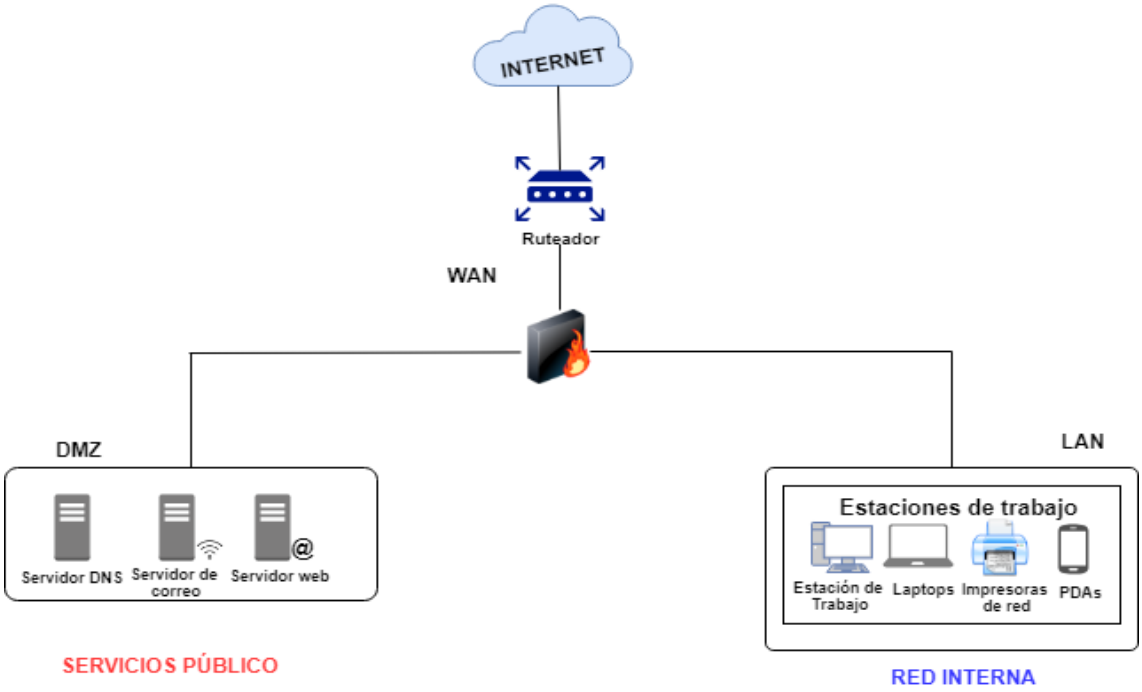


***Ilustración 9**. Modelo de Arquitectura de Red Segura propuesta por CSIRT*

En la ilustración anterior puede observarse, la Arquitectura de Red Segura que se propone CSIRT según los estudios realizados , está compuesta por un firewall que esta antes de los DMZ que son todos los servidores con los que la institución cuenta y la red LAN en donde están inmersos las diferentes estaciones de trabajo que vendría hacer la red interna de la misma.

3.3.2. Características de la solución de la Red Segura

Para la presente solución de la Arquitectura seleccionada se han tomado los siguientes requerimientos.

***Tabla 9.** Definiciones, abreviaturas*

Definiciones de especificaciones de la Arquitectura

Nombre	Descripción
Firewalls	Como se mencionó anteriormente, es un aplicativo o dispositivo que están diseñados para crear reglas de bloqueo o de permiso, cabe recalcar que existen diferentes tipos de aplicaciones en este caso para realizar las pruebas se utilizó PfSense.
QOS	Toda Calidad de servicios debe contar con los 5 parámetros establecidos (Rendimiento, Retardo, Variación de retardo de transmisión, Perdida de paquetes o fiabilidad, Ancho de banda) que indican el tiempo de entrada y llegada de la información de los datos.

Hardening	Este proceso debe tener toda empresa, para el endurecimiento de su seguridad, la generación de las claves públicas y privadas por medio de certificados para obtener su red segura.
VLAN	Crea redes independientes, dentro de una red física.

En esta tabla se muestran los conceptos básicos que contiene la Red Segura propuesta por CSIRT.

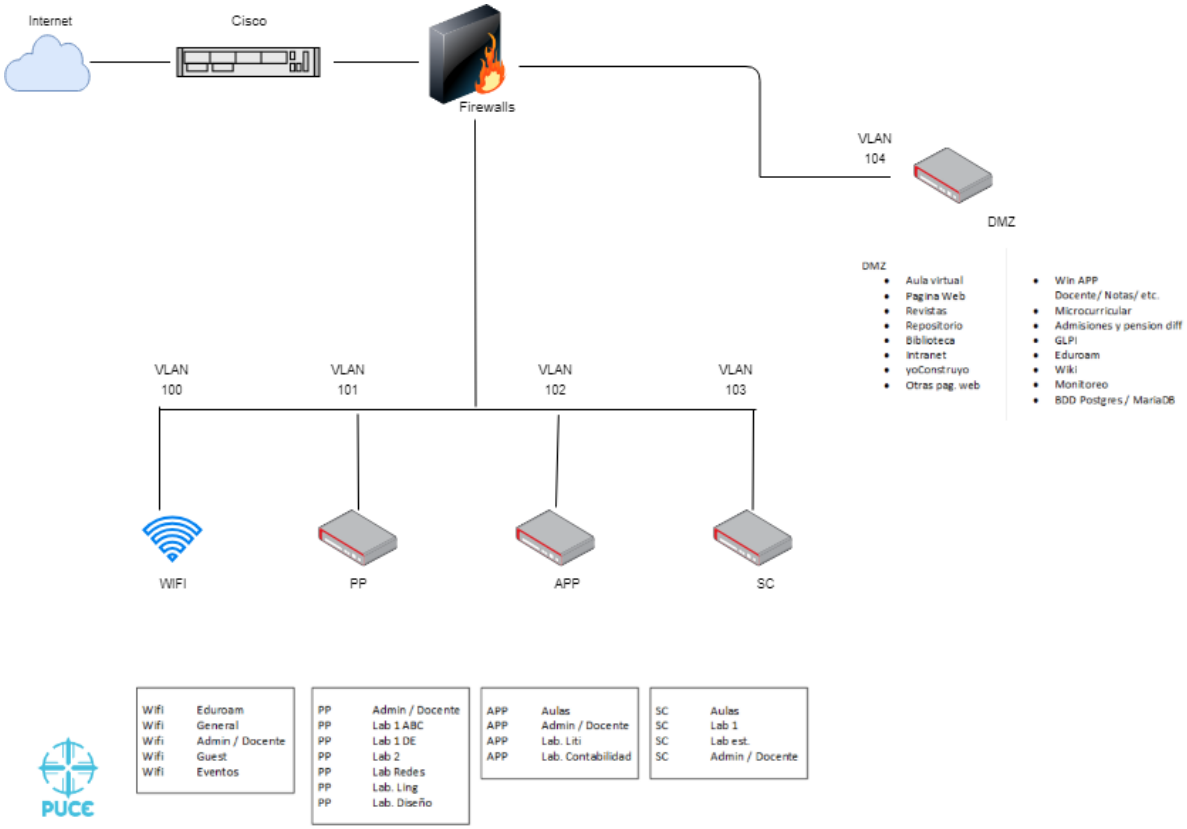


Ilustración 10. *Propuesta de la Infraestructura.*

3.3.3. Descripción General

El firewall elegido para esta prueba de ambiente fue PfSense que es de código abierto, porque tiene más documentación, una interfaz amigable y tiene 12 años lanzados en la web por lo que se podría decir que es una aplicación estable en la tabla 1 del marco teórico se pueden ver las características del mismo, esto lo afirman en un estudio comparativo que hicieron entre Pfsense y OPNsense[7].

3.3.4. Ambiente de prueba para la propuesta

Para la realización de las pruebas se necesitó de los siguientes recursos.

Tabla 10. Características del Ambiente de Pruebas.

Servidor	CentOS/3 Tarjetas de Red
Cliente	Linux/Windows
Router	1
Portátiles	3
Firewall	Pfsense

Se detallan los materiales utilizados para la prueba de ambiente de la Red Segura.

Es necesario realizar la elaboración del diagrama del ambiente de prueba realizado en esta investigación.

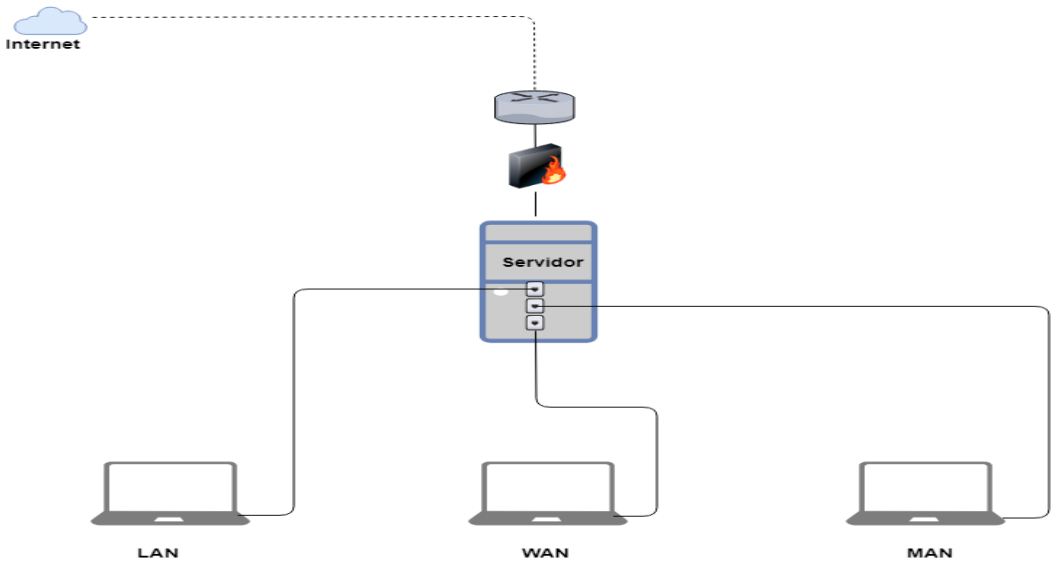


Ilustración 11. *Ambiente de Prueba de Arquitectura de Red.*

En la ilustración anterior puede observarse, el ambiente de prueba que se realizó donde se trabajó con un router, se instaló el firewall pfsense, un servidor con CentOS, tres laptops, cables

El ambiente de prueba se realizó dentro de la institución PUCESE es totalmente operativo y funcional, se levantó una red con un router dentro de la red de la institución, se instaló el firewall Pfsense en un CPU con el sistema operativo CentOS se le añadió 2 tarjetas de red adicional para simular las redes LAN, WAN, DMZ.

Reglas de Nat

Dentro de este firewall se creó las tres interfaces (LAN, WAN, DMZ) en donde se le asigno una IP a cada una de ellas, luego del análisis de la infraestructura que tiene la PUCESE, aquí se configuro las reglas de antibloqueo, permitir las reglas para IPV4, IPV6.

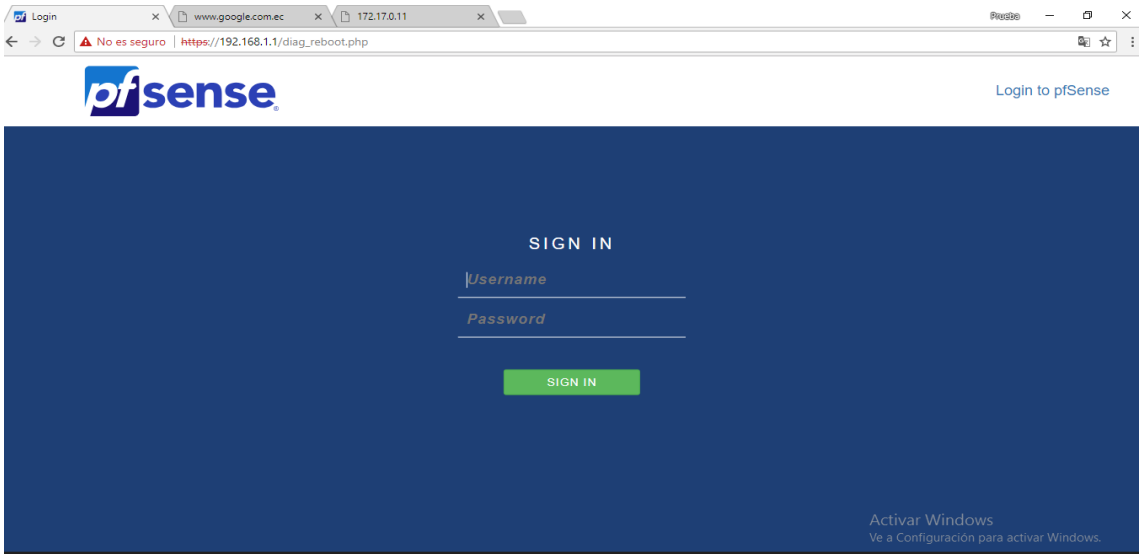


Ilustración 12. *Ingreso al Servidor PfSense.*

En la ilustración anterior puede observarse, el ingreso al firewall donde se debe colocar la IP en el buscador de internet que se le ha asignado al PfSense que vendría a ser la red LAN, donde se colocara el usuario y contraseña que le haya asignado.

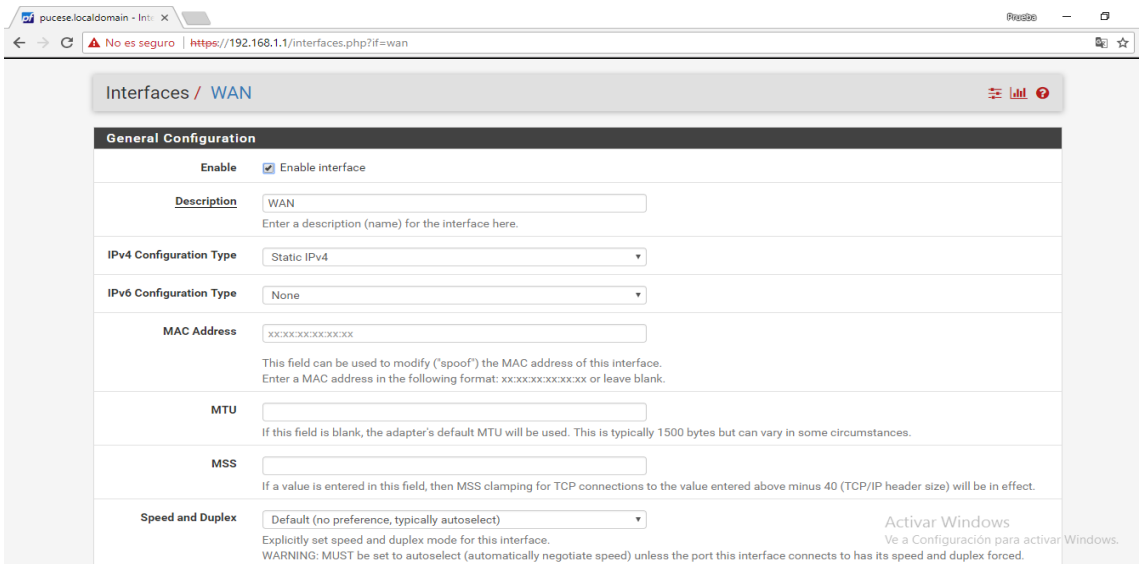


Ilustración 13*. Interfaz / WAN.*

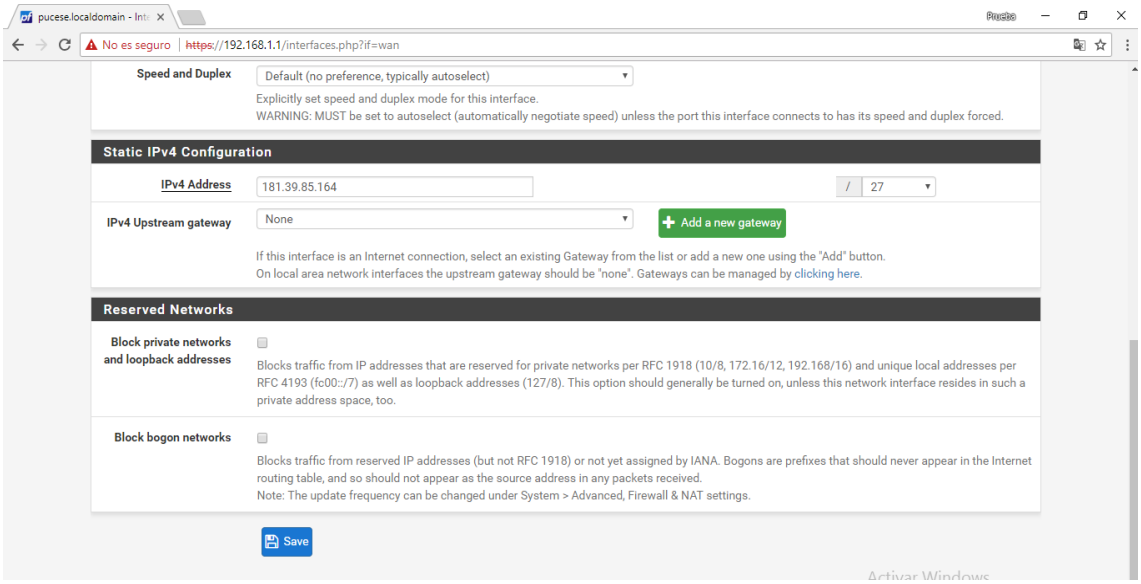


***Ilustración 14**. Interfaz / Configuración WAN*

En la ilustración 12 y 13 puede observarse, la creación de la Interfaz WAN en el firewall pfSense donde se le asigna una ip estática a la WAN de la red donde se va a trabajar.

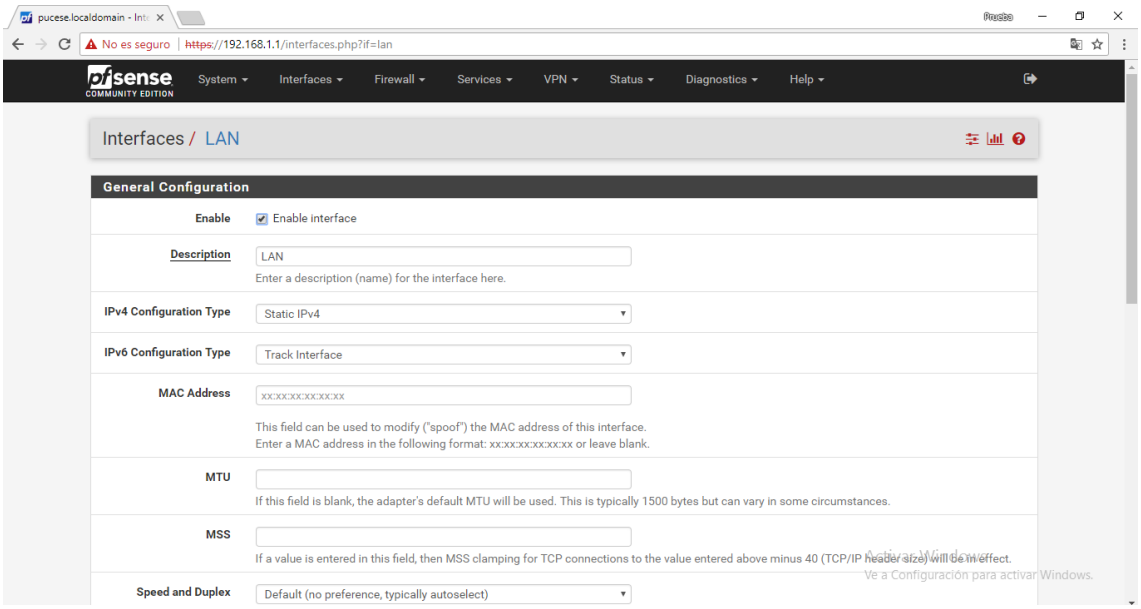


***Ilustración 15**. Interfaz / LAN*

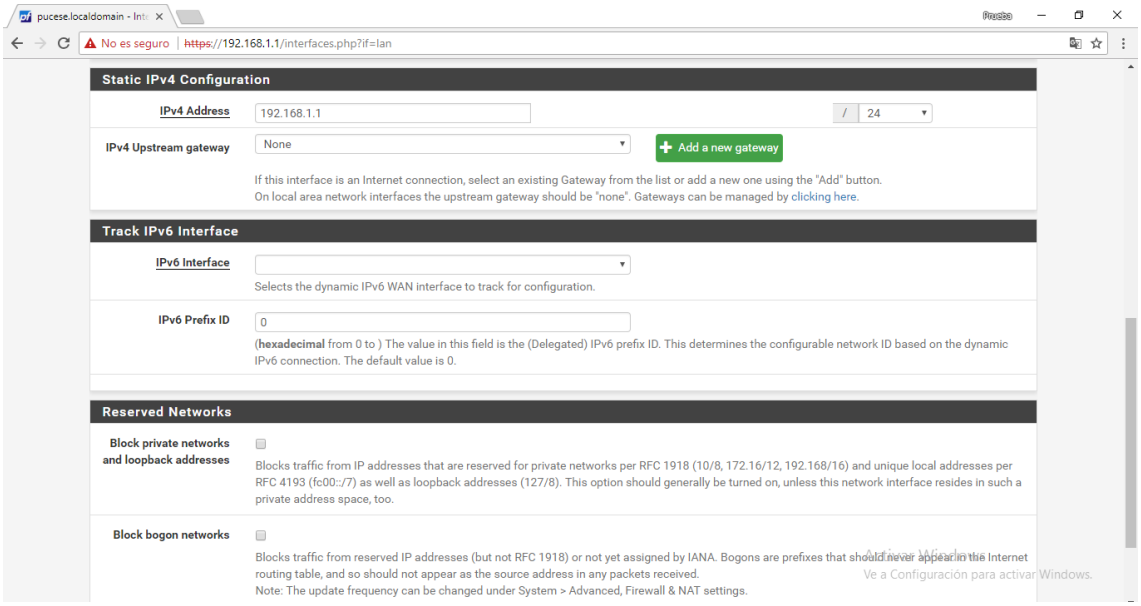


Ilustración 16. *Interfaz / Configuración LAN*

En la ilustración 14 y 15 puede observarse, la creación de la Interfaz LAN en el firewall pfSense donde se le asigna una ip estática a la LAN de la red donde se va a trabajar.

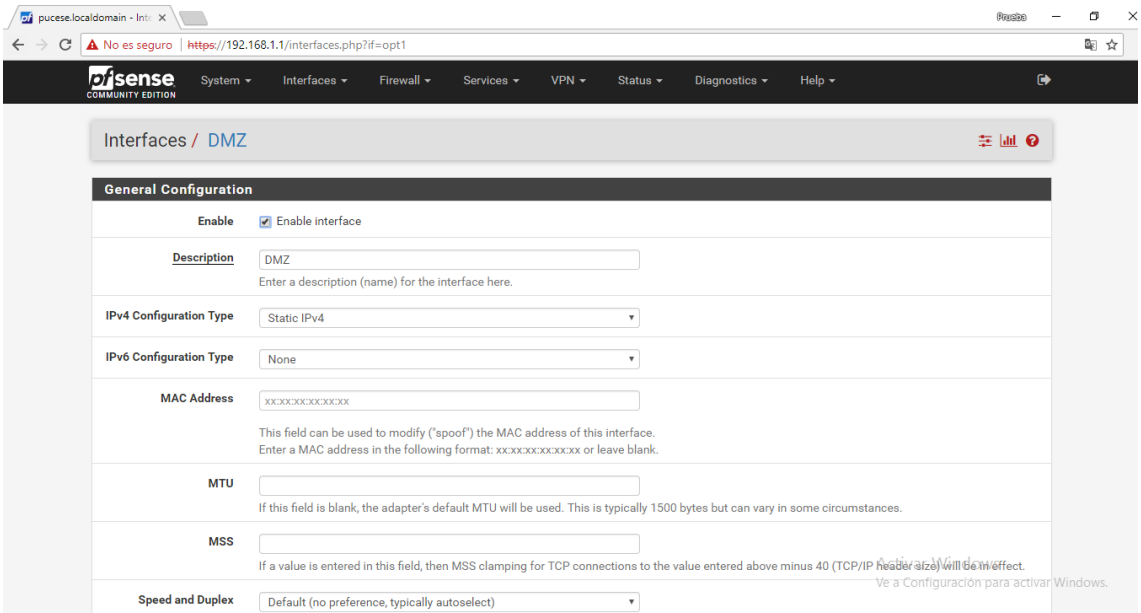


Ilustración 17*. Interfaz / DMZ*

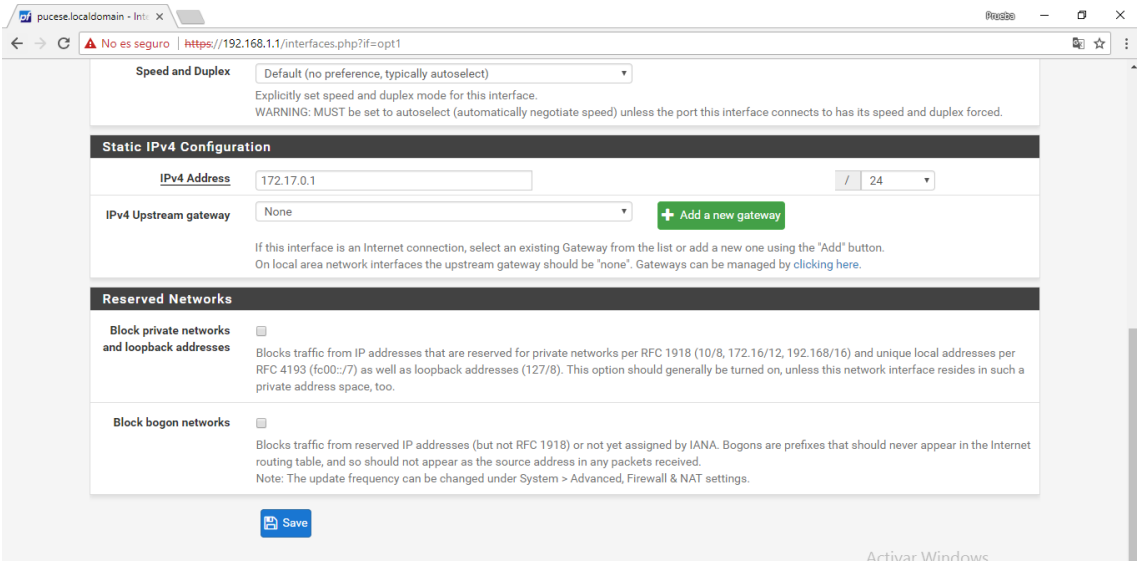


***Ilustración 18**. Interfaz /Configuración DMZ*

En la ilustración 16 y 17 puede observarse, la creación de la Interfaz DMZ en el firewall pfSense donde se le asigna una ip estática a la DMZ de la red donde se va a trabajar.

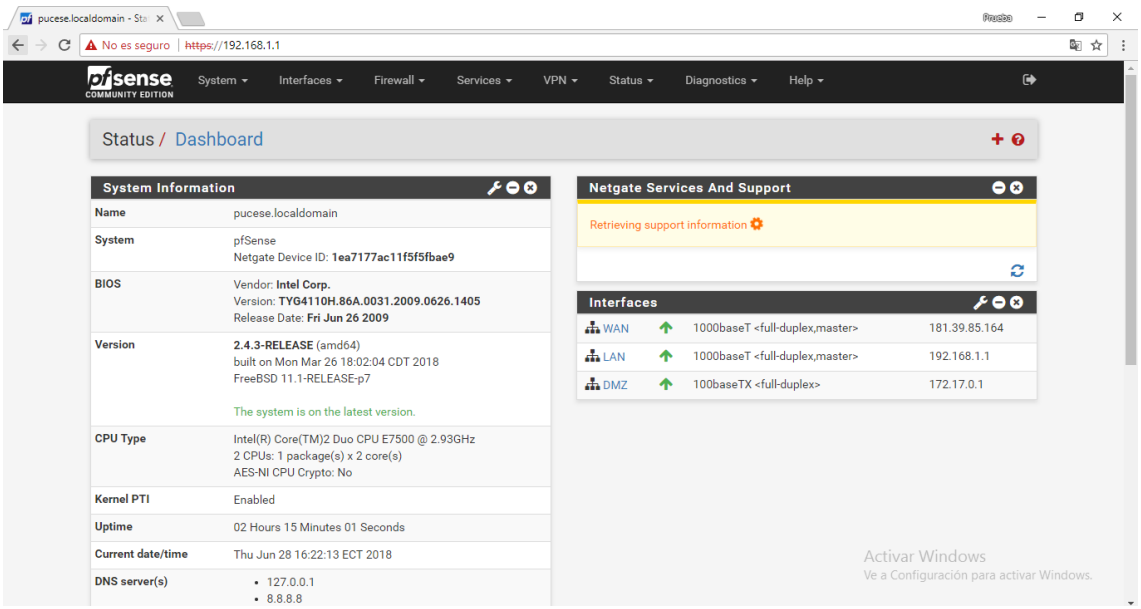


***Ilustración 19.** Interfaces (LAN, WAN, DMZ)*

En la ilustración anterior puede observarse, que en el Firewall se tiene el ambiente de prueba que se ha generado, en este caso se utilizó la red WAN, LAN y DMZ, asignándole ip referentes a la institución y previamente analizados los datos de estas.

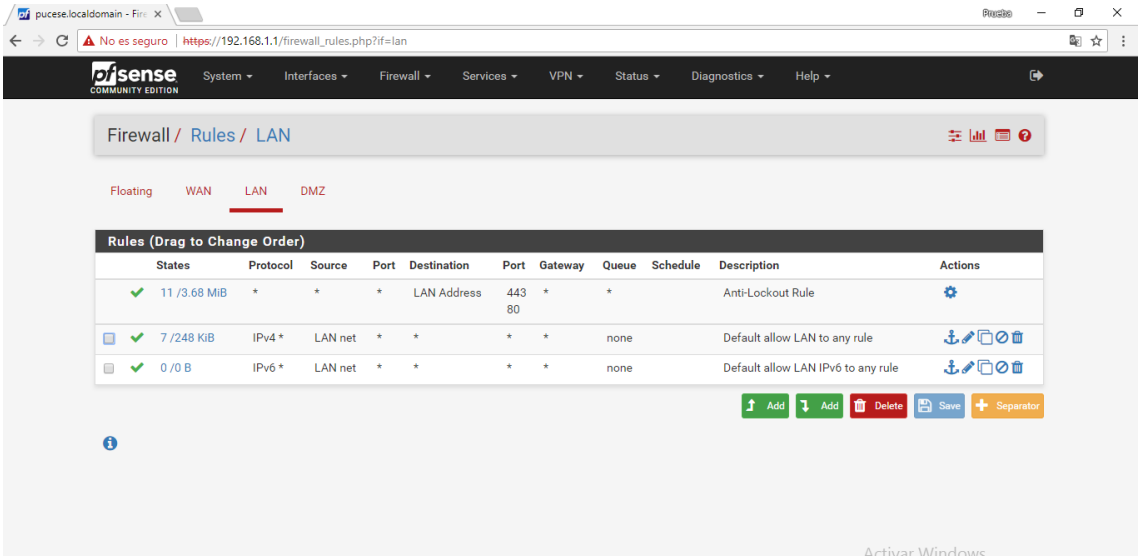


Ilustración 20. *Reglas de LAN.*

En la ilustración anterior puede observarse, las reglas de la red LAN, donde se coloca las reglas de antibloqueo, permitir las reglas para IPV4, IPV6 las mismas reglas se realizó para la interfaz WAN.

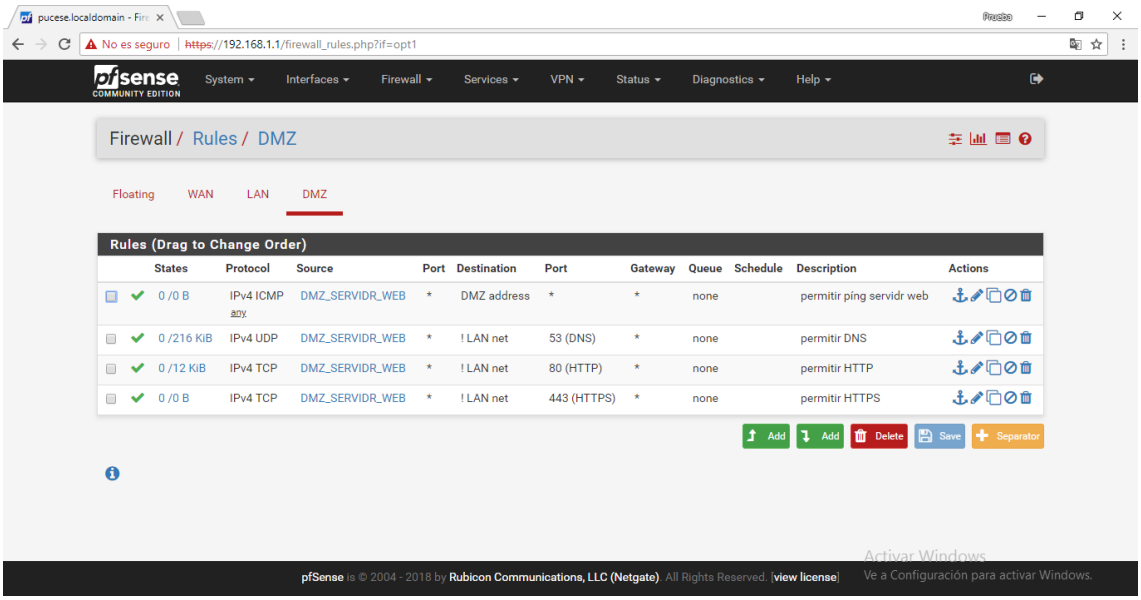


Ilustración 21. *Reglas DMZ*

En la ilustración anterior puede observarse, las reglas de la DMZ, donde se coloca las reglas de permitir ping al servidor web para obtener internet, permitir DMZ, HTTP Y HTTS.

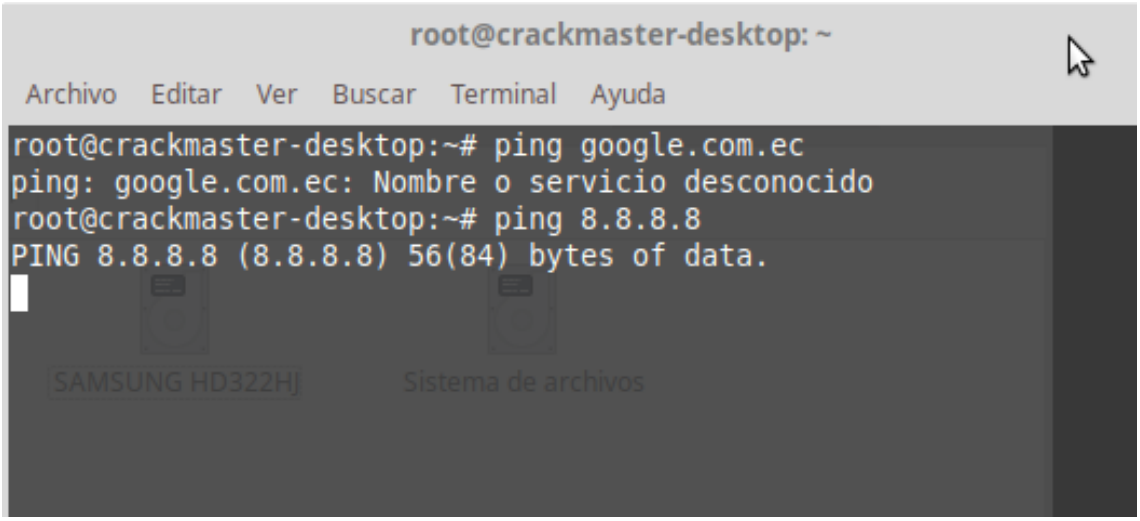


Ilustración 22. *Probar acceso a Internet*

En la ilustración anterior puede observarse, las pruebas de acceso a internet luego de hacer las pruebas de permitir ping al servidor se comprobó el acceso a internet colocando el comando ping 8.8.8.8 de Google.

3.4. Criterio General

Luego del análisis de la infraestructura de la universidad se pudo evidenciar que están incrementando seguridades en sus redes actualmente cuentan con una arquitectura divida en dos segmentos de DMZ interna y externa, están implementando un firewalls, que según esta investigación y avalada por estudios realizados los firewalls de códigos abiertos más recomendados son Pfsense y OPNsense por su alto grado en seguridad, interfaz amigable con el usuario ,en el firewalls se debe incrementar las reglas de NAT para bloquear o permitir comunicaciones o configuraciones, la creación de los roles con certificados de claves públicas y privadas encriptadas para cada usuario, la creación de VPN además de ello se recomienda separación de la red una para la DMZ y otra para la red interna.

CAPÍTULO IV: DISCUSIÓN

Una vez concluida la investigación se pudo comprobar que contar con una buena Arquitectura de Red ayuda a que las empresas o instituciones tengan una mayor seguridad en su red y por lo tanto tenga mayor confiabilidad en sus datos. La PUCE-Esmeraldas tiene una arquitectura de red que se está actualizando a las tecnologías actuales; de acuerdo con la encuesta y el análisis previo se estableció a la arquitectura en un estado "moderado", es decir que se está tratando de adaptarse a nuevas tecnologías.

En el estudio realizado por Bonilla y Gonzales [25] titulada "Modelo de Seguridad de la Información " recalcan que antes de realizar o proponer cualquier modelo de Seguridad es necesario identificar y analizar los riesgos, definir las políticas de seguridad y diseñar la arquitectura de red, una vez que analizaron todos los datos se obtuvieron como resultado que se debe implementar mayor inversión en la seguridad de la organización sin descuidar las demás zonas y concluyen que no basta con un buen análisis e implementación de un buen sistema de seguridad sino se realiza un seguimiento, sin embargo en esta investigación solo se enfocan en la seguridad de la información y en su arquitectura propuesta no tienen un firewalls ni un balanceo de carga en su red.

Las investigaciones anteriormente analizadas concuerdan que lo más importante en la infraestructura de una red es la seguridad, rapidez y confiabilidad de su información.

La Pontificia Universidad del Ecuador Sede Esmeraldas necesita una arquitectura de red que cumpla con todos sus requisitos para satisfacer las necesidades del personal (administrativos, docentes y estudiantes), en los datos obtenidos en la entrevista resulto que la arquitectura de la institución está separada en dos segmentos una de estudiantes y una administrativa, tiene seguridades en sus servidores.

En la investigación de Rodríguez [31] titulada "Implementación de un prototipo de laboratorio para el estudio de ataques de seguridad de redes" analizaron los principales ataques de la red y con los datos obtenidos realizaron un prototipo de código abierto para reducir los ataques para ello utilizaron VNX, para la virtualización de los sistemas, pero con ello solo se protegen de los ataques que puedan sufrir, a diferencia de esta diferencia se creó un prototipo de arquitectura que se protege por medio de un firewalls de los posibles ataques, seguridad en sus información, balanceo de carga y segmentación en la red.

CAPÍTULO V: CONCLUSIONES

Esquematizando los resultados obtenidos en esta investigación, se puede percibir que se cumplieron con los objetivos descritos al principio, lográndose palpar de las fuentes bibliográficas, así también mediante la técnica de la entrevista donde se logró recolectar información de cómo se encuentra actualmente la infraestructura de la institución, obteniendo con esto la recopilación de datos de las carencias de la infraestructura de red y pudiéndose recomendar un prototipo de arquitectura de red segura.

Una vez que se revisaron las fuentes bibliográficas se concluye que tener una buena Arquitectura de red segura ayudara al buen servicio de la institución, se analizaron cada una de la arquitectura propuesta por CSIRT y para esta investigación se escogió la Arquitectura de red segura, ya que tiene un alto grado de seguridad y el bajo costo en su implementación a diferencia de las demás arquitecturas.

La infraestructura que tiene la institución actualmente no cuenta con todas las seguridades que debería tener como segmentación de los DMZ y la red LAN, actualmente está separada solo por los segmentos de DMZ interna y externa, deben estar separadas tanto los servidores como el área de trabajo para una mayor seguridad de estos. El acceso mediante los VPN se debe realizar por medio de la generación de claves públicas y privadas comprando principalmente un certificado e incorporándolo en las VPN, y para una mayor confiabilidad de los datos que cada administrativo o docente tenga su propio usuario con su respectiva clave encriptada.

Aplicar la Arquitectura de red Segura propuesta por CSIRT y previamente realizadas las pruebas de esta en la institución, contribuirá a una red más confiable, protegida, que podrá dar soluciones inmediatas a cualquier inconveniente que se pueda presentar.

CAPÍTULO VI: RECOMENDACIONES

Una vez que se analizaron todas las arquitecturas de red propuestas por CSIRT se recomienda a la PUCE-ESMERALDAS implementar la Arquitectura de Red Segura y con ello obtener una red más confiable, que se adapte a los requerimientos de la institución.

Luego del análisis y la observación de la infraestructura de la institución se recomienda que se acoplen a nuevas seguridades, como la incorporación de una nueva arquitectura que ayuden a dar respuestas inmediatas a cualquier problema que se pueda presentar en la red.

Se recomienda a la universidad se incorpore una infraestructura más confiable con la incorporación de un firewall en sus servidores sea este pfSense o OPNsense que según la investigación son recomendados para empresas ya que son de código abierto, por su alta seguridad y su interfaz de fácil uso, luego de incorporarlos colocarle las diferentes reglas de NAT, ya sean esta para permitir accesos o bloquear ciertos permisos a los usuarios, utilizar las VPN para el acceso remoto de los administrativos de la institución con seguridades.

REFERENCIAS

[1] WEB-MASTERS, «topologia de redes LAN», *DOMINGO, 25 DE MAYO*, 2008. .

[2] I. Avalos, «“EVALUACIÓN DE LOS ATAQUES DE NAVEGACIÓN DE SERVICIO Y FORMAS DE PROTECCIÓN APLICADAS A LA RED DE DATOS DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANÁ.”», 2015.

[3] C. E. Lazo Vélez, «Implementación de un Laboratorio de Redes de Telecomunicaciones utilizando Infraestructura Mikrotik», 2017.

[4] Bonilla Margarita, «Análisis y diseño de un sistema de seguridad de red perimetral en la empresa aseguradora del sur-matriz», Pontificia Universidad del Ecuador, 2016.

[5] Gómez R y L. V Vazquez, «Definiendo un esquema de seguridad para redes ATM en base a firewalls».

[6] Salo Miro, «PfSense kotiverkon verkonhallinnassa», 2018.

[7] Firewall Hardware, «pfSense® vs OPNsense®: technical comparison». [En línea]. Disponible en: http://opnsense.firewallhardware.it/en/pfsense_vs_opnsense.html. [Accedido: 13-ene-2019].

[8] A. Hils, J. D’hoinne, y R. Kaur, «Magic Quadrant for Enterprise Network Firewalls», 2017.

[9] J. Webb, «Network Demilitarized Zone (DMZ)», *infosec*, 2015.

[10] D. Fernando y S. Vizcarra, «ALTERNO COMO SITIO DE RECUPERACIÓN ANTE DESASTRES, PARA UNA ENTIDAD PRIVADA " Informe final caso de estudio previo la obtencion del título de: Magíster en Redes de Comunicaciones», 2017.

[11] D. Matute, «Mejorar la seguridad de redes locales en la empresa "Servicios y Comercio XEROX " mediante la utilizacion de VPN(Redes privadas virtuales)», UNIVERSIDAD TECNOLÒGICA ISRAEL, 2014.

[12] J. G. A. Montes, J. Corona, «PROPUESTA DE IMPLEMENTACION DE UNA VPN», 2012.

[13] I. Z. MORALES MARIA, «IMPLEMENTACION DE LA CALIDAD DE SERVICIOS (QoS) Y MONITOREO DE REDES PARA GESTIONAR EL BALANCEO DE CARGA DEL ENLACE A INTERNET EN LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA», 2012.

[14] S. Ran, «A Model for Web Services Discovery With QoS», 2003.

[15] F. De, R. De Tesis, T. De Graduación, O. Caicedo, y J. German, «II REPOSITORIO NACIONAL DE REGISTRO Y TECNOLOGÍA».

[16] «Preguntas frecuentes sobre Calidad de servicio (QoS) - Cisco», *2009*. [En línea]. Disponible en: https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/22833-qos-faq.html#gen. [Accedido: 13-ene-2019].

[17] D. J. Joza Calderón, «Aseguramiento y endurecimiento (Hardening) de la infraestructura del sitio web de la Corporación Registro Civil de Guayaquil.», 2018.

[18] F. Hernandez, J. Lugo, y A. Arturo, «Apuntes Digitales-REDES DE COMPUTADORAS». [En línea]. Disponible en:

http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro35/12_caractersticas_de_la_arquitectura_de_red.html. [Accedido: 12-ene-2019].

[19] W. G. Chango Sailema, «Análisis, consideraciones de diseño e implementación en laboratorio de un sistema de respaldo de datos de máquinas virtuales y usuario final a través de la red LAN. Caso de estudio AVAMAR», *Pontif. Univ. Católica del Ecuador*, 2015.

[20] Instituto Colombiano de Normas Técnicas y Certificación, «GUÍA TÉCNICA GTC-ISO/IEC COLOMBIANA 27035 TECNOLOGÍA DE LA INFORMACIÓN. TÉCNICAS DE SEGURIDAD. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN», 2012.

[21] A. L. P. M. Herrero Collantes, «Protocolos y seguridad de red en infraestructuras SCI», 2015.

[22] E. C. R. Aquino , J.L. Chavez , L. Vidal , L. Ferreyro, A. A. Bou, «GESTION DE INCIDENTES DE SEGURIDAD INFORMATICA», 2012.

[23] M. . H. C. O.J HERNÁNDEZ JIMÉNEZ, «Actualización de una red local plana a una red local segura , segmentada con servicios de voz y datos en el IFAI».

[24] M. J. González Martínez, «Tecnologias de la Información», en *Tecnologias de la Información*, 2010.

[25] Sandra M. y J. A. González, «Modelo de Seguidad de la Información», *Ing. USBMed*, vol. 3, n.º 1, pp. 6-14, jun. 2012.

[26] J. A. Monsalve Pulido, F. A. Aponte Novoa, y F. Chaparro Becerra, «Security analysis of a WLAN network sample in Tunja, Boyacá, Colombia», *DYNA*, vol. 82, n.º 189, pp. 226-232, feb. 2015.

[27] A. M. Yacchirema Espín, «Análisis de los sistemas de ataque y protección en redes inalámbricas WIFI bajo el sistema operativo LINUX-», 2014.

[28] Ecuador, «Codigo Organico de la economia social de los conocimientos, creatividad e inovacion», 2016. [En línea]. Disponible en: http://www.wipo.int/edocs/lexdocs/laws/es/ec/ec075es.pdf. [Accedido: 01-jul-2018].

[29] C. E. Mendez Álvarez, «Investigación Exploratoria», *Guía para Elabor. diseños Investig. en ciencias económicas, Contab. Adm.*, 2000.

[30] J. D. Lopera-Echavarría, C. Ramírez-Gómez, M. U. Zuluaga-Aristízábal, y J. Ortiz-Vanegas, «El método analítico como método natural», *Rev. Crítica Ciencias Soc. y Jurídicas*, 2010.

[31] G. A. Rodríguez Paladines, «Implementación de un prototipo de laboratorio para el estudio de ataques de seguridad en redes», mar. 2016.

ANEXOS

Anexo 1.Entrevista al jefe del departamento de TIC'S de la PUCESE.

ESCUELA DE INGENERÍA EN SISTEMAS Y COMPUTACIÓN

La siguiente entrevista está dirigida al jefe del departamento de TIC'S de la Pontificia Universidad Católica del Ecuador "Sede Esmeraldas" con la finalidad de recolectar información que sea de ayuda para mi trabajo investigativo de la tesis que estoy desarrollando. Cuyo objetivo principal es la obtención del título de Ingeniera en Sistemas y Computación.

1.- ¿Qué tipo de Arquitectura de red tiene la institución?

La red de la universidad actualmente está separada en dos segmentos una para los estudiantes y otra para la parte administrativa, pero actualmente se está modificando con VLAN para evitar doble infraestructura

.

2.- ¿Qué seguridad tiene la red de la Universidad libre o pagado?

Cuenta con un sistema de antivirus que está en cada punto final que es pagado, seguridades en los servidores (configuración) por medio de contenedores, está aislado es libre por la utilización de Docker, cuentan con Mikrotik es el ruteador principal y el firewall que está incluido en el paquete de Mikrotik.

3.- ¿La red de la PUCESE tiene DMZ?

Si tienes dos áreas separadas por los servidores, la primera para los servicios generales de la universidad y otro para pruebas.

4.- ¿El internet de la Universidad cuenta con un balanceo de cargas?

No solo se tiene un enlace por medio de las fibras y por el momento no se necesita.

5.- ¿Para el ingreso a los servidores se lo hace por medio de claves públicas o privadas?

Se tienen unas configuraciones, pero no se las tiene aseguradas con VPN para la encriptación, se está utilizando el sistema operativo base (proxy, citrix) para acceder a los servidores.

6.- ¿Con qué tipo de VPN cuenta la PUCESE?
No se tienen VPN, para los estudiantes hay tres enlaces para la administración de redes, donde el equipo del departamento tiene acceso en caso de una emergencia.

7.- ¿Cuántos servidores tiene la institución?
Físicamente se cuenta con 7 servidores en producción.

8.- ¿Cuentan con seguridades dependiente en el rol que se esté trabajando (estudiantes, docentes, administrativos)?
El acceso a servidores no solo como administrador con su seguridad, pero el acceso a las aplicaciones sí.

Anexo 2. Código para configuración Hardening.

```
yum -y install fail2ban
rpm -Uvh https://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-11.noarch.rpm
yum -y install fail2ban
sudo yum check-update
sudo yum update
sudo yum install fail2ban-firewalldyyiFAI
vi /etc/fail2ban/jail.local
vi /etc/fail2ban/jail_ssh.local
        [DEFAULT]
        bantime = 3600
        banaction = iptables-multiport
        [sshd]
        enabled = true
systemctl start fail2ban.service
firewall-cmd --direct --get-all-rules
fail2ban-client status
fail2ban-client status sshd
vi /etc/fail2ban/jail.conf
vi /etc/fail2ban/jail_ssh.local
        [DEFAULT]
        bantime = 3600
        banaction = iptables-multiport
        [sshd]
        enabled = true
        port = ssh
        logpath = %(sshd_log) s
systemctl start fail2ban.service
systemctl status fail2ban
journalctl -b -u fail2ban
fail2ban-client status
fail2ban-client status sshd
iptables -L -n
iptables -S
fail2ban-client set sshd unbanip x.x.x.x
```