Fecha de presentación: diciembre, 2020, **Fecha de Aceptación**: febrero, 2021, **Fecha de publicación**: marzo, 2021

25

ANÁLISIS UNIVERSITARIO DE LA FACTIBILIDAD DEL MODELO DE ADMINISTRACIÓN DE CONECTIVIDAD EN REDES DE UNIDADES OPERATIVAS DEL DISTRITO 23D03 LA CONCORDIA

UNIVERSITY ANALYSIS OF THE FEASIBILITY OF THE CONNECTIVITY MANAGEMENT MODEL IN DISTRICT 23D03 LA CONCORDIA OPERATING UNIT NETWORKS

Diego Paúl Palma Rivera[1]
E-mail: us.diegopalma@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-7684-7721
Silvio Amable Machuca Vivar[1]
E-mail: us.silviomachuca@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-4681-3045
Carlos Roberto Sampedro Guamán[1]
E-mail: us.carlossampedro@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-1937-100X
Bolívar Enrique Villalta Jadan[1]
E-mail: us.bolivarvillalta@uniandes.edu.ec
ORCID: https://orcid.org/0000-0002-8349-2842
[1] Universidad Regional Autónoma de Los Andes. Ecuador.

Cita sugerida (APA, séptima edición)

Palma Rivera, D. P., Machuca Vivar, S. A., Sampedro Guamán, C. R., & Villalta Jadan, B. E. (2021). Análisis universitario de la factibilidad del modelo de administración de conectividad en redes de unidades operativas del distrito 23D03 La Concordia. ***Revista Conrado, 17(79)***, 199-205.

RESUMEN

El estudio realizado con la colaboración de los estudiantes de la carrera de sistema posibilitó valorar sobre el constante cambio en la tecnología a nivel mundial que no tiene una limitación y el incremento acelerado del uso de aplicaciones web y móviles para desarrollar todas las actividades que realizan las personas y principalmente orientadas al ámbito laboral ha ocasionado varios inconvenientes, en nuestro país ha generado mucha repercusión en las empresas públicas y privadas, ya que las mismas no invierten en infraestructura de redes y seguridades, es de vital importancia cambiar la forma de administración de redes así como implementar tecnología acorde a la necesidad de cada institución, ya que la misma busca brindar un servicio eficiente y oportuno a los diferentes usuarios. El objetivo principal del trabajo es analizar la factibilidad del nuevo modelo de Administración de Conectividad en redes de Unidades Operativas empleando una investigación Cualitativa – Cuantitativa, además se emplearon técnicas como observación y entrevistas que permitieron recopilar información importante para el desarrollo de la investigación, luego se estableció un modelo adecuado de conectividad así como mejorar la seguridad en redes con la infraestructura adecuada y definiendo un modelo de políticas en la administración de los diferentes servicios que se prestan en la Dirección Distrital 23D03 La Concordia – Salud y sus Unidades Operativas.

Palabras clave:

Modelo, administración de redes, seguridad, políticas, unidades de salud.

ABSTRACT

The study carried out with the collaboration of the students of the system career made it possible to assess about the constant change in technology worldwide that has no limitation and the accelerated increase in the use of web and mobile applications to develop all the activities that people do and mainly oriented to the work environment has caused several drawbacks, in our country has generated much impact on public and private companies, since they do not invest in network infrastructure and security, it is of vital importance to change the form of network administration as well as implement technology according to the need of each institution, as it seeks to provide efficient and timely service to different users. The main objective of the work is to analyze the feasibility of the new model of Administration of Connectivity in networks of Operative Units using a Qualitative - Quantitative investigation, in addition techniques like observation and interviews were used that allowed to gather important information for the development of the investigation, soon a suitable model of connectivity was established as well as to improve the security in networks with the suitable infrastructure and defining a model of policies in the administration of the different services that are lent in the District Direction 23D03 La Concordia - Health and its Operative Units.

Keywords:

Model, network administration, security, policies, health units.

INTRODUCCIÓN

En la actualidad, en las entidades públicas y privadas el uso de tecnología se convierte en una necesidad, debido a que toda actividad económica o social tiene relación con la comunicación y el manejo de ciertas cantidades de información, que dependiendo de la empresa requieren de mejor y mayor infraestructura tecnología que se acople a sus necesidades.

Por tanto, es indispensable que, al hablar de comunicación se trate un tema concepto fundamental denominado "conectividad", para hacer énfasis en la dependencia y uso de la conexión entre dispositivos o datos dentro de un sistema.

Según Serrano Mascaraque (2009), actualmente las empresas están dejando a un lado los sistemas de información y similares, para optar por el uso de las tecnologías de la información y comunicaciones concurrentes, por implementar redes más grandes a nivel local y regional, utilizando recursos o equipos tecnológicos de cómputo cada vez más avanzados y con mejor procesamiento en cada generación, servidores de mayor capacidad para lograr una interconexión con más computadores para lograr alcances mundiales con herramientas que incluyan virtualización.

De igual modo, es importante mencionar que, a partir de la citada convergencia de tecnologías de la información, se da razón y utilidad al término conocido de Internet, que forma parte estructural y fundamental de todo tipo de empresas en sus objetivos, debido al principal papel que juega para la comunicación y la forma de interactuar con el usuario final, además de poder presentar sus servicios y enlaces con otras instituciones o gobierno, así como otros beneficios que se le puedan atribuir.

Por otro lado, Dussan Clavijo (2006), establece la importancia de la implementación de una política de seguridad necesaria, debido al grado del contenido que se maneja a nivel institucional y al aseguramiento de la parte tecnológica en cuanto a hardware, software y data.

Es por esta razón que una política de seguridad necesita que se involucren ciertos aspectos de mucha importancia en el asunto como: La instrucción dentro de la organización para originar mejores políticas en base al entorno institucional, los instrumentos y el monitoreo. Esto abarca a la participación directa del personal de la organización en la elaboración de socializaciones de actualización de conocimientos a los usuarios de la empresa.

La posibilidad de contar con los recursos económicos, técnicos y tecnológicos es de vital importancia, y más aún la disponibilidad de actividades que permitan reconocer los puntos bajos y retroalimentar las vulnerabilidades de la organización para avanzar con potenciales mejoras haciendo uso de las mejores prácticas.

Así mismo, es necesario conocer acerca del auge e importancia de la necesidad de seguridad, según Sarubbi (2008), establece que, como resultado de la aceptación de arquitectura de red, los usuarios, la innovación, el descenso en los precios de equipo físico, es decir hardware, y el perfeccionamiento de nuevas y mejores aplicaciones, se originaron las redes LANs y WANs, que en conjunto con la virtualización han creado un hábitat computacional más complicado.

La idea central del proyecto abarca los beneficios de la implementación de un Internet Service Provider (ISP), debido a la privatización del internet como tal, existe congestión en la mayoría de proveedores, con el aporte de Cosoi (2000), se conoce actualmente que tanto los servicios empresariales como los de casa tienen buena demanda, pero en la mayoría de los casos, los usuarios finales quienes prueban el servicio a todo tiempo, presentan quejas sobre la capacidad de ancho de banda presentada, el precio y la saturación e intermitencia de servicio.

Uno de los objetivos principales de esta idea, es la de aportar seguridad y control al tráfico de datos, o seguridad en la información, tal y como apoya este análisis, según Ungerman & Kiely (2006), dice que al implementar un ISP se puede implementar servicios necesarios para dicha empresa, además de poder contar con recursos que según la capacidad de la empresa se puedan adquirir, como por ejemplo equipos de enrutamiento con protocolos de seguridad y equipos anti-spoofing.

MATERIALES Y MÉTODOS

La investigación de campo consistió en observaciones recopiladas, de la infraestructura tecnológica, procesos administrativos, seguridad y calidad en la comunicación en el Distrito 23D03, en el cantón La Concordia y sus 6 unidades de salud, también se entrevistó a la encargada de TIC del centro de salud La Concordia además se aplicaron encuestas a los médicos de cada unidad y personal de tipo administrativo, lo cual permitió denotar los diferentes problemas que se tienen en la actualidad en cuanto a los diferentes servicios que se prestan, problemas de seguridad, deficiencias en la infraestructura, problemas de servicios centralizados y el estado de la administración vinculada a las políticas y lineamientos que se establecen en el Ministerio de Salud (López Barajas Zayas, 2015)

RESULTADOS Y DISCUSIÓN

Entre los resultados de obtenidos de la entrevista (Hernández Sampieri, et al., 2018) realizada a la encargada del área Tecnologías de Información y Comunicación TIC se encontraron las siguientes novedades:

En la entrevista realizada a la encargada de TIC del Distrito 23D03 La Concordia – Salud se obtuvo que actualmente se cuenta con un área específica para servidores, cámaras y telefonía, pero es ambigua al área de TIC y la misma requiere mejoras de infraestructura, así como actualización de equipos.

Existe un servidor basado en software libre específicamente Centos que cumple como firewall y proxy para los diferentes usuarios administrativos y Centro de Salud la Concordia. Las unidades de rurales Plan Piloto, Monterrey y La Villega y sector urbano Alianza y Nueva Concordia no disponen de equipos intermediarios, ya que son conectados directamente a un switch y con la administración del proveedor.

Se cuenta con Políticas de Seguridad, pero las mismas son planteadas a nivel de MSP Planta central y las mismas deben ser adoptadas en cada Dirección Distrital a nivel nacional que dificulta a veces el trabajo ya que no se adaptan a la realidad y condiciones de cada entidad desconcentrada.

No se dispone de protección proxy para filtrado de páginas web inadecuadas y navegación de redes sociales que generan lentitud y desvían la atención de los servidores públicos. Todos los usuarios de centros de salud utilizan el servicio de internet para acceder a los diferentes servicios que se prestan por el MSP y algunos que son administrados por el Distrito 23D03, el mismo se lo realiza con el proveedor local que en este caso se trabaja con CNT en todas las unidades operativas y administrativos.

No se cuentan con un plan de crecimiento de redes ya que la misma se la realiza de acuerdo a requerimientos de usuarios y necesidades que se generan a través de soportes técnicos. Mensualmente se envía reportes a la Coordinación zonal 4 indicando novedades referentes a los servicios que se prestan en el Distrito 23D03 La Concordia – Salud, donde se hace denotar la necesidad de incremento de ancho de banda en los diferentes Centros de Salud y la necesidad de implementar equipos de red que ayuden al control y un adecuado uso del servicio.

A continuación, se describen los análisis actuales de la conexión de red en los diferentes Centros de Salud que pertenecen al Distrito 23D03 La Concordia – Salud (Terán Pérez, 2011) (Tabla 1).

Tabla 1. Centros de Salud del Distrito 23D03 La Concordia – Salud y su tipología.

ZONA	DISTRITO	CENTRO DE SALUD	TIPOLOGÍA
4	23D03	ALIANZA	Centro de Salud, Tipo A
4	23D03	LA CONCORDIA	Centro de Salud, Tipo C
4	23D03	MONTERREY	Centro de Salud, Tipo A
4	23D03	NUEVA CONCORDIA	Centro de Salud, Tipo A
4	23D03	PLAN PILOTO	Centro de Salud, Tipo A
4	23D03	LA VILLEGAS	Centro de Salud, Tipo A

En la tabla 1 se puede evidenciar los establecimientos de salud por su tipología establecidos por acuerdo ministerial 00005212 para la homologación de los establecimientos de salud por niveles de atención y servicios de apoyo del sistema nacional de salud (Raya Cabrera, 2009).

Estado actual del servicio de internet por unidades operativas y Administrativo referenciada por el área de Tecnologías de Información y Comunicaciones de la Dirección Distrital (Tabla 2).

Tabla 2. Estado actual del servicio de internet y sus características de acuerdo al proveedor.

CENTRO DE SALUD	PROXY DE RED	PROVEEDOR	¿TIENE ACCESO A ¿INTERNET?	TIPO DE ACCESO A INTERNET	No. DE COMPUTADORAS	ANCHO DE BANDA INTERNET	BLOQUEO DE PAGINAS WEB NO OFICIALES PARA USO LABORAL
ALIANZA	NO	CNT	SI	FO	7	2 Mb	NO
LA CONCORDIA	SI	CNT	SI	FO	32	8Mb	SI
MONTERREY	NO	CNT	SI	DSL	7	1Mb	NO
NUEVA CONCORDIA	NO	CNT	SI	FO	6	2Mb	NO
PLAN PILOTO	NO	CNT	SI	FO	9	2Mb	NO
LA VILLEGAS	NO	CNT	SI	FO	6	2Mb	NO

Por estatuto orgánico sustitutivo de gestión organizacional emitido por el Ministerio de Salud Pública de Ecuador (2012): "Supervisar la ejecución de los diferentes proyectos a nivel nacional en el área de redes, desarrollo informático y mantenimiento de toda la infraestructura tecnológica al servicio del Ministerio de Salud Pública". (Dordoigne, 2015)

En la actualidad todas las unidades de salud tipo A y tipo C del Distrito 23D03 La Concordia cuentan con un modelo de administración similar, así como también la infraestructura de redes (Almanza, 2008) Se denotan algunas debilidades como inexistencia de equipos intermediarios proxy que se encargue de bloquear páginas web que estén fuera del ámbito laboral, no se cuenta con bloqueo de puertos ni reglas firewall que mejoren la seguridad de los diferentes usuarios y el ancho de banda en algunos casos es inadecuado, ya que las redes crecen sin ningún tipo de control y un análisis oportuno que permita a su vez distribuir adecuada del servicio de internet (Figura 1).

Figura 1. Modelo de conexión actual de red tipo estrella en Unidades de Salud y Distrito con proveedor CNT.

A continuación, se presentan los servicios utilizados por los usuarios de todos los establecimientos de salud tipo A y C.

Servidor de correo: Administrado bajo entorno de software libre específicamente con Zimbra, el equipo se encuentra ubicado en el área de TIC y es de uso oficial ya que los usuarios deben regirse al uso obligatorio del correo institucional además está configurado con una IP pública brindada por CNT.

Servidor de archivos: Se encuentra actualmente trabajando sobre un equipo tipo escritorio en Tics la administración está implementada sobre Linux con el servicio samba que permite la interacción con clientes Windows y su función principal es respaldar la información que se generan en todas las áreas administrativas de la Dirección Distrital trabaja únicamente en entorno LAN y los respaldos son descargados en discos duros externos.

Servidor de telefonía IP: funciona bajo elastix y específicamente es usado para la parte administrativa permite a usuarios salidas externas al Distrito, interprovinciales y celulares y las extensiones con sus respectivas claves son consideradas por el área de Tics.

Servidor proxy y firewall: Este servidor intermediario basado en software libre en centos 5.5 trabaja sobre los servicios de squid para bloqueos de páginas web y contenido entre otras funciones de firewall específicamente ayuda a la administración únicamente de las áreas administrativas del Distrito 23D03.

Servidor Nube: Este servidor fue implementado por requerimiento de la coordinación Zonal 4 hace un año en owncloud basado en software libre con el objetivo de que todos los usuarios de los Centros de Salud y administrativos almacenen información de tipo temporal y que tenga un tamaño fuera de lo permitido por Zimbra y Quipux por lo que permite generar enlaces públicos para que puedan compartirse.

Servidor de agendamiento de pacientes: En la actualidad se trabaja con un software denominado ÁNGEL que permite el agendamiento de pacientes, pero únicamente del centro de salud La Concordia las otras unidades de salud no tienen acceso a este servicio ya que trabaja sobre entorno local y está instalado sobre Windows 7.

Servidor FTP: Servidor implementado con el objetivo de crear un repositorio digital para todos los usuarios actualmente en fase de pruebas.

En la propuesta del nuevo modelo de administración de red jerárquica se controlara de una forma mucho más adecuada todos los servicios de comunicación y seguridades de los Centros de Salud, ya que se centralizarán todas las conexiones a un punto principal el mismo que estará ubicado en la Dirección Distrital 23D03 La Concordia – Salud, además se cuenta con soporte de la Coordinación Zonal 4 y si fuera necesario y de acuerdo al orgánico estructural del Ministerio de Salud se puede solicitar a nivel de planta central.

Propuesta de red jerárquica: Considerando la infraestructura actual de redes del área donde se implementará el Centro de Datos principal y referenciando un costo bajo en cuanto gastos de inversión se muestra el nuevo diseño a efectuar.

Nueva propuesta de red jerárquica Punto principal CPD Distrito 23D03 – Enlaces

CNT y servicios por Centros de Salud

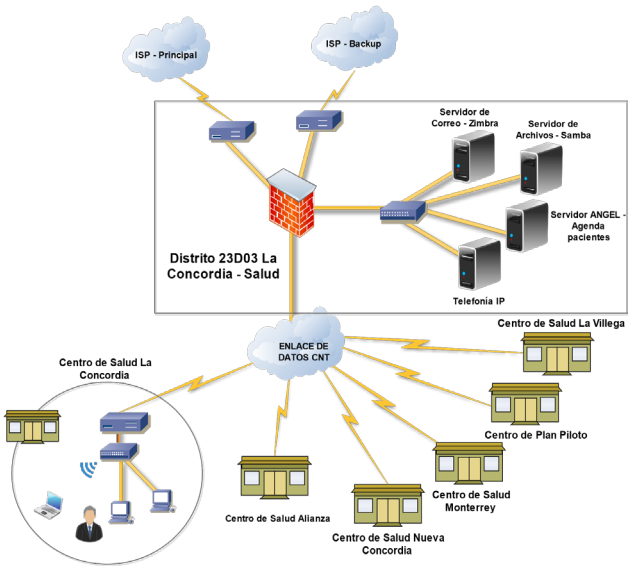

Figura 2. Nueva propuesta de red jerárquica Punto principal CPD Distrito 23D03 – Enlaces CNT y servicios por Centros de Salud

Para la adopción del nuevo modelo de red se plantea que los enlaces de datos sean intervenidos por la empresa CNT actual proveedor de servicio de internet y tomando en cuenta los lineamientos establecidos por el MSP donde se recomienda como opción de implementación primaria los servicios de comunicaciones que presta esta empresa.

Como se describe en la figura 2 se puede observar que los Centros de Salud tanto urbanos como rurales tendrán como punto principal el Distrito 23D03 de Salud que será la responsable de garantizar los servicios de TI y donde se implementarán algunas mejoras para la optimización y fortalecimiento de datos e internet (Tabla 3).

Tabla 3. Distribución de funcionarios en Unidades Operativas.

UNIDADES DE SALUD	APROXIMACIÓN DE USUARIOS
Tipo A, Puestos de Salud y Unidades Móviles	Mayor o igual a 10
Tipo B	Mayor o igual a 50
Tipo C	Mayor o igual a 100

Objetivo de la administración centralizada:

Conectividad directa sin dependencia del servicio de Internet para el acceso a los aplicativos y servicio web descritos a continuación. Los servicios que se podría brindar son los siguientes:

- Correo electrónico
- Sistema de telefonía
- Sistema de almacenamiento de nube privado
- Sistema de administración de red (NAT – DHCP)
- Seguridad informática perimetral
- Administración de los equipos de redes y comunicaciones o Monitoreo constante de switch y puntos de acceso inalámbrico o Acceso centralizado hacia los equipos de redes en switch y puntos de acceso inalámbrico para su administración remota.
- Resolución de problemas y mantenimientos centralizados preventivos hacia los equipos de redes.
- Centralizar los servicios informáticos con el fin de consolidar y repotenciar en una sola infraestructura lo necesario para garantizar una alta disponibilidad.
- Centralizar el sistema de telefonía donde se asignarán extensiones para cada área y seccionando los centros de salud.
- Administrar de forma centralizada seguridades de filtrado web y apertura de puertos en un firewall.

Políticas básicas de seguridad informática

La arquitectura de seguridad informática permitirá garantizar la conectividad desde el internet hacia la red interna, para lo cual se debe aplicar configuraciones de acceso y bloqueo básicas. Las mismas son configuradas de acuerdo a la necesidad del Distrito 23D03 (Tabla 4).

Tabla 4. Políticas básicas de seguridad informática.

Puerto	Protocolo	Acción	Descripción
443	HTTPS	Permitir	Se permite el tráfico encriptado de navegación web
80	HTTP	Permitir	Se permite el tráfico de navegación web
21	FTP	Permitir	Se permite la transferencia de archivos.
25	SMTP	Permitir	Se permite la transferencia de Correo electrónico
110	POP	Permitir	Se permite la transferencia de Correo electrónico

143	IMAP	Permitir	Se permite la transferencia de Correo electrónico
995	POP3s	Permitir	Se permite la transferencia de Correo electrónico encriptado
993	IMAP3s	Permitir	Se permite la transferencia de Correo electrónico encriptado
53	DNS	Permitir	Se permite el tráfico para la resolución de nombres de dominio
8 y 30	ICMP	Permitir	Se permite el tráfico de pruebas de conectividad básicas ping
Cualquiera	Cualquiera	Denegar	Denegar todos los demás puertos

Filtrado Web

Las normas de filtrado web deben garantizar el acceso y bloqueo de contenido web, estas normas deben personalizarse de acuerdo a las necesidades del Distrito 23D03 y conservando las normas básicas ya descritas (Tabla 5).

Tabla 5. Filtrado web – Restricción.

Contenido	Acción	Descripción
Adulto	Denegar	Contenido inapropiado
Citas	Denegar	Contenido inapropiado
Entretenimiento	Denegar	Contenido inapropiado
Juegos	Denegar	Contenido inapropiado
Anuncios	Denegar	Contenido inapropiado
Violencia	Denegar	Contenido inapropiado
Drogas	Denegar	Contenido inapropiado

Dominios gubernamentales

Se debe garantizar la conectividad a los siguientes dominios gubernamentales e institucionales, existen dominios adicionales a los cuales se debe garantizar el acceso cabe mencionar que estos dominios son adaptados a las necesidades de los usuarios por cada Distrito.

- Dominios Gubernamentales Principales
  - www.gestiondocumental.gob.ec
  - www.esigef.finanzas.gob.ec
  - www.compraspublicas.gob.ec
- Dominios Institucionales Principales
  - sgrdacaa.msp.gob.ec
  - Sgi01.msp.gob.ec
  - externalizacion.msp.gob.ec
  - tamizaje.msp.gob.ec
  - rpis.msp.gob.ec
  - Infosalud.msp.gob.ec
  - requerimientosalud.msp.gob.ec
  - capacitacion.msp.gob.ec
  - almacenamiento.msp.gob.ec
  - capacitación.msp.gob.ec

La preferencia se la enfocará a dominios gubernamentales.

CONCLUSIONES

Con la implementación del nuevo modelo de administración de conectividad en Unidades Operativas se logrará mejorar al acceso a los diferentes servicios locales que se prestan como son: Zimbra (Correo electrónico), VoIP (sistema de telefonía), Samba (Servidor de archivos), Cámaras de seguridad y FTP (Repositorio digital) los mismos que no requieren de internet para su funcionamiento por lo que se optimiza el recurso.

La centralización de la infraestructura de redes de datos en la Dirección Distrital 23D03 La Concordia permitirá un monitoreo constante de los diferentes dispositivos activos y pasivos, así también se logrará una asistencia remota más oportuna para la solución de problemas que se presentan por parte de los usuarios.

Se mejorará la velocidad de navegación promedio de los usuarios ya que se restringirá el contenido inapropiado, filtrado web, acceso de redes sociales y todo tipo de navegación fuera del espacio laboral además se garantizará la disponibilidad a páginas gubernamentales y que vayan en beneficio de los intereses de los usuarios del Ministerio de Salud Pública.

REFERENCIAS BIBLIOGRÁFICAS

Almanza, A. (2008). Seguridad en Redes y Sistemas Operativos. ***Bucaramanga: Facultad de Ingeniería Informática***, 231.

Cosoi, E. (2000). Elección de empresas de acceso a Internet. (ISP: Internet Service Provider). ***Revista Chilena de Pediatría***, ***71***(5), 451–452.

Dordoigne, J. (2015). ***Redes informáticas-Nociones fundamentales. Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6.*** Ediciones Eni.

Dussan Clavijo, C. A. (2006). Políticas de seguridad informática. Entramado, 2(1), 86-92.

Ecuador. Ministerio de Salud Pública. (2012). Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública. https://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/ESTATUTO-SUSTITUTIVO-MSP-ALCANCE-REFORMA-ABRIL17.pdf

Hernández-Sampieri, R., Méndez Valencia, S., & Mendoza Torres, C. P. (2018). ***Metodología de la investigación*** (Vol. 4). McGraw-Hill Interamericana.

López Barajas Zayas, E. (2015). ***Introducción a la metodología científica: (siete piezas fáciles)***. Universidad Internacional de La Rioja.

Raya Cabrera, J. L. (2009). ***Redes locales***. RA-MA, 2000.

Sarubbi, J. P. (2008). Seguridad Informática Técnicas de defensa comunes bajo variantes del sistema operativo Unix. Universidad Nacional de Luján.

Serrano Mascaraque, E. (2009). Accesibilidad vs usabilidad web: evaluación y correlación. ***Investigación bibliotecológica***, ***23***(48), 61-103.

Terán Pérez, D. M. (2011). ***Redes convergentes: diseño e implementación***. Marcombo.

Ungerman, M. E., & Kiely, K. M. (2006). ***U.S. Patent No. 7,002,076***. Patent and Trademark Office.