IMPLEMENTACIÓN DE UN SERVIDOR FIREWALL-PROXY BAJO LA PLATAFORMA DE GNU/LINUX PARA LA FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS, A FIN DE LIBERAR PROCESAMIENTO DE LOS EQUIPOS DEL DATA CENTER DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Galo Israel Espinosa Padilla

***Abstract*— The data network of the Technical University of the North is administered by the Directorate of Technological and IT Development, the same that has the management of the network segments of the different dependencies of the institution, including the VLANs of each one of faculties.**

The management of the institutional data network is centralized, leading to congestion of traffic and processing information in a single sector. The project allows to manage the network traffic of each faculty of the Technical University of North in order to optimize access to the Internet service and manage the same independently.

It focused in the first instance on data collection and analysis of the situation, which allowed to clarify doubts that served as a basis to guide the solution better. The design of the project was based on a layered model based on the TCP / IP network architecture.

For the implementation of the solution and the fulfillment of the objectives, it was tried to use tools that are able and need to play with the raised about an operating system that contemplates the criteria of free software.

In this way it was possible to conclude with the implementation of an alternative that allows to administer the internet access service and manage the same according to requirements requested by users.

I. INTRODUCCIÓN

Debido al incremento de flujo de información y procesamiento de los equipos en las redes computacionales se tiende a tener puntos de congestión, un firewall es un sistema que nos conlleva a tener mayor control en el filtrado y enrutamiento de los paquetes que atraviesan por un segmento de red y nos proveen alguna forma de sectorización, permitiendo gestionar de una manera más óptima el tráfico; mientras que el proxy tiene la funcionalidad de un intermediario, conservando el contenido solicitado por los usuarios, acelerando las respuestas en futuras peticiones.

La red de la Universidad técnica del Norte se encuentra administrada y gestionada de una manera centralizada, condescendiendo a congestionar el tráfico y procesando la información en un solo sector, acarreando un elevado procesamiento, no acceso a servicios, encolamiento de paquetes y saturación de los Equipos del data center.

El objetivo es el de utilizar mecanismos que permitan liberar procesamiento de los equipos del data center por medio de la implementación de un firewall y proxy en cada facultad, bajo la plataforma de GNU/Linux, que ayuden a controlar el contenido de la información que atraviesa cada segmento de la red.

Para poder cumplir con el objetivo se presenta el diseño de la solución, tomando como referencia la arquitectura de red TCP/IP, el proceso de implementación y pruebas de funcionamiento del proyecto realizado procurando puntualizar las conclusiones y recomendaciones al trabajo realizado.

II. MARCO TEÓRICO

A. *Redes Computacionales*

Las redes computacionales y las tecnologías de comunicación se han desarrollado de tal manera que se ha integrado nuevos servicios y aplicaciones que permiten el evidente proceso y perfeccionamiento de la transmisión de la información a través de las entidades y sistemas de transmisión.

Existen 4 clasificaciones de redes computacionales.

CLASIFICACIÓN:

- Redes de área local (LAN).
- Redes de área metropolitana (MAN).
- Redes de área amplia (WAN).
- Redes inalámbricas

B. *Arquitectura de Red*

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo.

El propósito de la capa física es transportar un flujo de datos de una maquina a otra. Es posible utilizar varios medios físicos para la transmisión. Cada medio de transmisión tiene sus propias características como; ancho de banda, retardo, costo, facilidad de instalación y mantenimiento [1].

La capa enlace de datos prepara los paquetes para transportarlos a través de los medio locales mediante su

E. R. Carlosama estudia en la Carrera de Ingeniería Electrónica y Redes de Comunicación, Universidad Técnica del Norte, Ibarra, Ecuador (e-mail: ercarlosama@utn.edu.ec).

encapsulación con encabezado y un tráiler para crear una trama.

La capa de internet se encarga de llevar los paquetes desde el origen hasta el destino. Llegar al destino puede requerir muchos saltos por enrutadores intermedios. Por lo tanto, la capa de red es la capa más baja que maneja la transmisión de extremo a extremo.

La capa de transporte permite la segmentación de datos y proporciona el control necesario para rearmar estos segmentos en los distintos streams de comunicación.

Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación.

C. Jerarquía de Redes

Para optimizar el ancho de banda, la red debe estar organizado de manera que el tráfico se conserve de manera local y no se propague innecesariamente a otras partes de la red. El uso del modelo de diseño jerárquico de tres capas ayuda a organizar la red [2].

La capa de acceso nos brinda conectividad a los usuarios finales, típicamente está conformado solo por switch's de acceso.

La capa distribución interconecta la capa de acceso a la capa de núcleo. Se puntualiza los enlaces redundantes para distribuir la información del nivel de acceso.

La capa de núcleo representa una capa troncal de alta velocidad entre redes dispersas.

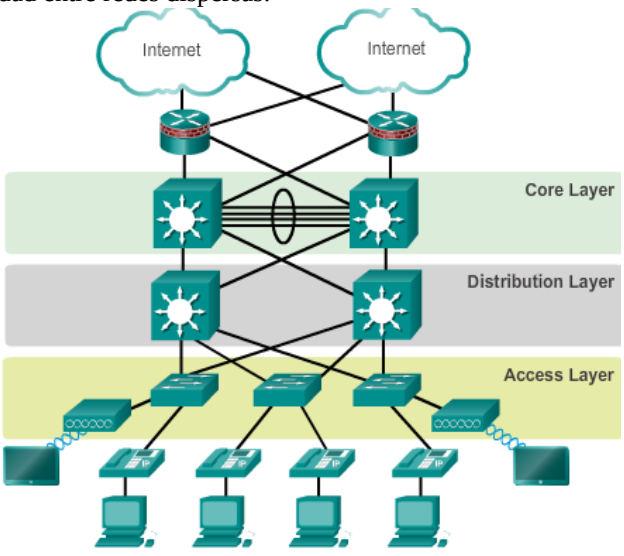

Fig. 1 Diseño de red jerárquica

D. Firewall-Proxy

Un firewall es una entidad confiable que se asienta para separar áreas sensibles dentro de una red de computadoras. El cortafuegos (firewall) se configura con un conjunto de reglas que dependen de las políticas de seguridad de la organización, que determinan a que tráfico de red se le permitirá pasar y cual será bloqueado o rechazado [3].

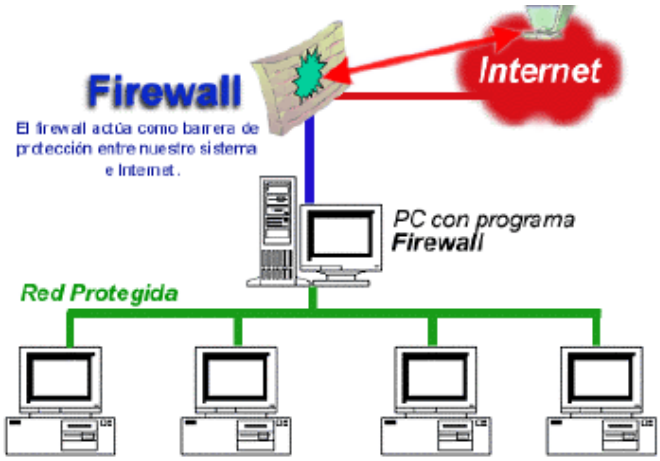

Fig2. Esquema de un Firewall.

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial [4].

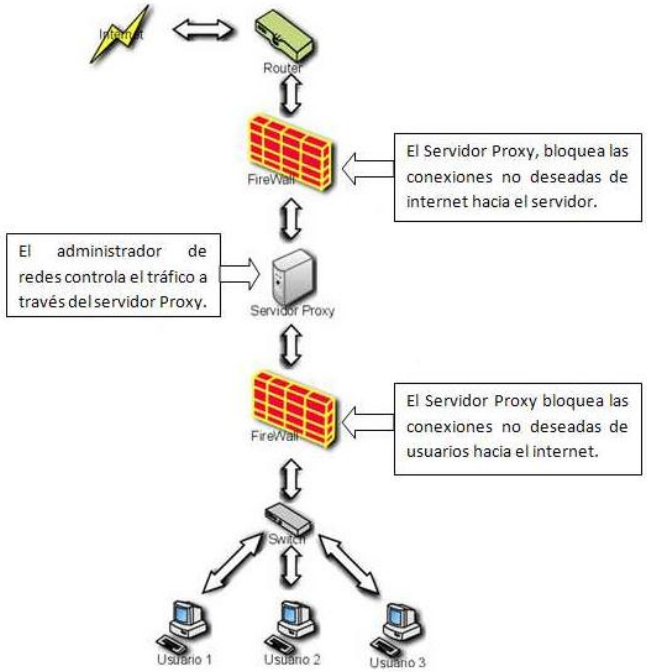

Fig3. Funcionamiento de un servidor proxy

E. Diseño

La primera parte del diseño empieza con el diagrama lógico, Este modelo detalla la topología de red sin detalles de instalación del cableado. Es un mapa de ruta básico.

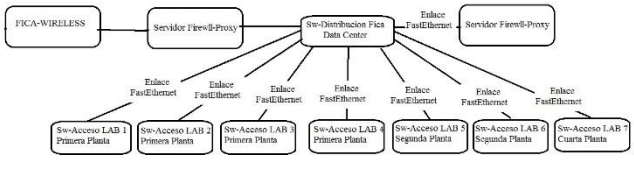

Fig4. Diagrama Lógico FICA-UTN

El diseño de capa 2 detalla cuantos puertos del switch están siendo utilizados y la velocidad en que trabaja cada uno medido en bits por segundo.

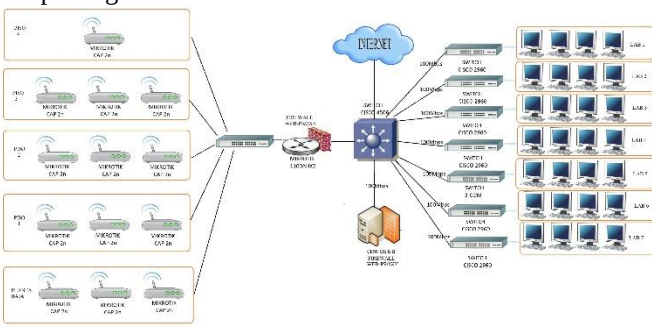

Fig5. Diagrama de capas 2 Firewall-Proxy FICA

El diseño de capa 3 detalla cómo fueron creadas las VLAN´s de laboratorios de la Facultad de Ingeniería en Ciencias Aplicadas (FICA). Estas subredes permiten la comunicación entre segmentos basados en direcciones de Capa 3 o direcciones IP. Por seguridad, el direccionamiento mostrado en esta sección solo hace referencia al último octeto; los primeros tres octetos son representados con letras x,y.

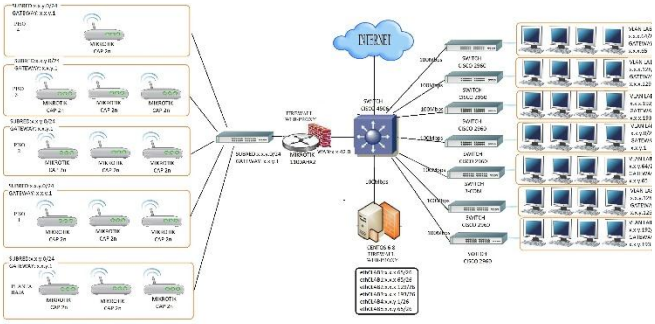

Fig6. Diagrama de capa 3 Firewall-Proxy FICA

F. Implementación.

Interfaces Virtuales VLAN´s.

Las VLAN´s son todas las interfaces instaladas en el servidor y que se configurarán para la implementación de las reglas de seguridad en el Firewall.

Nombre	Tipo	Dirección IP	Máscara de red
eth0	Ethernet	172.17.41.250	255.255.254.0
eth0:64	Ethernet (Virtual)	172.17.40.65	255.255.255.192
eth0:128	Ethernet (Virtual)	172.17.40.129	255.255.255.192
eth0:192	Ethernet (Virtual)	172.17.40.193	255.255.255.192
eth0:410	Ethernet (Virtual)	172.17.41.1	255.255.255.192
eth0:4164	Ethernet (Virtual)	172.17.41.65	255.255.255.192
lo	Loopback	127.0.0.1	255.0.0.0

Fig7. . Interfaces de red configuradas.

POLITICAS Y REGLAS IPTABLES

Las políticas se orientan en denegar todo tráfico Input, Output y Forward.

- iptables -P INPUT DROP
- iptables -P OUTPUT DROP
- iptables -P FORWARD DROP

Input

• Se aceptan todo tráfico que se origina en la interfaz de loopback, esto permite procesar tareas que se originan en el sistema.
  - iptables -A INPUT -i lo -j ACCEPT

• Se acepta tráfico que sea relacionado y establecido, esto permite el tránsito de datos que sea peticionado por los clientes de los laboratorios.
  - iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

• Se permite tráfico con destino al puerto SSH.
  - iptables -A INPUT -p tcp --dport 22 -j ACCEPT

• Se permite el tráfico a Webmin.
  - iptables -A INPUT -p tcp --dport 10000 -j ACCEPT

• Se permite tráfico ICMP
  - iptables -A INPUT -s $SUBREDLABS -p icmp -j ACCEPT

• Se Acepta tráfico entrante por el puerto 80 ya sea udp o tcp
  - iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
  - iptables -A INPUT -p udp -m state --state NEW --dport 80 -j ACCEPT
  - iptables -A INPUT -p tcp -m state --state NEW --dport 80 -j ACCEPT

• Se acepta trafico que este direccionado al puerto del proxy
  - iptables -A INPUT -s $SUBREDLABS -p tcp --dport 3128 -j ACCEPT

Output

• Se permite todo tráfico Loopback
  - iptables -A OUTPUT -o lo -j ACCEPT

• Se permite todo tráfico establecido
  - iptables -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

Forward

• Se permite el tráfico Relacionado y establecido
  - iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

• Se permite tráfico SSH.
  - iptables -A FORWARD -p tcp --dport 22 -j ACCEPT

• Se permite tráfico destinado al servidor de archivos.
  - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 139 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p tcp --dport 445 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 137 -j ACCEPT
  - iptables -A FORWARD -s $SUBREDLABS -p udp --dport 138 -j ACCEPT

• Se permite consultas de servidor DNS con origen en la VLAN de Laboratorios.
  - iptables -A INPUT -s $SUBREDLABS -m state --

state NEW -m tcp -p tcp --dport 53 -j ACCEPT

- iptables -A INPUT -s $SUBREDLABS -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT

REGLAS PROXY

Para implementar las reglas en el Proxy hay que establecer los puertos y trabajo en red en la que va actuar el servidor.

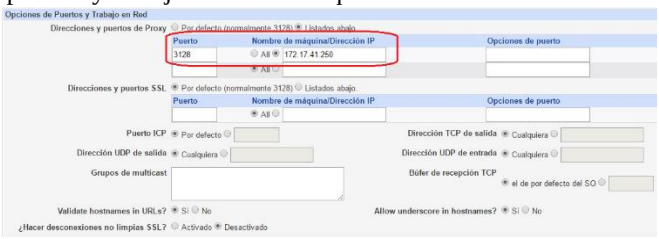

Fig8. . Dirección y Puerto de Comunicación de Proxy

CONTROL DE ACCESO

Se han implementado seis listas de control de acceso cada una de estas representa la VLAN de cada laboratorio.

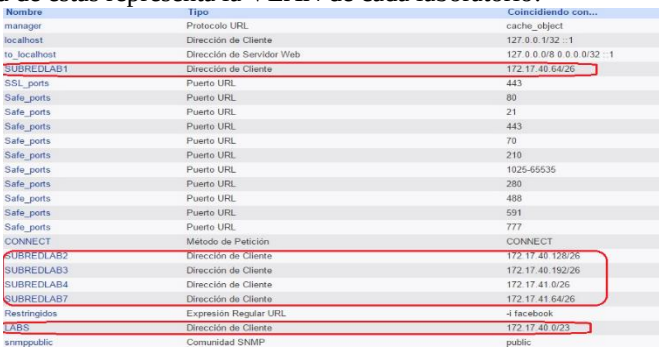

Fig9. Lista de control de acceso Proxy

G. Pruebas de funcionamiento.

USO DEL PROXY PARA ACCESO A INTERNET

Se puede verificar que se hace una petición al sitio Web Facebook pero la respuesta siempre la hace el servidor Firewall-Proxy implementado

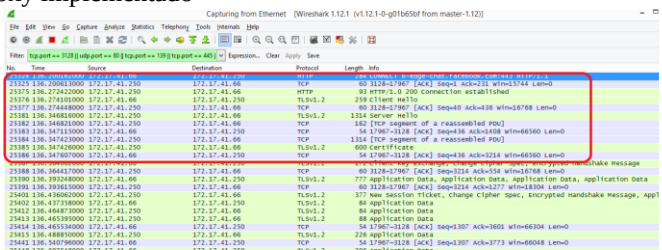

Fig10. Trafico que responde el Proxy

TIEMPOS DE ACCESO

Se puede comprobar que los tiempos de acceso se reducen debido al uso del servidor proxy.

El método de prueba se presenta mediante la carga de un sitio web sin el direccionamiento hacia el proxy y otra con direccionamiento al servidor.

Fig. 11 Tiempo de Carga de un sitio Web

GENERADOR DE REPORTES SARG

El generador de reportes SARG es una herramienta de desarrollo libre que se implementó en el proxy nos presenta detalles en forma gráfica y en tiempos de la cantidad de Bytes que se han transportado por la red.

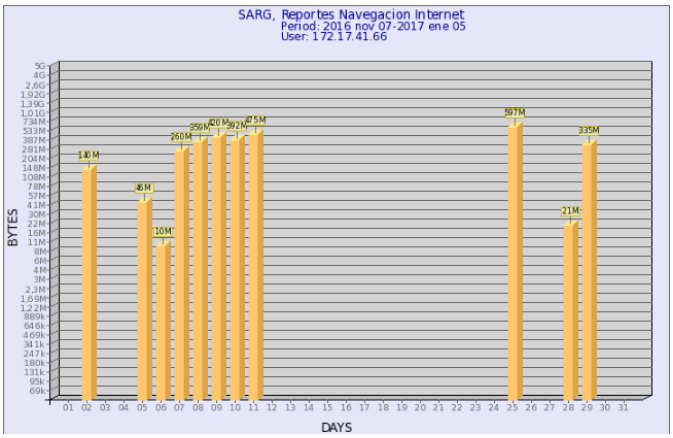

Fig. 12 Generador de Reportes Gráfico SARG.

PROCESAMIENTO EN EQUIPOS

Para esta prueba de funcionamiento se toma como escenario experimental con los siguientes detalles:

- Se realiza en un laboratorio con 34 equipos.
- El procesamiento se mide en el switch de distribución del data center de la Fica.
- Se mide el procesamiento del equipo de distribución con el servidor Firewall-proxy y la otra medición se realiza sin el servidor Firewall-proxy.
- Se realizan dos mediciones: una en horario normal de uso de los laboratorios de 14:50 pm durante 20 minutos y otra en un horario donde se pueda registrar el procesamiento de los equipos en un horario donde no existe mucho tráfico de datos 20:30 pm durante 15 min. En los dos casos se procuró generar la mayor cantidad de tráfico posible.

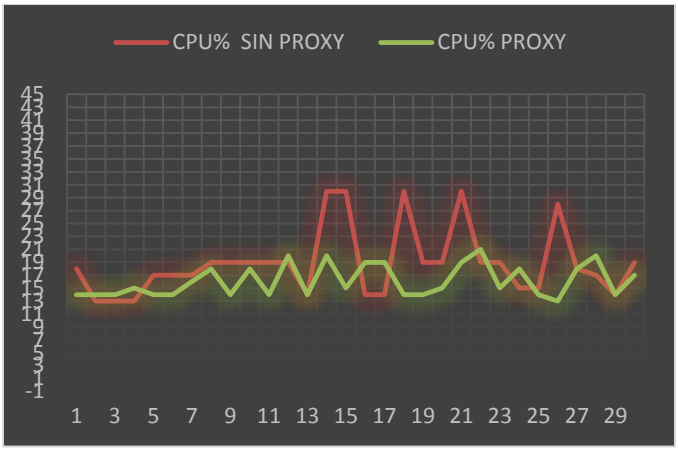

Fig. 13 Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 1.

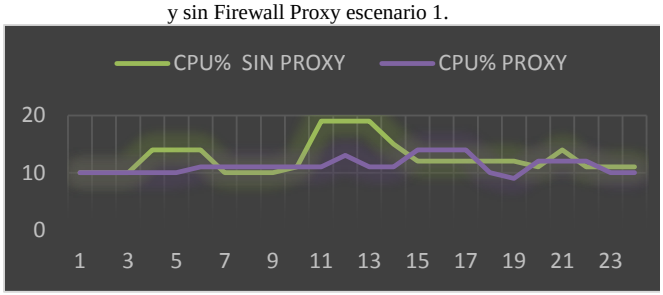

Fig. 14 Consumo de Procesamiento Sw-Dist. con servidor Firewall-Proxy y sin Firewall Proxy escenario 2.

III. CONCLUSIONES

- El servidor Firewall-Proxy se instaló sobre el sistema operativo CentOs, el mismo que cumple los conceptos de libertad, y se implementó en la Facultad de Ingeniería en Ciencias Aplicadas, verificando el ahorro en tiempo de respuestas de páginas web y constatando la disminución de procesamiento de los equipos del Data Center mismo que se ve afectado en el aumento del porcentaje de uso de CPU del servidor Firewall-Proxy.
- La documentación de las bases teóricas, permitió esclarecer dudas sobre el proceso que se tomó en consideración para el desarrollo del proyecto, se concluyó que para el diseño fue fundamental tomar como referencia la arquitectura de red TCP/IP, misma que sustentó la determinación de requerimientos, detección de errores, corrección de errores, pruebas y mantenimiento en el proceso de implementación del servidor Firewall-Proxy.
- La creación de subredes en la VLAN de laboratorios permitió gestionar de manera autónoma cada laboratorio, con lo cual se ha cumplido un objetivo específico dentro del desarrollo del proyecto, controlando el acceso al servicio de internet así como la gestión de sitios web a los que se quiere acceder.
- Las políticas y reglas asignadas al Firewall fueron definidas en base a las necesidades de cada Facultad, considerando el reglamento interno de uso de laboratorios y acorde con las políticas institucionales manejadas por el administrador de la red de datos, esto facilitó la asignación de reglas tanto de entrada, salida y enrutamiento en el servidor, así como la documentación de las políticas establecidas.
- Es recomendable dimensionar el hardware acorde con las necesidades y funciones que este debe realizar, y considerar un estándar IEEE 29148 para la elección de un software, ya que de esta manera se podrá obtener una visión clara de que requerimientos son los necesarios, como se estructurará y que actores formarán parte del sistema.

IV. REFERENCIAS

[1] A. S. &. W. Tanenbaum, Redes decomputadoras, Pearson New International Edition, 2012.

[2] C. N. Academy, «Exploracion de la red,» 2015.

[3] J. Esparza Morocho, Implementacion de un Firewall sobre plataforma Linux, Quito, 1013.

[4] L. G. &. V. T. G. A. Arévalo Galárraga, nalisis, diseño e implementación de un software prototipo de firewall y servidor proxy, 2010.

V. BIOGRAFÍAS

Galo I. Espinosa P. nació en Ibarra en Ecuador, el 27 de abril de 1990. Sus estudios de primaria los realizó en la Unidad Educativa Hermano Miguel “La Salle” Se graduó como técnico en Informática y estudió Electrónica y redes de comunicación en la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad de Técnica del Norte de la ciudad de Ibarra - Ecuador.