IMPLEMENTACIÓN DE CLOUD SECURITY EN UN SISTEMA BASADO EN XEN CLOUD PLATFORM

Natalia Carolina Matiz Moya
Ing. Carlos Romero Gallardo
Ing. Rodolfo Gordillo Orquera

Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejército
Av. General Rumiñahui S/N, Sangolquí – Ecuador

natymatiz2989@gmail.com
caromero@espe.edu.ec
rxgordillo@espe.edu.ec

Resumen.- Actualmente, *Cloud Computing* es considerada como una tecnología moderna en donde se tiene la posibilidad de consumir servicios de TI y aplicaciones de una forma ágil y flexible. Al ser una tecnología tan cotizada en el mercado, también demanda por parte del proveedor; ofrecer servicios en la nube, y que estos sean seguros para que los usuarios puedan acceder a ellos con total confianza. Por esta razón, nace el concepto de *Cloud Security,* con lo cual el proveedor garantiza dar servicios y aplicaciones cloud; y por su parte, el cliente se compromete en cumplir con las normas de seguridad en lo que se refiere al trato de su información e identidad.

El presente proyecto se ha desarrollado específicamente para implementar *Cloud Security* en una nube montada bajo la plataforma de virtualización llamada Xen Cloud Platform. Esta nube provee Software como Servicio (SAAS) a los usuarios de los Laboratorios del DEEE de la Escuela Politécnica del Ejército.

I. INTRODUCCIÓN

El concepto de "*Cloud Computing*" ha ganado popularidad debido a que las infraestructuras de TI se han vuelto demasiado complejas y frágiles para soportar el ritmo y el dinamismo de la empresa actual [1]., es decir, debido a la gran demanda de aplicaciones comerciales tradicionales, ya que al ser costosas y cada una con requerimientos específicos necesarios de hardware y de software para ejecutarlas, se requiere de cierto conocimiento para la instalación, configuración, pruebas de funcionamiento y ejecución, seguridad y actualizaciones, o bien de un técnico que realice el trabajo.

Se puede definir a "*Cloud Computing*" como una solución para tener los servicios y las aplicaciones requeridas por el usuario a través de internet; es decir, es **un nuevo concepto tecnológico que se basa en que las aplicaciones de software** y los equipos (hardware) con capacidad de proceso y almacenaje de datos no están en el PC o equipos del usuario, sino que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y los servicios disponibles a través de Internet [2].

Al tener las aplicaciones y los servicios en una nube, es importante tomar en cuenta ciertas consideraciones de seguridad de los datos y la información que se montarán sobre la misma, para precautelar la privacidad de los usuarios y su información; a esto se lo conoce como *Cloud Security*.

"***Cloud Security es una evolución de la seguridad informática, seguridad de la red y seguridad de la información. Se refiere a un amplio conjunto de políticas, tecnologías y controles implementados para proteger los datos, las aplicaciones y la infraestructura asociada de la computación en nube."*** [3]

Al hacer uso del "C*loud Computing"*, una parte importante de la seguridad del sistema recae sobre la empresa que provee los servicios en la nube.[4]; por lo que podemos concluir que, así como "*Cloud Computing*" es considerada como una solución tecnológica importante que proporciona una fórmula mucho más eficaz, flexible y rentable para las empresas en constante crecimiento; es también vulnerable a obstáculos y amenazas que puedan frenar su avance tecnológico y pongan en riesgo la privacidad de los usuarios.

II. MARCO TEÓRICO

Una nube de Cloud Computing se encuentra estructurada según su infraestructura, misma que se encuentra compuesta de un conjunto de elementos y recursos que proporcionan servicios que los usuarios pueden usar según sus necesidades, esta infraestructura se la puede categorizar en modelos de despliegue que describen el tipo de nube, es decir como se la crea y se la pone en funcionamiento; y, en modelos de servicios que son todos aquellos que puede proporcionar la nube, como software, plataforma o infraestructura.

2.1 Tipos de Infraestructura Cloud

2.1.1 Modelos de Despliegue

Nube Pública: La nube pública tiene una infraestructura a gran escala que pone a disposición los servicios y recursos de ésta, de forma dinámica a través de internet, para cualquier usuario o grupo empresarial que lo requiera en cualquier momento y lugar.

El proveedor de los servicios de la nube es dueño de la infraestructura física, además de ser el administrador que gestiona los servicios, recursos, procesos y datos.

Nube Privada: La nube privada es aquella que es creada y administrada por una sola organización u empresa; y no ofrece servicios a terceros. Las instalaciones y servidores se encuentran dentro de la misma; es decir, es una plataforma administrada por una sola organización y es utilizada para la obtención de hardware, como máquinas, almacenamiento e infraestructura de red (IaaS), y también aplicaciones como Plataforma como Servicio (PaaS) e incluso aplicaciones Software como Servicio (SaaS).

Nube Comunitaria: Este tipo de nube tiene una infraestructura que es compartida por varias organizaciones o empresas, de tal manera que comparten los servicios y recursos de la nube, a manera de una comunidad en donde los usuarios tienen intereses compartidos y objetivos similares; como por ejemplo, requisitos de seguridad, políticas y condiciones de cumplimiento, privacidad de los datos, etc.

Nube Híbrida: Este tipo de modelo de nube es considerado como una combinación de los modelos ya descritos.

"El modelo híbrido combina los modelos anteriormente descritos, sobre nubes públicas y privadas, de manera que se aprovecha la ventaja de localización física de la información gestionada por las nubes privadas con la facilidad de ampliación de recursos de las nubes públicas" [5]

2.1.2 Modelos de Servicio

Software como servicio (SAAS): Este modelo brinda la capacidad al usuario de tener un despliegue de software como aplicación a través del internet, en el cual las aplicaciones y los recursos computacionales están diseñados para usarlos bajo demanda.

Plataforma como servicio (PAAS): Este modelo propone un entorno software en el cuál un desarrollador puede crear y gestionar soluciones dentro de un contexto de herramientas de desarrollo que la plataforma proporciona. [6]

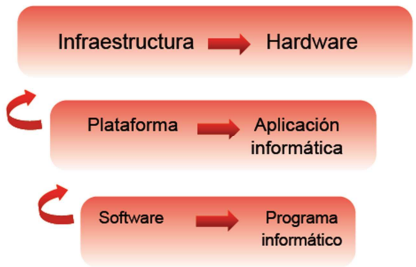
Este tipo de nube proporciona al consumidor la capacidad de desplegar aplicaciones creadas por el consumidor de la infraestructura de la nube, utilizando lenguajes de programación específicos y herramientas como java, Python, etc. El servicio de la nube se entrega bajo demanda, desplegando aplicaciones en hardware y software.

Infraestructura como servicio (IAAS): Este modelo está definido como un modelo de servicios de computación escalables según sean las necesidades del usuario.

La capacidad que proporciona al cliente es la provisión de procesamiento, almacenamiento, redes y recursos de computación en donde el usuario puede desplegar y ejecutar sistemas operativos y desarrollar o probar aplicaciones.

Adicionalmente, en la figura 1 se puede observar cómo se distinguen y caracterizan los tres niveles de servicio; en el lado izquierdo se observa como unos servicios se constituyen sobre los otros, mientras que en el lado derecho se especifican las características de los componentes de cada nivel de servicio.

Figura 1. Niveles de servicio del Cloud Computing [4]



III. SEGURIDAD EN CLOUD COMPUTING

Cloud Computing al ser uno de los elementos más importante en las TIC's tiene como objetivo principal precautelar la integridad de los datos y la privacidad de los usuarios.

Si la infraestructura informática utilizada es compleja, mas vulnerabilidades y riesgos pueden aparecer, por lo tanto es importante conocer los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos de la nube. Además de las medidas de seguridad que deben tomar tanto los proveedores de la nube como los clientes; así como en la virtualización.

Las encuestas realizadas por CSI desde el año 2004 hasta el 2010 muestran que se ha incrementado el índice de ataques por malware, phishing y botnets, tal como se puede observar en la siguiente figura: [8]

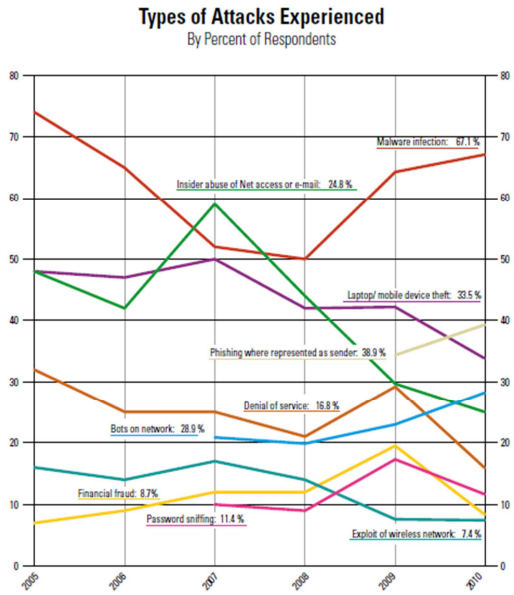


Figura 2. Tipos de ataques [8]

Como se puede observar, existen varias formas de hacer mal uso de la información que se encuentra en la nube, lo importante es que tanto el proveedor de servicios como el cliente tomen las medidas de seguridad necesarias para controlar las diferentes amenazas. En el siguiente cuadro, se pueden observar los mecanismos de seguridad que deben tomar tanto el proveedor como el cliente.

Tabla 1. Mecanismos de Seguridad: Proveedor vs. Cliente

MODELOS DE SERVICIO	MECANISMOS DE SEGURIDAD POR PARTE DE:	
	PROVEEDOR	**CLIENTE**
IAAS	Seguridad a los equipos y por ende a la localidad donde se encuentre.	Responsable de mantener el sistema operativo actualizado.
	Seguridad necesaria en datacenter, equipos y programas, para garantizar la disponibilidad de la información.	Mantener políticas de seguridad como el control de usuarios, el borrado de cuentas inutilizadas.
	Garantizar que la información no se pierda y contar con copias de seguridad.	Instalación y configuración de sistemas de firewall.
	Especificar en el contrato de prestación de servicios los riesgos y la responsabilidad que recae en el cliente si hace uso ilícito de la nube.	Autenticación, autorización, administración y configuración de usuarios.
	Equipos actualizados tanto a nivel hardware como software.	Copias de seguridad periódicas de la información.
PAAS	Control de sistemas operativos, hardware, infraestructura de red y gestión de recursos	El cliente crea, despliega y ejecuta, una aplicación, administra los upgrades y parches para todas las funcionalidades de la misma.
	Protección de los datos, además de la administración del acceso a las aplicaciones	
	Mecanismos de control y eliminación del software malintencionado.	El cliente usa hojas de cálculo, procesadores de texto, copias de seguridad, cobros, procesamiento de nómina y facturación.
SAAS	Administración del acceso a aplicaciones específicas que se ofertan en la nube	El único control que un usuario final tiene es acceder a la aplicación del usuario final desde un desktop, laptop o teléfono móvil.
	Control de los sistemas operativos, hardware, infraestructura de red, upgrades de aplicaciones y parches.	
	El proveedor define los niveles de umbral de los usuarios.	

IV. DISEÑO E IMPLEMENTACION DE CLOUD SECURITY EN EL SISTEMA BASADO EN XEN CLOUD PLATFORM

Para identificar de forma clara las vulnerabilidades en la plataforma de estudio, se ha elaborado un esquema que muestra las topologías de la nube implementada, tanto la parte física, como se observa en la figura 3; como la parte virtual, en la figura 4. El proyecto implementado en los Laboratorios de Electrónica, está diseñado para brindar infraestructura como servicio (IAAS), es decir capacidad de almacenamiento y procesamiento, además de software como servicio (SAAS), con servicios como *web hosting*, servidor web, correo electrónico, cortafuegos, *DHCP*, *DNS* y almacenamiento en nube. Tal como se observa en las figuras.

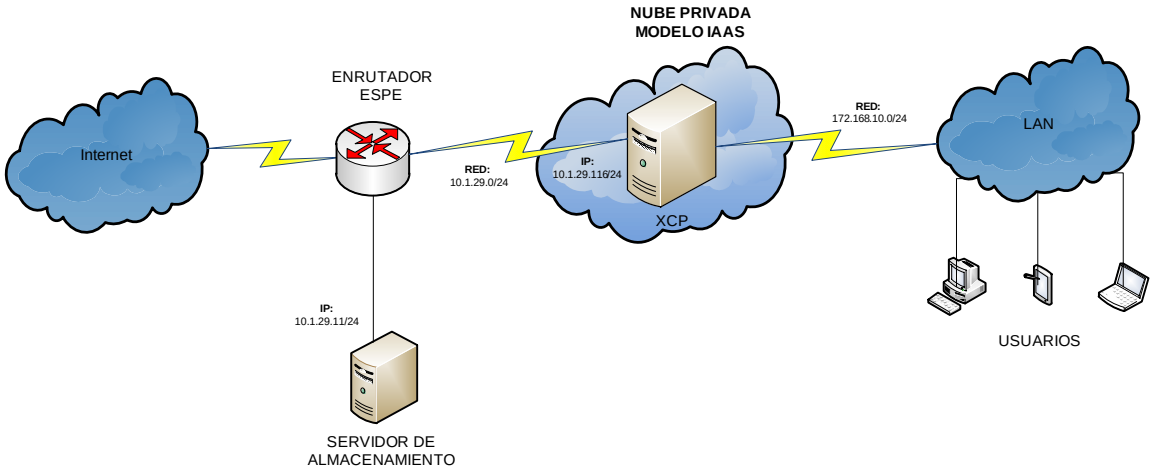


Figura 3. Topología Física

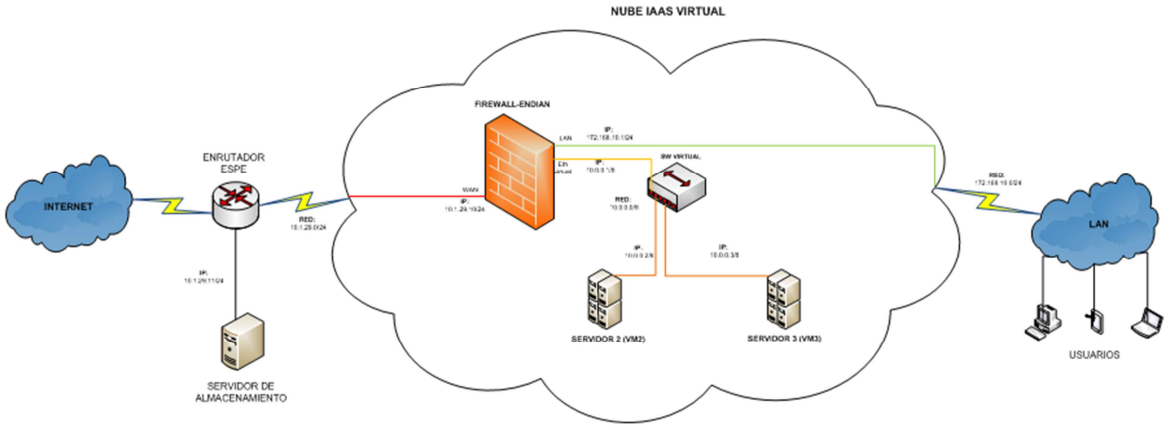


Figura 4. Topología Virtual

Las figuras muestran los elementos que conforman la nube y los servicios que esta oferta a los usuarios del DEEE; en base a esto, se ha realizado un análisis de la nube según los modelos de servicio que esta oferta, es decir IAAS, PAAS y SAAS.

Como resultado de este análisis, se determinó que la nube no cuenta con Cloud Security; es decir, la configuración de políticas, mecanismos y parámetros de seguridad que garanticen la integridad, confidencialidad y disponibilidad de los servicios que forman parte de la nube.

Las tablas 2 y 3, muestran las vulnerabilidades detectadas en los modelos de servicios IAAS y PAAS respectivamente.

Tabla 2. Vulnerabilidades en IAAS

Modelo de servicio	Vulnerabilidades detectadas	
	Infraestructura física	**Infraestructura lógica**
IAAS	Condiciones de la localidad inadecuadas	No existe configuración de alta disponibilidad física y lógica
	Localidad sin sistema de autenticación de usuarios	Distribución incorrecta de la topología física de la nube.
	Falta protección de los equipos ante fallas eléctricas	No se han establecido políticas de prestación de servicios para usuarios.
		No existe un plan de mantenimiento de elementos de la nube.

Tabla 3. Vulnerabilidades en PAAS

MODELO DE SERVICIO	VULNERABILIDADES DETECTADAS
PAAS	No existe ningún método o control independiente de los sistemas operativos o máquinas virtuales.
	No se encuentra implementado ningún sistema de administración de acceso a los usuarios.
	Faltan medidas de seguridad para garantizar un acceso seguro a los clientes hacia la plataforma requerida
	No existe ninguna protección de la plataforma mediante mecanismos como firewall, IDS y antivirus

Mientras que para SAAS, se han analizado los servicios que oferta la nube, y en base a su configuración se determinó las vulnerabilidades que presentan.

Los servicios son: un servidor de correo (Zimbra), y una plataforma de almacenamiento (OwnCloud). Los usuarios harán uso de la nube para tener acceso a estos dos servicios, por lo que es necesario implementar políticas de seguridad, como autenticación de usuarios, protección de los datos (correo electrónico, información, fotos, etc.), administración de los recursos, etc. Además de configuración de reglas de seguridad en el firewall para evitar que los usuarios tengan acceso a los servidores que se encuentran dentro de la DMZ.

En base a este análisis se ha propuesto e implementado la siguiente solución:

4.1 Solución Física

- Para el ingreso al datacenter se debe colocar un lector biométrico de huellas dactilares para el ingreso de personal autorizado.
- Colocación de una alarma con sensores en la puerta que detecte el ingreso del personal.
- Colocación de cámaras de video como sistema de vigilancia.
- Diseño de un datacenter con condiciones necesarias para soportar desastres naturales como incendios, inundaciones, ambiente climático, etc.
- Colocación de un sistema de ventilación comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe ser entre el 45% y el 65%.
- Colocación de sistemas de abastecimiento de energía eléctrica.

4.2 Solución Lógica

A. Instalación de Firewalls de alta disponibilidad

Con el uso de firewalls redundantes se consiguió garantizar que exista alta disponibilidad de los servicios y aplicaciones de la nube, además de robustecer la seguridad en la nube tanto en la parte de infraestructura como en la plataforma. Tal como se observa en la figura 5, donde se encuentra el diseño final de la implementación de la solución de Cloud Security en la nube.

B. Redistribución de recursos de la nube

Gracias a que se reubicaron los recursos de la nube, (traspaso del servidor de almacenamiento FreeNAS y todos los parámetros de configuración que lo contemplan) hacia la red DMZ se logró proteger el servidor de posibles riesgos que puedan afectar a su funcionamiento o la información almacenada en el mismo. Figura 5.

C. Instalación de un sistema de detección de intrusos

Con la instalación de un IDS (Intrusion Detection System), se logró detectar y proteger de intrusiones hacia la red. Además de garantizar que el administrador de la misma, siempre se encuentre alerta e identifique si existe algún intruso.

D. Instalación antivirus

Con la instalación de HAVP (HTTP Proxy Antivirus), que es una solución proxy con un filtro anti virus llamado ClamAV, se logró tener un escaneo permanente del tráfico de la red WAN y LAN, permitiendo detectar código malicioso en navegación HTTP, y bloqueándolo para evitar riesgos.

E. Instalación de Citrix Web Self Service

Con la instalación de una aplicación a manera de consola de gestión, se logró delegar funciones y perfiles a usuarios que requieran hacer uso de la nube como plataforma como servicio. Y, además de permitir una fácil administración de las máquinas virtuales de la nube para usuarios PAAS. Figura 5.

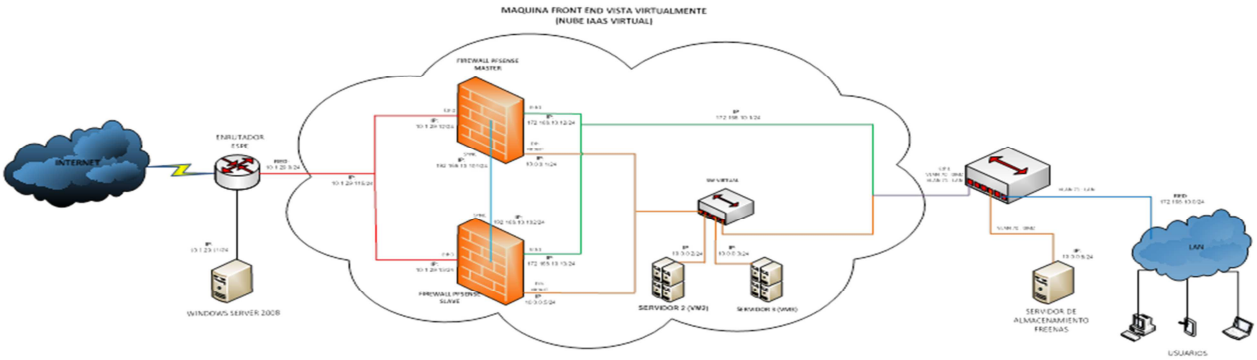


Figura 4. Diseño de Topología Cloud Security

V. CONCLUSIONES

Cloud Computing, al ser una nueva tecnología que permite el uso de aplicaciones y servicios en una nube, cuyo modelo dependerá de las necesidades del cliente; demanda la necesidad de, no solo proveer servicios y recursos; sino también *Cloud Security*. La responsabilidad de su implementación y cumplimiento recae sobre el proveedor y el usuario según el tipo de nube implementada.

Para implementar Cloud Security se debe realizar un análisis de las vulnerabilidades a las cuales se encuentra expuesta la nube, para tomar todas las medidas necesarias en el diseño de una nube que garantice integridad, confiabilidad y disponibilidad de sus recursos, servicios y aplicaciones.

Cloud Computing es una buena opción para implementar como solución en pequeñas y grandes empresas que manipulan información sensible, ya que ofrece ventajas como reducción de costos, alta disponibilidad de servicios y aplicaciones. Siempre y cuando el usuario o cliente de los servicios Cloud se cercioren de que su proveedor cumpla con los requisitos y políticas de seguridad.

VI. REFERENCIAS BIBLIOGRÁFICAS

[1] *VMWare*. (2012). Recuperado en Octubre de 2012, de http://www.vmware.com/es/cloud-computing/

[2] Castellón, A. (2010, Mayo 27). *Cosas de Tecnología*. Recuperado de 2012, http://www.tecnocosas.es/que-cloud-computing/

[3] Anónimo. (2012, Septiembre 11). *Wikipedia*. Recuperado de http://en.wikipedia.org/wiki/Cloud_computing_security

[4] Pérez, P., Gutierrez, C., & fuente, S. d. (10 de 2001). *Inteco*. Recuperado el 2012, de https://www.inteco.es/file/3LeSufa2tYmC_bcRKSFfbg

[5] Reese, G. (2009). En *Cloud Application Architectures: Building Applications and Infrastructure in the CloudTheory in Practice (o'Reilly) Series.* O'Reilly Media, Inc.

[6] Williams, D. M. (2010). In *A quick start guide to Cloud Computing, moving your business into the cloud.*

[7] Director, Richardson. R. (Diciembre de 2010). Recuperado en Diciembre de 2012, de http://gocsi.com/survey

[8] *Tissat*. (21 de Febrero de 2012). Recuperado en Marzo de 2013, de http://tissat.wordpress.com/2012/02/21/cloud-comuting-taxonomia-por-niveles-o-modelos-de-servicio-iaas-paas-y-saas/

VII. BIBLIOGRAFÍA

Natalia Carolina Matiz Moya

Nace el 22 de Noviembre de 1989, en la ciudad de Quito – Ecuador. Sus estudios secundarios los realizó en la Unidad Educativa Experimental Autónoma “Academia Almirante Nelson”, donde se graduó con el título de bachiller Físico Matemático en el año 2007.

Obtuvo el título de Ingeniera Electrónica especialidad Redes y Comunicación de Datos en la Escuela Politécnica del Ejército en el año 2013.

Carlos Gabriel Romero Gallardo

Ingeniero en Electrónica y Telecomunicaciones en la Escuela Politécnica del Ejército (2002) y Especialista en Proyectos de Investigación Científica y Tecnológica en la Universidad Complutense de Madrid (2006). Candidato a PhD Universidad Nacional de la Plata. Es profesor de la Escuela Politécnica del Ejército. Sus áreas de interés e investigación son Seguridad de la Información, Networking con TCP/IP e Implementación de servicios y aplicaciones con software libre

Rodolfo Gordillo

Rodolfo Gordillo Orquera, Es Ingeniero en Electónica y Telecomunicaciones graduado en la Escuela Politécnica del Ejército en el año de 1996. Obtuvo su Masterado en Ingeniería Electrónica el año 2008 en la misma institución. Actualmente se desempeña como profesor a tiempo completo en el Departamento de Eléctrica y Electrónica en la ESPE- Ecuador. Adicionalmente es Coordinador de Investigación de su Departamento y profesor tiempo completo en el Área de Automática y Robótica. Sus intereses investigativos radican en las redes de comunicación industriales, comunicaciones inalámbricas y los sistemas de control avanzados.