Artículo original

Rediseño de la infraestructura de red local del Centro de Investigaciones Médico Quirúrgicas (CIMEQ). Cuba

Redesign Local Network Infrastructure of CIMEQ. Cuba

Rodney Flores Robaina [1*] 0000-0002-7564-6178
José Felipe Ramírez Pérez [2] 0000-0002-0765-0685
Madelayne Muñoz Morejón[3] 0000-0001-9646-1626

[1] Centro de Investigaciones Médico Quirúrgicas. La Habana, Cuba.
[2] Universidad Autónoma de Baja California, Ensenada, Baja California, México.
[3] Escuela Nacional de Salud Pública. La Habana, Cuba.

* Autor para la correspondencia: rodneyfr@infomed.sld.cu

R**ESUMEN**

El empleo de las tecnologías de la información y la comunicación en el sector de la salud mejoran considerablemente el funcionamiento de los procesos asistenciales y de gestión médico-administrativa, todo lo cual contribuye a una mayor eficiencia hospitalaria y desempeño competitivo de las instituciones. La presente investigación aborda la problemática existente con el diseño de la infraestructura de red del Centro de Investigaciones Médico Quirúrgicas (CIMEQ), la cual afecta los procesos sustantivos de la institución, como la gestión de pacientes y la trasmisión de imágenes médicas. El objetivo de la investigación es rediseñar la infraestructura de red del CIMEQ, lo que permitirá elevar su rendimiento y seguridad. La investigación tiene un enfoque cuantitativo, con alcance descriptivo, de tipo retrospectivo y diseño experimental, de corte longitudinal. Se emplearon los métodos científicos de modelación y análisis documental. Como resultado se rediseñó la infraestructura de red de área local del CIMEQ, a través de métodos de segmentación que permitieron crear grupos de trabajo de manera dinámica, aprovechar las bondades de los equipos gestionables instalados y la implementación de nuevos cortafuegos. La propuesta de segmentación obtenida, por medio de redes de área local virtual, aplicación de medidas de seguridad a nivel de capa 2 y capa 3 del modelo OSI y la administración del ancho de banda mediante la implementación de calidad de servicio QoS para las aplicaciones que requieran prioridad en el tráfico de la red, mejoró el rendimiento y seguridad de la infraestructura de red del CIMEQ, lo cual impacta en un mayor desempeño competitivo y eficiencia hospitalaria desde el empleo de las tecnologías de la información y la comunicación.

Palabras clave: desempeño competitivo, infraestructura de red, red de área local virtual, eficiencia hospitalaria, tecnologías de la información y la comunicación.

ABSTRACT
Using of information and communication technologies In the health sector improve considerably the functioning of healthcare processes and medical-administrative management, all of which it contributes to greater hospital efficiency and competitive performance of the institutions. This research addresses the existing problem with the design of the network infrastructure of the Medical Surgical Research Center (CIMEQ), which affects the substantive processes of the institution, such as patient management and the transmission of medical images. The objective of the research is to redesign the CIMEQ network infrastructure, which allows increase its performance and security. The research has a quantitative approach, with a descriptive scope, of a retrospective type and an experimental design, of longitudinal cut. Scientific methods of modeling and documentary analysis were used. As a result, the CIMEQ local area network infrastructure was redesigned, through segmentation methods that allowed dynamic workgroups to be created, take advantage of the benefits of installed manageable equipment and the implementation of new firewalls. The segmentation proposal obtained, through virtual local area networks, application of security measures in the layer 2 and layer 3 of the OSI model and bandwidth management through the implementation of quality of service for applications that require priority in network traffic, improved the performance and security of the CIMEQ network infrastructure, which impacts in a greater competitive performance and hospital efficiency
Keywords: competitive performance, hospital efficiency, information and communication technology, network infrastructure, virtual local area network.

Recibido: 08/09/2020
Aprobado: 28/11/2020

Introducción

El desarrollo de la ciencia y la tecnología ha situado a la sociedad del nuevo milenio en la era de la información e incluso, más recientemente, la Sociedad de la Información [(1), (2)]. La información es la materia prima del conocimiento, el cual se ha ido convirtiendo cada vez más en la principal fuente de poder y de riqueza de las naciones [(3)]. En este sentido, la organización de las redes de información, como apoyo a la investigación, es una necesidad inaplazable.

Las redes de información están llamadas a jugar un papel de primer orden en el desarrollo del conocimiento y en la consolidación de comunidades científicas alrededor del mundo. Por eso, la creación y desarrollo de redes informáticas es una exigencia del entorno académico y social, toda vez que su función no solo responde a la investigación básica, sino también a la producción de conocimiento orientado a resolver problemas prácticos y cotidianos de las comunidades [(4),(5)]. Con la aparición del Internet, las posibilidades de conformar y desarrollar

redes mundiales, nacionales y locales de información están al alcance de prácticamente todas las comunidades [1],[6].

Las tecnologías de información y comunicación (TIC) han revolucionado el concepto de producción y distribución de la información. Las TIC han evolucionado desde las formas más primitivas de comunicación, hasta llegar a la etapa actual de la revolución informática. Se denominan TIC al conjunto de recursos, herramientas, equipos, aplicaciones informáticas, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, en cualquier formato: voz, datos, texto, video e imágenes [7].

Las redes informáticas tienen en la actualidad un impacto social y económico muy grande, marcan un cambio en la forma de pensar, actuar y de trabajar [8],[9]. Actualmente, la administración de la información de modo eficiente constituye una de las principales preocupaciones dentro de cualquier sector de la sociedad y sobre todo si se hace referencia al sector de la salud [10]. Asimismo, disímiles investigaciones en el campo de las TIC y la eficiencia hospitalaria evidencian su aplicabilidad, con resultados satisfactorios para mejorar el funcionamiento y el desempeño competitivo en el sector [11], [12], [13].

Son muchas las herramientas que facilitan al hombre el manejo del recurso informativo, así como el acceso a este. Una de estas herramientas, que permite utilizar el recurso de la información de manera más eficiente, rápida y confiable, la constituyen las redes de computadoras, las cuales aparecen enmarcadas dentro del vertiginoso avance tecnológico que ha caracterizado al presente siglo [14]. Las redes informáticas en los hospitales deben garantizar la accesibilidad, integridad, confidencialidad y disponibilidad de la información que interviene en los procesos asistenciales, docentes, investigativos y administrativos. Velar por su correcto funcionamiento contribuirá a la calidad de los servicios que se brindan en la institución. De igual manera, un fallo en la red se traduce en un impacto negativo en cualquiera de estos procesos.

La red informática, como columna vertebral del hospital, debe estar disponible y funcionando correctamente las 24 horas del día, para desarrollar todos los procesos de trabajo médico y de gestión de información con garantías. Las redes informáticas pueden ser de varias categorías, tales como: red de acceso personal (PAN), red de área local (LAN), red de acceso metropolitano (MAN) y red de acceso extendida (WAN). Dentro de estas, en Cuba, las LAN son las que toman mayor protagonismo en los centros hospitalarios. Esto se debe fundamentalmente a la cobertura que ellas abarcan y a las velocidades que pueden alcanzar, que van desde los 10 hasta los 1000 Mbps [14], [15].

Generalmente, las redes de área local se conectan entre diferentes pisos de un edificio o en edificios muy cercanos [16]. La topología de red más usada para el entorno hospitalario en Cuba es la jerárquica o de árbol, la cual es similar a la topología en estrella extendida, su principal diferencia es que no tiene un nodo central. Actualmente en el CIMEQ, a pesar de contar con una gran cantidad de computadoras, sistemas y servicios que contribuyen a la gestión hospitalaria, existen problemas de diversa índole en la infraestructura de red, los cuales se abordan a continuación:

1. No se cuenta con documentación detallada de la red, que incluya el diagrama de la red a todos los niveles y el diagrama de red de los equipos que se conectan a cada subnodo.

2. La red es plana en su diseño lógico. Todo el equipamiento se integra en el mismo segmento de red, por lo que todos pueden comunicarse entre sí, convirtiéndose esto en un problema.

3. Debido a su diseño lógico, la infraestructura de red existente brinda menor flexibilidad en el tráfico de red, así como poca seguridad,

4. Este problema trae como consecuencia el aumento del nivel de colisión y tráfico *broadcast*.

5. Hay un aumento del tiempo de respuesta de los servicios de red más demandados, fundamentalmente en los horarios picos de 9:00 am a 3:00 pm, como son la navegación y la transmisión de imágenes médicas de los equipos de adquisición.

6. Hay insuficientes medidas de seguridad relacionados a la comunicación entre estaciones de trabajo, equipos médicos y servidores.

7. No están establecidos los niveles de prioridad en el tráfico de la red.

8. Los *switchs* gestionables se encuentran subutilizados.

9. No existe una herramienta que permita monitorear el estado de los activos de red y servidores.

10. Se cuenta con un solo firewall ubicado en la frontera de la red, regulando el tráfico que puede salir y entrar hacia la red interna, definiendo además cuales son las direcciones IP y puertos destinos con los que se puede tener comunicación.

11. Los dispositivos de conectividad gestionables (Switchs capa 2) son de diferentes marcas y presentan la configuración de fábrica. En muchos casos, cuando estos activos son de la misma marca y modelo, viene definido con la misma dirección IP que traen por defecto, representando esto direcciones IP repetidas en la red y generando colisiones en la misma.

12. No existen políticas de seguridad rigurosas. Estas tampoco están de acuerdo con los nuevos procesos de trabajo. Además, el acceso a la información se establece a nivel de los usuarios definidos por las aplicaciones, faltando por establecer el acceso a la misma a nivel de estaciones de trabajo.

De acuerdo a las necesidades anteriormente expuestas y a las vulnerabilidades que pueden ocasionar estos problemas de diseño de la red, es necesario encontrar soluciones que permitan reorganizar la estructura actual de la red de manera física y lógica. El flujo de información del CIMEQ es alto y requiere del establecimiento de políticas de seguridad que garanticen la disponibilidad, confidencialidad, integridad y accesibilidad de todos los servicios en tiempo real. El objetivo general de la investigación es rediseñar la infraestructura de red LAN del Hospital CIMEQ, que permita elevar su rendimiento y seguridad.

Antecedentes

A continuación, se abordan los antecedentes de la investigación, que fundamenta la situación y los problemas existentes, en torno a la infraestructura de red de la institución [17], [18].

La especialidad de informática del CIMEQ en el año 1993 comenzó a desplegar una red con topología de anillo. Para ello, utilizaba como enlace físico el cable coaxial, el cual conectaba tres computadoras, una en el primer piso donde se ubicaba el área de informática y dos en el segundo piso, en las áreas de dirección y admisión. Esta red sirvió para comprobar los beneficios de la misma, además de motivar a la dirección del centro a planificar en años posteriores una inversión para desplegar una red en todo el centro. Este fue un logro de la especialidad de informática.

A partir de 1997 se adquirieron los primeros switchs y se incrementaron las computadoras. Se inició una inversión para desplegar una red Ethernet con topología jerárquica, la que se extendió fundamentalmente al tercer y cuarto piso, priorizando las áreas médicas. Ello permitió conectar a la red alrededor de 70 computadoras. Junto con este equipamiento, se adquirieron también tres servidores. Con ellos se pudo implementar un directorio activo para el registro de los usuarios de la red. Además, se sumaron servicios como el DHCP, DNS, correo institucional, se creó el dominio “cimeq.sld.cu” y se diseñó la primera intranet institucional.

Desde el punto de vista de conectividad se logró establecer dos enlaces con Infomed, uno para la navegación nacional mediante módem router, con una velocidad de 256 kbit/s para todas las computadoras que se conectaron a la red. El segundo enlace fue para la navegación a internet mediante un módem, a una velocidad de 54 kbit/s, el cual radicaba en un local independiente. A esta red, que comenzaba a crecer, se fueron incorporando los equipos de diagnóstico por imágenes médicas de altas tecnologías, como fueron las resonancias magnéticas, tomógrafos y ultrasonidos. Además, se desarrollaron aplicaciones cliente-servidor orientadas a la gestión de pacientes, como fueron el registro de pacientes, movimiento hospitalario, facturación, estadística y otras adquiridas a terceros, como fue el caso del Imagis para la visualización de imágenes médicas.

A partir del 2007 el hospital recibió una fuerte inyección tecnológica, con un incremento considerable de computadoras. Además, se adquirieron por esta vía cinco servidores profesionales y más de 25 switchs gestionables. Se construyó el nodo de informática y se comenzaron a establecer los enlaces de fibra óptica hacia los nuevos subnodos que se comenzaban a crear, con el objetivo de aumentar el ancho de banda. Además, se instalaron nuevos servicios como fueron servidores proxys para la navegación nacional e internacional. Posteriormente, en el 2012 se implementa una red inalámbrica en el área de la biblioteca con navegación nacional. La especialidad de informática en este periodo se subordinó a la Dirección de Tecnología y Sistemas del MININT (DTS), mediante la cual se continuó recibiendo equipamiento tecnológico para las nuevas necesidades que demandaba el hospital, lo que ha venido sucediendo en los últimos 12 años.

Dentro de este equipamiento se encuentra un grupo de servidores con los cuales se pudo implementar la virtualización de los servicios que se encontraban hasta ese momento desplegados en máquinas físicas. Esto fue posible gracias al montaje de una infraestructura profesional para aplicar tecnología VMWare ESX. Esta tecnología permitió solucionar el problema de obsolescencia tecnológica que se venía presentando en el centro de datos con los servidores más antiguos. El hospital no solo había alcanzado un crecimiento considerable de tecnología informática, sino también en lo relacionado con equipos médicos. Todo ello permitió una progresión escalonada en los equipos conectados a la red, llegándose a conectar al mismo segmento lógico de la red una cifra considerable de estos equipos. Estos antecedentes propiciaron que se comenzara a evidenciar una latencia superior en la red, incidentes de seguridad informática, así como problemas con el rendimiento y la seguridad.

Método

La investigación tiene un enfoque cuantitativo, con alcance descriptivo, de tipo retrospectivo y diseño experimental de corte longitudinal [19]. Se realizó en el periodo comprendido de marzo de 2018 a agosto de 2020, utilizando como escenario de aplicación el Centro de Investigaciones Médico Quirúrgicas (CIMEQ), de La Habana, Cuba. En la investigación se emplearon diversos métodos científicos de carácter teórico y práctico, tales como:

1. Análisis documental: fue empleado en el análisis bibliográfico, para soportar las afirmaciones realizadas, asociadas con el objeto de la investigación. Se realizó consulta de libros y de artículos científicos indexados en bases de datos de alto impacto.
2. Histórico-lógico: permitió abordar con alto grado de detalle los antecedentes y problemas existentes en el hospital CIMEQ, relacionados con la infraestructura de red.
3. Inductivo-deductivo: posibilitó la inferencia del objeto de estudio en cuestión, sus principales variables y dimensiones a medir, relacionadas con el rendimiento y la seguridad de la red LAN del CIMEQ. Es por ello que se identifica la necesidad de realizar el rediseño de la infraestructura de red en la institución para solucionar las dificultades existentes.
4. Análisis-síntesis: fue utilizado en el estudio del estado del arte, así como en la descomposición de los componentes y relaciones que hacen posible que la red LAN constituya la infraestructura más eficiente y segura para la trasmisión de información.
5. Observación: a través de este método se pudo apreciar con mayor grado de detalle todos los aspectos, problemas y condicionantes asociadas con el tráfico que se genera en la red LAN, con el uso de herramientas específicas para tal fin.
6. Modelación: se utilizó a partir del software de simulación de redes *Cisco Packet Tracer* [20]. Por medio del mismo se pudo desarrollar y simular la infraestructura de red y probar

en un primer momento su efectividad en la mejora del rendimiento y seguridad de la red.

Consideraciones éticas

El cumplimiento de la ética profesional en la informática es de gran importancia, sobre todo en el sector de la salud. Desde los sistemas de información en salud y las plataformas digitales de gestión, procesamiento de datos, transmisión de información, diagnóstico y tratamiento de enfermedades se debe garantizar la disponibilidad, confiabilidad, seguridad e integridad de la información. Asimismo, en los procesos administrativos y de apoyo a la asistencia, la docencia y la investigación. Todas las medidas que se puedan tomar tienen que ir dirigidas en este sentido.

Las redes informáticas son un recurso indispensable para la implementación de cualquier sistema de información en salud. Sobre este recurso va dirigida la investigación, para contribuir a minimizar los riesgos de un uso indebido de la información e incurrir en acciones no éticas, la cual se entiende como que no se debe utilizar las computadoras para cometer fraude, robar información, ni utilizar recursos a los cuales no se está autorizado, siempre garantizando que las TIC se utilicen de manera que se respeten los derechos de los demás.

Resultados y discusión

Actualmente en el CIMEQ se encuentran conectados de manera alámbrica a la red más de 450 equipos, incluyendo los equipos médicos de diagnóstico con sus estaciones de trabajo. Además, los equipos inalámbricos suman más de 300 dispositivos entre celulares, tabletas y laptops. El escenario anterior hace de esta institución una red compleja, con un tráfico de datos e información elevado, situación que ha ameritado el desarrollo de investigaciones para optimizar su infraestructura. Todo ello tiene el objetivo de lograr un mayor aprovechamiento de la tecnología instalada, que impacte en un mayor desempeño competitivo y eficiencia hospitalaria, en cuanto al cumplimiento satisfactorio de sus procesos sustantivos.

La red de datos del CIMEQ se clasifica como LAN debido a su alcance, con una topología jerárquica o de árbol, que permite su crecimiento de manera rápida. La institución cuenta con un nodo central, donde se encuentran todos los servidores del centro, así como el SwitchBlade Modular Capa 3 Allied Telesyn SB-4000, en el que se conectan todos los enlaces de fibra óptica y UTP del primer nivel de la red. Además, se han incrementado los equipos de conectividad (switches), dentro de los cuales el 78% de ellos trabajan en la capa 2 del modelo OSI (Open System Interconnection), permitiendo aumentar el rendimiento y la seguridad [21]. Algunas de las ventajas que suponen, empleadas para fundamentar la investigación y desarrollar la propuesta son:

1. Segmentación de la red mediante la creación de Redes de Área Local Virtuales (VLAN, por sus siglas en ingles), y dentro de este método las VLAN estáticas en lugar de las dinámicas. Se hizo de esta manera por no contar con el 100% de los activos de red

gestionables. Con este método se crean grupos virtuales en función del trabajo que se realiza en el centro. Además, se divide el tráfico de broadcast por cada segmento de red lógico creado o grupo virtual.

2. Aplicación de medidas de seguridad en los switch gestionables para que no se conecten equipos a la red sin la autorización del administrador de la red. Se configuró de manera estática la dirección MAC de las computadoras al puerto del switch donde se conecta y se tomó como acción el apagado del mismo si esta regla se viola.
3. En los switchs donde se encontraban configuradas las VLANs de imágenes médicas se aplicó además la protección de puertos o puertos aislados. De esta manera se evita la comunicación entre los equipos médicos que se encontraban en esta VLAN, a excepción del servidor de imágenes, al cual todos tenían que tener comunicación para poder enviar los estudios imageneológicos.
4. Configuración de límites de ancho de banda por puerto de cada switch para evitar tormentas de broadcast, estas configuraciones se realizan a nivel de capa 2.
5. La implementación de políticas de prioridad en el tráfico de la red que tributen a la calidad del servicio.
6. La implementación de un nuevo esquema de seguridad que permita proteger y regular el acceso a los servidores y equipos de imagenología.

En este sentido, la VLAN es un mecanismo efectivo para extender los cortafuegos o firewalls. Permiten proteger sub-redes de interés para la institución, ante problemas de tormentas de broadcast, los cuales son potencialmente peligrosos en ataques que pueden producirse en la capa 2. Algunas de las áreas sensibles en la institución son: Servidores e Imágenes Médicas.

Teniendo en cuenta que los firewalls tienen como principal función el control del acceso a una red, es de vital importancia su empleo en la red donde se maneja información sensible y confidencial, como lo es la información de pacientes, administrativos y ensayos clínicos. En la Figura 1 se muestra el plano general físico del primer nivel de la red ya debidamente rediseñada, basado en la utilización de VLAN para la segmentación de la red, la aplicación de medidas de seguridad a nivel de capa 2 y capa 3 del modelo OSI y una priorización de ancho de banda con el empleo de Calidad de Servicio *QoS* para el tráfico que lo requiere.

Como se muestra en la Figura 1 los switch de capa 2 y el switch de capa 3 contienen un número en su interior, el cual responde a la identificación de la ficha técnica de ese switch. Esta ficha, además de tener las características técnicas del switch, contiene también qué equipo se conecta a él a nivel de puerto físico, incluyendo su dirección MAC y la VLAN a la que pertenece. Estos datos son necesarios para poder aplicar cada una de las configuraciones anteriormente mencionadas.

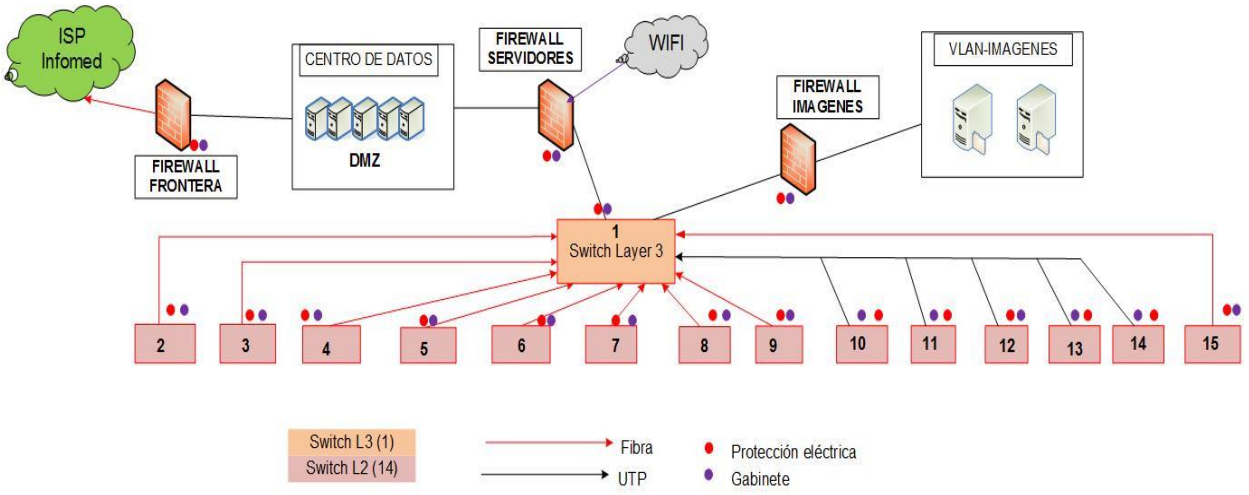

Fig. 1- Plano general físico del primer nivel de la red. Fuente: elaboración propia.

Asimismo, en la Figura 2 se presenta el esquema lógico que finalmente se emplea en la red. Para ello, se tiene en cuenta una implementación con estándares de calidad para la gestión del tráfico, la existencia de políticas de seguridad alineadas a las necesidades de la institución y un aprovechamiento del rendimiento de los equipos de comunicación instalados. Es por ello que la velocidad de transferencia mejora, así como el rendimiento y seguridad de la red, posibilitando optimizar la ejecución de los procesos sustantivos de la institución, como la gestión de pacientes y la trasmisión de imágenes médicas DICOM Compatibles, generadas por los equipos de imagenología.

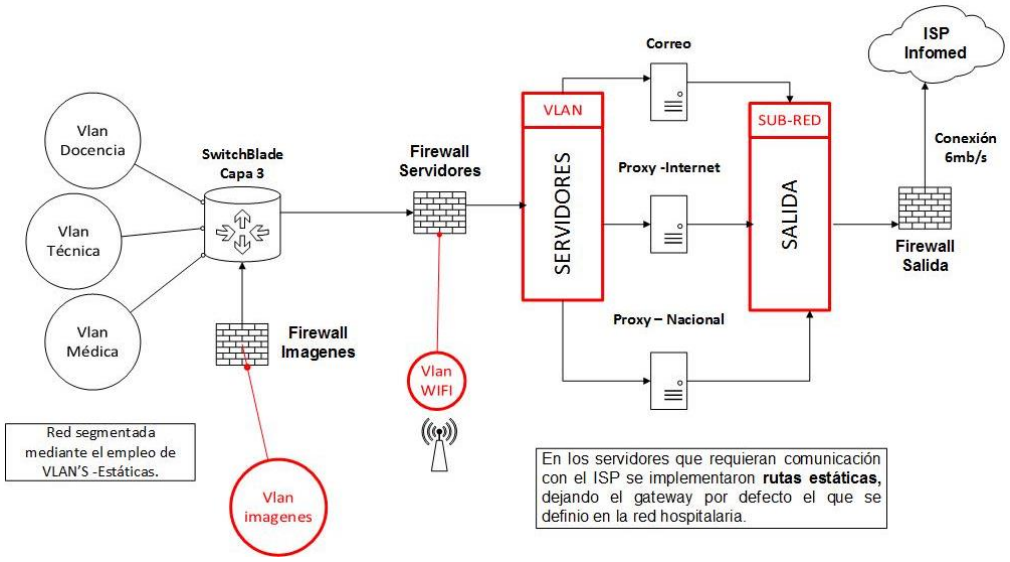

Fig. 2- Esquema lógico de la red del CIMEQ. Fuente: elaboración propia.

El primer firewall implementado cubrió las subredes de los servidores y la inalámbrica. Se creó una Zona Desmilitarizada (DMZ) o zona segura, a pesar de no brindar ningún servicio hacia internet o red nacional. Esta medida permitió proteger el acceso a los servicios en la subred de los servidores. Además, regula el acceso de los dispositivos inalámbricos en la red para mayor seguridad, limitándose en su mayoría a los servicios institucionales como la navegación nacional mediante un proxy, FTP y correo. En la red inalámbrica, dependiendo del tipo de usuario, se le brinda acceso a otros servicios como es la visualización de imágenes médicas, siempre desde el servidor principal de imágenes. No se permite a los dispositivos inalámbricos la comunicación con ninguna estación de trabajo conectada a la red interna como medida de seguridad.

Con este tipo de diseño se logra una zona segura, la cual utiliza dos firewalls, uno conectado a la red interna y el otro a la red externa, por el cual solo se permite el paso a los servicios que requieren de esta comunicación, como son el caso del servidor DNS, correo y los proxys. Este esquema eleva la seguridad y disminuye las vulnerabilidades que existían antiguamente.

El tercer firewall reguló el acceso a la subred de imágenes, controlando cuáles son los dispositivos que pueden descargar estudios y de qué estación de trabajo. Para ello se estableció que la única comunicación dentro de esa subred es hacia el servidor de imágenes, al cual llegan los estudios que se realizan en todos los equipos de imagenología. El CIMEQ cuenta actualmente con el Sistema para el almacenamiento, visualización y transmisión de imágenes médicas XAVIA PACS, el cual es desarrollado por la Universidad de las Ciencias Informáticas (UCI), como solución para la visualización de los estudios, los cuales proveen la seguridad necesaria de la información [22],[23].

Como último elemento que interviene en la seguridad de la red está el SwitchBlade Modular de Capa 3 Allied Telesyn SB-4000. Además de tener configuradas las redes virtuales VLAN, los Gateway o puertas de enlace de cada VLAN y las tablas de enrutamientos para encaminar todo el tráfico de la red; tiene la importantísima función de permitir o denegar la comunicación entre VLANs, mediante el empleo de reglas y filtros, lo que eleva la seguridad de la red.

Proceso experimental para evaluar el funcionamiento de la nueva infraestructura de red

Experimento 1. Tráfico Broadcast

El proceso experimental que se presenta tiene el objetivo de evaluar el rediseño de la red propuesto. El experimento fue realizado antes (diseño anterior de la red) y después (con el nuevo diseño de red), el cual evidenció la variación de algunos parámetros medidos. Se analizó el tráfico de broadcast que se originaba en la red, los cuales se pudieron dividir en 2 orígenes fundamentales:

1. Las estaciones de trabajo que envían broadcast de pedidos ARP (Protocolo de Resolución de Direcciones). Esta se genera cada vez que una computadora necesita localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast

son causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho o por la acción maliciosa de un atacante.

2. Cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Estos clientes por lo general repiten este pedido después de un relativo corto "timeout", posiblemente debido a una respuesta lenta del servidor, lo que produce las conocidas tormentas de broadcast. Estas, a su vez, producen retardos anormales de otros tráficos cliente/servidor, los cuales también pueden empezar a retransmitir.

El tráfico broadcast es observable en todas las computadoras que se encuentran conectadas al mismo segmento de red. La falta de su control incide en la disponibilidad de ancho de banda y puede suponer riesgos en la red, como los ataques de suplantación. El primer experimento consistió en analizar el tráfico broadcast del diseño inicial de la red, desde una computadora del área de informática, donde se encontraban registradas más de 50 direcciones MAC. En su totalidad, las entradas dinámicas ARP que se registraron en la computadora fueron generadas por otras estaciones de trabajo dentro de la red, como se muestra en la Figura 3.

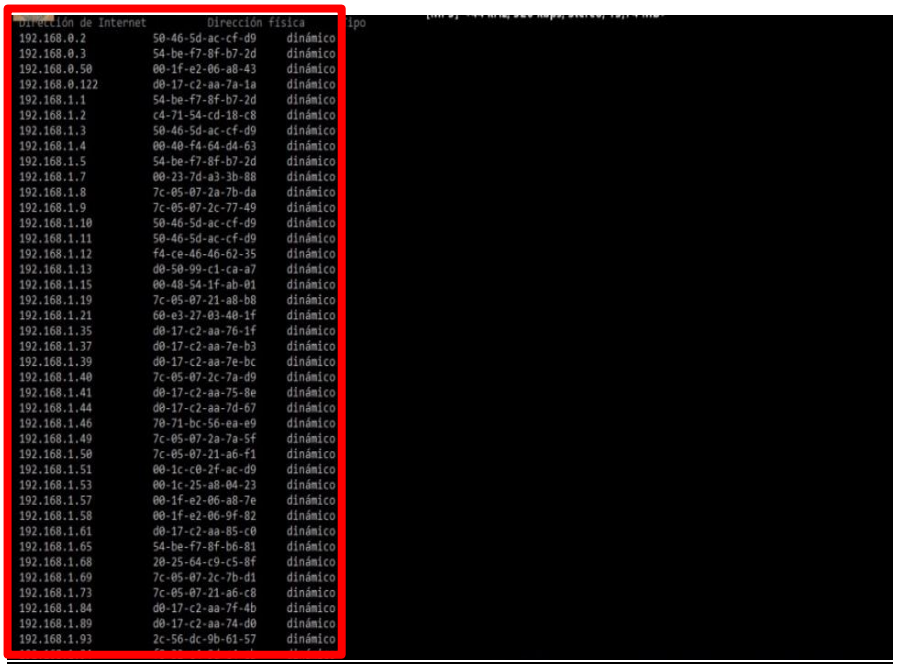

Fig.3- Tabla ARP (diseño anterior de la red). Fuente: elaboración propia.

Luego de rediseñar la infraestructura de red, se volvió a consultar la tabla ARP en la misma computadora de informática. En esta ocasión se pudo comprobar que disminuyeron las entradas dinámicas ARP. En este caso solo se registraron las direcciones MAC de las computadoras que se encontraban en la VLAN de informática, como se muestra en la Figura 4.

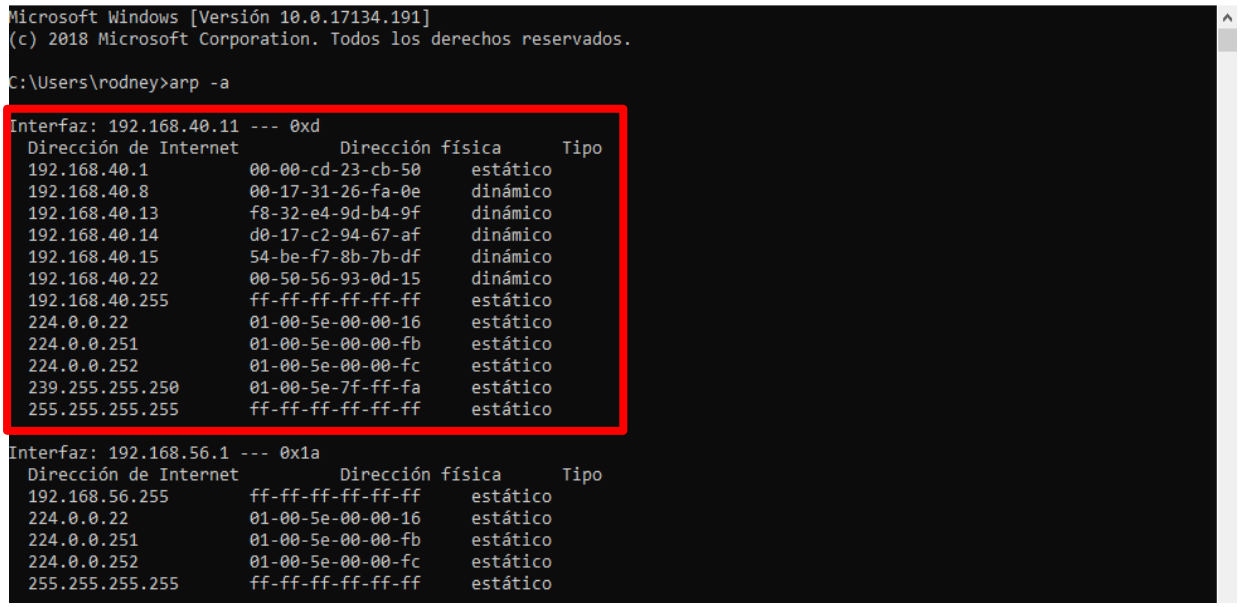

Fig. 4- Tabla ARP (diseño actual de la red). Fuente: elaboración propia.

Experimento 2. Desbordamiento de la Memoria de direcciones MAC (CAM) de un Switch

Este experimento se basa en la limitación del hardware del switch para mantener la tabla que relaciona las MAC con los puertos, dicha tabla se denomina CAM. Esta tabla es finita y cuando llega a su tope un switch comienza a trabajar como un HUB. Esto significa que todo paquete que recibe el switch, si la dirección MAC destino no se encuentra en la tabla, envía el paquete por todos sus puertos. Tal hecho permite al atacante capturar todo el tráfico o tramas que se dirigen a las MAC que no se encuentren en la tabla. Las asignaciones en estas tablas son temporales. Es por ello que si se envía al switch direcciones MAC falsas, en intervalos de tiempo lo suficientemente cortos para que se llene esta tabla, se puede lograr que las direcciones MAC verdaderas caigan por vencimiento de tiempo. Estos espacios se llenan con más MAC falsas y se lograría realizar este tipo de ataque al switch.

Se puede resumir el desbordamiento overflow como la acción de enviar muchas tramas con direcciones MAC distintas a un puerto del switch, hasta que en un momento determinado se comience a recibir las tramas que se dirigen a otras máquinas. Estas tramas se pueden capturar con un sniffer, como puede ser la herramienta Wireshark. De esta manera una persona puede apoderarse de contraseñas de los usuarios de la red.

Este tipo de acciones producen inestabilidad en la red. En estas circunstancias no es raro que se produzca una denegación de servicio (DoS) o bloqueo por parte del switch, en vez de empezar a enviar paquetes a través de sus puertos.

Para realizar este experimento, se utilizó una herramienta para producir este tipo de ataques, denominada Macof. Dicha herramienta forma parte de la suite de paquetes de Dsniff, el cual se puede encontrar en el repositorio de cualquier distribución de Linux. Para utilizarlo, solo se debe instalar el paquete Dsniff y ejecutar Macof mediante una consola o terminal.

Seguidamente, se generan de manera automática muchas direcciones MAC, como se muestra en la Figura 5, hasta llenar la memoria CAM del switch. En el experimento se utilizó el puerto 3 del switch.

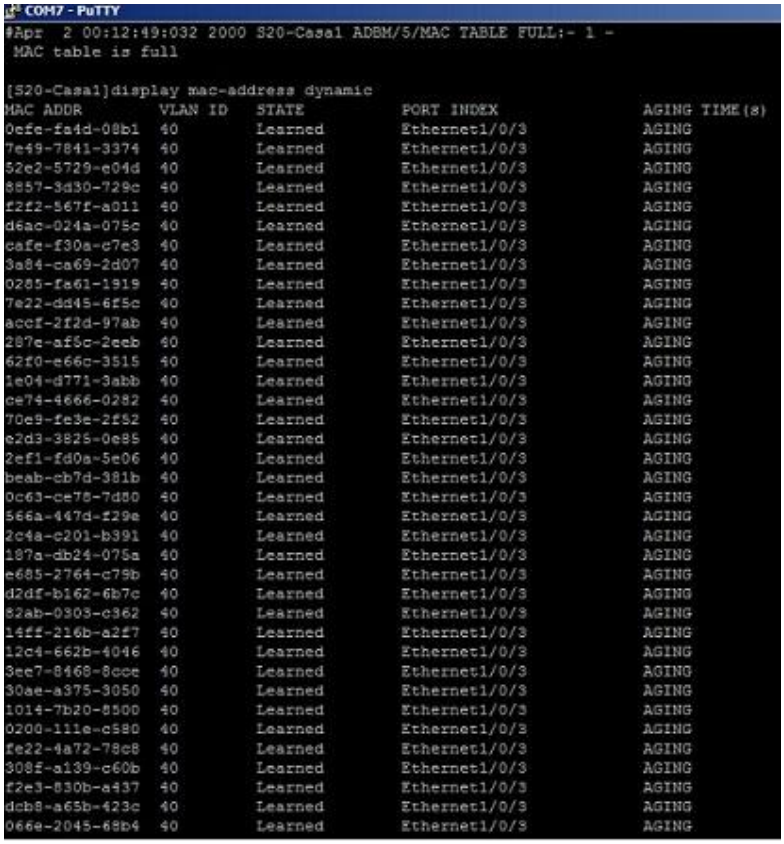

Fig. 5- Direcciones MAC generadas automáticamente por la interfaz 3 del *switch*.
Fuente: elaboración propia.

Después de aplicar medidas de seguridad a nivel del puerto en el switch de capa 2 o gestionable, se pudo comprobar que este tipo de ataque es inefectivo. Dentro de las medidas empleadas para mitigar este ataque se implementó la asignación de direcciones MAC de manera estática al puerto. De producirse el ingreso de una dirección MAC diferente a la definida previamente, se ejecuta una determinada acción. Para el caso del experimento, la acción ejecutada fue el apagado del puerto, aunque el puerto también puede ser suspendido de manera temporal. Posteriormente, después de un tiempo dado, el puerto se restablece de manera automática.

Experimento 3. Ataque de la red mediante BetterCap

Además, se realizó un ataque a la nueva red diseñada con BetterCap. Este es un programa que permite realizar ataques de suplantación de identidad en la red, posibilitando la denegación de servicio y la captura del tráfico que se trasmite por la red. Con la utilización de este programa se realizaron dos experimentos fundamentales. En el primer caso se cambió la dirección MAC

asociada a la puerta de salida de las computadoras conectadas a la red y en el segundo caso se cambió una dirección IP determinada, para recibir en la computadora atacante todo el tráfico que saliera de la computadora víctima.

Ejemplo 1: Ataque de suplantación de la dirección MAC de la puerta de enlace de todas las computadoras de la red. Comando empleado: bettercap –x

Resultado: De este ataque todas las computadoras conectadas a la red cambiaron la dirección MAC de su puerta de enlace por la del atacante, desviando todo el tráfico que va dirigido hacia afuera de la red, primero hacia la computadora del atacante.

Ejemplo 2**:** Ataque de suplantación de la dirección MAC de la puerta de enlace a una computadora especifica en la red. Comando empleado: bettercap –X –T 192.168.40.11

Resultado: Después de ejecutar este ataque, se pudo visualizar en la computadora del atacante las credenciales del usuario víctima, para acceder al servidor FTP de la institución. Ver Figura 6.

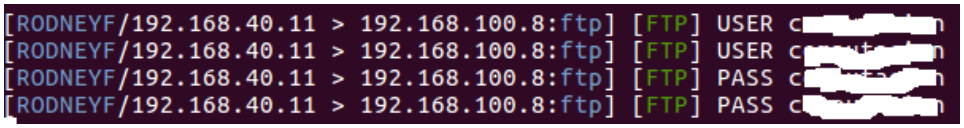

Fig. 6- Captura de credenciales mediante bettercap. Fuente: elaboración propia.

Estos dos ataques generaron un gran tráfico ARP en la red por parte de la computadora atacante. Además, se mantuvo durante todo el tiempo que duró el ataque, como se muestra en la Figura 7.

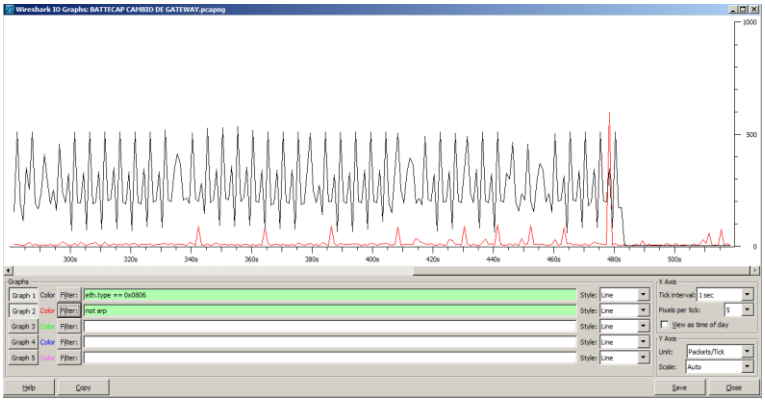

Fig. 7- Gráfico de Wireshark durante el ataque de bettercap en la computadora víctima. Fuente: elaboración propia.

Los dos ejemplos vistos no fueron efectivos después de cambiar el diseño de la red, el cual deja sin opciones las intenciones de un atacante mediante el bettercap:

1. La segmentación de la red mediante VLAN reduce la efectividad del ataque solo a las estaciones que se encuentren en la misma subred.
2. Las medidas de seguridad aplicadas a los switch capa 2 permiten controlar las tormentas de broadcast.
3. La asignación de manera estática de las direcciones MAC en la tabla ARP de la computadora permite evitar este tipo de ataques.

Conclusiones

Como resultado de la investigación se obtuvo la nueva infraestructura de red de área local del CIMEQ, fundamentada en nuevos métodos de segmentación que permitieron crear grupos de trabajo de manera dinámica, aprovechando las bondades de los equipos gestionables instalados y la implementación de nuevos cortafuegos. Asimismo, parte de la implementación con estándares de calidad para la gestión del tráfico, la existencia de políticas de seguridad alineadas a las necesidades de la institución y un aprovechamiento del rendimiento de los equipos de comunicación instalados.

La propuesta de segmentación obtenida, por medio de redes de área local virtual VLAN, aplicación de medidas de seguridad a nivel de capa 2 y capa 3 del modelo OSI y la priorización de ancho de banda mediante la implementación de Calidad de Servicio QoS, mejoró el rendimiento y seguridad de la infraestructura de red del Hospital CIMEQ, lo cual impacta en un mayor desempeño competitivo y eficiencia hospitalaria desde el empleo de las tecnologías de la información y la comunicación.

El proceso experimental realizado, mediante la medición del tráfico Broadcast, y el ataque a la nueva infraestructura de red diseñada para evaluar suplantación de identidad, mediante la herramienta BetterCap, permitieron validar que la nueva propuesta presentada evidencia resultados superiores y positivos respecto al diseño anterior existente en la institución, pudiendo concluir que el nuevo diseño implementado elevó el rendimiento y la seguridad de la red en el CIMEQ.

Referencias

1. Romero A. Las redes de información y su importancia para la investigación científica. Revista Venezolana de Gerencia [Internet]. 2002 [citado 17 Dic 2020];7(19):425-41. Disponible en: https://www.redalyc.org/pdf/290/29001906.pdf.

2. Martin WJ. The global information society. Second edition. New York, USA: Taylor & Francis Group. 2017.

3. Ramírez Pérez JF, Estrada Sentí V, Morejón Valdés M, Arza Pérez L. Modelo para la gestión y análisis de conocimiento para la selección de equipos de trabajo quirúrgico en sistemas de información en salud mediante técnicas de inteligencia organizacional. Revista cubana de información en ciencias de la salud [Internet]. 2017 [citado 17 Dic 2020];28(1):43-60. Disponible en: http://www.acimed.sld.cu/index.php/acimed/article/view/1017.

4. Roig Vila R, Mondéjar L, Lledó GL. Redes sociales científicas. La Web social al servicio de la investigación. International Journal of Educational Research and Innovation. 2016;(5):170-83.

5. Froufe NQ. La emergencia de las redes sociales académicas: su impacto académico. Opción. 2016;32(10):517-28.

6. Ramírez Pérez JF, Batista Téllez R. Propuesta de red cubana Aurora para la colaboración médica a través de Infomed utilizando un enfoque de redes sociales. Memorias Convención Internacional de Salud. La Habana: Cuba Salud; 2015.

7. Grande M, Cañón R, Cantón I. Tecnologías de la información y la comunicación: evolución del concepto y características. IJERI: International Journal of Educational Research and Innovation [Internet]. 2016 [citado 17 Dic 2020];(6):218-30. Disponible en: https://www.upo.es/revistas/index.php/IJERI/article/view/1703.

8. Gil Vázquez P, Pomares Baeza J, Candelas Herías F. Redes y transmisión de datos. España: Universidad de Alicante; 2010.

9. Barceló Ordinas JM, Íñigo Griera J, Martí Escalé R, Peig Olivé E, Perramon Tornil X. Redes de computadores. Primera edición. 2004. Cataluña, España: Eureca Media. 354 p.

10. MINCOM. Resolución 129-2019 del Ministerio de Comunicaciones. Metodología para la Gestión de la Seguridad Informática (2019).

11. Delgado Ramos A, Vidal Ledo M. Informática en la salud pública cubana. Revista Cubana de Salud Pública [Internet]. 2006 [citado 17 Dic 2020];32(3). Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662006000300015.

12. Vidal Ledo M. Primera estrategia para la informatización del sector de la Salud Pública Cubana. Una propuesta para el desarrollo. La Habana: Ecimed; 2007.

13. Ramírez Pérez JF, Rodríguez Rodríguez T, Olivera Fajardo D, Morejón Valdés M. Componente para la toma de decisiones en salud. Un enfoque de análisis de redes sociales desde la minería de procesos. Rev cuba inform méd [Internet]. 2016 [citado 17 Dic 2020];8(1):46-63. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592016000100004.

14. Pérez S, Facchini H. Dispositivos y protocolos de redes LAN y WAN. Argentina: CERECON; 2017.

15. Chan KK, Hartmann PW, Lamons SP, Lyons TG, Milonas AC. U.S. Patent No. 4,823,338. Washington, DC: U.S. Patent and Trademark Office. 1989.
16. Clark DD, Pogran KT, Reed DP. An introduction to local area networks. Proceedings of the IEEE. 1978;66(11):1497-517.
17. Antón Rodríguez S. CIMEQ: 35 años de historia. Infomed [Internet]; 2017 [citado 17 Dic 2020] . Disponible en: https://instituciones.sld.cu/cimeq/2017/03/25/cimeq-35-anos-de-historia/.
18. Centro de Investigaciones Médico Quirúrgicas [Internet]. Cuba; 2020 [2020; citado Ago 2020]. Disponible en: http://www.sld.cu/sitios/cimeq/.
19. Sampieri RH, Collado CF, Lucio PB. Metodología de la Investigación. Sexta Edición. México: Interamericana Editores (Mc Graw Hill); 2014.
20. Hernández EA, Bautista JC, Zenil AEG, Medellín AAH, Hernández SH, Hernández GH. Comparacón de los modelos OSI y TCP/IP. Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla. 2017;5(10).
21. Tarkaa NS, Iannah PI, Iber IT. Design and simulation of local area network using cisco packet tracer. The International Journal of Engineering and Science [Internet]. 2017 [cited 2020 Dec 17];6(10):63-77. Available from: http://www.theijes.com/papers/vol6-issue10/Version-2/I0610026377.pdf.
22. Vega Izaguirre L, López Cossio F, Ramírez Pérez JF, Orellana García A. Impacto de las aplicaciones y servicios informáticos desarrollados por la Universidad de las Ciencias Informáticas para el sector de la salud. Rev cuba inform méd [Internet]. 2020 Jun [citado 17 Dic 2020];12(1):58-75. Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592020000100058&lng=es.
23. Ceruto Marrero G, Ramírez Pérez JF, Castro Limones AN, Pérez Delgado B. Componente informático para el cálculo de volumen en imágenes de tomografía axial computarizada. Cuba: III Convención Internacional de Salud Pública, Cuba Salud; 2018.

Conflicto de interés

Los autores declaran que no existe conflicto de intereses.

Declaración de autoría

Rodney Flores Robaina y José Felipe Ramírez Pérez: conceptualización y diseño del estudio, aplicación de los experimentos, análisis e interpretación de los resultados. Redacción del borrador del manuscrito y aprobación de la versión final a publicar.

Madelayne Muñoz Morejón: recogida de datos, análisis e interpretación de los resultados, revisión crítica del manuscrito y aportes intelectuales importantes a su contenido. Aprobación de la versión final a publicar.