Universidad Continental

FACULTAD DE INGENIERÍA

Escuela Académico Profesional de Ingeniería de Sistemas e Informática

Trabajo de Suficiencia Profesional

Implementación de una red virtualizada, empleando el sistema operativo Linux Centos para mejorar la seguridad y el control de acceso a internet, para la Empresa ASR Consultores EIRL

Rene Alejandro Zamudio Ariza

Para optar el Título Profesional de Ingeniero de Sistemas e Informática

Lima, 2023

Universidad Continental

DECLARACIÓN JURADA DE AUTENTICIDAD

Yo, RENE ALEJANDRO ZAMUDIO ARIZA, identificado(a) con Documento Nacional de Identidad No. 40618954, de la E.A.P. de Ingeniería de Sistemas e Informática de la Facultad de Ingeniería la Universidad Continental, declaro bajo juramento lo siguiente:

1. El trabajo de suficiencia profesional titulado: "Implementación de una red virtualizada, empleando el Sistema Operativo Linux CentOS para mejorar la seguridad y el control de acceso a internet, para la Empresa ASR CONSULTORES EIRL", es de mi autoría, la misma que presento para optar el Título Profesional de Ingeniero de Sistemas e Informática.
2. El trabajo de suficiencia profesional no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas, por lo que no atenta contra derechos de terceros.
3. El trabajo de suficiencia profesional es original e inédita, y no ha sido realizado, desarrollado o publicado, parcial ni totalmente, por terceras personas naturales o jurídicas. No incurre en autoplagio; es decir, no fue publicado ni presentado de manera previa para conseguir algún grado académico o título profesional.
4. Los datos presentados en los resultados son reales, pues no son falsos, duplicados, ni copiados, por consiguiente, constituyen un aporte significativo para la realidad estudiada.

De identificarse fraude, falsificación de datos, plagio, información sin cita de autores, uso ilegal de información ajena, asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a las acciones legales pertinentes.

4 de diciembre de 2023.

La firma del autor y del asesor obra en el archivo original
(No se muestra en este documento por estar expuesto a publicación)

TSP - ZAMUDIO ARIZA RENE ALEJANDRO

INFORME DE ORIGINALIDAD

28%	27%	2%	10%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.continental.edu.pe Fuente de Internet	6%
2	hdl.handle.net Fuente de Internet	4%
3	www.coursehero.com Fuente de Internet	2%
4	repository.ucc.edu.co Fuente de Internet	1%
5	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
6	es.libreoffice.org Fuente de Internet	1%
7	www.researchgate.net Fuente de Internet	1%
8	www.euroinnova.co Fuente de Internet	<1%
9	repository.unad.edu.co Fuente de Internet	

		<1 %
10	ojs.unemi.edu.ec Fuente de Internet	<1 %
11	Submitted to Universidad de Cartagena Trabajo del estudiante	<1 %
12	S. Asha Varma, K. Ganesh Reddy. "An AI Based IDS Framework For Detecting DDoS Attacks In Cloud Environment", Information Security Journal: A Global Perspective, 2023 Publicación	<1 %
13	journal.poligran.edu.co Fuente de Internet	<1 %
14	cybertesis.uni.edu.pe Fuente de Internet	<1 %
15	www.scilit.net Fuente de Internet	<1 %
16	repositorio.ucv.edu.pe Fuente de Internet	<1 %
17	pe.jooble.org Fuente de Internet	<1 %
18	alfapublicaciones.com Fuente de Internet	<1 %
19	Submitted to National University College - Online	<1 %

Trabajo del estudiante

20	sol.sbc.org.br Fuente de Internet	<1 %
21	www.isaca.org Fuente de Internet	<1 %
22	revistas.unisimon.edu.co Fuente de Internet	<1 %
23	Submitted to Pontificia Universidad Catolica del Ecuador - PUCE Trabajo del estudiante	<1 %
24	Submitted to Universidad de Burgos UBUCEV Trabajo del estudiante	<1 %
25	usermanual.wiki Fuente de Internet	<1 %
26	risti.xyz Fuente de Internet	<1 %
27	multicom.com.ar Fuente de Internet	<1 %
28	worldwidescience.org Fuente de Internet	<1 %
29	core.ac.uk Fuente de Internet	<1 %
30	ctscafe.pe Fuente de Internet	<1 %

31	Submitted to Colorado State University, Global Campus Trabajo del estudiante	<1 %
32	repositorio.ug.edu.ec Fuente de Internet	<1 %
33	revistas.utp.edu.co Fuente de Internet	<1 %
34	Submitted to Columbia Central University Trabajo del estudiante	<1 %
35	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
36	Submitted to consultoriadeserviciosformativos Trabajo del estudiante	<1 %
37	polipapers.upv.es Fuente de Internet	<1 %
38	vdoc.pub Fuente de Internet	<1 %
39	www.firma-e.com Fuente de Internet	<1 %
40	pe.jobsyd.com Fuente de Internet	<1 %
41	cdn.www.gob.pe Fuente de Internet	<1 %

42	riunet.upv.es Fuente de Internet	<1 %
43	www.slideshare.net Fuente de Internet	<1 %
44	ciberinseguro.com Fuente de Internet	<1 %
45	dokumen.pub Fuente de Internet	<1 %
46	teknologico.net Fuente de Internet	<1 %
47	la.regions.comsoc.org Fuente de Internet	<1 %
48	learn.microsoft.com Fuente de Internet	<1 %
49	revistas.uco.edu.co Fuente de Internet	<1 %
50	"Inter-American Yearbook on Human Rights / Anuario Interamericano de Derechos Humanos, Volume 2 (1986)", Brill, 1988 Publicación	<1 %
51	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1 %
52	Submitted to Universidad Internacional del Ecuador	<1 %

Trabajo del estudiante

53	www.anarchistfederation.net Fuente de Internet	<1 %
54	dl.dell.com Fuente de Internet	<1 %
55	fr.slideshare.net Fuente de Internet	<1 %
56	tesis.pucp.edu.pe Fuente de Internet	<1 %
57	docplayer.es Fuente de Internet	<1 %
58	documentop.com Fuente de Internet	<1 %
59	es.slideshare.net Fuente de Internet	<1 %
60	pesquisa.bvsalud.org Fuente de Internet	<1 %
61	pt.slideshare.net Fuente de Internet	<1 %
62	tesis.ipn.mx Fuente de Internet	<1 %
63	www.cesel.com.pe Fuente de Internet	<1 %

64	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	<1 %
65	dblp.dagstuhl.de Fuente de Internet	<1 %
66	doczz.es Fuente de Internet	<1 %
67	dokumen.tips Fuente de Internet	<1 %
68	elm.cojusd.org Fuente de Internet	<1 %
69	foundstone.com.au Fuente de Internet	<1 %
70	issuu.com Fuente de Internet	<1 %
71	openigo.com Fuente de Internet	<1 %
72	repositorio.utn.edu.ec Fuente de Internet	<1 %
73	revistas.ufps.edu.co Fuente de Internet	<1 %
74	www.bib.ub.es Fuente de Internet	<1 %
75	www.classcentral.com	

	Fuente de Internet	<1 %
76	www.ivpressonline.com Fuente de Internet	<1 %
77	www.mediummultimedia.com Fuente de Internet	<1 %
78	www.sena.edu.co Fuente de Internet	<1 %
79	www.spa.gba.gov.ar Fuente de Internet	<1 %
80	Submitted to Corporación Universitaria Minuto de Dios, UNIMINUTO Trabajo del estudiante	<1 %
81	doaj.org Fuente de Internet	<1 %
82	humano2.com Fuente de Internet	<1 %
83	medium.com Fuente de Internet	<1 %
84	noticiaslogisticaytransporte.com Fuente de Internet	<1 %
85	repositorio.unap.edu.pe Fuente de Internet	<1 %
86	repositorioacademico.upc.edu.pe Fuente de Internet	

		<1 %
87	www.alfa-redi.com Fuente de Internet	<1 %
88	www.arcoiris.iiesa.es Fuente de Internet	<1 %
89	www.ausejo.net Fuente de Internet	<1 %
90	www.comfama.com.co Fuente de Internet	<1 %
91	www.comunidadstartup.com Fuente de Internet	<1 %
92	www.fao.org Fuente de Internet	<1 %
93	www.grafiati.com Fuente de Internet	<1 %
94	www.info-magazine.net Fuente de Internet	<1 %
95	www.quobis.com Fuente de Internet	<1 %
96	www.reddit.com Fuente de Internet	<1 %
97	www.scribd.com Fuente de Internet	<1 %

98	www.ulpiano.com Fuente de Internet	<1 %
99	www.villanuevawireless.net Fuente de Internet	<1 %
100	es.unionpedia.org Fuente de Internet	<1 %
101	dspace.ucuenca.edu.ec Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

AGRADECIMIENTO

A Dios, a mi familia, a mis amigos y a la universidad Continental, por darme la oportunidad de poder titularme como ingeniero.

Al Mg. Edson Raúl Lazo Álvarez, asesor del presente informe de trabajo de suficiencia profesional, por su colaboración y orientación.

DEDICATORIA

El presente trabajo de suficiencia profesional en principio se lo dedico a mi amada esposa quien siempre me alienta a avanzar en mis metas y proyectos, en segundo lugar, mis hijos que son mi mayor orgullo y el motor para seguir avanzado.

Universidad Continental

INDICE

Universidad Continental

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo se desarrolló en la empresa ASR CONSULTORES EIRL, la cual se sitúa en la ciudad de Lima, distrito de San Isidro.

En la actualidad, la estabilidad de la red de Internet se ha vuelto fundamental para el funcionamiento eficiente de la sociedad en su conjunto. Con la creciente dependencia de la tecnología y la digitalización de nuestras vidas, la estabilidad de la red se ha convertido en un factor crítico en numerosos aspectos, desde el comercio y la comunicación hasta la educación y la salud.

La estabilidad de la red de Internet se refiere a su capacidad para mantener un rendimiento consistente y confiable en términos de velocidad de conexión, disponibilidad y capacidad de respuesta. Cuando la red es inestable, se producen interrupciones en el servicio, lo que puede tener consecuencias negativas significativas.

La estabilidad de la red de Internet es esencial para la comunicación. La mayoría de las formas de comunicación moderna, como las llamadas de voz sobre IP (VoIP), las videoconferencias y las aplicaciones de mensajería instantánea, dependen de una conexión estable. Las interrupciones o la calidad deficiente del servicio pueden dificultar la comunicación efectiva, tanto a nivel personal como empresarial.

ABSTRACT

This assignment was developed in the company ASR CONSULTORES EIRL, located in the district of San Isidro (Lima, Peru).

Nowadays, the stability of the internet network has become a fundamental aspect of the efficient functioning of society as a whole. With the increase in technology dependence and digitization of our lives, network stability has become critical in numerous aspects, from commerce and communication to education and health.

Internet network stability refers to its ability to maintain consistent and reliable performance in terms of connection speed, availability, and responsiveness. When the network is unstable, there are several service interruptions, which can bring negative consequences.

Internet network stability is essential for modern communication. Most of its ways, such as voice-over IP (VoIP) calls, video conferencing, and instant messaging applications, depend on a stable connection. Interruptions or poor quality of service can hinder effective communication at a personal and business level.

INTRODUCCIÓN

El presente trabajo se desarrolló en la empresa ASR CONSULTORES EIRL, la cual se sitúa en la ciudad de Lima; tuvo como objetivo la implementación de una red de gestión perimétrica para el negocio, utilizando un Sistemas Operativos Open Source (CentOS/Debian Linux), esto permitió que con el tiempo se tenga un servicio de comunicación estable con un crecimiento sostenido en puestos de trabajos.

El contar con un sistema eficiente de comunicaciones, permitió que con la llegada de la pandemia la empresa no se vea perjudicada, logrando así que los trabajadores puedan realizar sus actividades laborales con el estatus de home Office al 100% y no se vea afectada en sus actividades con él negocio.

Teniendo en cuenta lo antes mencionado, se podría considerar que el trabajo realizado previamente en la seguridad de las redes permitió tener una gestión de las comunicaciones de manera eficiente, estable y escalable.

CAPÍTULO I

1 ASPECTOS GENERALES DE LA EMPRESA Y/O INSTITUCIÓN

En el presente capítulo, se detallan información general, de las principales actividades, así como la reseña histórica, misión, visión y valores de la empresa ASR CONSULTORES EIRL, de igual manera se describirán algunos procesos internos de competencia de competencia del área de TI

1.1 DATOS GENERALES DE LA INSTITUCIÓN

La empresa ASR CONSULTORES es una empresa individual de responsabilidad limitada (EIRL), fue fundada en agosto del año 2010, en el distrito de Lima, provincia de Lima, es una empresa que tiene más de 12 años de experiencia en el rubro de procesamiento de datos.

1.2 ACTIVIDADES PRINCIPALES DE LA INSTITUCIÓN Y/O EMPRESA

1.2.1 Procesamiento de datos

ASR Consultores es una empresa que realiza actividades de procesamiento de datos y cumple con las 3 actividades de rigurosidad solicitadas por el principal cliente que tiene.

1.2.2 Recopilación de datos

El procesamiento y análisis de datos parte recopilando los datos de las fuentes de almacenamiento que estén disponibles y que contengan información de calidad.

Estas fuentes pueden estar compuestas por ejemplo de un almacén de datos o de un data lake.

El segundo, es un almacén centralizado de información del big data de diversas fuentes que pueden estar o no estructuradas, con almacenamiento en la nube y con etiquetas de búsqueda.

1.2.3 Preparación de datos

En este punto comienza la preparación para su organización, la detección de errores y el descarte de información repetitiva e incompleta. De este modo, pasa a seleccionar la información necesaria y puntual con la que se trabajará para el procesamiento y análisis de datos.

1.2.4 Introducción de datos

Los datos ya seleccionados ahora son enviados a sus destinos correspondientes, traducidos a un lenguaje entendible y en los idiomas según requerimiento de los clientes.

A partir de aquí, los datos en bruto comienzan a tomar forma como información útil, que podrá visualizarse, por ejemplo, en un CRM o en un almacén de datos. Por ello también se define como el "preprocesamiento".

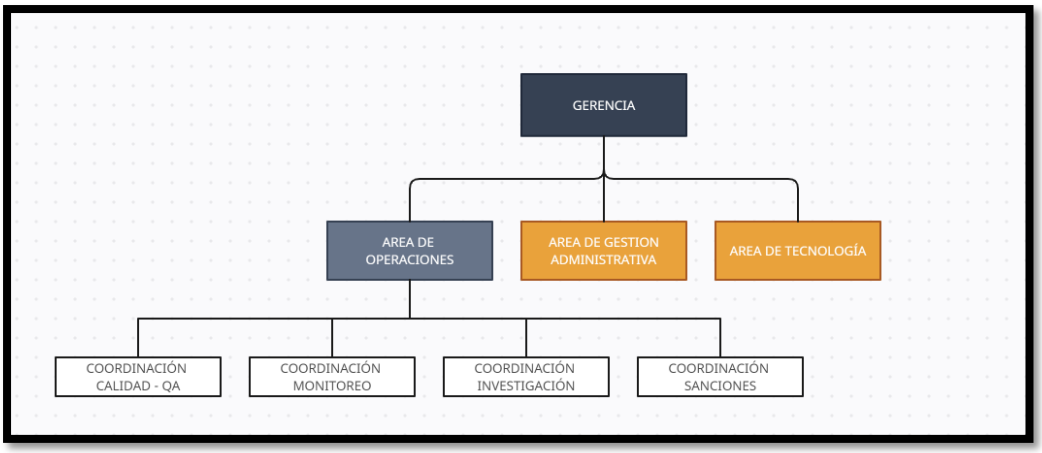
1.3 RESEÑA HISTÓRICA DE LA INSTITUCIÓN Y/O EMPRESA

La empresa ASR CONSULTORES es una empresa individual de responsabilidad limitada (EIRL), fue fundada en agosto del año 2010, en el distrito de Lima, provincia de Lima, es una empresa que tiene más de 12 años de experiencia en el rubro de procesamiento de datos.

Inicialmente la empresa se creó para digitalizar datos en un CRM global, al pasar los meses el requerimiento fue creciendo y acompañado de la buena calidad del entregable por parte del ASR Consultores, el cliente (Lexis Nexis) solicitó que se escale al siguiente nivel que correspondía a preparar al personal para realizar trabajos de procesamiento de datos.

1.4 ORGANIGRAMA DE LA INSTITUCIÓN Y/O EMPRESA

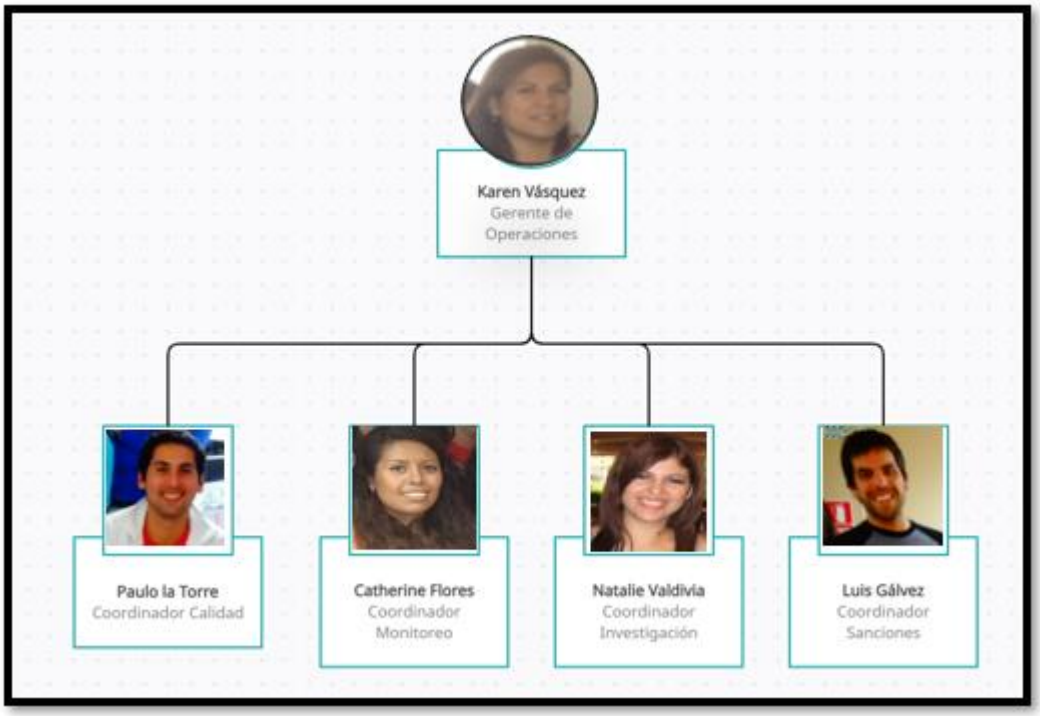
Ilustración 1 *Organigrama funcional: Asr Consultores EIRL*



Nota: Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023.

En la figura 1, se aprecia el organigrama conformado por la gerencia general y las áreas estratégicas del negocio, asimismo se podría indicar que las funciones del gerente generan es también administrador, las áreas de operaciones cumplen un rol de trabajo operativos bajo el mando de una Gerente de Operaciones, que a su vez tiene a cargo 4 líneas de trabajo operativos las cuales se verifican en el organigrama de la empresa.

Ilustración 2 *Organigrama vertical: ASR Consultores EIRL*



Nota: Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023.

En la figura 2, se muestra más a detalle el área de operación con sus respectivos responsables (Coordinadores), cabe resaltar que dicho equipo es el encargado de realizar las tareas de procesamiento de datos y revisión de calidad de los entregables.

1.5 VISIÓN, MISIÓN Y PROPÓSITO

1.5.1 Visión:

Ser una empresa líder en el mercado global de investigación de datos, elegida por nuestras soluciones y servicios, y reconocida por la calidad de nuestro trabajo.

1.5.2 Misión:

Ser la mejor empresa en servicios de investigación a nivel global, ofreciendo la máxima calidad en los servicios digitales y productividad óptima para satisfaciendo las necesidades del mercado, brindando los mejores servicios diferenciados por calidad y eficiencia.

1.5.3 Propósito:

Brindar seguridad en temas de cumplimiento legal, ayudar a la sociedad creando un entorno de seguridad dando fiabilidad a las áreas requeridas sobre transacciones y relaciones comerciales, estableciendo marcos seguros para las relaciones internacionales y nacionales a clientes globales.

1.6 BASES LEGALES O DOCUMENTOS ADMINISTRATIVOS

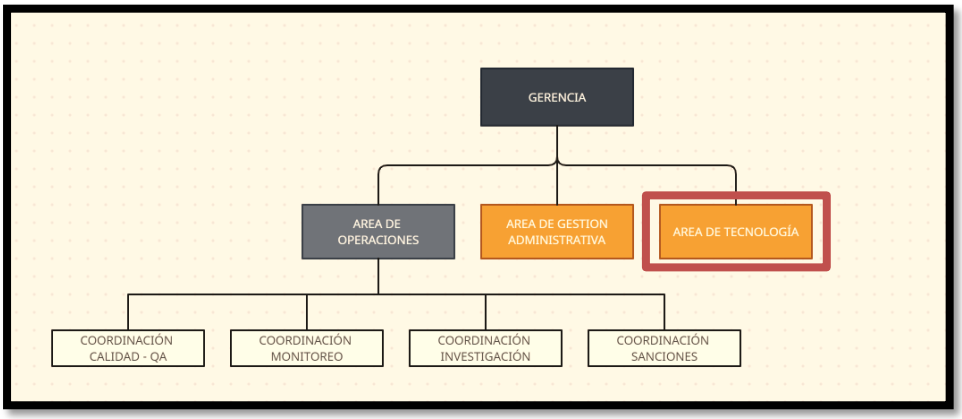
Ilustración 3 *Consulta RUC*

Resultado de la Búsqueda			
Número de RUC:	20537232090 - ASR CONSULTORES E.I.R.L.		
Tipo Contribuyente:	EMPRESA INDIVIDUAL DE RESP. LTDA		
Nombre Comercial:	-		
Fecha de Inscripción:	26/08/2010	Fecha de Inicio de Actividades:	05/10/2010
Estado del Contribuyente:	ACTIVO		
Condición del Contribuyente:	HABIDO		
Domicilio Fiscal:	JR. ICA NRO. 270 DPTO. 202 LIMA - LIMA - LIMA		
Sistema Emisión de Comprobante:	MANUAL	Actividad Comercio Exterior:	SIN ACTIVIDAD
Sistema Contabilidad:	MANUAL/COMPUTARIZADO		
Actividad(es) Económica(s):	Principal - 6311 - PROCESAMIENTO DE DATOS, HOSPEDAJE Y ACTIVIDADES CONEXAS Secundaria 1 - 6399 - OTRAS ACTIVIDADES DE SERVICIOS DE INFORMACIÓN N.C.P. Secundaria 2 - 6209 - OTRAS ACTIVIDADES DE TECNOLOGÍA DE LA INFORMACIÓN Y DE SERVICIOS INFORMÁTICOS		
Comprobantes de Pago c/aut. de impresión (F. 806 u 816):	NINGUNO		
Sistema de Emisión Electrónica:	FACTURA PORTAL DESDE 28/03/2018		
Emisor electrónico desde:	28/03/2018		
Comprobantes Electrónicos:	FACTURA (desde 28/03/2018)		
Afiliado al PLE desde:	01/01/2015		
Padrones:	NINGUNO		
Fecha consulta: 04/06/2023 12:41			

Nota: Tomado de SUNAT por la empresa ASR Consultores EIRL. 2023.

1.7 DESCRIPCIÓN DEL ÁREA DONDE REALIZA SUS ACTIVIDADES PROFESIONALES

Ilustración 4 *Organigrama funcional: ASR Consultores EIRL - Órgano de Apoyo TI*



Nota: Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023.

El área de tecnología, también denominada área de TI es un órgano de apoyo que realiza tareas de soporte a usuarios de forma presencial y remota, tiene personal que desarrolla actividades para esa finalidad, asimismo cuenta con personal que está revisando constantemente las redes de comunicaciones, estas redes de comunicaciones permiten al equipo de operaciones realizar su tarea de manera eficiente y sin incidencias.

1.8 DESCRIPCIÓN DEL CARGO Y DE LAS RESPONSABILIDADES DEL BACHILLER EN LA INSTITUCIÓN Y/O EMPRESA.

1.8.1 Descripción del cargo:

Cargo: Jefe del área de Tecnología.

Unidad: Área de Tecnología de la Información (TI).

Línea de dependencia: Gerencia General.

1.8.2 Responsabilidades del cargo:

La siguiente lista hace referencia a las principales funciones del puesto de jefe responsable del área

de Tecnología de la información.

- Planificar, organizar, controlar, desarrollar y evaluar las operaciones relacionadas a los servicios internos de comunicación (redes de internet, redes internas).
- Diseñar, desarrollar y evaluar los sistemas informáticos, así como también los procedimientos para su uso.
- Administrar la seguridad y el acceso a los recursos de tecnología de la empresa
- Dirigir y evaluar las actividades realizadas por el personal a su cargo y, en especial, las actividades ejecutadas por el personal de soporte técnico informático.
- Mantener la operatividad y disponibilidad de los sistemas de información y servicios basados en Tecnología de Información y Comunicaciones.
- Supervisar el cumplimiento de las políticas internas del área y las políticas informáticas de la empresa.
- Coordinar y hacer seguimiento al plan de mantenimiento anual
- Coordinar y hacer seguimiento al plan de desarrollo de la empresa
- Investigar y evaluar tecnologías aplicables a la empresa para la mejora de procesos, innovación o transformación digital de cada necesidad
- Dar tratamiento y cerrar a los casos reportados por los usuarios en la herramienta de HelpDesk
- Gestionar y administrar el funcionamiento de las redes, su disponibilidad y seguridad

CAPÍTULO II

2 ASPECTOS GENERALES DE LAS ACTIVIDADES PROFESIONALES

Teniendo en cuenta las crecientes actividades y solicitudes por parte del cliente, se tuvo a bien considerar un mejoramiento de las redes computacionales, este mejoramiento permitiría a la organización permitirse realizar un escalamiento según la necesidad del cliente.

2.1 ANTECEDENTES O DIAGNÓSTICO SITUACIONAL

Para dar inicio a las actividades se tuvo que realizar un estudio situacional dado que la red de la organización era extremadamente básica, se contaba con 2 servicios de internet del proveedor American Móvil (Claro); un servicio era de casa y se tenía 60 MB del cual, el proveedor garantizaba solo el 40% de descarga, así como un 10% de carga, el otro servicio era de internet de negocios de 20 MB el cual estaba garantizado un 50% de descarga y un 30% de carga, se agrega un cuadro para mayor detalle.

Ilustración 5 *Tabla de ISP contratado*

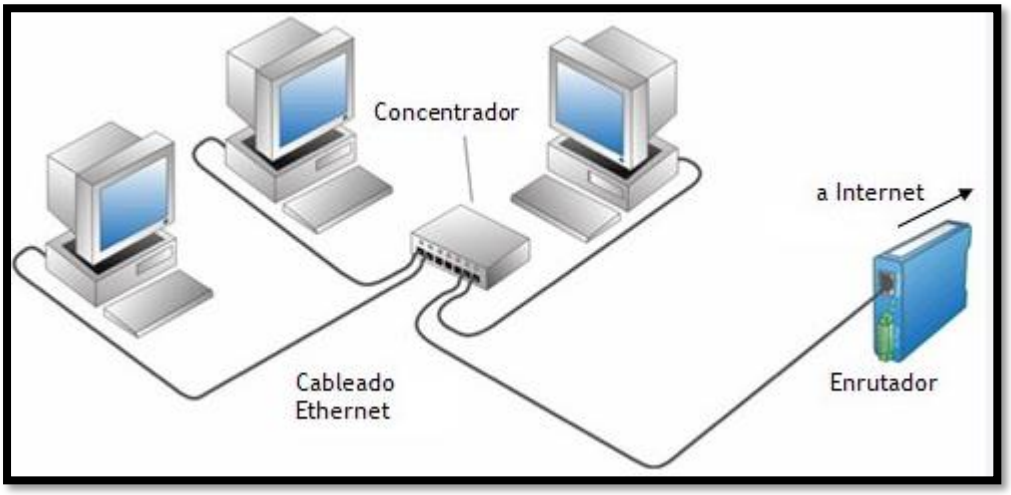
VELOCIDAD CONTRATADA			
		SERVICIO GARANTIZADO	
	SERVICIO CONTRATADO	DESCARGA	CARGA
ISP CLARO	60MB	24 MB	6 MB
ISP CLARO NEGOCIO	20 MB	10 MB	6MB

Nota: Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023.

Este hecho generaba una constante intermitencia en el servicio de navegación y hasta se tenía perdidas de conexión por varias horas.

Adicionalmente se tenía una red sin protección interna (firewall), era un esquema de trabajo muy básico como se muestra en la imagen:

Ilustración 6 *Esquema de Red inicial*



Nota: Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023.

Teniendo en cuenta que la empresa había estado operando de esa forma durante los años 2010 al 2014, y dado que hasta ese momento su operación era pequeña no se había notado mucho la problemática que se presentaba en la red interna.

Para el año 2014 la empresa tomo la decisión de adquirir unos equipos Core I7 de 3ra generación que para ese momento eran equipamiento top, adicionalmente compraron un servidor HP, lo que permitió esquematizar una solución que permita un escalamiento progresivo a corto y mediano plazo.

2.2 IDENTIFICACIÓN DE OPORTUNIDAD O NECESIDAD EN EL ÁREA DE ACTIVIDAD PROFESIONAL

Como se detalla en el punto anterior, la empresa en principio no contaba con un área de soporte técnico permanente, tampoco había control de la data que se manejaba hasta ese momento, todo se cargaba en el CRM del cliente mediante el acceso por IP.

No se tenía equipos de seguridad informática como firewall.

No se contaba con un sistema gestor de accesos como un directorio activo.

No se contaba con un servicio de internet propicio para el tipo de trabajo que se realizaba.

No se tenía una solución de negocio acorde a las exigencias del mercado actual.

No se tenía el mantenimiento preventivo de los equipos de cómputo en los plazos que correspondían.

2.3 OBJETIVOS DE LA ACTIVIDAD PROFESIONAL

2.3.1 OBJETIVO GENERAL

- Implementación de las redes de telecomunicaciones, empleando tecnología Open Source (Linux CentOS/Debian).

2.3.2 OBJETIVO ESPECÍFICO

- Implementar un servidor Linux que gestione sistemas virtualizados.
- Implementar sistemas firewall virtualizados para la red interna para operaciones y red de visita.
- Implementar un sistema de red perimetral basado en sistemas Linux Open Source para la conexión presencial y remota.
- Gestionar el mantenimiento preventivo de los dispositivos de cómputo de la empresa.
- Monitorear la red.
- Generar la migración a un servicio de internet propicio acorde a la nueva estructura de trabajo.

2.4 JUSTIFICACIÓN DE LA ACTIVIDAD PROFESIONAL

2.4.1 TEÓRICA

La justificación teórica de los niveles de seguridad en Linux se basa en la implementación de una serie de mecanismos y políticas diseñadas para proteger el sistema operativo y los datos contra

amenazas y ataques maliciosos. Estos niveles de seguridad se establecen para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para prevenir el acceso no autorizado y la manipulación indebida de los recursos del sistema.

El presente trabajo de suficiencia profesional tiene la finalidad de crear los mecanismos y políticas, como el control de acceso obligatorio, los permisos de usuario y grupos, la autenticación, el cifrado, las actualizaciones de seguridad y la auditoría.

2.4.2 PRÁCTICA

El desarrollo de este proyecto permitió generar una mejora sustancial en el funcionamiento de la red, creando una red sólida y estable, esto generó un crecimiento importante para el negocio.

2.4.3 METODOLÓGICA

El presente trabajo de suficiencia profesional es de tipo descriptivo y mostrará paso a paso como se desarrolló la implementación de la red de telecomunicación de la empresa Asr Consultores.

2.4.4 ECONÓMICA

Con la identificación de la problemática y la posterior implementación de la red de negocios, ha generado en la empresa ASR Consultores un crecimiento sostenido importante, esto permitió a un corto plazo poder cumplir con la necesidad del cliente de ASR Consultores y de este modo lograr obtener más posiciones de trabajo generando un incremento de puestos laborales lo que permitió duplicar su fuerza laboral y productividad.

2.4.5 SOCIAL

Con la implementación de la nueva red, ASR Consultores se permitió solicitar un incremento de actividades al cliente, lo que generó nuevos puestos laborales tanto en los campos de operaciones como en el área de TI.

2.4.6 TECNOLÓGICA

La implementación de la red bajo el esquema de un sistema Open Source (Linux), ha representado una mejora tecnológica en ASR Consultores, generando estabilidad y seguridad, algo que se requería para el tratamiento de datos según necesidad del cliente de ASR Consultores.

2.5 RESULTADOS ESPERADOS

Los resultados esperados en relación con las redes de ASR Consultores fueron los siguientes:

- Cumplir 100% con la instalación del SO Linux CentOS
- Montar al 100% sobre el sistema operativo los servicios virtualizados de firewall intranet, firewall redes compartidas, sistema de chat local y servicios DHCP.
- Disponer de información para que la organización pueda tomar la decisión de contratar un servicio de internet simétrico.
- Lograr tener alta disponibilidad de servicio de internet sin cortes de conexión o intermitencias.
- Escalamiento de conectividad hasta en un 200% (la red con problemas solo estaba habilitado para 20 estaciones host, hoy en día tenemos 50 estaciones conectadas ocupando un ancho de banda promedio de 20MB y contando con un servicio contratado de hasta 100MB simétricos.)

Teniendo en cuenta lo antes mencionado, se puede indicar que el plan de mejoramiento de la red de ASR Consultores, ha logrado una mejora fundamental, lo que permite que la organización pueda realizar su trabajo operativo con eficiencia y eficacia, generando así un incremento de productividad en las áreas de producción.

CAPÍTULO III:

3 MARCO TEÓRICO

Este capítulo se basa en una combinación de principios, tecnologías y prácticas diseñadas para proteger los sistemas operativos de Windows y Linux de amenazas y ataques maliciosos. Aquí hay algunos aspectos clave del marco teórico de seguridad en Linux.

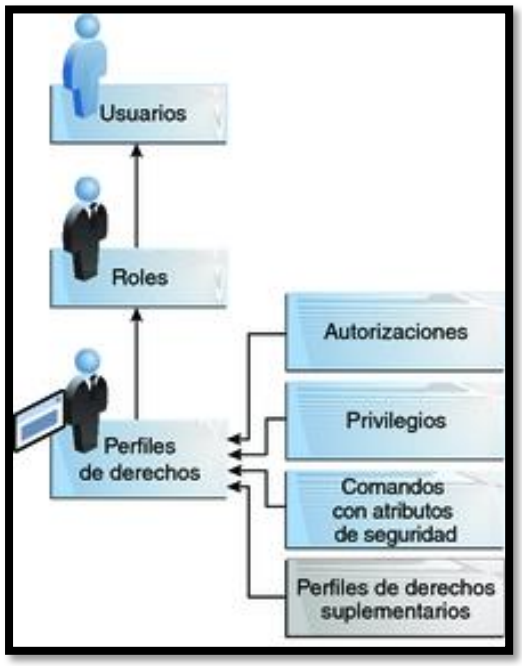
3.1 BASES TEÓRICAS DE LAS METODOLOGÍAS O ACTIVIDADES REALIZADAS

3.1.1 Modelo de seguridad basado en privilegios:

La gestión de la seguridad basada en los comportamientos es un proceso que ha demostrado ser efectivo en la mejora de la seguridad en las organizaciones (Oropesa, 2015). Este enfoque se centra en promover comportamientos seguros entre los usuarios y fomentar una cultura de seguridad en toda la organización. Al implementar un modelo de seguridad basado en privilegios en Linux, se pueden establecer políticas y controles que refuercen los comportamientos seguros y limiten los accesos y acciones de los usuarios según sus privilegios asignados.

Teniendo en cuenta lo antes mencionado Linux utiliza un modelo de seguridad basado en privilegios conocido como Modelo de Control de Acceso Discrecional (DAC). En este modelo, los usuarios y procesos tienen diferentes niveles de privilegios y el acceso a los recursos del sistema se controla mediante permisos y políticas de seguridad. Los usuarios administrativos tienen privilegios elevados (root) que les permiten realizar acciones que los usuarios normales no pueden.

Ilustración 7 *Esquema de usuarios y roles*



Nota: La imagen representa el esquema de privilegios de seguridad basado en roles de usuario.

3.1.2 Separación de privilegios:

En el contexto de Linux, existen varias técnicas y enfoques para lograr la separación de privilegios. Una de ellas es el Control de Acceso Basado en Roles (RBAC), que es un modelo de control de acceso que asigna roles a los usuarios y define qué acciones pueden realizar los usuarios en función de sus roles. El modelo RBAC también puede implementar la Separación de Deberes (SoD), que es una restricción que evita que un usuario tenga permisos que puedan conducir a un conflicto de intereses.

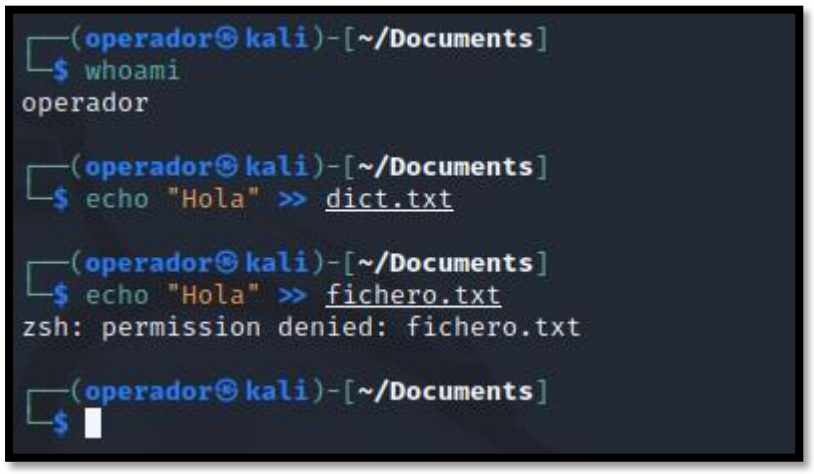
Otro enfoque para la separación de privilegios en Linux es el uso de módulos de seguridad del kernel. Estos módulos permiten al administrador del sistema restringir las capacidades de los programas mediante perfiles específicos. Por ejemplo, se pueden permitir o denegar ciertas capacidades, como el acceso a la red o la lectura/escritura de archivos, en función de rutas específicas.

Además, se ha propuesto la combinación de confianza y riesgo en la toma de decisiones de control de acceso para equilibrar la accesibilidad a la información y la protección de esta. Esto implica tomar decisiones de control de acceso en función de la confiabilidad de los usuarios y el valor de riesgo de los permisos. Este enfoque puede proporcionar más oportunidades de acceso a usuarios confiables y, al mismo tiempo, hacer cumplir las restricciones tradicionales de control de acceso.

Es importante destacar que la seguridad en Linux no se limita solo a la separación de privilegios. También se han investigado y propuesto otros enfoques y técnicas para mejorar la seguridad en sistemas Linux, como la detección de ataques de escalada de privilegios en aplicaciones de Android, el desarrollo de sistemas operativos de plano de datos de alto rendimiento y eficiencia, y la mejora de la seguridad en sistemas de control industrial.

Linux utiliza el principio de separación de privilegios para limitar el alcance de los ataques. Los servicios y aplicaciones se ejecutan con los privilegios mínimos necesarios para realizar sus funciones, lo que ayuda a reducir el impacto de posibles vulnerabilidades.

Ilustración 8 *Principio de separación de privilegios*



Nota: La separación de privilegios, limita el alcance de los ataques.

3.1.3 Sistema de archivos seguro:

Una de las herramientas utilizadas para proteger los archivos en sistemas Linux es SecBox. SecBox

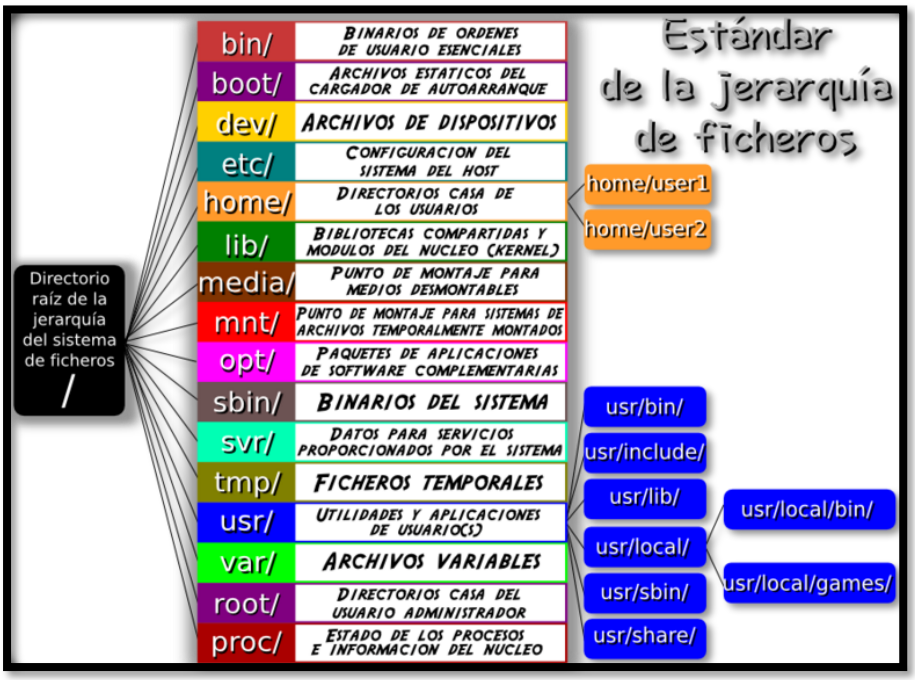
es una solución alternativa que utiliza una combinación de algoritmos de criptografía y esteganografía para proteger los archivos de sistema y multimedia en set-top boxes con Linux (Carvalho et al., 2007). Esta herramienta puede prevenir ataques a los dispositivos de almacenamiento y la piratería digital.

Además, los sistemas de control de versiones son aplicaciones que ayudan en el proceso de desarrollo de software y también pueden contribuir a la seguridad de los archivos en Linux. Estos sistemas facilitan la gestión del control de versiones de los archivos de código fuente generados por los desarrolladores, permitiendo la fusión y generación de nuevas versiones de un proyecto y evitando la pérdida de datos o bloqueos de archivos (Tello-Leal et al., 2012).

En cuanto a la interfaz gráfica de las distribuciones Linux, a diferencia de los sistemas operativos Microsoft Windows y MacOS, las distribuciones Linux permiten a los usuarios elegir el proyecto de interfaz gráfica más adecuado para su uso (Vieira & Seabra, 2023). Algunas de las interfaces gráficas más populares en Linux incluyen KDE Plasma, Cinnamon, Gnome y Pantheon Desktop. La usabilidad de estas interfaces gráficas ha sido evaluada utilizando la metodología de evaluación de "prueba de usabilidad" y los criterios definidos en la norma ISO 9241-11, y se ha encontrado que KDE Plasma tiene la mejor usabilidad entre las interfaces evaluadas (Vieira & Seabra, 2023).

Linux utiliza un sistema de archivos seguro con controles de acceso a nivel de archivo y directorio. Los permisos de archivo y directorio, como lectura, escritura y ejecución, se pueden establecer para diferentes usuarios y grupos, lo que permite restringir el acceso no autorizado a archivos y directorios sensibles.

Ilustración 9 *Estándar de la jerarquía de ficheros*



Nota: Los permisos de archivo y directorio, como lectura, escritura y ejecución, se pueden establecer para diferentes usuarios y grupos.

3.1.4 Mecanismos de autenticación y control de acceso:

Uno de los mecanismos de autenticación más comunes en Linux es el uso de contraseñas. Los usuarios deben proporcionar una contraseña válida para acceder al sistema. Sin embargo, es importante tener en cuenta que el uso de contraseñas por sí solo puede no ser suficiente para garantizar una seguridad sólida. Por lo tanto, se recomienda implementar medidas adicionales, como la autenticación de dos factores, que combina el uso de contraseñas con otro factor de autenticación, como un token de seguridad o una huella dactilar (Pinto et al., 2017).

Además de las contraseñas, Linux también admite otros mecanismos de autenticación, como el uso de certificados electrónicos y tarjetas inteligentes. Estos mecanismos utilizan claves criptográficas para autenticar a los usuarios y proporcionar un nivel adicional de seguridad (Rodriguez & Páez, 2019).

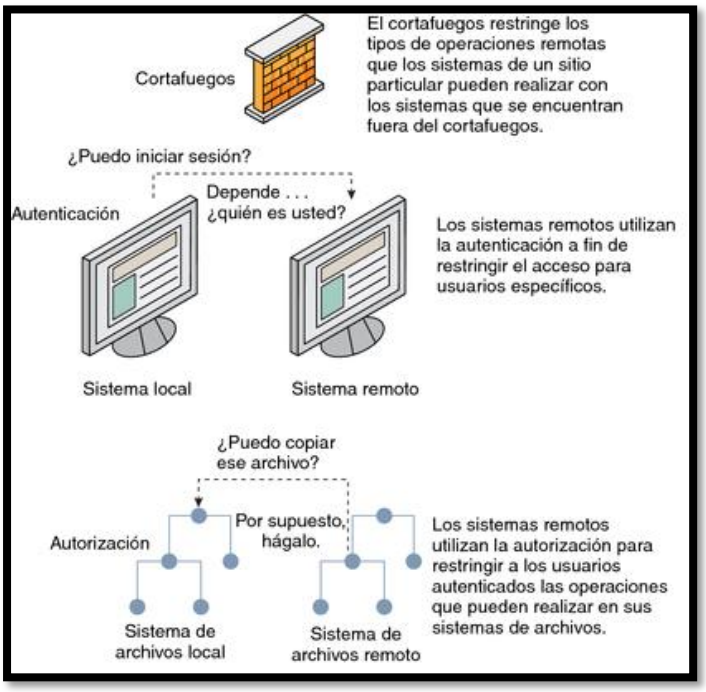
En cuanto al control de acceso, Linux ofrece varias opciones. Una de ellas es el uso de listas de control de acceso (ACL), que permiten especificar permisos detallados para archivos y directorios. Esto permite controlar qué usuarios o grupos tienen acceso a qué archivos y qué acciones pueden realizar sobre ellos (Ramos & Días, 2015).

Otro mecanismo de control de acceso en Linux es el uso de roles y políticas de seguridad. Esto implica asignar roles a los usuarios y definir políticas que determinen qué acciones pueden realizar los usuarios en función de su rol. Esto ayuda a garantizar que los usuarios solo tengan acceso a los recursos y acciones que son necesarios para realizar sus tareas (Benavides & Castro, 2021).

Además, Linux también ofrece la posibilidad de implementar mecanismos de detección de intrusiones, como firewalls virtualizados, que pueden proteger contra ataques no autorizados y garantizar la integridad y confidencialidad de los datos (Narváez et al., 2021).

Linux proporciona mecanismos de autenticación sólidos, como contraseñas, claves SSH, certificados digitales, entre otros. Además, ofrece herramientas para configurar y administrar políticas de control de acceso, como el archivo /etc/sudoers, que permite otorgar privilegios de administrador a usuarios específicos de forma controlada.

Ilustración 10 *Esquema de mecanismos de autenticación*



Nota: Linux ofrece herramientas para configurar y administrar políticas de control de acceso, como el archivo /etc/sudoers.

3.1.5 Actualizaciones y parches:

Una forma común de actualizar Linux es a través de parches de seguridad. Estos parches se aplican al kernel de Linux para corregir vulnerabilidades conocidas y mejorar la seguridad del sistema (Garces et al., 2019). Por ejemplo, el parche RT_PREEMPT se utiliza para modificar el kernel de Android/Linux y proporcionar capacidades de tiempo real (Garces et al., 2019).

Además de los parches de seguridad, también se realizan actualizaciones para mejorar la funcionalidad y corregir errores en otros componentes de Linux. Por ejemplo, en el caso de Android, se pueden realizar modificaciones en el recolector de basura en la máquina virtual de Java para mejorar el rendimiento y la eficiencia del sistema (Garces et al., 2019).

Estas actualizaciones y parches se pueden aplicar en diferentes entornos de Linux, como máquinas que utilizan el sistema operativo Windows o UNIX (Fernández, 2011). Esto permite que los

usuarios de diferentes plataformas se beneficien de las mejoras y correcciones realizadas en Linux.

Es importante destacar que las actualizaciones y parches en Linux no solo se aplican al sistema operativo en sí, sino también a las aplicaciones y programas que se ejecutan en él. Por ejemplo, se pueden desarrollar aplicaciones Java para controlar equipos RB Mikrotik en empresas proveedoras de servicios de Internet, y estas aplicaciones pueden ser compiladas y ejecutadas en plataformas Windows y Linux (Alvarado et al., 2018).

Mantener el sistema operativo Linux actualizado es esencial para protegerlo contra nuevas vulnerabilidades y amenazas. Los proveedores de distribuciones de Linux suelen lanzar actualizaciones y parches de seguridad para corregir vulnerabilidades conocidas y mejorar la seguridad del sistema.

3.1.6 Firewalls y filtrado de paquetes:

Los cortafuegos y el filtrado de paquetes son componentes esenciales de la seguridad de la red, especialmente en los sistemas Linux. Los sistemas operativos basados en Linux se han basado durante mucho tiempo en el marco Netfilter, que incluye el filtro de paquetes iptables, como la herramienta de firewall más común (Melkov & Paulikas, 2021).

Iptables se ha utilizado ampliamente durante más de dos décadas y es capaz de filtrar paquetes, equilibrar la carga y otras manipulaciones de tráfico de red (Melkov & Paulikas, 2021).

En 2014, se introdujo el sucesor de iptables, llamado nftables, para superar algunas de las limitaciones de iptables (Melkov & Paulikas, 2021).

Sin embargo, nftables no ha ganado una gran popularidad y la transición de iptables a nftables aún está en curso (Melkov & Paulikas, 2021).

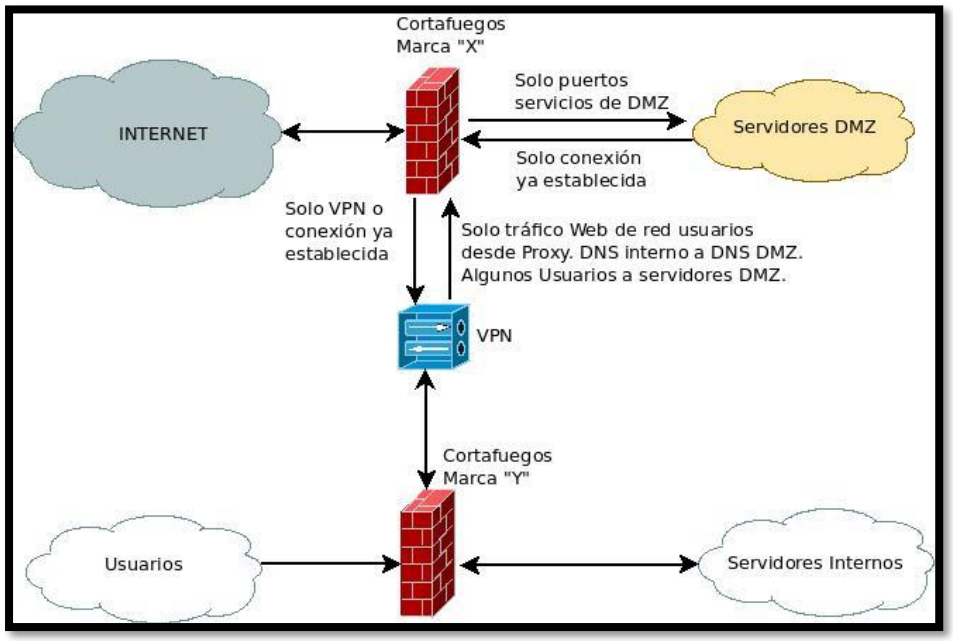
El marco de Netfilter, incluidas las iptables, se basa en el concepto de filtrado de paquetes, que implica examinar los encabezados de los paquetes de red y tomar decisiones sobre si permitirlos o

bloquearlos en función de reglas predefinidas (Chanu et al., 2022). Las reglas de filtrado configurables de IPtables en servidores Linux proporcionan una solución de firewall eficiente y de alto rendimiento (Chanu et al., 2022).

Estas reglas se pueden diseñar para centrarse en los parámetros estadísticos de los encabezados de los paquetes, lo que permite un control detallado sobre el tráfico de la red (Chanu et al., 2022). En los últimos años, los investigadores y desarrolladores han estado explorando formas de mejorar el rendimiento de las herramientas de procesamiento de paquetes en los sistemas Linux. Un enfoque es utilizar eBPF (Extended Berkeley Packet Filter) con ruta de datos XDP (Express Data Path) (Melkov & Paulikas, 2021).

XDP es un enfoque novedoso para el procesamiento de paquetes programables que permite que las aplicaciones de procesamiento de paquetes personalizadas se ejecuten en el propio kernel del sistema operativo proporcionando un entorno de ejecución seguro (Høiland-Jørgensen et al., 2018) Linux cuenta con herramientas integradas, como Netfilter y iptables, que permiten configurar reglas de firewall y filtrado de paquetes. Estas herramientas permiten controlar el tráfico de red y definir políticas de seguridad para proteger el sistema contra ataques de red.

Ilustración 11 *Esquema de cortafuegos*



Nota: Linux tiene herramientas que permiten controlar el tráfico de red y definir políticas de seguridad.

3.1.7 Auditoría y registros del sistema:

La auditoría y registros del sistema en Linux es un tema relevante en la gestión de la seguridad y el control de los sistemas operativos basados en Linux. La auditoría del sistema implica la recopilación y análisis de datos para evaluar la integridad, confidencialidad y disponibilidad de los recursos del sistema. Los registros del sistema son una parte fundamental de la auditoría, ya que proporcionan información detallada sobre las actividades y eventos que ocurren en el sistema.

En el contexto de la auditoría de sistemas de información en el ámbito de la salud, se destaca la importancia de los registros y los sistemas de información para la gerencia de los servicios de salud (Camarena, 2022). Los registros clínicos son auditados para evaluar la calidad del registro y la calidad de la atención médica (Camarena, 2022). Estas auditorías permiten verificar si se han registrado todos los antecedentes preestablecidos y si están legibles y de acuerdo con los estándares de calidad (Camarena, 2022). Además, se utilizan criterios de auditoría basados en normas y

estándares preestablecidos para evaluar la calidad de la atención médica (Camarena, 2022).

En el ámbito de la seguridad de redes inalámbricas, se han realizado auditorías en redes basadas en el protocolo IEEE 802.11xx utilizando software libre en sistemas operativos Linux (Ballesteros & Chaparro, 2016; Ballesteros & Chaparro, 2016). Estas auditorías se centran en verificar la seguridad de las redes inalámbricas y evaluar la efectividad de las medidas de seguridad implementadas, como la encriptación WEP y WPA (Ballesteros & Chaparro, 2016; Ballesteros & Chaparro, 2016). Se utilizan herramientas como Aircrack para realizar pruebas de seguridad, como ataques de denegación de servicio y autenticaciones falsas (Ballesteros & Chaparro, 2016; Ballesteros & Chaparro, 2016).

Linux ofrece herramientas de auditoría y registro del sistema, como el servicio syslog, que permiten registrar eventos de seguridad y monitorear el sistema en busca de actividades sospechosas. Estos registros son útiles para la detección de intrusiones y el análisis forense en caso de incidentes de seguridad.

3.1.8 Uso de herramientas de seguridad:

En el ámbito de la seguridad informática en Linux, existen diversas herramientas que pueden ser utilizadas para garantizar la protección de los sistemas y redes. Estas herramientas son fundamentales para prevenir y mitigar posibles ataques cibernéticos y vulnerabilidades en los sistemas operativos.

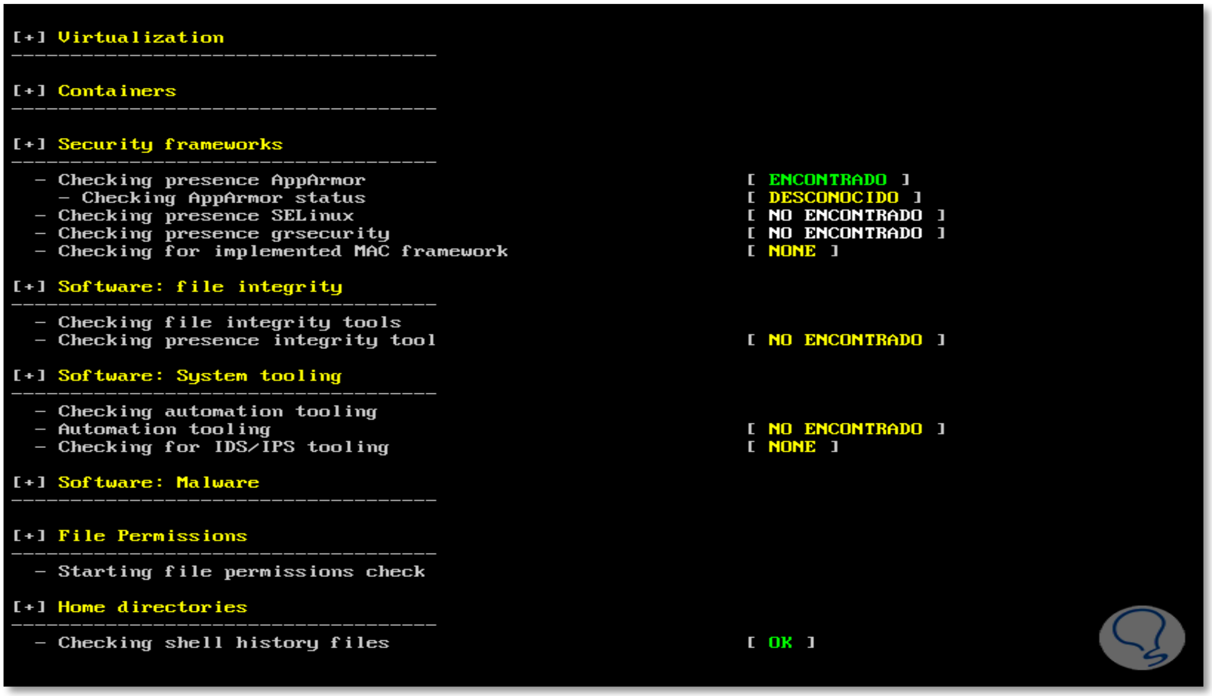
Una de las herramientas más utilizadas en Linux para evaluar la seguridad de los sistemas es Kali Linux. Kali Linux es una distribución de Linux especializada en pruebas de penetración y hacking ético. Esta herramienta proporciona una amplia gama de herramientas y utilidades que permiten identificar y explotar vulnerabilidades en los sistemas, como Maltego, Set Toolkit, Nmap, Armitage y Metasploit (Veloz et al., 2017).

Otra herramienta importante en el ámbito de la seguridad informática en Linux es VEGA. VEGA es una herramienta de análisis de seguridad web que permite identificar y mitigar vulnerabilidades en los servicios web. Esta herramienta utiliza la metodología MAGERIT para realizar el análisis de seguridad y proporciona resultados detallados sobre las vulnerabilidades encontradas (Fiallos et al., 2019).

Además, para garantizar la seguridad perimetral de una red, es fundamental implementar un sistema de seguridad que incluya una red privada virtual (VPN), un cortafuegos y un sistema de detección de intrusos (IDS). Estos componentes trabajan en conjunto para proteger la red de posibles ataques externos. La implementación de este sistema de seguridad perimetral puede realizarse utilizando herramientas disponibles en Linux, como OpenVPN para la VPN, iptables para el cortafuegos y Snort para el IDS (Valencia et al., 2020).

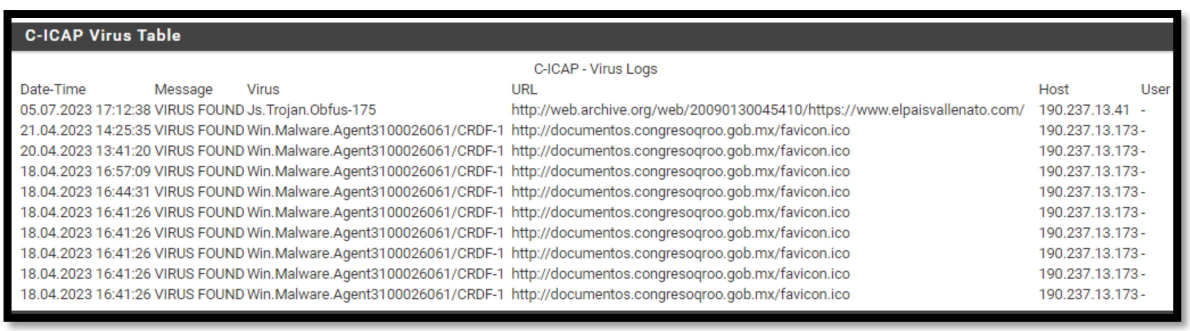
Existen numerosas herramientas de seguridad disponibles para Linux, como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS), antivirus, herramientas de escaneo de vulnerabilidades, entre otros. Estas herramientas pueden ayudar a fortalecer la seguridad del sistema y detectar posibles amenazas.

Ilustración 12 *Herramientas de seguridad disponibles para Linux*



Nota: Herramientas disponibles para Linux en virtualización, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 13 *C-IAP tabla de virus*



C-ICAP Virus Table

C-ICAP - Virus Logs

Date-Time	Message	Virus	URL	Host	User
05.07.2023 17:12:38	VIRUS FOUND	Js.Trojan.Obfus-175	http://web.archive.org/web/20090130045410/https://www.elpaisvallenato.com/	190.237.13.41	-
21.04.2023 14:25:35	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
20.04.2023 13:41:20	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:57:09	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:44:31	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-

Nota: Herramienta C-ICAP de Clav antivirus Linux, Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Es importante tener en cuenta que la seguridad en Linux es un tema complejo y en constante evolución. Además de estas medidas teóricas, es esencial seguir las mejores prácticas de seguridad, como la implementación de políticas.

El otro punto del marco teórico se trata de la seguridad de la información que se trata de un

conjunto de conceptos, principios y mejores prácticas diseñados para proteger la confidencialidad, integridad y disponibilidad de la información en diferentes entornos, como organizaciones, sistemas informáticos y redes.

A continuación, se presentan algunos elementos clave que suelen formar parte del marco teórico de seguridad de la información:

3.1.9 Triángulo de la seguridad de la información:

El triángulo de la seguridad de la información se compone de tres elementos principales: confidencialidad, integridad y disponibilidad. Estos tres aspectos deben equilibrarse y protegerse adecuadamente para garantizar la seguridad de la información.

Ilustración 14 *Triángulo de la seguridad informática*

- **Confidencialidad:** Se refiere a la protección de la información contra el acceso no autorizado. Los controles de seguridad, como el cifrado y la autenticación, se utilizan para preservar la confidencialidad de los datos.
- **Integridad**: Se relaciona con la protección de la información contra la modificación no

autorizada. Los mecanismos de integridad garantizan que los datos no sean alterados de manera no autorizada y se mantengan precisos y completos.

- **Disponibilidad**: Hace referencia a garantizar que la información esté disponible y accesible para aquellos usuarios autorizados que la necesitan. Esto implica proteger los sistemas y redes contra ataques y fallas que puedan interrumpir la disponibilidad de los servicios.

3.1.10 Principio de menor privilegio:

Este principio establece que los usuarios deben tener solo los privilegios necesarios para realizar sus tareas y que estos privilegios deben limitarse a lo mínimo requerido. Al restringir los privilegios, se reduce el riesgo de que los usuarios realicen acciones maliciosas o accedan a información sensible de manera indebida.

3.1.11 Modelo de defensa en profundidad:

Este modelo se basa en la idea de que una sola medida de seguridad no es suficiente para proteger completamente los sistemas y datos. Consiste en implementar múltiples capas de seguridad, como firewalls, sistemas de detección de intrusiones, antivirus y políticas de acceso, con el fin de aumentar la seguridad global y mitigar los riesgos.

3.1.12 Ciclo de vida de la seguridad de la información:

Este ciclo se compone de varias fases, que incluyen la identificación de activos de información, evaluación de riesgos, implementación de controles de seguridad, monitoreo y respuesta ante incidentes, y mejora continua. Este enfoque cíclico permite gestionar y mantener la seguridad de la información de manera efectiva a lo largo del tiempo.

3.1.13 Normas y marcos de referencia:

Existen diversos marcos y normas reconocidos internacionalmente que proporcionan directrices y

mejores prácticas para la seguridad de la información, como ISO 27001, NIST SP 800-53 y CIS Controls. Estos marcos ofrecen un enfoque estructurado para establecer y mantener un programa de seguridad de la información eficaz.

Estos son solo algunos elementos del marco teórico de seguridad de la información. Es importante destacar que la seguridad de la información es un campo amplio y en constante evolución, por lo que es fundamental mantenerse actualizado sobre las nuevas amenazas, tecnologías y mejores prácticas en este ámbito.

CAPÍTULO IV:

4 DESCRIPCIÓN DE LAS ACTIVIDADES PROFESIONALES

El trabajo de suficiencia profesional en un entorno de redes de comunicación implica una serie de actividades relacionadas con el diseño, implementación, mantenimiento y gestión de redes de comunicación. Estas actividades se centran en garantizar que las redes de comunicación sean eficientes, seguras y confiables para facilitar la transmisión de datos, voz y video entre diferentes dispositivos dentro de la organización.

4.1 DESCRIPCIÓN DE ACTIVIDADES PROFESIONALES

4.1.1 Enfoque de las actividades profesionales

Las actividades profesionales están orientadas a principalmente a 2 enfoques:

- **Enfoque estratégico**: Bajo este enfoque se planificó y se tomó decisiones estratégicas para alcanzar el objetivo a corto plazo, se analizó el entorno inicial, se identificaron las oportunidades y se diseñaron los planes de acción para lograr el objetivo propuesto.
- **Enfoque técnico**: En la cual aplicamos las habilidades y conocimientos técnicos específicos para desempeñar el trabajo propuesto, bajo este enfoque se cumplió con las competencias técnicas y la eficiencia al ejecutar las tareas.

4.1.2 Alcance de las actividades profesionales.

Bajo los 2 enfoques propuestos anteriormente se procede a indicar:

El alcance de actividades profesionales de acuerdo con el enfoque estratégico busca que la planificación e implementación de las actividades estén sujetas a los objetivos estratégicos de la

organización y que contribuyen a su éxito a largo plazo; se buscan objetivos claros para el desarrollo de las actividades propuestas:

- El desarrollo de planes detallados.
- La implementación y monitoreo de las estrategias, con la finalidad de lograr los resultados deseados.

En cuanto al alcance de actividades profesionales de acuerdo con el enfoque técnico incluye:

- **Implementación de Software**: Comprende el diseño, implementación y mantenimiento de las aplicaciones informáticas que satisfagan las necesidades de una organización.
- **Gestión de la infraestructura**: Comprende la gestión de los recursos de hardware y software, como servidores, redes, sistemas operativos y bases de datos.
- **Seguridad de la información**: Comprende la importancia de las actividades en esta área incluyan la implementación de medidas de seguridad para proteger la información sensible, tales como los procedimientos para la gestión de firewalls, sistemas de detección de intrusos, políticas de acceso e incidentes de seguridad.
- **Soporte técnico**: Como parte de nuestro enfoque técnico, se ayuda a los usuarios finales a resolver problemas técnicos, brindar capacitación y orientación sobre cómo usar la aplicación y resolver incidentes relacionados con la infraestructura de TI.

4.1.3 Entregables de las actividades profesionales

En la gestión de TI, dentro de las actividades propuestas se realizaron los siguientes entregables:

- Manual de procedimientos de instalación de sistema base (SO CentOS 7).
- Manual de implementación de servicios virtualizados.
- Manual de configuración de Firewall de la red de negocios.
- Manual de configuración de red de las estaciones de trabajo.

- Inventario de equipos físicos y virtuales
- Manual de Backup de sistemas virtuales.

4.1.4 Metodologías

El presente trabajo de suficiencia profesional se sustenta bajo la metodología de aspectos técnicos en Tecnología de la información, teniendo en cuenta algunos enfoques de los cuales procederemos a detallar:

- **Análisis de requisitos**: Antes de iniciar la implementación, fue fundamental realizar un análisis exhaustivo del estado de las comunicaciones en la organización, esto implicó comprender las necesidades, definir los objetivos y alcances, identificar los recursos y establecer las limitaciones y restricciones.
- **Diseño de solución**: Una vez establecido el punto anterior (Análisis de requisitos), se procede al diseño de la solución, esto implicó la creación de una arquitectura técnica que aborde los requisitos identificados, redefinir la infraestructura necesaria, los protocolos de comunicaciones, las interfaces y otros aspectos técnicos relevantes.
- **Implementación y despliegue**: Una vez que se procedió con el diseño de la solución, se procede a su implementación y despliegue en un entorno de producción, donde se incluyen la configuración de servidores, la instalación del software y la puesta en marcha de los sistemas.
- **Mantenimiento y soporte**: Teniendo en cuenta los 3 puntos anteriores es una buena práctica recurrente, pensar en proporcionar el mantenimiento y soporte continuo de los sistemas, así mismo pensar que la tecnología evoluciona, es por ello la importancia de aplicar actualizaciones continuas

4.1.5 Técnicas

En cuanto a las técnicas empleadas para el análisis inicial de la solución, se utilizaron las siguientes técnicas:

- Escaneo de red.
- Entrevistas con el personal (identificar el horario recurrente de caídas de servicio).
- Revisión y estatus de equipos de comunicación.

4.1.6 Instrumentos

- Guía de entrevistas
- Resultados de escaneo de red
- Estado de los equipos de comunicaciones

4.1.7 Equipos y materiales utilizados en el desarrollo de las actividades

En este acápite vamos a distinguir la parte de gestión y la parte de operaciones o también denominada hardware.

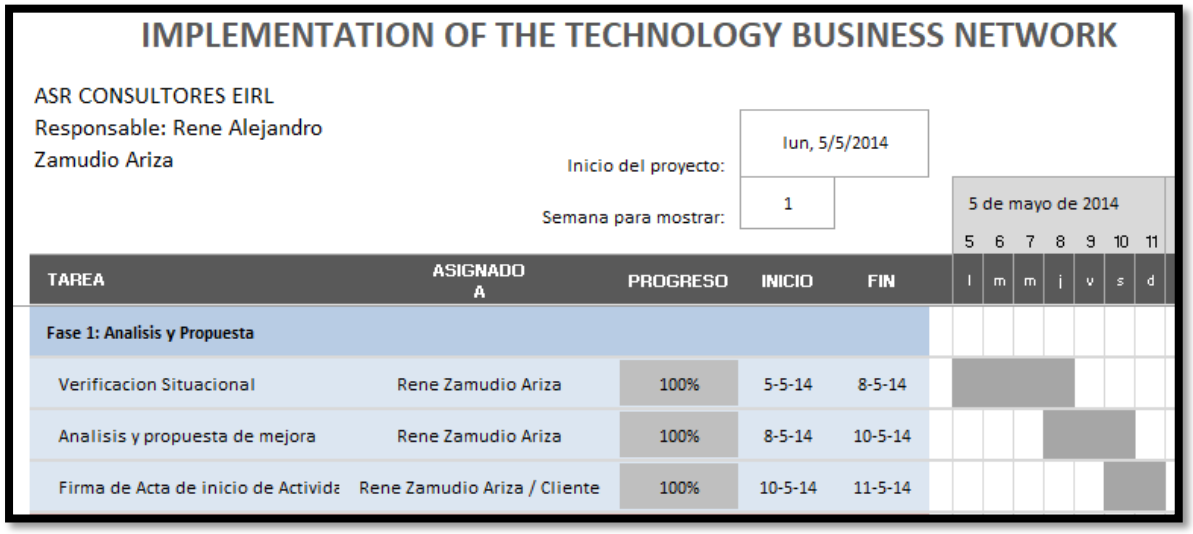
- **Materiales para la gestión:**
    - **Suite ofimática de Libre Office**: LibreOffice es una poderosa suite de oficina; su interfaz limpia y sus potentes herramientas permiten hacer crecer tu productividad. LibreOffice incorpora varias aplicaciones que lo convierten en la más potente suite de oficina Libre y de Código Abierto del mercado: Writer, el procesador de textos, Calc, la hoja de cálculos, Impress, el editor de presentaciones, Draw, nuestra aplicación de dibujo y diagramas de flujo, Base, nuestra base de datos e interfaz con otras bases de datos, y Math para la edición de fórmulas matemática.
    - **Trello**: Herramienta que ayuda con la planificación de la gestión de tareas, el seguimiento de actividades e incluso la comunicación entre los equipos de trabajo

- **Equipos tecnológicos y software:**
  - Server HP
  - Pc CORE I7 de 3ra generación.
  - 2 switch de 48 puertos.
  - 3 tarjetas de redes 10/100/1000
  - Iso CentOS 7.
  - Iso Pfsense.

4.2 EJECUCIÓN DE LAS ACTIVIDADES PROFESIONALES

4.2.1 Cronograma de actividades realizadas.

Ilustración 15 *Fase 1: Análisis y Propuesta*



IMPLEMENTATION OF THE TECHNOLOGY BUSINESS NETWORK

ASR CONSULTORES EIRL
Responsable: Rene Alejandro Zamudio Ariza

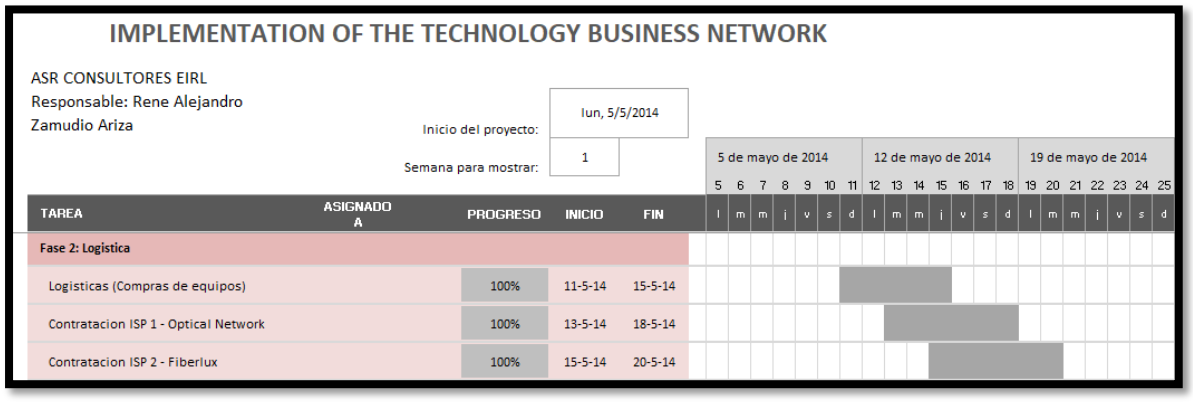
Inicio del proyecto: lun, 5/5/2014
Semana para mostrar: 1

TAREA	ASIGNADO A	PROGRESO	INICIO	FIN
Fase 1: Analisis y Propuesta				
Verificacion Situacional	Rene Zamudio Ariza	100%	5-5-14	8-5-14
Analisis y propuesta de mejora	Rene Zamudio Ariza	100%	8-5-14	10-5-14
Firma de Acta de inicio de Activida	Rene Zamudio Ariza / Cliente	100%	10-5-14	11-5-14

5 de mayo de 2014
5 6 7 8 9 10 11
l m m j v s d

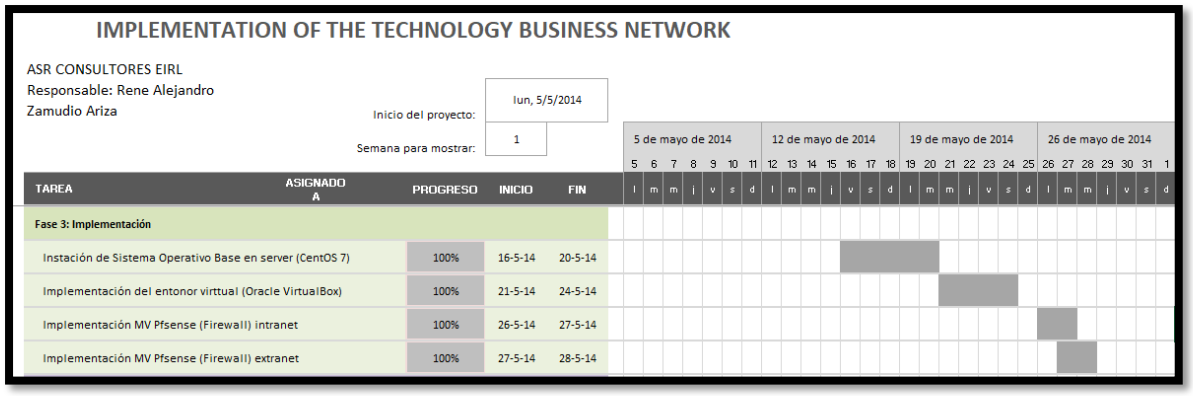
Nota: En la fase 1 se realizaron entrevistas al personal operativo, verificación de equipos (hardware), pruebas de software y funcionamiento de la red, asimismo se plantearon las propuestas de solución, determinando que lo mejor era migrar a una solución basada en Linux.

Ilustración 16 *Fase 2: Logistica*



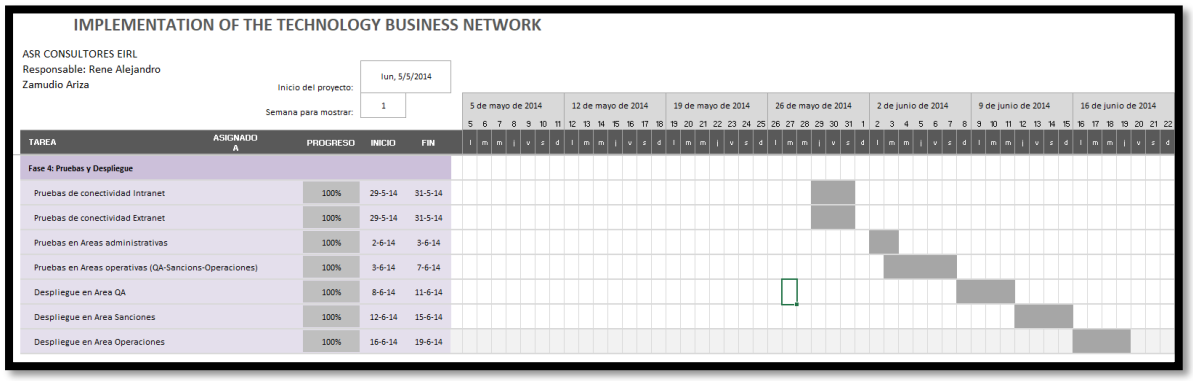
Nota: Ya habiendo determinado la solución, se procedió a solicitar propuesta para la compra de equipamiento a utilizar, esto implicaba verificar diferentes proformas de proveedores, por último, ya teniendo determinado la compra y el proveedor se pasó a logística para la adquisición de dichos dispositivos, a la par se determinó con cuales proveedores se trabajarían.

Ilustración 17 *Fase 3: Implementación*



Nota: En la fase 3 se procedió con la implementación del servidor Linux bajo el SO CentOS 7, luego se procedió a la implementación de 4 máquinas virtuales con diferentes características, los cuales se detallarán en los siguientes capítulos.

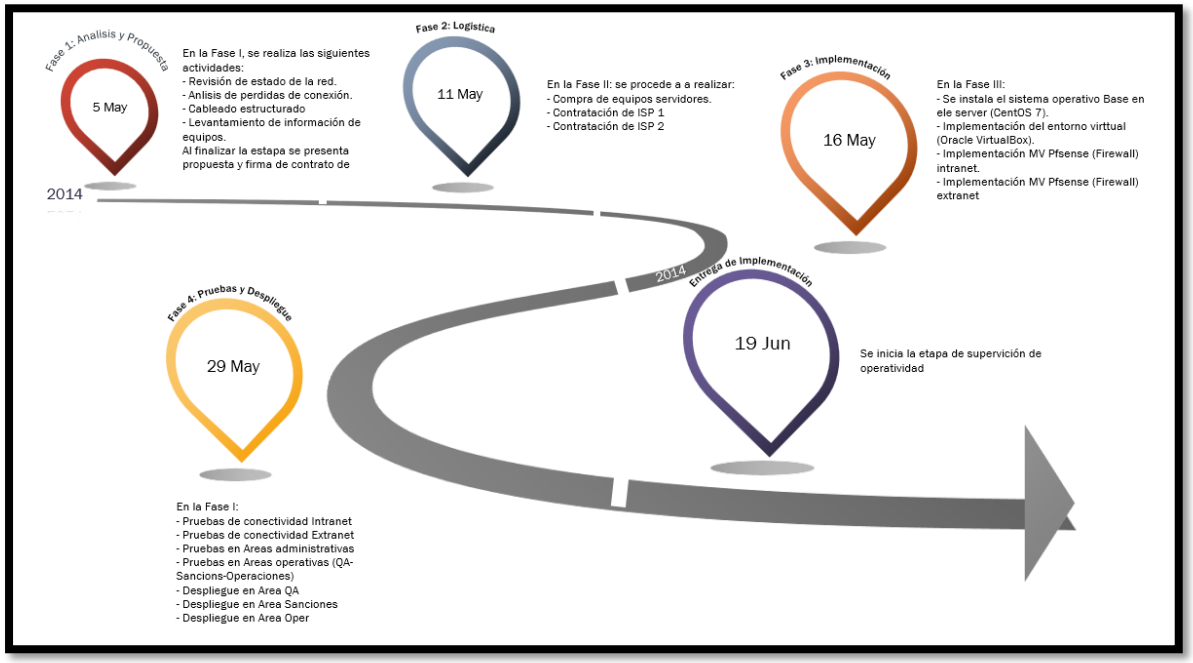
Ilustración 18 *Fase 4: Pruebas y despliegue*



Nota: La fase 4 inicia con las pruebas de conectividad sobre la intranet y extranet luego las áreas de operaciones, así como despliegue de las conexiones.

4.2.2 Proceso y secuencia operativa de las actividades profesionales.

Ilustración 19 *Secuencia operativa de las actividades profesionales*



Nota: en esta imagen se muestra el circuito completo de las actividades planteadas para la solución de la problemática.

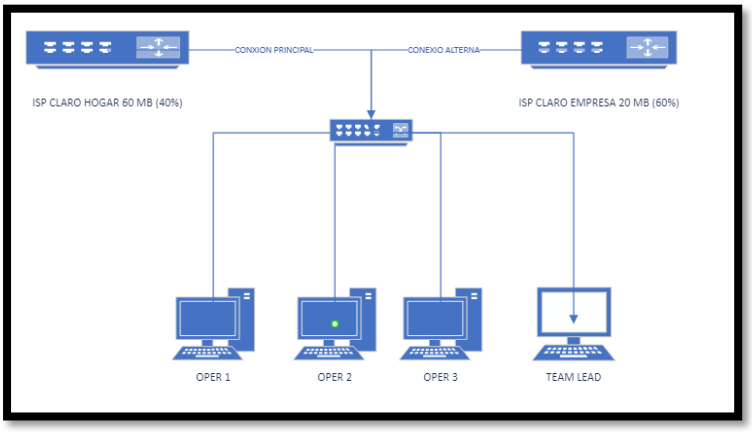
4.2.3 DESARROLLO DE LAS ACTIVIDADES PROFESIONALES.

- ANÁLISIS PRELIMINAR DEL PROBLEMA IDENTIFICADO

  Dentro del circuito preliminar se realizó un trabajo de revisión y verificación del hardware

y el servicio de internet el cual procedemos a detallar mediante secuencia de imágenes del trabajo realizado:

Ilustración 20 *Esquema de red inicial*



Nota: en esta imagen se demuestra que se contaba con una red básica, no tenían control de la navegación, una de las causas era que el personal utilizaba constantemente los servicios de streeming como YouTube, y se generaba una lentitud extrema lo que daba la sensación de perdida de conexión

- Otras de las causales era que el servicio de internet no estaba a acorde a la necesidad solicitada, este indicador fue testeado constantemente teniendo perdidas de conexión por la inestabilidad del servicio, la zonificación del momento no permitía migrar con ese mismo proveedor a un servicio de fibra óptica lo que se imposibilitaba la permanencia del servicio.
- Otro detalle en particular era que no se tenía un controlador de dominio, lo que permitiese trabar con las sesiones de usuario y permisos de acceso.

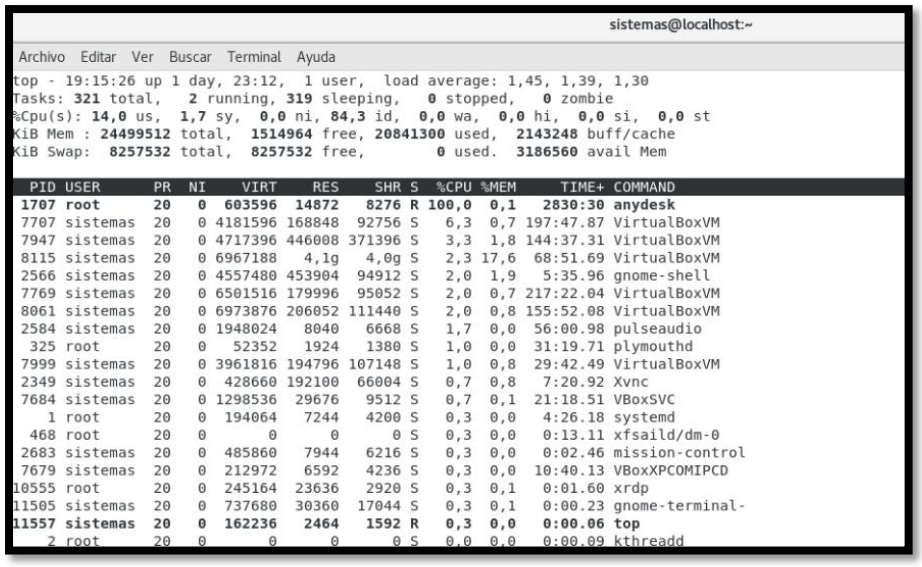
- IMPLEMENTACIÓN

  En el proceso de implementación se procedió a instalar el Sistema operativo CentOS 7 en un servidor con las siguientes características:

  - Procesador Core i7 de 3ra Generación
  - Disco duro de 1 TB

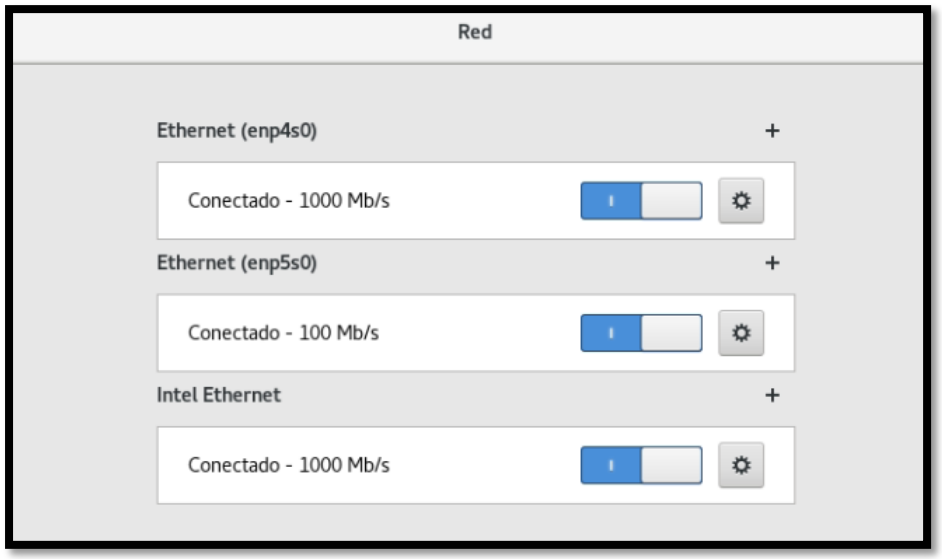
- 24 Gb de Memoria RAM
- 3 tarjeta de red 10/100/1000
- Generando el siguiente esquema de trabajo:

Ilustración 21 *Top uso de terminal para verificar característica y procesos del servidor*



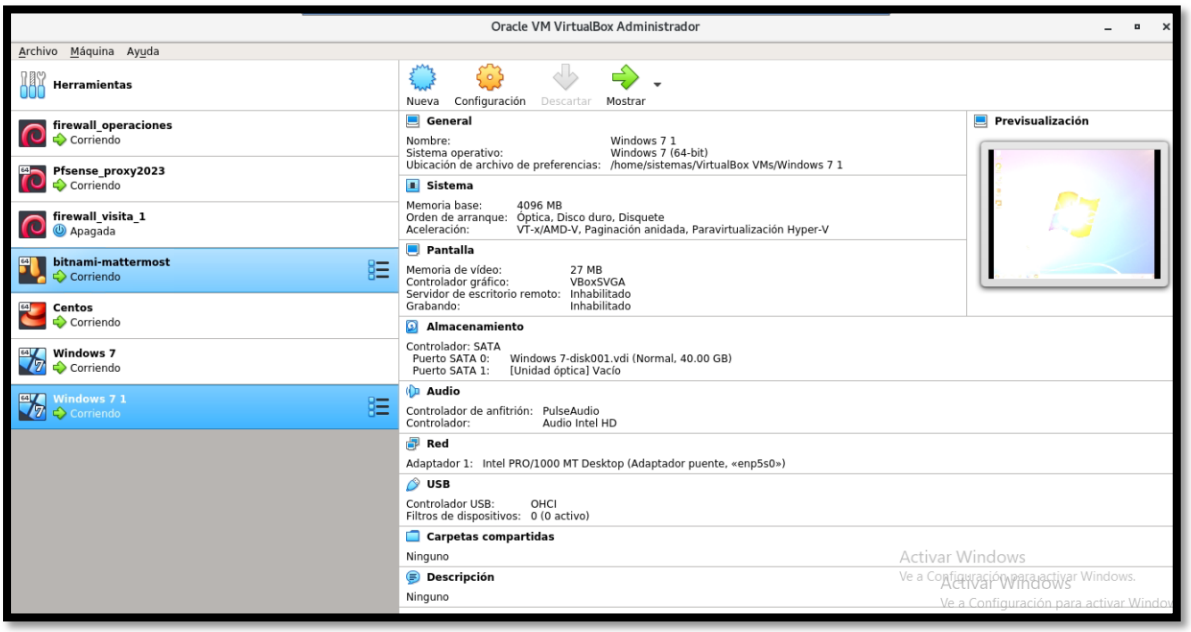
Nota: En esta imagen se verifica el comando Top que se es muy usado en CLI para verificar uso de los servicios de Linux, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 22 *Representación gráfica de las tarjetas de red*



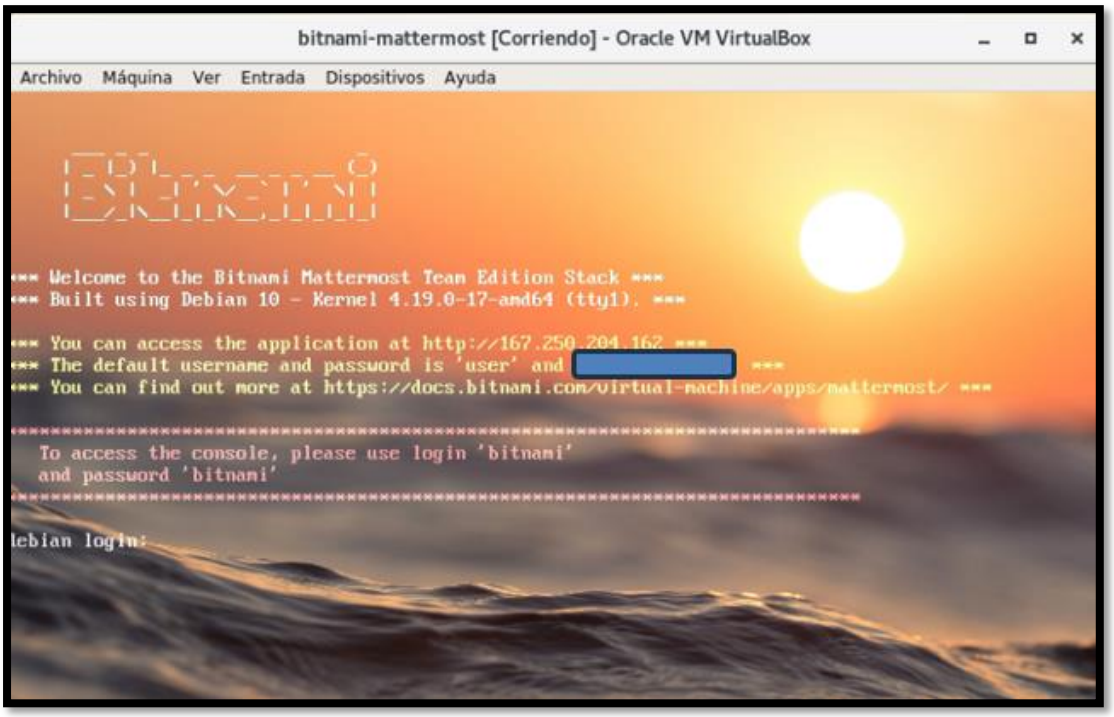
Nota: Esta imagen demuestra que el servidor cuenta con 3 tarjeta de red según los planificado (1 tarjeta destinada a la red LAN y 2 tarjetas de red destinadas a ISP 1 - ISP2 redundante), tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 23 *Oracle virtual box*



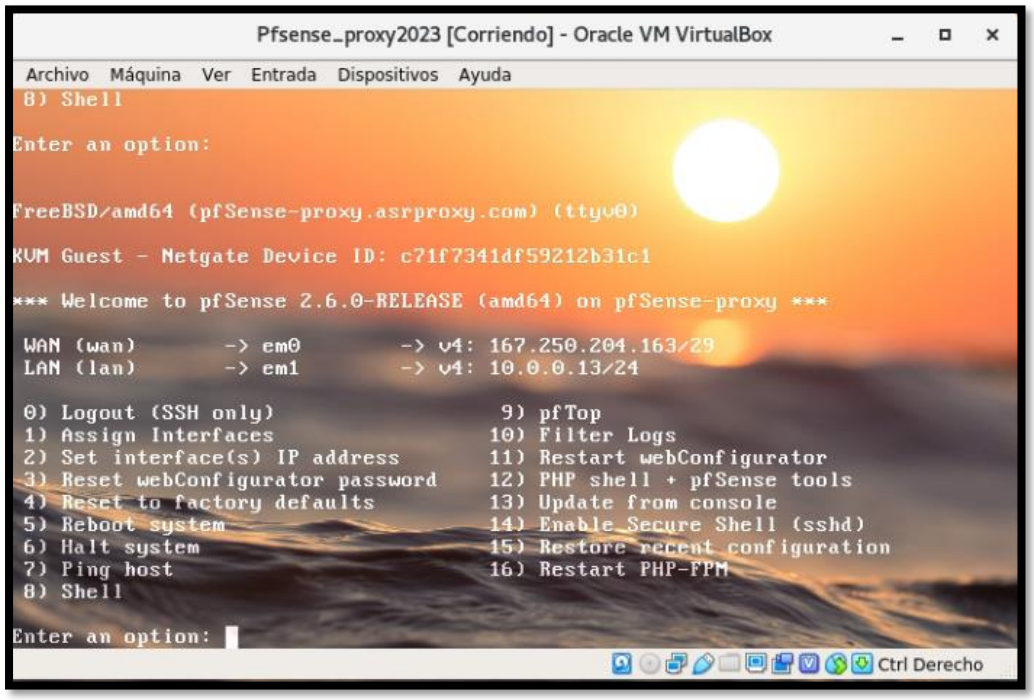
Nota: Esta imagen demuestra la implementación completa del sistema Oracle virtual box, cuyo fin fue la de montar el resto de las máquinas virtuales que permitiría la conectividad de la intranet y la extranet, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 24 *Máquina Virtual de Mattermost (chat de comunicaciones)*



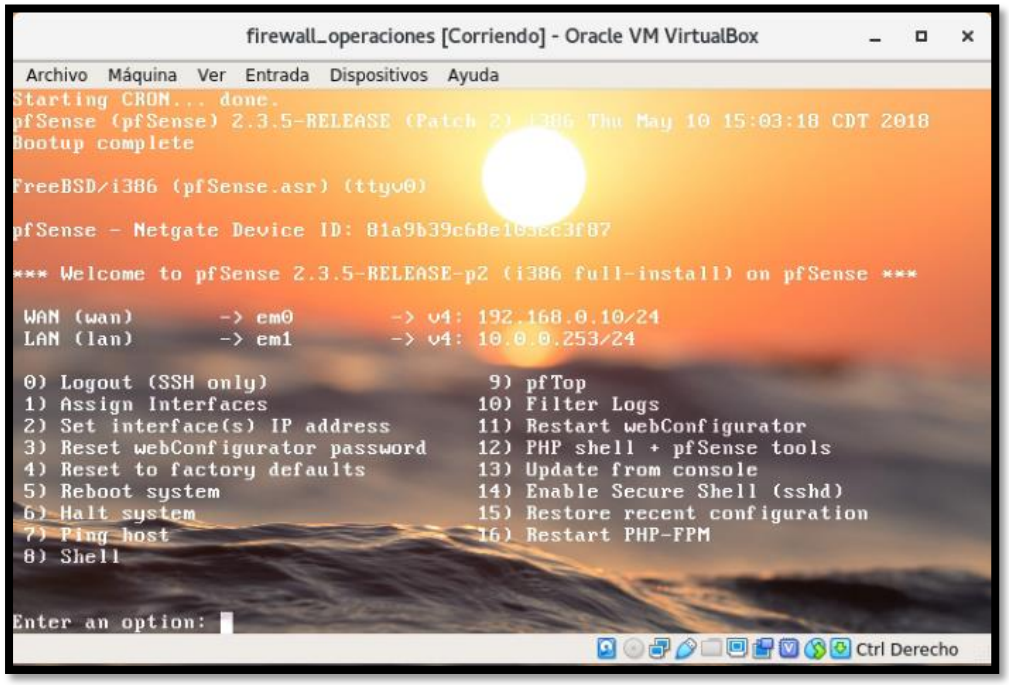
Nota: Servicio de chat corporativo local, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 25 *Pfsense firewall-proxy perimetral*



Nota: En la imagen se demuestra que el servicio está activo y en uso, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

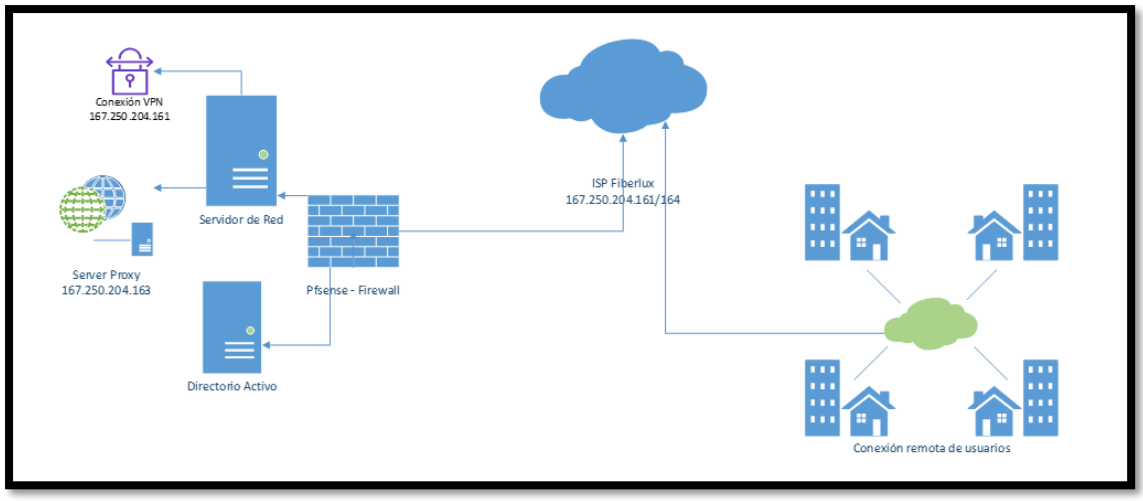
Ilustración 26 *Pfsense firewall operaciones*



Nota: En la imagen se demuestra que el servicio está activo y en uso, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

- El diagrama de red actual es:

Ilustración 27 *Esquema actualizado del diagrama de Red*

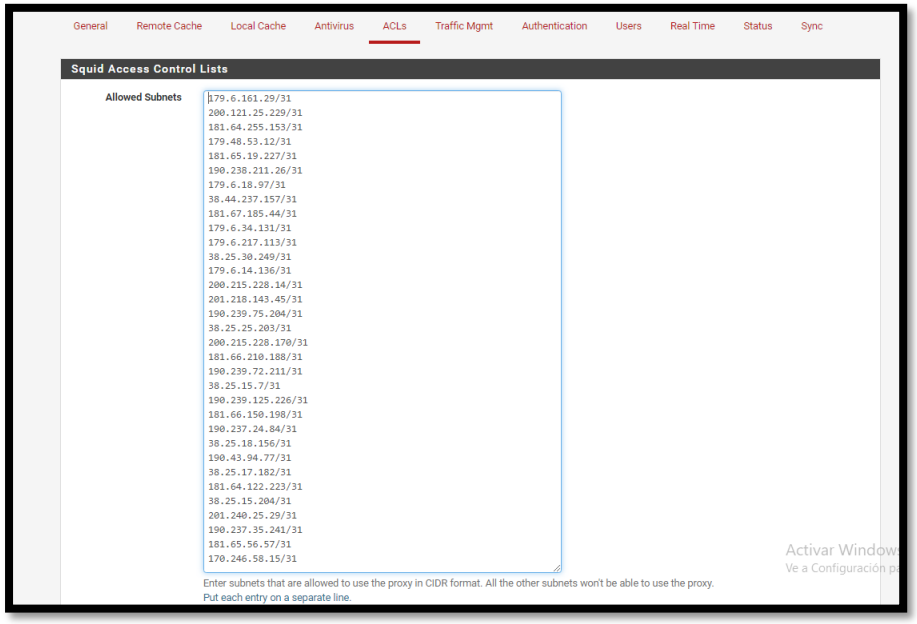


Nota: El esquema actual solo demuestra la conexión que existe por el home office dado que la empresa sigue en trabajo remoto al 100%, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

- DESPLIEGUE DE LA SOLUCIÓN

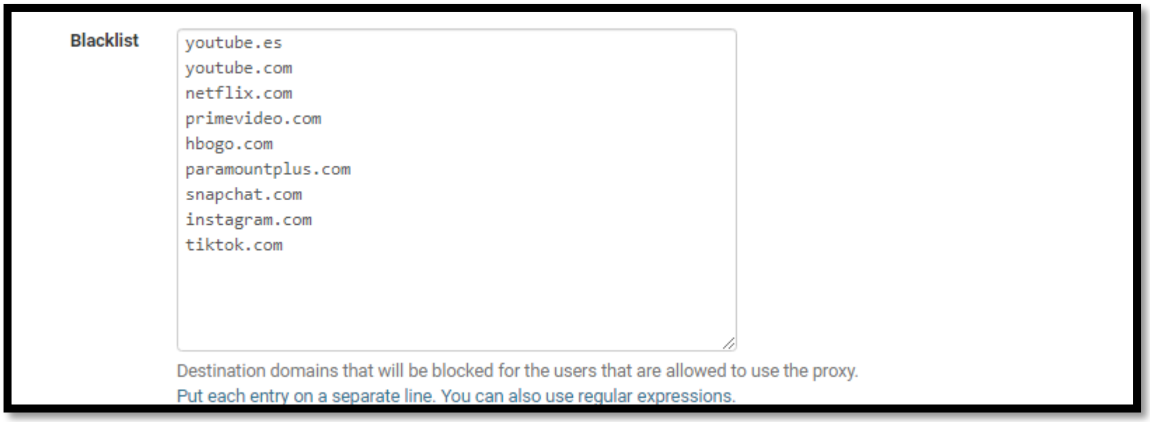
  En la actualidad al estar en trabajo remoto al 100% tenemos conectividad vía proxy mediante el uso de nuestros recursos ya demostrados anteriormente:

Ilustración 28 *Lista de control de acceso*



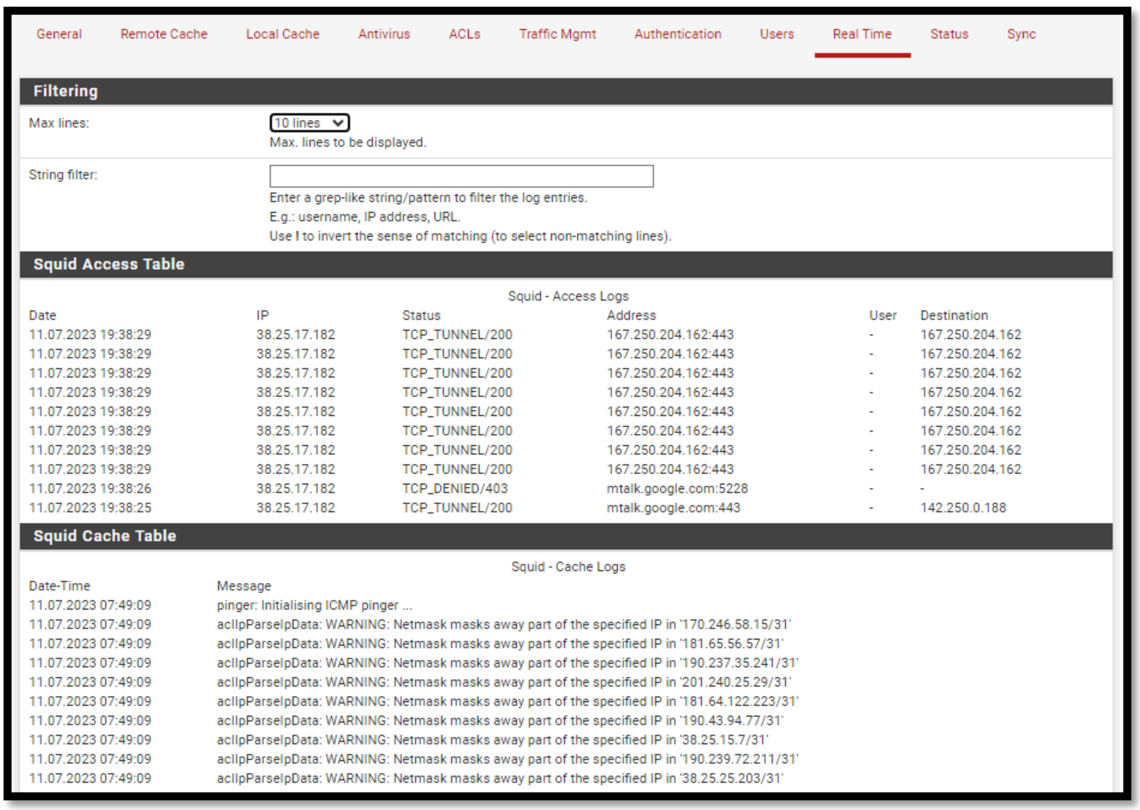
Nota: En esta imagen se demuestra el permiso de acceso a la lista de control, Tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 29 *Blacklist (Lista Negra)*



Nota: En esta imagen se verifica que existe una lista de legra de prohibición de acceso, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 30 *Tabla de acceso proxy*

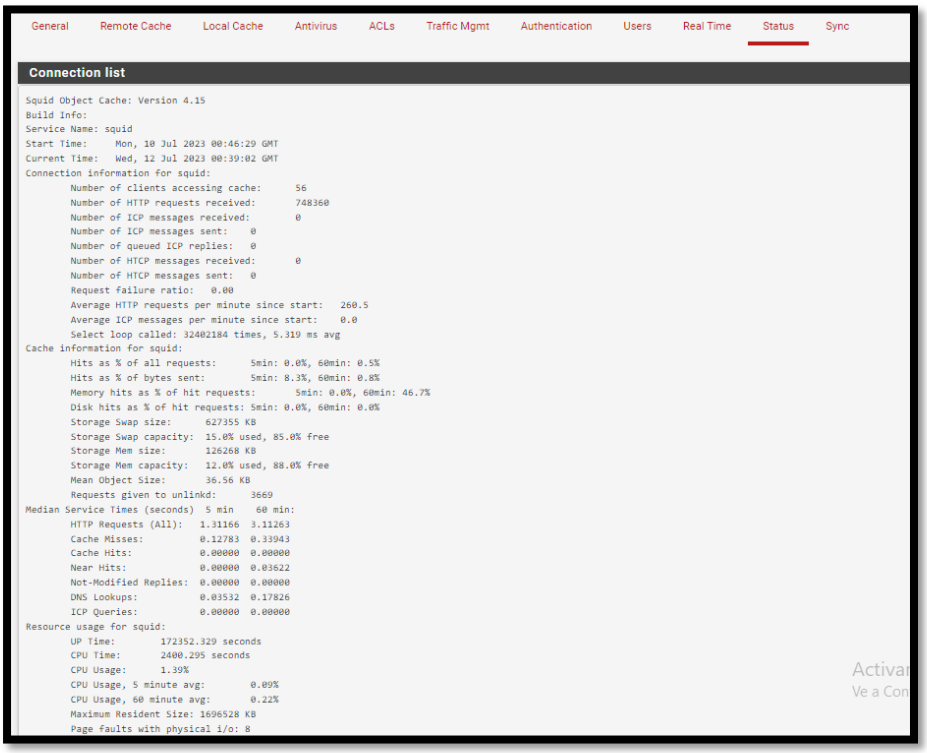


Date	IP	Status	Address	User	Destination
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:29	38.25.17.182	TCP_TUNNEL/200	167.250.204.162:443	-	167.250.204.162
11.07.2023 19:38:26	38.25.17.182	TCP_DENIED/403	mtalk.google.com:5228	-	-
11.07.2023 19:38:25	38.25.17.182	TCP_TUNNEL/200	mtalk.google.com:443	-	142.250.0.188

Date-Time	Message
11.07.2023 07:49:09	pinger: Initialising ICMP pinger ...
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '170.246.58.15/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '181.65.56.57/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '190.237.35.241/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '201.240.25.29/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '181.64.122.223/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '190.43.94.77/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '38.25.15.7/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '190.239.72.211/31'
11.07.2023 07:49:09	aclIpParseIpData: WARNING: Netmask masks away part of the specified IP in '38.25.25.203/31'

Nota: La imagen demuestra una fracción de tiempo en conexión, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 31 *Lista de conexión*



Nota: En la imagen se demuestra l lista de conexión durante el día, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

CAPÍTULO V:

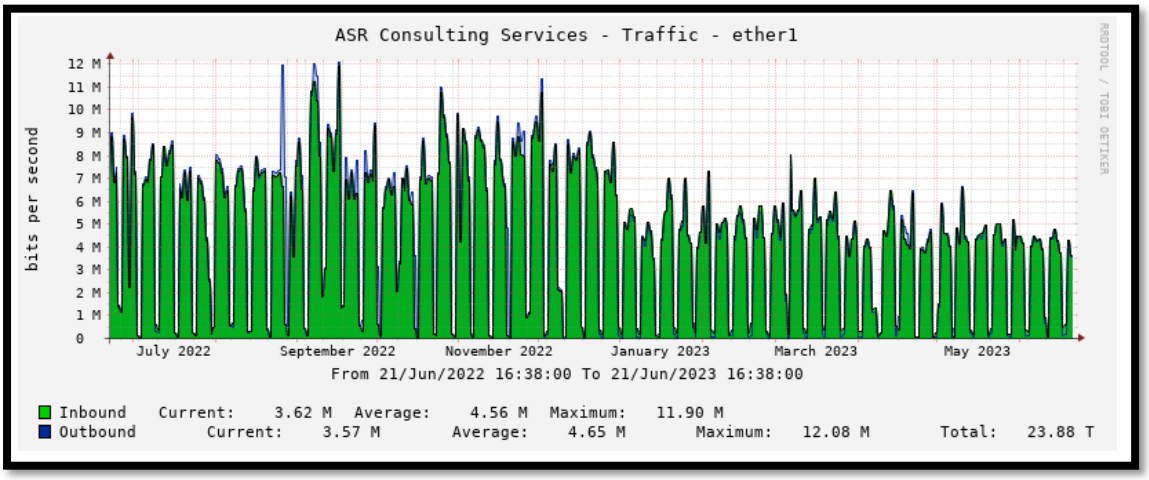
5 RESULTADOS

A continuación, el siguiente capítulo describe los resultados obtenidos al culminar la implementación basados en el análisis, investigación e implementación, generando un gran valor a la organización.

5.1 RESULTADOS FINALES DE LAS ACTIVIDADES REALIZADAS

El resultado de la implementación fue un sistema de red basado en Linux CentOS/Debian que nos ha permitido en los últimos 7 años lograr una estabilidad en cuanto a la navegación, nos ha permitido seguridad por el tipo de filtro que se maneja con el sistema Linux; a continuación, algunas imágenes de sustento por parte del proveedor de servicio:

Ilustración 32 *Tráfico desde el servicio de monitoreo del ISP*

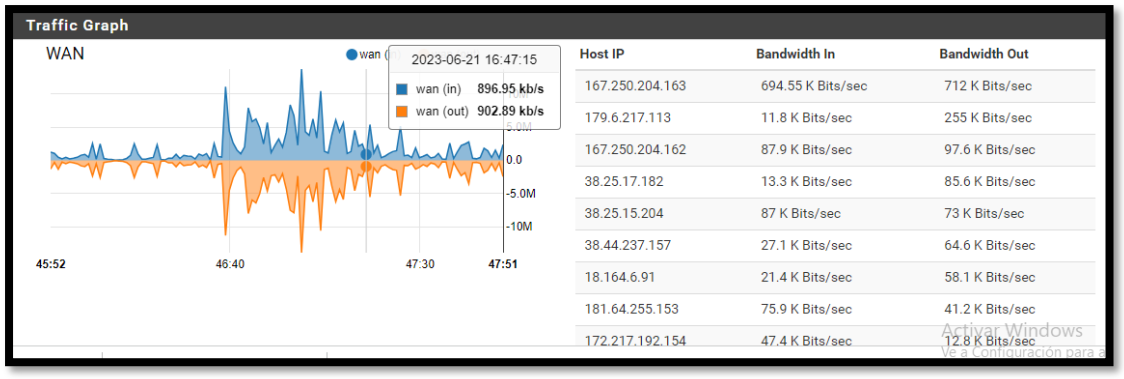


Nota: En la imagen se verifica el consumo de internet desde julio del 2022 hasta mayo del 2023, siendo un consumo máximo de hasta 12 MB con 50 host conectados simultáneamente, el dato es extraído desde la plataforma dl proveedor ISP Fiberlux.

Se Procede a mostrar las imágenes de nuestro servidor que monitorea el consumo de ancho de

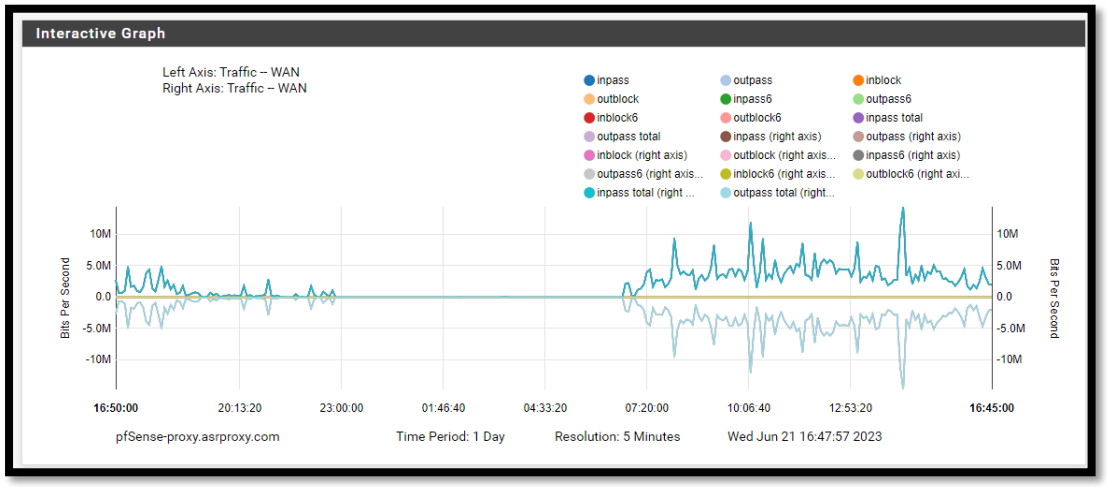
banda:

Ilustración 33 *Grafica de tráfico de internet desde pfsense*



Nota: En la imagen se la conexión WAN desde el monitoreo del pfsense, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

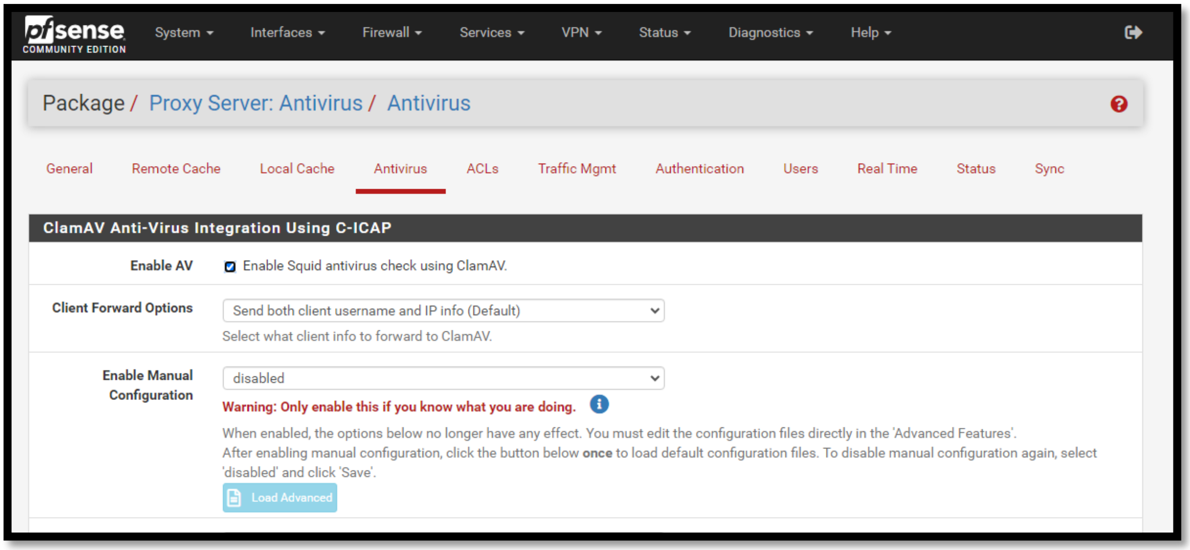
Ilustración 34 *Gráfico interactivo durante 1 día de conexión*



Nota: En la imagen se verifica el consumo del servicio de internet en un día en el horario de 7am a 16:45 pm.

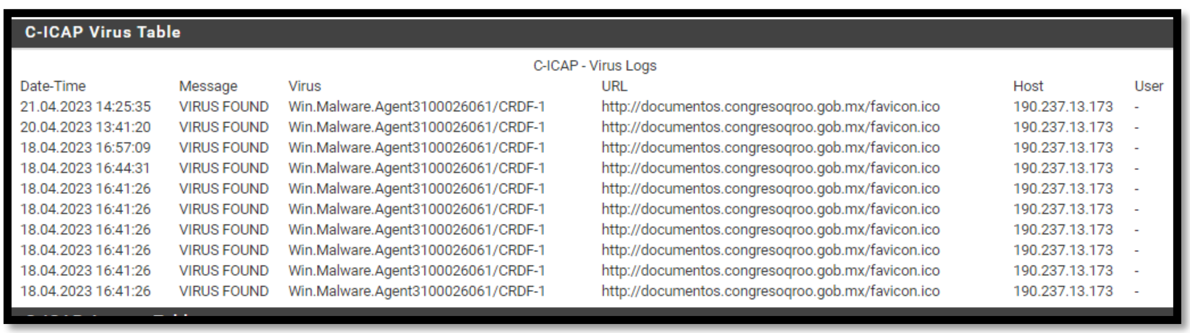
Por otro lado, tenemos en consideración que hemos habilitado otros servicios como un antivirus en red basado en Linux en cual se muestra a continuación:

Ilustración 35 *Configuración de antivirus en Linux*



Nota: En la imagen se demuestra que el servicio de antivirus esta activo, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

Ilustración 36 *Tabla de bloqueo de virus*



C-ICAP Virus Table

C-ICAP - Virus Logs

Date-Time	Message	Virus	URL	Host	User
21.04.2023 14:25:35	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
20.04.2023 13:41:20	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:57:09	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:44:31	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-
18.04.2023 16:41:26	VIRUS FOUND	Win.Malware.Agent3100026061/CRDF-1	http://documentos.congresoqroo.gob.mx/favicon.ico	190.237.13.173	-

Nota: En esta imagen se muestra la actividad del filtro antes de la descarga de algún malware, tomado del documento institucional de la empresa ASR Consultores EIRL. 2023

5.2 LOGROS ALCANZADOS

Al término de la implementación se denota algunos logros alcanzados lo cuales procedemos a listar:

- Red estable y confiable.
- Seguridad y estabilidad de la red.
- Se determino que post implementación el personal mejoro la productividad.

Con la implementación y no teniendo en cuenta la pandemia la empresa obtuvo un crecimiento de

hasta un 75% al incrementar los puestos laborales generando oportunidades a un crecimiento sostenido.

Logros alcanzados en pandemia (Covid)

- Se procedió implementar un proxy recursivo lo que permitió que los trabajadores puedan conectarse y acceder a la página del cliente con la ip pública la empresa, esto permitió una escalabilidad segura y filtrado de malware dentro del proxy.
- Continuidad del negocio.

5.3 DIFICULTADES ENCONTRADAS

A continuación, se detallan algunas dificultades que se encontraron antes y durante la implementación:

- Por parte de la empresa su total rechazo inicial de una implementación basada en un Sistema Operativo Linux.
- Incertidumbre en un proveedor de internet corporativo.
- Rechazo a la solicitud de compra de hardware de servidor.
- Desconocimiento en el sistema de virtualización open Source.

5.4 PLANTEAMIENTO DE MEJORAS

En este punto ha de considerarse que, ante un primer análisis situacional en el año 2014, se logró entender la necesidad de mejorar la infraestructura y el concepto de una red de negocio, esto permitió que la red sea escalable y estable para una mayor exigencia si el caso lo amerite.

5.4.1 Metodologías propuestas

Al momento de la implementación, se describió una entrega modular simulando un sprint del framework scrum, esto me permitió identificar un backlog de trabajo y en conjunto con el interesado (CEO de la empresa) se validó el periodo de cada entregable en funcionamiento, tanto

a nivel de pruebas como a nivel de despliegue.

5.4.2 Descripción de la implementación

Se gestionó la implementación de una red de negocio, dando lugar a la seguridad perimetral, seguridad de accesos y la gestión de usuarios, lo que generó una mayor eficiencia en la red y optimizar los recursos de hardware.

5.5 ANÁLISIS

Este informe de suficiencia profesional se ha realizado con información real, los esquemas de trabajo y la implementación, así como la ejecución de estos, al momento del despliegue de la red de la empresa ASR CONSULORES.

Dentro del análisis podríamos nombra algunos puntos relevantes que hacen referencia a las consecuencias del mejoramiento de la red:

- **Seguridad red:** En este punto hacemos referencia a las medidas y precauciones tomadas para proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos en una red
- **Antivirus Linux:** ClamAV es una opción popular y de código abierto para Linux. Es conocido por su capacidad para detectar virus, gusanos y otros tipos de malware. Puedes utilizar ClamAV desde la línea de comandos o mediante una interfaz gráfica.
- **Pfsense**: Se optó por usar el firewall de red basado en Linux por que pfSense es un software de enrutamiento y firewall de código abierto basado en el sistema operativo FreeBSD. Está diseñado para proporcionar capacidades avanzadas de seguridad y redes para redes pequeñas y medianas. pfSense ofrece una amplia gama de funciones y se puede utilizar como cortafuegos, enrutador, servidor VPN, modelador de tráfico y más.

5.6 APORTE DEL BACHILLER EN EL EMPRESA Y/O INSTITUCIÓN

Los aportes realizados en el desarrollo del trabajo de suficiencia profesional se dividen en 3 aspectos:

5.6.1 ASPECTO ADMINISTRATIVO

- Restructuración del departamento de IT.
- Implementación de políticas de seguridad.
- Implementación de políticas de continuidad de negocio.
- Implementación de políticas de seguridad informática.
- Implementación de sistemas de biométrico.
- Implementación de manuales e instalación e implementación de red.

5.6.2 ASPECTO OPERATIVO

- Instalación de sistemas operativos Linux en servidores.
- Instalación de sistemas firewall Pfsense para la red interna.
- Instalación de sistemas firewall Pfsense para la red externa.
- Instalación de sistema chat Mattermost basados en Linux.
- Implementación de un servidor DHCP.
- Mejoramiento del cableado estructurado de la red interna.

5.6.3 ASPECTO ACTITUDINAL

- Proactividad y liderazgo en el transcurso del proyecto.
- Análisis y apoyo en el levantamiento de requerimientos.
- Generar capacitaciones al personal para el buen uso de las redes del negocio.
- Seguimiento y mejoramiento de la red.
- Trabajo en equipo.

CONCLUSIONES

La realización del presente informe de suficiencia profesional que lleva por título: “Implementación de una red virtualizada, empleando el Sistema Operativo Linux CentOS para mejorar la seguridad y el control de acceso a internet, para la Empresa ASR COSULTORES EIRL”, permite darles solución a sus redes computacionales, dado que por un tiempo prolongado estuvieron aquejando de perdida de conexión y lentitud extrema; esto también influía en la producción de las áreas operativas dado que se sentían desmotivados por que no podían cumplir con los objetivos trazados por el cliente, luego de una etapa de incertidumbre por las fallas técnicas se procedió a realzar las siguientes tareas:

1. Al realizar el análisis situacional, se verificaron que los equipos que se usaban no eran los adecuados, así como el equipamiento de comunicaciones estaban en un estado de no mantenimiento; se realizaron las entrevistas al personal operativo para entender su percepción y partir de ese momento construir una posible solución.
2. Un tema muy importante es la parte de la logística, así lo entendió la empresa y lo asumió como un objetivo prioritario, esto ayudo mucho a conseguir el equipamiento de manera casi inmediata.
3. En la etapa de implementación se inició con el desarrollo de un escenario de laboratorio que permitía ir revisando la existencia de alguna incidencia, para que posteriormente se pase a producción (Implementación), esto permitió que la realización de las actividades propuestas fuera mucho más sencillas y prácticas.

4. En la etapa de pruebas y despliegue inicialmente encontramos unos inconvenientes, pero era por el lado de terceros el ISP principal dado que aún no terminaban con la instalación del servicio, lo que complicó las pruebas iniciales y estas tuvieron que realizarse con el proveedor American móvil, pero después de unos días este impase se solucionó con la instalación del servicio y las pruebas fueron de manera exitosa y en tal sentido se tomó la decisión de realizar el despliegue.

RECOMENDACIONES

En cuanto a las recomendaciones que se dará estarán en la línea de la solución que se emplearon:

1. Planificar el mantenimiento de hardware cada 6 meses, (revisión y limpieza de componentes internos del servidor físico)
2. Planificar las actualizaciones del software Linux cada 4 meses (estructurar updates de las versiones de CentOS tanto del entorno físico como virtualizado).
3. Generar backup de las máquinas virtuales 1 vez al mes (almacenarlo en un ambiente seguro libre de virus informáticos).
4. Revisar los servicios de seguridad, almacenamiento en red, privilegios de usuario, monitoreo de los servicios internos.
5. Monitorear el uso optimizado de la conectividad y que esta no supere el 20% de la línea contratada.
6. Realizar manuales de fallos y manuales de usuarios.

BIBLIOGRAFÍA

Las referencias de las citas

1. Oropesa, C. (2015). *La Gestión De La Seguridad Basada En Los Comportamientos. ¿Un Proceso Que Funciona?*. Med. segur. trab., 241(61), 424-435. https://doi.org/10.4321/s0465-546x2015000400002
2. Helil, N., Kim, M., Han, S. (2011). *Trust and Risk Based Access Control And Access Control Constraints*. KSII TIIS, 11(5). https://doi.org/10.3837/tiis.2011.11.022
3. Carvalho, D., Milanez, M., Avelino, M., Bruschi, S., Goularte, R. (2007). *Secbox: Uma Abordagem Para Segurança De Set-top Boxes Em Tv Digital*.. https://doi.org/10.5753/sbseg.2007.20922
4. Vieira, R., Seabra, R. (2023). *Avaliação Da Usabilidade De Interfaces Gráficas Para Distribuições Linux*. *RENOTE*, 2(20), 104-113. https://doi.org/10.22456/1679-1916.129157
5. Narváez, J., Villalba, K., Donado, S. (2021). *Arquitectura Basada En Tecnologías Emergentes Y Tecnología De Monitoreo De Tráfico De Red. Investigación e Innovación en Ingenierías*, 3(9), 18-31. https://doi.org/10.17081/invinno.9.3.5340
6. Benavides, D., Castro, A. (2021). Administrar *El Ciclo De Vida De Los Usuarios*. *Poli*. https://doi.org/10.15765/poli.v1i1.2082
7. Ramos, M., Días, O. (2015). *Componente De Autenticación Para El Generador Dinámico De Reportes*.. https://doi.org/10.18687/laccei2015.1.1.020

8. Rodriguez, W., Páez, M. (2019). *Tecnología Microchip Para Acceder a Información Vehicular Como Apoyo A Procesos De Control Y Seguridad. Sci. tech*, 2(24), 264. https://doi.org/10.22517/23447214.20241

9. Benavides, D., Castro, A. (2021). *Administrar El Ciclo De Vida De Los Usuarios. Poli*. https://doi.org/10.15765/poli.v1i1.2082

10. Garces, A., Rivas, M., Harbour, M. (2019). *Aplicaciones Ada En Android Con Requisitos De Tiempo Real*. Rev. iberoam. autom. inform. ind., 3(16), 264. https://doi.org/10.4995/riai.2019.10604

11. Fernández, C. (2011). *Nuevo Formato De Datos Para El Laboratorio De Ingeniería Sísmica Del Instituto De Investigaciones En Ingeniería De La Universidad De Costa Rica. Ingeniería*, 2(16). https://doi.org/10.15517/ring.v16i2.667

12. Alvarado, J., Quezada-Sarmiento, R., García-Galarza, K. (2018). *Aplicación Java Para El Control De Rb Mikrotik En Empresas Proveedoras De Servicio De Internet // Java Application For Mikrotik Rb Control In Companies Providing Internet Service*. CU, 26(11), 161-169. https://doi.org/10.29076/issn.2528-7737vol11iss26.2018pp161-169p

13. Melkov, D., Paulikas, Š. (2021). *Analysis Of Linux Os Security Tools For Packet Filtering and Processing. Science - Future of Lithuania*, 0(13), 1-5. https://doi.org/10.3846/mla.2021.15180

14. Chanu, U., Singh, K., Chanu, Y. (2022). *An Ensemble Method For Feature Selection and An Integrated Approach For Mitigation Of Distributed Denial Of Service Attacks. Concurrency and Computation*. https://doi.org/10.1002/cpe.6919

15. Camarena, J. (2022). *Importancia De Los Registros, La Estadística Y Los Sistemas De Información Para La Gerencia De Los Servicios De Salud*. saluta, 4, 10-30.

https://doi.org/10.37594/saluta.v1i4.606

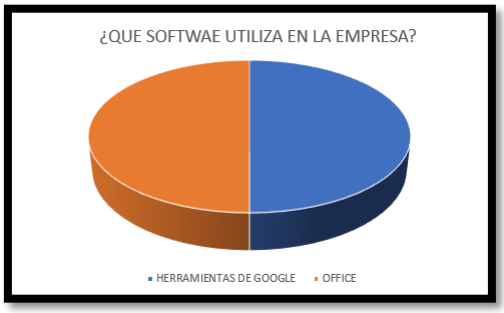
16. Ballesteros, J., Chaparro, F. (2016). *Seguridad En Redes Inalámbricas De Acceso Local Bajo Parámetros De Uso De Herramientas Libres. TECNIA*, 1(26), 57. https://doi.org/10.21754/tecnia.v26i1.7
17. Valencia, M., Larrea, N., Vaca, M. (2022). *Mejora Del Sistema De Almacenamiento De Un Servidor De Backups Mediante La Evaluación De Los Sistemas De Duplicación Opendedup* (Sdfs) Y Zfs. AP, 3(4), 209-225. https://doi.org/10.33262/ap.v4i3.248
18. Fiallos, J., Barahona, A., Naranjo, P., Segovia, D. (2019). *Modelo Para La Reducción De Riesgos De Seguridad Informática En Servicios Web. Cumbres* (En línea), 2(4), 19-30. https://doi.org/10.48190/cumbres.v4n2a2
19. Veloz, J., Alcivar, A., Salvatierra, G., Silva, C. (2017). *Ethical Hacking, Una Metodología Para Descubrir Fallas De Seguridad En Sistemas Informáticos Mediante La Herramienta Kali-linux. Inf. y Sistemas*, 1(1). https://doi.org/10.33936/isrtic.v1i1.194
20. Valencia, J., Valencia, A., Bedoya, J. (2020). *Implementación De Un Sistema De Seguridad Perimetral Informático Usando Vpn, Firewall E Ids. Rev. Univ. Catol. Oriente*, 45(31), 84-99. https://doi.org/10.47286/01211463.284

ANEXOS

FASE I:

- **Entrevistas**

ENTREVISTA CON EL PERSONAL DE ASR CONSULTORES EIRL								
APELLIDO Y NOMBRE	¿QUE SOFTWAE UTILIZA EN LA EMPRESA?	¿QUE SOFTWARE UTILIZA PARA LA CONEXION A INTERNET?	¿QUE SOFTWARE UTILIZA PARA LA CONEXION A CLIENTE?	¿QUE SOFTWARE UTILIZA PARA VER VIDEOS O ESCUCHAR MUSICA?	¿EN QUE HORARIO SIENTE QUE EL SERVICIO DE CONEXION A INTERNET FALLA?	¿ESTARIA DISPUESTO A DEJAR DE USAR SU SERVICIO DE STREMING EN LA PC DE LA OFICINA?	¿ENTIENDE QUE LA PC DE LA OFICINA SOLO ES PARA USO DE TRABJO Y NO PARA EL USO DE SERVICIOS DE ENTRETENIMIENTO?	¿CUANDO SE PIERDE LA CONEXION DE INTERNET EN QUE TIEMPO REGRESA?
DE LA TORRE B. PAULO	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	YOUTUBE	10:00 AM - 11:30 AM	SI	SI	15 MIN
FLORES V. CATHERINE	OFFICE	CHROME	INTERNET EXPLORER	SPOTIFY	09:00 AM - 11:30 AM	SI	SI	10 MIN
GALVEZ V. LUIS	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	YOUTUBE	09:30 AM - 11:30 AM	SI	SI	MAS E 20 MIN
VALDIVIA A. NATALIE	HERRAMIENTAS DE GOOGLE	FIREFOX	INTERNET EXPLORER	YOUTUBE	10:00 AM - 11:30 AM	SI	SI	15 MIN
VASQUEZ D. KAREN	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	YOUTUBE	09:00 AM - 11:30 AM	SI	SI	MAS E 20 MIN
AGÜERO B. VANIA	OFFICE	CHROME	INTERNET EXPLORER	SPOTIFY	10:00 AM - 11:30 AM	SI	SI	10 MIN
ASENCIOS B. CARLOS	OFFICE	FIREFOX	INTERNET EXPLORER	SPOTIFY	10:00 AM - 11:30 AM	SI	SI	15 MIN
BARREDA Q. SANDRA	OFFICE	CHROME	INTERNET EXPLORER	SPOTIFY	09:00 AM - 11:30 AM	SI	SI	MAS E 20 MIN
HEROS P. JULIO	OFFICE	CHROME	INTERNET EXPLORER	YOUTUBE	09:30 AM - 11:30 AM	SI	SI	MAS E 20 MIN
JIMENEZ A. VIRGINIA	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	SPOTIFY	10:00 AM - 11:30 AM	SI	SI	15 MIN
LEONARDO R. GERALDINE	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	SPOTIFY	10:00 AM - 11:30 AM	SI	SI	MAS E 20 MIN
OCHOA O. JESSICA	OFFICE	FIREFOX	INTERNET EXPLORER	YOUTUBE	09:00 AM - 11:30 AM	SI	SI	MAS E 20 MIN
RIVERO M. SANDRA	HERRAMIENTAS DE GOOGLE	CHROME	INTERNET EXPLORER	SPOTIFY	09:30 AM - 11:30 AM	SI	SI	10 MIN
YOSHIMOTO S. ANDREA	OFFICE	CHROME	INTERNET EXPLORER	YOUTUBE	09:00 AM - 11:30 AM	SI	SI	10 MIN



- **Revisión de equipamiento de comunicaciones:**

- **Acta de Información del Proyecto:**

Información del Proyecto

Datos

Empresa / Organización	ASR CONSULTORES EIRL
Proyecto	Implementación de red basado en Linux – firewall perimetral
Fecha de preparación	May 2014
Cliente	Julio Campos Martos
Patrocinador principal	Julio Campos Martos
Gerente de Proyecto	Rene Zamudio Ariza

Patrocinador / Patrocinadores

Nombre	Cargo	Departamento / División	Rama ejecutiva (Vicepresidencia)
Julio Campos Martos	**Gerente General**	**Gerencia**	

Propósito y Justificación del Proyecto

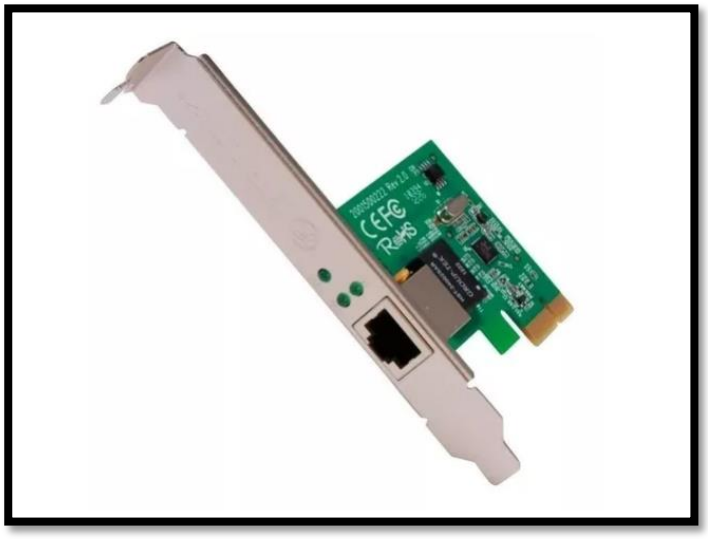
Implementar la red de negocio de ASR CONSULTRES, teniendo en cuenta los parámetros solicitados por el negocio

Descripción del Proyecto y Entregables

Instalación de un servidor con el sistema operativo Linux CentOS
Implementación de la solución con equipos virtuales con software Oracle Virtual box
Instalación y configuración de Pfsense para la red local
Instalación y configuración de Pfsense para la red de visita
Mantenimiento de equipos tecnológicos computacionales

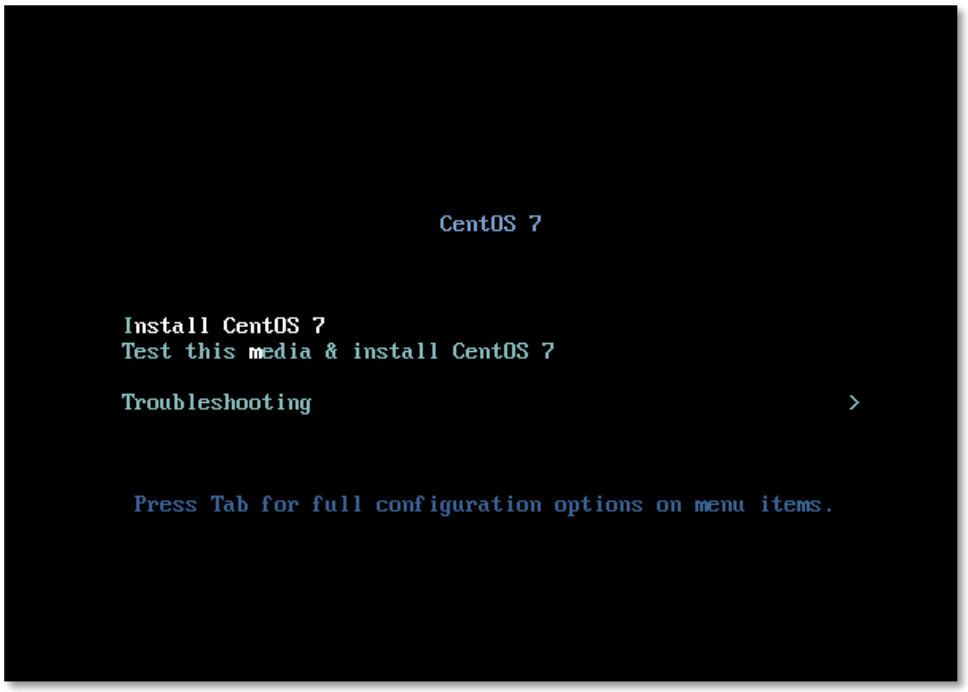
- **Fase II: Compra de equipamiento**
    - Servidor hp proliant ml 110

    - **Tarjetas de red (3)**

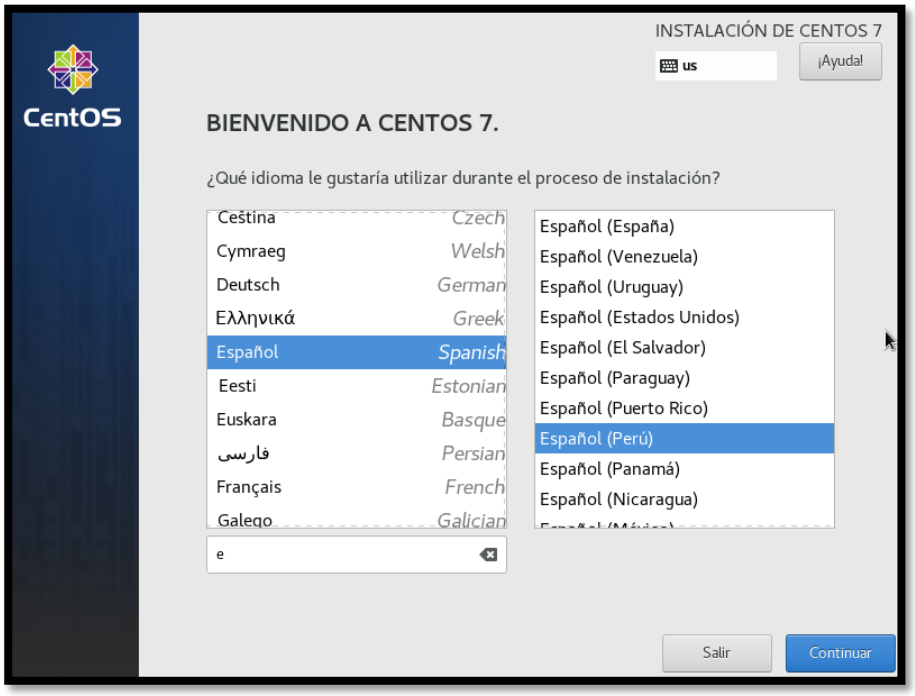


- **Fase III:**
    - **Instalación de CentOS 7**

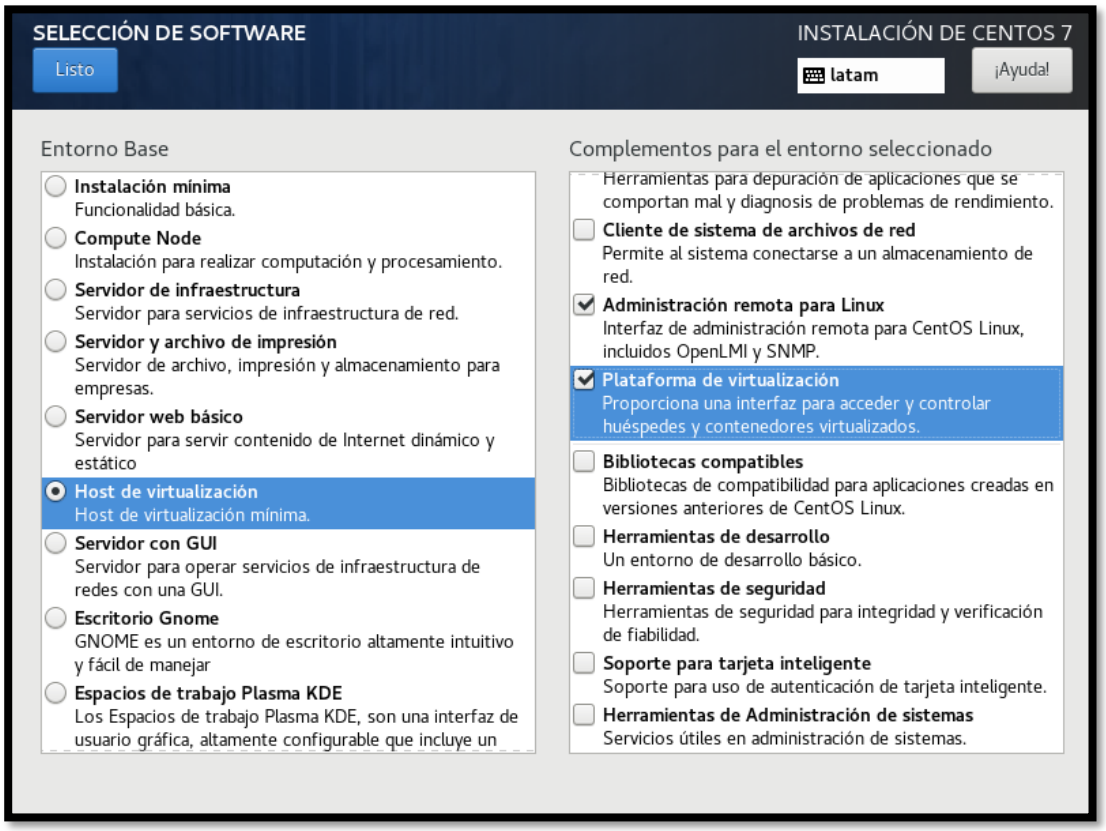
1. **Se bootea desde el portable del sistema operativo**
2. **Se selecciona Install CentOS 7**



3. **Se selección el idioma de instalación.**



4. **Se selecciona el paquete de instalación.**



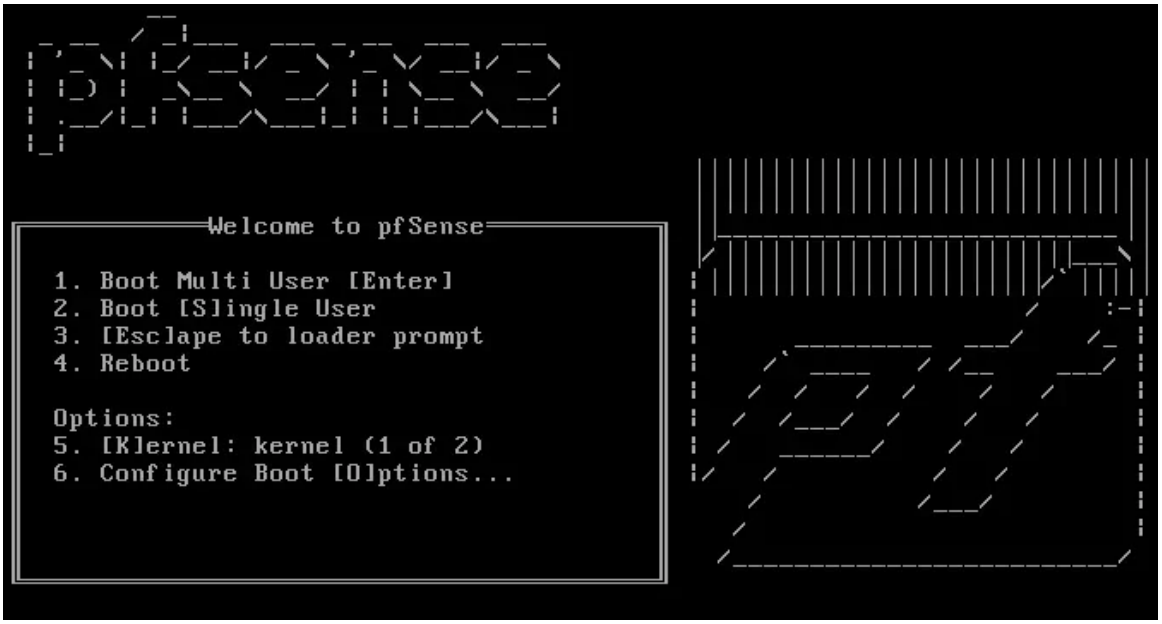
5. **Se configura la IP del sistema (Configuración de red).**

6. **Se configuran las contraseñas de Root y usuario admin**

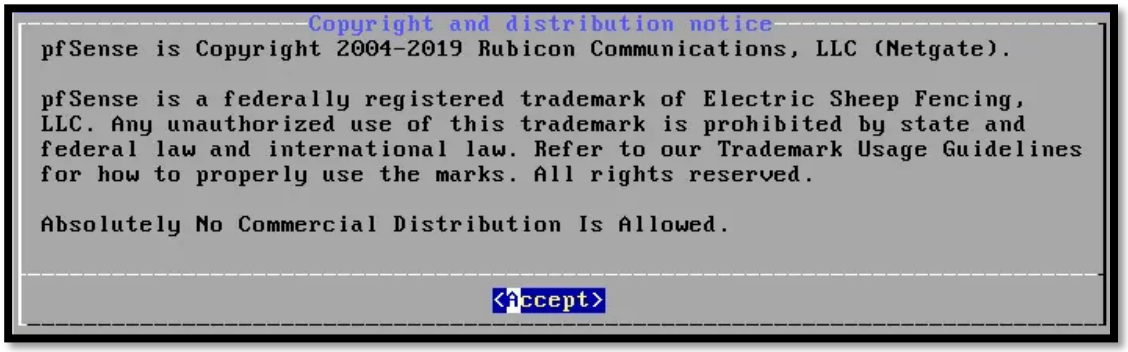
7. **Reiniciar el servidor.**

- **Instalación de Pfsense (intranet - extranet)**

1. **Realice el arranque de la computadora usando los medios de instalación de Pfsense.**
2. **En la pantalla de bienvenida, presione Entrar para iniciar el proceso de instalación de Pfsense**.

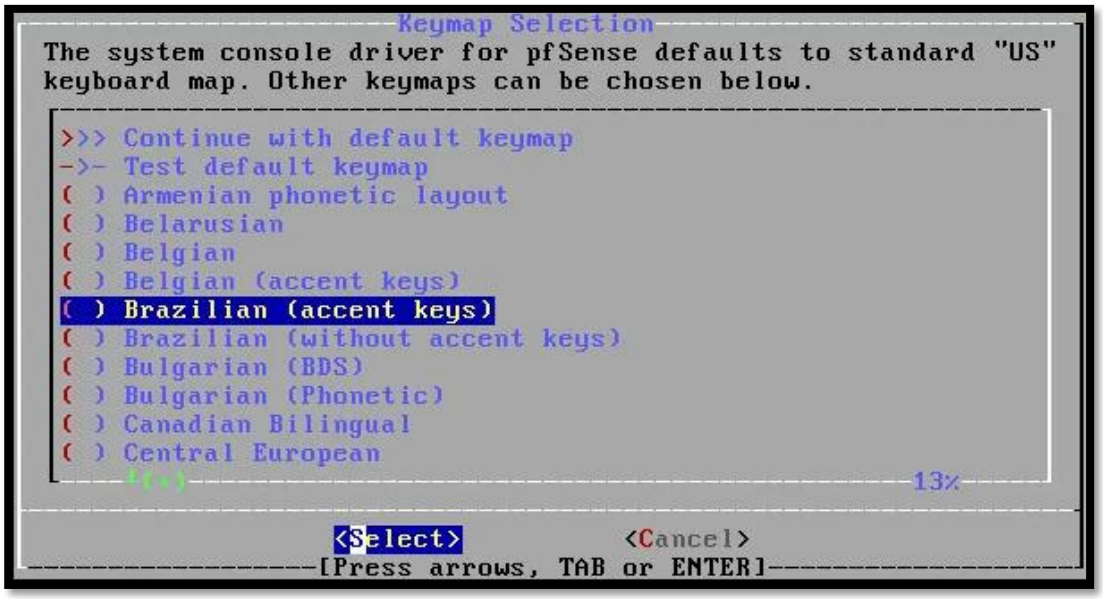


3. **Acepte el Acuerdo de licencia de usuario final de Pfsense**.



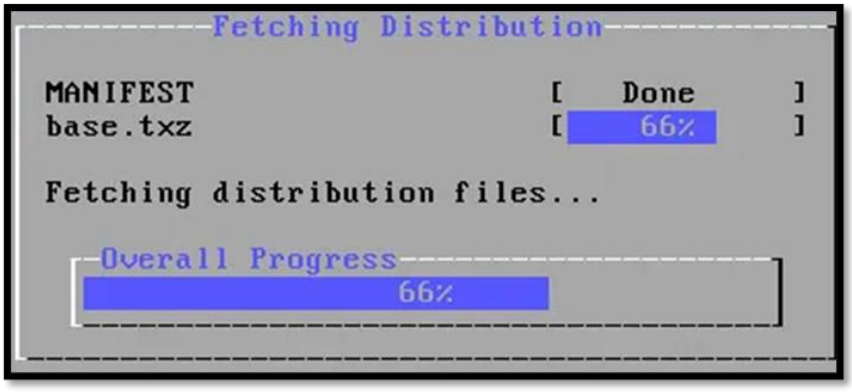
4. **Seleccione la opción Instalar en la pantalla de bienvenida**

5. **Seleccione el diseño de teclado Pfsense deseado.**

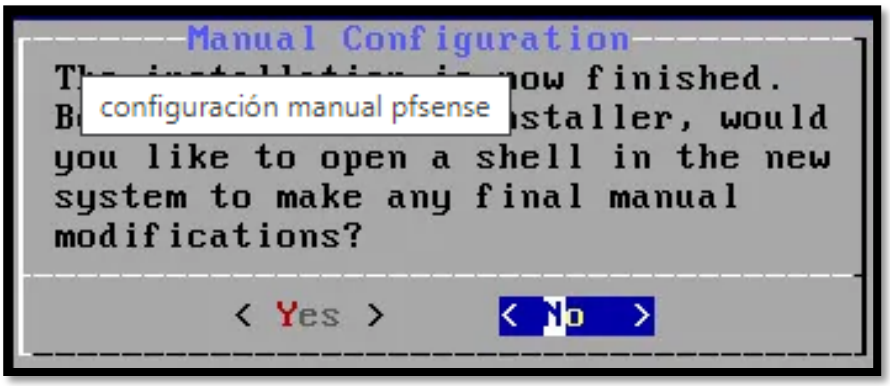


6. **Seleccione la opción Auto (UFS) para realizar la partición del disco automáticamente.**

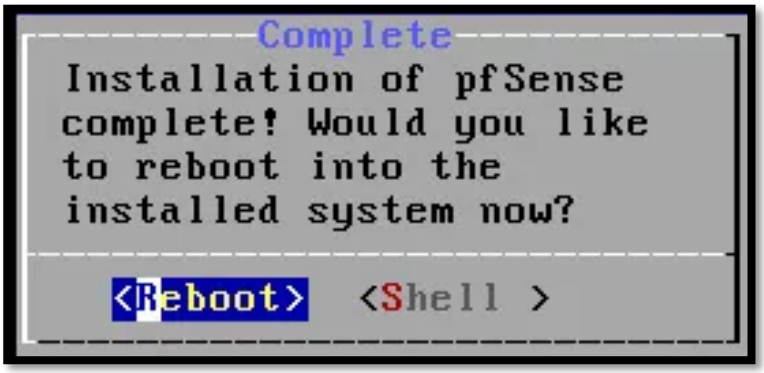
7. **El sistema iniciará la instalación del servidor Pfsense.**
8. **Espera a que termine la instalación.**



9. **Seleccione la opción No en la pantalla de configuración manual.**



10. **Retire los medios de instalación y presione Entrar para reiniciar la computadora.**



11. **Después de reiniciar, la consola de Pfsense.**
12. **A continuación, el sistema intentará detectar la lista de interfaces de red disponibles.**
13. **El sistema le pedirá que elija 1 interfaz como interfaz externa (WAN).**
14. **El sistema le pedirá que elija 1 interfaz como interfaz interna (LAN).**

- **Acta de conformidad del Proyecto**

ASR Consultores EIRL

ACTA DE CONFORMIDAD

Conste por el presente documento que en la fecha el servicio realizado por **Rene Alejandro Zamudio Ariza.**

Se deja constancia de que el servicio de **IMPLEMENTACIÓN DE UNA RED VIRTUALIZADA, EMPLEANDO EL SISTEMA OPERATIVO LINUX CENTOS PARA MEJORAR LA SEGURIDAD Y EL CONTROL DE ACCESO A INTERNET.**

Se ha realizado y efectuado a entera satisfacción de **ASR CONSULTORES EIRL** de acuerdo con lo solicitado y coordinado con la Gerencia General.

Habiendo culminado el servicio en los plazos establecidos correspondientes, se firma la presente por parte de **ASR CONSULTORES EIRL,** en señal de conformidad.

Se expide el presente documento

Lima, 30 de junio de 2014

JR. ICA NRO. 270 DPTO. 202 LIMA - LIMA - LIMA