



PROPUESTA DE SOLUCIONES DE SEGURIDAD UTILIZANDO ENTORNOS DE VIRTUALIZACIÓN SOBRE SOFTWARE LIBRE PARA LA EMPRESA DE DESOFT VILLA CLARA

Ing. Alberto Rodríguez Carvajal
Desoft
alberto.rodriguez@vcl.desoft.cu

RESUMEN

El presente trabajo tiene como objetivo principal una propuesta de seguridad aplicada al entorno de la infraestructura de red y servicios informáticos de la División de Desoft Villa Clara. En él se recoge un enunciado de los principios determinantes de la seguridad informática aplicada a entornos de virtualización, un estudio de la multiplataforma de virtualización proxmox. Se realiza una caracterización de los entornos de red de la División, debilidades infraestructurales y posibilidades para un posible mejoramiento del sistema de seguridad. Se realiza un levantamiento de la tecnología de hardware existente en la División recomendando la más idónea para la virtualización, siempre teniendo en cuenta las prestaciones que brinda esta empresa a sus usuarios y clientes.

Por último se realiza una propuesta de mejoras para el sistema de seguridad con que cuenta esta empresa, desde la propia arquitectura de red hasta los servicios sobre software libre desde las perspectivas del lado del usuario y un grupo de herramientas para la gestión, supervisión, análisis de conectividad, tráfico así como la confidencialidad de los paquetes que viajan a través de la red de datos para los administradores de red. Se tendrán en cuenta las herramientas de software libre, previamente probadas sobre recreaciones sencillas de entornos a los que se podrían aplicar.

1. INTRODUCCIÓN

El crecimiento de los ordenadores y de la tecnología de la información ha sido explosivo. Nunca antes una tecnología completamente nueva se ha propagado por todo el mundo con tal velocidad y con tan gran penetración de prácticamente todas las actividades humanas. Las computadoras han traído gran beneficios a campos tan diversos como los estudios del genoma humano, exploración espacial artificial en Inteligencia, y una serie de aplicaciones, desde la más trivial a la que mejora la vida.[1]

Hasta finales de 1988 muy poca gente se tomaba en serio el tema de seguridad en redes de computadores de propósito general. Sin embargo, el 22 de noviembre de 1988 Robert T. Morris protagonizó el primer gran incidente de seguridad informática: uno de sus programas se convirtió en el famoso *worm* o gusano de Internet. Miles de ordenadores conectados a la red se vieron inutilizados durante días, y las pérdidas se

estiman en millones de dólares. Desde ese momento el tema de la seguridad en sistemas operativos y redes ha sido un factor a tener muy en cuenta por cualquier responsable o administrador de sistemas informáticos. [2]

El desarrollo de Internet ha creado un ambiente en el que millones de ordenadores en todo el mundo están todos conectados el uno al otro. Además, el acceso a esta red es bastante ubicuo y barato, lo que permite a cualquier ladrón en el mundo atacar su equipo, independientemente de su ubicación física. Después de encontrar una nueva vulnerabilidad y desarrollar un *exploit*, pueden atacar sistemas similares en todo el mundo. Por lo tanto, la manera de proteger sus activos informáticos tiene que cambiar para adaptarse a esta nueva amenaza. Además, el carácter internacional y distribuido de la Internet hace que sea muy difícil de regular y controlar los ataques contra los sistemas informáticos. [3]

En los últimos años la seguridad informática en Cuba ha ido tomando un rol protagónico de gran importancia, ya que nuestro país no queda exento de todas las amenazas anteriormente expuestas a las TIC. Cuba es un país en desarrollo económico y además bloqueado por EEUU, hay mucho sitios a los que desde nuestro país no se puede acceder a través de Internet, debido a que se encuentran bloqueados solo para nuestro país, y por lo tanto conseguir a veces a través de vías alternativas información tales como software, libros, manuales, etc, se hace muy dificultoso, cualquier pérdida de esta información que pueda ser provocada debido a un delito informático, contaminación por virus o desastre natural provocaría pérdidas considerables a la economía del país. La División Desoft Villa Clara tiene como misión fundamental la informatización de la sociedad cubana, en esta empresa se maneja información de carácter sensible de diferentes proyectos de carácter nacional e internacional, la ocurrencia de cualquier desastre provocaría la interrupción del flujo de trabajo en el sistema informático, proponer un grupo de soluciones de seguridad utilizando las posibilidades que brinda el software libre para mejorar la seguridad existente en la División de Desoft Villa Clara es la finalidad de este trabajo.

2. FUNDAMENTOS TEÓRICOS SOBRE SEGURIDAD EN ENTORNOS VIRTUALES

El diseño de una solución de seguridad depende de cómo se lleven a la práctica los servicios fundamentales de identificación, autorización, autenticación, no repudio, integridad y confidencialidad. [4]

“Aun cuando el término virtualización ha sido acuñado en el contexto de los sistemas mainframe de IBM, introducidos en la década de los 60's” (Polze y Tröger, 2012), uno de los retos actuales es el aseguramiento de este tipo de entornos, que a diferencia de la infraestructura física, plantea nuevos desafíos. En contraste con los entornos físicos, los entornos virtuales basan su operación en infraestructura física unificada, es decir, un servidor físico puede contener uno o varios sistemas operativos hospedados en una misma plataforma. Aquí el tema de seguridad de ambientes virtuales juega un papel importante.

Se puede hacer uso de herramientas de software libre para ayudar a resolver problemas de seguridad virtual, tanto en entornos virtuales puros como en mixtos. Para asegurar los entornos virtuales al igual que cualquier componente físico de TI, se debe comenzar con un plan de instrumentación de seguridad para los entornos virtuales, un buen punto de inicio es consultar a los principales proveedores de soluciones, los

cuales son unos de los primeros involucrados en el tema debido a la relevancia que tiene la seguridad en ambientes virtuales. [5]

3. LEVANTAMIENTO DE LA TECNOLOGÍA

El levantamiento en la división de Desoft Villa Clara dio como resultado que los servidores de la misma cuentan con una tecnología que no es la más idónea para realizar la virtualización ya que no son servidores profesionales, esta empresa cuenta con un total de 100 PCs conectados a los diferentes servicios de la red, sin contar con 60 PCs más que se encuentran en los municipios y que en un futuro se conectarán a la división. Con servidores profesionales se podría implementar un sistema de Backup (Salva) mucho más eficiente del que existe actualmente, así como facilitar el trabajo de gestión de los administradores de red de los diferentes servicios que brinda la división, como también mejorar la integridad, confidencialidad, disponibilidad para cada usuario conectado a la red, las características técnicas de los servidores actuales es: *INTEL SERVER BOARD S3000AH, [DualCore Intel Xeon 3050, 2133 MHz \(8 x 267\)](#), dos memorias de 2 GB DDR2-800 DDR2 CHC, dos discos duros de 500 GB*. Para contar con una red y a la vez con un sistema de seguridad mucho más eficiente y fiable del que actualmente existe se propone adquirir una tecnología para servidores que satisfaga las necesidades y prestaciones con que debe contar una empresa como lo es Desoft que se dedica principalmente a la informatización de la sociedad.

3. DISEÑO Y MODELACIÓN DE LA SEGURIDAD UTILIZANDO ENTORNOS DE VIRTUALIZACIÓN

Para el diseño de la seguridad es necesario detenerse brevemente en varios aspectos tales como: la selección del hardware (Servidores, Switch layer 3, Monitor), la topología que se utilizara en la red, el tipo de red, es decir si es una red LAN, MAN, CAN o una WAN, la distribución de las direcciones IP según el tipo de red, es decir si va utilizar IPv4, IPsec o IPv6, si se va a utilizar redes virtuales (VLAN) para disminuir el dominio de colisiones, el tipo de DMZ en que se montaran los servidores, la redundancia de las comunicaciones, como realizar el proceso de virtualización, la redundancia de los servicios (la réplica), la redundancia de la información guardada en los servidores y como realizar el sistema de salvallas, finalmente la modelación se realizara utilizando para ello máquinas virtuales para analizar el tráfico y probar en tiempo real la sobrecarga de los servicios más críticos en la red.

Selección del hardware

En la división Desoft Villa Clara se cuenta solo con PC de escritorio que hacen la función de servidores, estas últimas no cuentan con los requerimientos y prestaciones necesarios para comenzar el proceso de virtualización, ya que la mejor de ellas solo cuenta con las siguientes características: *INTEL SERVER BOARD S3000AH, [DualCore Intel Xeon 3050, 2133 MHz \(8 x 267\)](#), cuatro memorias de 2 GB DDR2-800 DDR2 CHC, dos discos duros de 500 GB*, y como mínimo el servidor de correo (Zimbra) necesita de 8 GB para que trabaje sin dificultades, esto último sin contar con los demás servicios que cuenta la división que entre ellos están: Ftp, jabber corporativo, Antivirus corporativo, OpenLdap, DNS, DHCP, más los demás servicios y aplicaciones del departamento de Desarrollo que en su mayoría manejan base de datos, utilizando para ello gestores de base de datos tales como: SQL.Server, PostgreSQL, Oracle, MySQL, que todos ellos en su mayoría consumen una gran

cantidad de recursos de hardware en la tabla 1 se puede observar algunas características técnicas y precios del hardware que se solicita [6] :

Tabla 1: Listado de precios y descripción del hardware.

Código	Descripción	Cantidad	Categoría	Precios cuc	Precios totales
NF5280 M3 GAMA ALTA RACK	Chassis 8 disk chassis (19" rack)// Processor E5-2630 / 6 cores / 2.2GHz Number of processors 2// Memory 8x8GB ECC DDR3 1600MHz// HDD 1TB 2.5" SAS hot swap Cant. HDD 5// RAID controller High performance RAID controller RAID level 5// NIC 4 x Gigabit ethernet NIC// Operating system No OS// Optical driver slim DVD-RW// Power supply	2	Servidor	\$ 4,862.30	\$ 9724.6
STORAGE AS1000 G6	Chassis 12 disk chassis (19" rack)// Cache 48GB cache// HDD 1TB 2.5" SAS hot swap Cant. HDD 12// Host interface 4 x 10GB iSCSI// Operating system No OS// Optical driver slim DVD-RW// Power supply redundant power supply //Accesories Sliding rails for 19" rack	1	Servidor	\$ 15,896.23	\$ 15,896.23
KVM 2162DS	Dell KVM 2162DS Remote Console Switch Keyboard/Video/Mouse Analog Switch (4x USB 2.0 Server Interface Ports, includes CAT 5 cables, TAA	1	Remote Console Switch Keyboard/Video/Mouse	\$ 3,563.45	\$ 3563.45
1020118 1	MONITOR LCD VIEWSONIC VG2228WM 22PULG	1	Monitor	\$ 275.00	\$ 275.00
AT-9924T	Switch layer 3 modular 24 port 10/100/1000	1	Switch layer 3	\$ 4,173.25	\$ 4,173.25
					\$ 33632.53

Topología de red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos, en particular la topología que se va a *utilizar es la topología*

en estrella, ya que un host no depende los demás cuando está conectado o desconectado de red. [7]

Selección del tipo de red

Hay muchos tipos de redes: redes de área local (LAN), redes de área amplia (WAN), redes de área metropolitana (MAN), redes de campus de Área (CANs), las redes Ethernet, redes Token Ring, Redes Fiber Distributed Data Interface (FDDI), modo de transferencia asíncrono (ATM), las redes Frame Relay , redes T1, redes DS3, redes de puentes, redes enrutadas y redes punto a punto, por nombrar algunos [8]. En este caso las soluciones de seguridad que se brindaran son enfocadas a la red LAN de la división de Desoft Villa Clara, los servidores se montarán en una *DMZ Lateral Three-part* configurada así una PC que se va a utilizar para que realice esta función instalándole un sistema operativo Linux y habilitándole un IPTABLES, para luego configurarlo.

Comunicaciones

Se definirá en el Switch-L3 las VLAN: 1, 2, 3, 4, 5, 6, 7,8, 9, esto disminuye el dominio de colisiones [8], y en los Switch-L2 de cada local se habilitarán dos puertos para cada VLAN y otros dos para redundancia, en estos Switch se definen untaggeando las VLAN, se les especifica mediante comandos los vid de cada VLAN y se untaggean los puertos para las mismas. Se utilizará solo las normas de cableado horizontal, ya que la distancia entre el Switch-L3 y los Switch-L2 es corta. [9]

Distribución de VLAN por departamento en la división Desoft Villa Clara

Se debe considerar la utilización de VLANs para la separación del tráfico entre máquinas virtuales, lo que permitirá cierto nivel de aislamiento entre cada una de ellas. La utilización de firewalls personales en cada una de las máquinas también constituye una línea de defensa, puede administrar el tráfico de red permitido desde y hacia cada una de las máquinas. Otra opción es el empleo de switches virtuales, éstos pueden segmentarla red y controlar el tráfico, sobre todo cuando varias máquinas virtuales hacen uso de una sola interfaz física. Mantener actualizados los sistemas también representa un menor riesgo en ambientes virtuales. [5]

Se utilizará dirección de Clase C con mascara variable e IPv4 y se definirá que se utilice IPsec, para aumentar la seguridad de los paquetes que viajan a través de la red LAN en la división donde se encuentran las PCs clientes, en caso que se migre en un futuro a IPv6 no sería necesario utilizar IPsec debido a que el IPv6 ya lo tiene implementado por defecto, mientras que los servidores de la división se montaran en una DMZ Lateral Three-part [10], estos últimos se conectaran a través del router a la VPN de Desoft. Las direcciones IP para las diferentes VLAN se pueden observar en la tabla 2, estas serán distribuidas por el servidor DHCP contra MAC Address, y se pondrán filtros MAC en la puerta de enlace y en cada firewall de cada servidor.

Tabla 2: rango de direcciones IP por departamento.

VLAN	Departamento	Direcciones de red	Rango de Direcciones IP	Cantidad de PC por departamento
VLAN 1	Economía	192.168.1.0/29	192.168.1.1-192.168.1.6	4

VLAN 2	Desarrollo	192.168.2.0/27	192.168.2.1-192.168.2.30	25
VLAN 3	administradores	192.168.3.0/29	192.168.3.1-192.168.3.6	3
VLAN 4	Recursos Humanos	192.168.4.0/29	192.168.4.1-192.168.4.6	4
VLAN 5	Dirección	192.168.5.0/29	192.168.5.1-192.168.5.6	5
VLAN 6	Negocios	192.168.6.0/28	192.168.6.1-192.168.6.14	12
VLAN 7	Despliegue	192.168.7.0/27	192.168.7.1-192.168.7.30	25
VLAN 8	Implementación	192.168.8.0/27	192.168.8.1-192.168.8.30	25
VLAN 9	Seguridad Informática	192.168.9.0/28	192.168.9.1-192.168.9.14	10

Redundancia en las comunicaciones

Se habilitará en cada uno de los Switch el uso de **spanning tree protocol** indicándole mayor prioridad al Switch-L3, con esto se buscara redundancia en las comunicaciones, si falla un enlace por algún motivo queda otro que automáticamente toma el lugar del que falló. [11]

4. VIRTUALIZACIÓN

Ventajas e inconvenientes de virtualizar un sistema operativo

La virtualización reduce los costes de espacio físico y de consumo eléctrico, aísla los fallos ya que, si un SO virtualizado da problemas no afectará al resto del sistema, ahorro en piezas de hardware, es posible migrar las máquinas virtuales en caliente ahorrando tiempo en la pérdida de servicio además de evitar servidores ociosos o congestionados. [12]

Las máquinas virtuales (virtual machines), a diferencia de un equipo físico, están reducidas a un simple archivo; que si bien representa flexibilidad para el administrador, también significa una vulnerabilidad que puede ser explotada para robar la máquina completa, incluyendo su contenido. Por otro lado, la seguridad virtual se extiende más allá de las máquinas virtuales, por ejemplo, los sistemas de almacenamiento de red se ven expuestos a amenazas y constituyen otra línea de acción para los atacantes. Una recomendación es mantener los sistemas de almacenamiento separados del resto de las máquinas virtuales. [5]

PROXMOX es una completa plataforma de virtualización basada en sistemas de código abierto que permite la virtualización tanto sobre OpenVZ como KVM. Es una distribución bare-metal, es decir no necesita de un sistema operativo previo, el propio entorno proporciona su propio sistema operativo base, en realidad monta un Debian con los servicios básicos. De esta forma se obtiene un rendimiento mucho mejor.

Características de Proxmox:

- Basado en Debian 7 a 64 bits.
- Amplio soporte de hardware.
- Anfitrión soporte para Linux y Windows de 32 y 64 bits.
- Soporte para los últimos procesadores Intel y el chipset AMD.
- La licencia es gratuita, no hay que pagarla.
- Web de administración con todas las características necesarias para crear y gestionar una infraestructura virtual.
- Gestión a través de la interfaz web sin necesidad de utilizar ningún software de cliente.
- La combinación de la tecnología de virtualización KVM dos y OpenVZ. [13]
-

Luego de la instalación de proxmox que se realiza de una forma sencilla, se debe introducir el login y acceder al menú principal donde podrá observar el estado del servidor, crear y configurar las máquinas virtuales y parámetros del servidor, en la siguiente figura 1 se puede observar el menú de inicio. Ver más detalle [13]

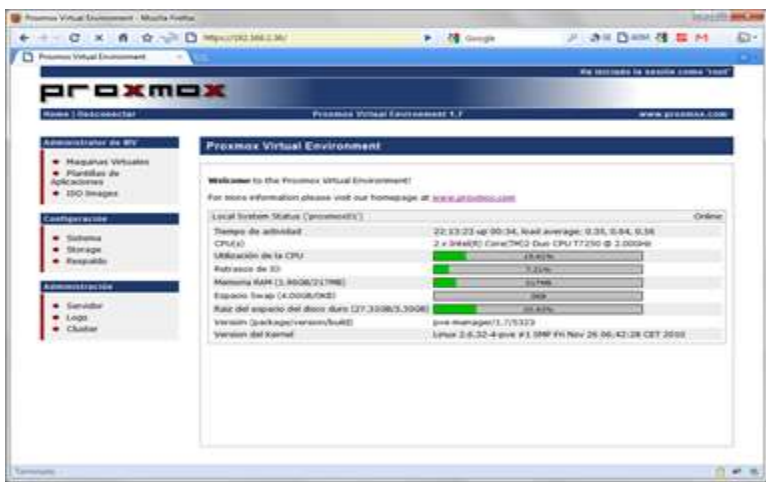


Figura 1 Menú principal de la WEB de Administración del Proxmox

Máquinas virtuales en los servidores con PROXMOX

En los dos servidores se va a realizar la instalación de PROXMOX para instalar todos los servicios necesarios de la empresa utilizando máquinas virtuales sobre este último. En estas máquinas virtuales se van a distribuir los diferentes servicios de toda la división, esta distribución puede variar según la necesidad cambio que vaya surgiendo con la dinámica de trabajo. Los sistemas operativos que se instalarán en las máquinas virtuales son: la última versión estable de Ubuntu server TLS, para instalar servicios como: Correo, Ftp, Proxy, Openldap, samba4, DNS y DHCP se hubiera podido utilizar otro sistema operativo, pero por una cuestión de experiencia, debido a su seguridad y estabilidad en servidores se propuso esta distribución de Linux.

Redundancia de la información

Con el Rsync y el Bacula se harán Backups (Salvas) de forma incremental un día determinado de la semana de los archivos de configuración de los servidores, imágenes de las máquinas Virtuales, bases de datos, software, otros tipos de datos y logs.

5. MODELACIÓN DE LA SEGURIDAD UTILIZANDO ENTORNOS DE VIRTUALIZACIÓN

Cálculo de la transferencia de datos

Aplicando la fórmula *tiempo de transferencia = tamaño del archivo / ancho de banda* ($T=T_m/AB$), un administrador de red puede estimar varios de los importantes componentes del rendimiento de una red. Si se conoce el tamaño típico de un archivo para una aplicación dada, al dividir el tamaño del archivo por el ancho de banda de la red, se obtiene una estimación del tiempo más rápido en el cual se puede transferir el archivo, y de esta forma darse cuenta si el diseño realizado fue el más correcto. [14]

Análisis de tráfico

Algo que no se puede dejar de considerar es la seguridad de la red y del sistema operativo, si se pretende que la información que hasta hoy era considerada privada, no caiga en manos equivocadas, o que se encontrase sorpresivamente el sistema de información inutilizado por la acción de algún código malicioso que pretende tomar el control de la máquina o simplemente sacarla de circulación.[15]

Para la análisis de seguridad se utilizara un entorno virtual, condicionado por máquinas virtuales principalmente montadas sobre un servidor de *proxmox*, y se realizará peticiones desde terminales montados sobre máquinas virtuales también y con herramientas de monitoreo se analizara el tráfico de estas terminales, a continuación se puede observar un resumen de algunas herramientas utilizadas.

- **Resumen de herramientas utilizadas para el Monitoreo de tráfico en la red**

- Netstat
- Wireshark
- Nagios
- iptraf
- tcpdump

- **Detección de vulnerabilidades**

- Nessus
- OpenVas
- Nmap
- Acunetix
- Kali (versión más avanzada de BackTrack)

- **Detector de intrusos (IDS)**

- arpwach
- psad
- - Análisis de los reportes de navegación del squid
- Sarg
- Lightsquid

- **Graficado de la navegación del squid**

- MRTG

- **Monitoreo del correo**
- Awstats

6. CONCLUSIONES

Se realizó el levantamiento y defectación del hardware que existe actualmente en la división, se seleccionó una tecnología de hardware que cumplirá con las necesidades y expectativas de la empresa para virtualizar. Se utilizaron herramientas de monitoreo que permitieron analizar el tráfico en la red LAN, entre las que fueron utilizadas están: MRTG, Wireshark, Nessus, Nagios. Fue seleccionada un grupo de herramientas de software libre que permitirán mejorar la gestión, el funcionamiento y seguridad de la red de área local. Con máquinas virtuales también se implementaron herramientas de gestión y supervisión que permitieron comprobar la seguridad de los paquetes que viajan encriptados a través de la red, entre ellas se utilizó principalmente la herramienta Kali (versión más avanzada de BackTrack) muy utilizada en el mundo entero hoy en día para detectar vulnerabilidades de diferentes magnitudes en las diferentes empresas y corporaciones.

7. RECONOCIMIENTOS

El autor desea agradecer a la profesora y compañera de trabajo Magdelis Moreno Ortega por su apoyo, al colectivo de profesores del departamento de comunicaciones de la facultad de eléctrica de la Universidad Central “Marta Abreu” de las Villas por sus enseñanzas y dedicación, y al profesor Manuel Castro Artilles por su ayuda y enseñanzas.

8. REFERENCIAS

1. John Wiley, Computer Security Handbook, Fourth Edition Edited by Seymour Bosworth and M.E. Kabay, 2002 part One Foundations of Computer Security.
2. P. Denning., Computers under attack. ACM Press, 1990
3. Earl Carter, Jonathan Hogue, Intrusion Prevention Fundamentals, 2006.
4. Orozco, E. (2008) Propuesta para la Implementación de una Infraestructura de Llave Pública en la Intranet de la UCLV. Santa Clara: Departamento de Telecomunicaciones y Electrónica, UCLV.
5. Seguridad cultura de prevención para las TI, Abril-mayo 2014
6. Listado de Precios Mayoristas, e-mail: oferta.tecun@cimex.com.cu, <http://tecun.cimex.com.cu/>
7. Diseño de Redes LAN para Ambientes Intranet, curso 2012 Dr Hector Cruz Enrriquez
8. Curso arquitectura de Redes 2012, Dr.C. Ing. Félix Alvarez Paliza
9. CCNA1 - Cisco Certified Network Associate, Epígrafe 7.1.5 “Cableado y arquitectura de 10BASE-T”
10. Gary A. Donahue, Network Warrior , part VIII “Designing Networks”, June 01, 2007
11. CCNA3 - Cisco Certified Network Associate, Epígrafe 7.2 “Protocolo Spanning-Tree”.
12. Marcos Martínez García, “Construcción de Laboratorios Virtuales para la Administración de Sistemas y Servidores” epígrafe 1.5.1 “Ventajas e inconvenientes de virtualizar un sistema operativo “sep. 2010.
13. Marcos Martínez García, “Construcción de Laboratorios Virtuales para la Administración de Sistemas y Servidores” Cap. 4 “Diseño” sep. 2010.

14. CCNA1 - Cisco Certified Network Associate, Epígrafe 2.2.6 “Cálculo de la transferencia de datos”.
15. ROBERTA BRAGG, K.S., MARK RHODES-OUSLEY, COMPLETE REFERENCE.

SOBRE LOS AUTORES

El autor de este trabajo es: Alberto Rodríguez Carvajal, es graduado de Ingeniería en Telecomunicaciones y Electrónica en el 2008 de la facultad de eléctrica de la Universidad Central “Marta Abreu” de las Villas, cursó los diplomados en esa misma facultad de administración de redes y redes de comunicación con buenos resultados, también cursó con buenos resultados el diplomado de seguridad informática de la facultad de matemática, física y computación de esa misma universidad, trabaja como administrador de red en la división de Desoft Villa Clara.