APLICACIÓN DE PRÁCTICAS DE SEGURIDAD IDÓNEAS PARA EL DISEÑO DE LA INFRAESTRUCTURA DE REDES A 10GB ETHERNET EN REDES CORPORATIVAS UNIVERSITARIAS

PRÁCTICAS DE SEGURIDAD IDÓNEAS PARA EL DISEÑO DE LA INFRAESTRUCTURA DE REDES

AUTORES: Paulina Mayorga Soria[1]
Martha Cecilia Cueva[2]
Patricio Navas Moya[3]
Rodolfo Matius Mendoza Poma[4]
Santiago Fernando Ramírez Jiménez[5]

DIRECCIÓN PARA CORRESPONDENCIA: ptmayorga@espe.edu.ec

Fecha de recepción: 16 - 11 - 2016 Fecha de aceptación: 14 - 01 - 2017

RESUMEN

Toda organización en la actualidad requiere contar con redes convergentes o multiservicio que soporten tráfico de voz, datos y video, estos nuevos requerimientos obligan al personal de ingeniería de redes de toda empresa a elaborar diseños apropiados que cuenten con ingeniería de tráfico, seguridades y mecanismos que garanticen calidad de servicio. Las universidades requieren de diseños de red complejos debido a la necesidad de múltiples servicios, así como por su diversidad de usuarios lo que hace imprescindible disponer de guías y políticas de seguridad, esto con la finalidad de minimizar los riesgos ante posibles ataques a los que se encuentra expuesta la información debido a los distintos servicios que se oferta a cada uno de los usuarios.

PALABRAS CLAVE: Amenaza; vulnerabilidad; riesgo; política de seguridad; red.

APPLICATION OF APPROPRIATE SAFETY PRACTICES FOR INFRASTRUCTURE DESIGN 10GB ETHERNET NETWORKS IN CORPORATE UNIVERSITY NETWORKS

[1] Ingeniera en Sistemas. Magister en Redes y Telecomunicaciones. Jefe de la Unidad de Tecnologías de Información y Comunicación de la Universidad de las Fuerzas Armadas ESPE, extensión Latacunga, Ecuador.

[2] Licenciada en Inglés. Magister en Docencia Universitaria y Administración Educativa. Facultad de Ciencias Administrativas. Carrera de Secretariado Ejecutivo Gerencial. Latacunga, Ecuador.

[3] Ingeniero en Sistemas. Magister en Gestión de Bases de Datos. Universidad de las Fuerzas Armadas ESPE, Departamento de Eléctrica y Electrónica. Carrera de Ingeniería de Software. Jefe de Laboratorio de Producción de Software e Investigación. Planificador de las áreas de Computación. Latacunga, Ecuador

[4] Ingeniero en Sistemas. Magister en Sistemas Informáticos Educativos. Universidad Técnica de Cotopaxi. Facultad de Ciencias Administrativas. Carrera de Secretariado Ejecutivo Gerencial. Administrador de la Plataforma MOODLE de la Facultad. Latacunga, Ecuador

[5] Ingeniero en Sistemas y Computación. MBA Master Bussines Administrator. Master en Gerencia de Sistemas. Universidad Técnica de Cotopaxi. Facultad de Ciencias Administrativas. Carrera de Secretariado Ejecutivo Gerencial. Latacunga, Ecuador.

ABSTRACT

Nowadays every organization requires possessing converged networks or multiservice support voice traffic, data and video. These new requirements need the engineering staff in networks of any company to develop appropriate designs that have traffic engineering, securities and mechanisms to guarantee ensure service quality. Universities require designs of complex network due to the need for multiple services, as well as its diversity of users makes essential for guidelines and security policies. This is vital in order to minimize risks from against possible attacks to which information is exposed due to the offer of various services to each user.

KEYWORDS: Threat; vulnerability; risk; security policy; network.

INTRODUCCIÓN

El activo más importante de las organizaciones es la información y como sus empleados pueden interactuar entre sí para lograr los objetivos institucionales, el avance tecnológico ha ayudado que los dispositivos puedan comunicarse entre dispositivos remotos con otros equipos y estos requieran de seguridades para precautelar todos sus activos y comunicaciones (Linares, J., Rivera, H., Cubillos, F. y Silva, A., 2013) (Ferreira, J.C., Acuña, G., (2012). Las buenas prácticas de seguridad e interconexión deben cumplir con políticas claramente definidas para prevenir el acceso a la información no autorizado la modificación o alteración de la información dentro de una red LAN (Bonilla, S.M. y González, J.A., 2015). La administración de las seguridades de las redes siempre dependerá de un buen diseño y de seleccionar los dispositivos apropiados, en el Ecuador las Universidades.

El mejoramiento tecnológico y la implementación de seguridades ayudan en las infraestructuras complejas y costosas con la finalidad de prever potenciales peligros en sus distintos estamentos, dado que estos puedan intentar atacar a la información, con la presente investigación se propone implementar una red LAN de calidad y segura a costos razonables y dentro de los parámetros y normas internacionales (Blanco, H.J., Bohorquez, E.W., Salinas, E.A. (2015).

DESARROLLO

Análisis de Trafico: Para tecnología basada en Ethernet, el análisis se lo debe realizar en base a sondas con interfaz Ethernet conectadas al bus, estas sondas con su interfaz Ethernet funcionan en modo promiscuo, capturan el tráfico a analizar y constituyen la plataforma que se ejecutaran de forma continua, aplicaciones propietarias o de uso libre que se encargaran de determinar el tipo de información que circule en la red, esto ayudará a determinar la existencia de virus o de aplicativos p2p que comúnmente degradan las prestaciones de la red sobre todo si esta tiene conexión a internet. Para las redes Universitarias es decir que tienen conexiones a conmutadores, estas sondas deben estar conectadas directamente.

Calidad de Servicio: Es el rendimiento de los servicios que presta la red y la forma como lo ve o como percibe el usuario final. Los parámetros de QoS medibles son: el retardo, la variación del retardo, y la pérdida de paquetes. Una red debe garantizar siempre un alto nivel de confiabilidad para un nivel de tráfico y más cuando se trata de redes universitarias en las cuales se tiene varios tipos de usuarios finales (Puspita, F.M. et al., 2013) (Lee, K.II. et al., 2012).

La Calidad de servicio en redes Universitarias deben estar de acuerdo a:

- Asignación del ancho de banda en forma diferenciada
- Administrar de forma adecuada la congestión que se pueda presentar.
- Modelar el tráfico de la red
- Priorizar el tipo de tráfico.

10 Gigabit Ethernet: es la tecnología base ideal para los nuevos centros de datos para satisfacer las nuevas necesidades de las organizaciones (Lin, J. et al., 2015).

Con esta nueva tecnología se aumenta el ancho de banda para soportar nuevas aplicaciones y cargas de trabajo que se consumen y producen (An, Fu-Tai, et al., 2014). Elimina cuellos de botella en el servidor tanto de entrada como de salida (E/S), para aumentar la densidad de virtualización de servidores. Permite la implantación de una estructura unificada en ambos centros de datos FCoE y iSCSI. (Zhao, W., 2012)

Red de Campus: es una red que conecta varias redes LAN dentro de un mismo sitio geográfico que no es más grande que una ciudad, en este tipo de redes encaja las universidades, es decir las tecnologías de redes que se usarían en una red LAN están compuestos de componentes incluyendo conmutadores, enrutadores, cableado y otros, le pertenecen a la misma organización. Este tipo de redes utilizan tecnologías como FDDI, Gigabit Ethernet para conectividad a través de medios de comunicación tales como fibra óptica e inalámbrica.

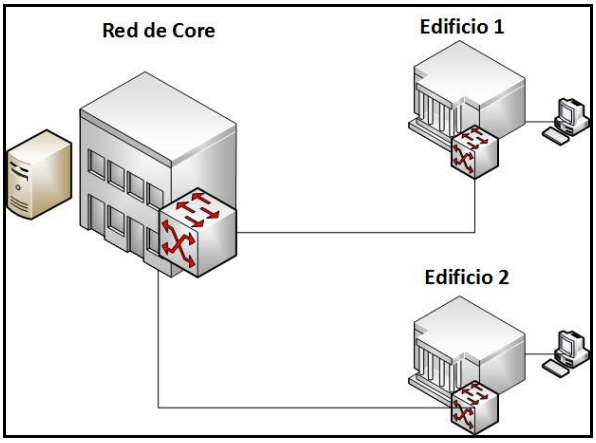

Figura 1: Diseño de una red de campus

En la figura 1 es como se representa en esta investigación de acuerdo a la Universidad tomada como ejemplo.

CONFIGURACIONES

1.1. Identificar y analizar los riesgos

Dentro de las seguridades en redes antes de proceder a elaborar los diseños para la implementación de un sistema de seguridad se debe considerar que se tiene y por supuesto que se va a proteger. Una vez realizado este análisis se debe identificar los riesgos que estén latentes en la organización realizar una evaluación de su impacto para establecer los controles y de esta manera mitigar en lo posible los impactos más significativos.

1.2. Definición de Jerarquías de la red en capas

De las buenas prácticas en diseño de redes LAN es utilizar un modelo de diseño jerárquico, el mismo que implica la división de la red en capas independientes, donde cada capa tiene su función, los modelos de redes jerárquicas tradicionales cuentan con 3 capas que son CORE, DISTRIBUCION Y ACCESO, para una red de campus universitario, se recomienda utilizar las dos capas CORE y ACCESO. Donde el propósito principal de la capa de acceso es proporcionar un medio de conexión a todos los dispositivos de la red y de esta manera controlar que dispositivos pueden comunicarse a la red. Esto permite contar con un mayor nivel de seguridad. Ya que la capa de CORE será diseñada exclusivamente para el backbone de alta velocidad de la red.

1.3. Definir políticas de seguridad

Una vez que se ha cuantificado los riesgos que se tiene en la red ya que se tiene sistemas de información que precautelar, de acuerdo a la jerarquía planteada se debe cubrir aspectos de diseño considerando diferentes tipos de usuarios que van desde el nivel gerencial, operacionales, particulares, los técnicos e incluso estudiantes los cuales se convierten en un riesgo potencial si no se cuenta con un diseño bien definido que facilite la implementación de políticas de seguridad.

Cuando se cuenta con políticas de seguridad claras se debe tener la capacidad de definir que se puede y que no se puede hacer dentro de la red corporativa.

En las redes Universitarias hay que tener en cuenta lo siguiente:

- Nombre del administrador o súper usuario, responsable de la política
- Grupo de personas que deben acatarla de acuerdo a las actividades que realicen en la Universidad.
- Enunciar las políticas, tener un procedimiento de acuerdo al objetivo de la Universidad.
- Deberá tener sanciones por el incumplimiento de políticas, esto hará que se tome en serio las buenas prácticas.

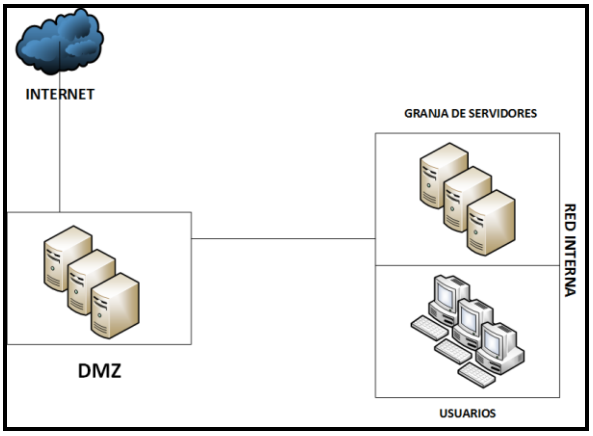

Figura 2. Diseño General de la Red

1.4. Definir velocidad en la red

La velocidad de la red en el campus universitario es fundamental debido a los grandes anchos de banda que se maneja, además de esto por los múltiples servicios que requieren los usuarios como: telefonía IP, videoconferencia, almacenamiento de información, WiFi, por lo que como buena práctica se debe elaborar diseños de switching con niveles de redundancia que permitan duplicar el backbone de red de 10Gb Ethernet, ya que al tener redundancia y ser configurado mediante etherchannel se consigue duplicar el enlace troncal a 20Gb Ethernet.

Para la tasa de red de datos y la estimación aproximada se partió de la fórmula de Mathis:

Tasa <(MSS/RTT)*(C/sqrt(Perdida)) [C=1]

Límite de red (MSS 15500 byte, RTT: 100,0 mseg,

Pérdida: 10-07 (10-05%)) = 379.47 Mbit/seg.

Retardo en el AB(ancho de banda) producto del tamaño de búffer:

BDP (20.000 Mbit/seg, 100,00 mseg.) = 250,00 MByte

Búffer TCP necesario para alcanzar 20.000 Mbps con RTT de 100 mseg >= 244.140,60 Kbyte

Throughput máximo con una ventana TCP (RWIN) de 256 KByte y RTT de 100,0 mseg. <= 20,97 Mbit/seg.

Donde:

RTT, retardo de ida y vuelta de un paquete (Round-trip delay time), es el tiempo requerido para que un paquete viaje desde un emisor a un destino específico y viceversa.

MSS, tamaño máximo de segmento (Maximum segment size), es la mayor cantidad de datos, en bytes, que un equipo de comunicaciones puede manejar en una sola trama, sin fragmentar.

RWIN, ventana de recepción TCP (TCP Receive Window), es la cantidad de datos que un dispositivo de red puede aceptar sin reconocer el remitente. Si el remitente no ha recibido un acuse de recibo para el primer paquete que envió, se detendrá y esperará, y si esta espera supera un cierto límite de tiempo (RTT), se puede solicitar la retransmisión; dicho procedimiento permite la transmisión confiable en capa de transporte (TCP).

De lo informado se garantiza que el backbone vertical FO (20Gbps) para el Campus, permite la transmisión de información de manera confiable, segura y sin saturación de los canales de comunicaciones (20,97 Mbps) por cada usuario Administrativo, Docente o Estudiante (apróx. 6.000 usuarios).

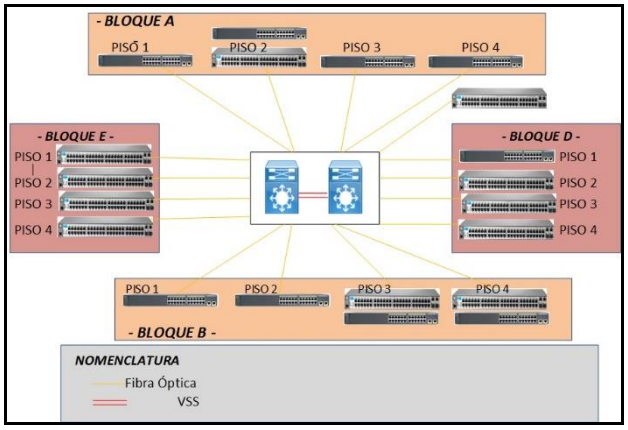

Figura 3: Diseño de red en capas

En la figura anterior se tiene la distribución de la red de acuerdo a los equipos con que cuenta la universidad que se toma por ejemplo, (CORE, ACCESO), se diseña dos enlaces del switch de CORE hacia cada switch de acceso, a fin de contar con redundancia y duplicar el backbone de red a 20GB Ethernet. Tanto los switchs de CORE como los switchs de acceso se configuran en stack.

1.5. Características de equipos de red

Para la selección de equipos se debe tomar en cuenta aspectos como el tamaño y complejidad de la red, para el caso de las Universidades se habla de redes corporativas (redes complejas con grandes cantidades de información), en el mercado existen gamas de equipos para cada capa del diseño de red jerárquica, los cuales deben ser respetados el momento de realizar una elección, en el sistema de switching se debe considerar varios factores como calidad del servicio, performance, estabilidad de la red, redundancia y seguridad de la red.

Para la elección del swith de CORE adicionalmente se deberá considerar el número de puertos con enlaces redundantes que se requiere conectar a cada switch de ACCESO. De igual manera para la elección de switchs de ACCESO se deberá tomar en cuenta dos puertos redundantes mismos que deberán soportar la velocidad del backbone de red diseñado y el número de puertos para los diferentes dispositivos a conectar.

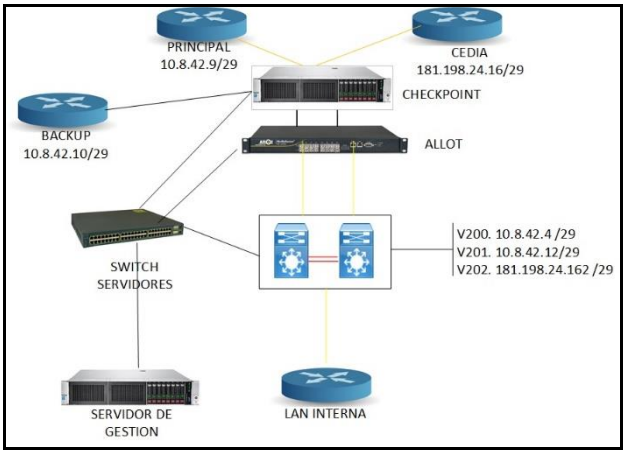

Figura 4: Diseño de la arquitectura de red

En la figura del diseño de la arquitectura de red se incluye los dispositivos necesarios para incrementar la seguridad en la red.

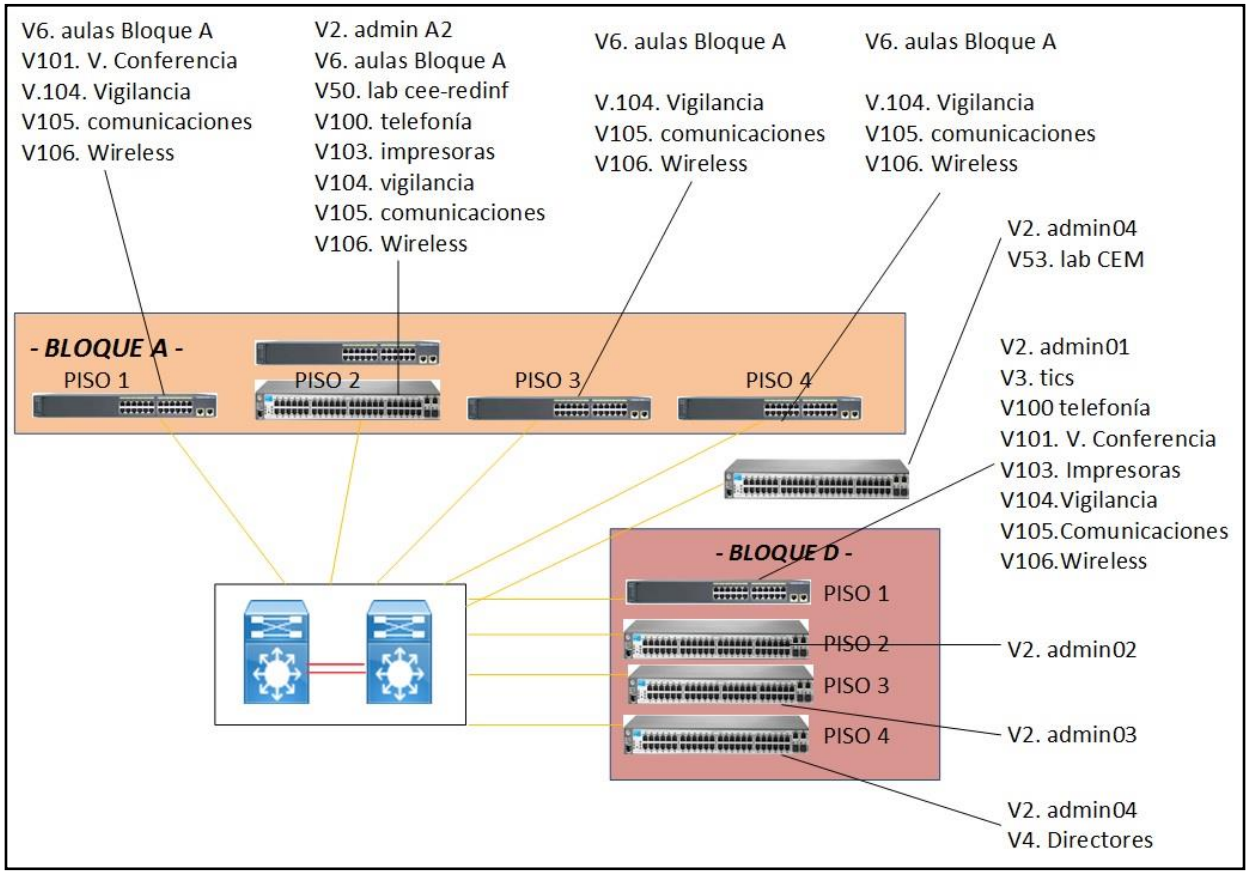

Figura 5: Diseño de VLAN's de servicios y de usuarios

1.6. VLAN y Segmentación

a. Creación de VLAN por equipos

Una vez que se ha elegido los equipos adecuados se debe empezar por trabajar en el diseño de VLAN's lo cual permitirá dotar de seguridades al segmentar a

red y además mejorar su desempeño ya que se limita el tráfico de broadcast, una buena práctica al diseñar VLAN's consiste en establecer VLAN's de uso general para identificar los servicios y VLAN's de uso particular para los diferentes tipos de usuarios. La diferencia entre las VLAN's de uso general y las VLAN's de usuario radica en que las primeras se crean en todos los switchs y las segundas se crean únicamente en las ubicaciones a las que se conectarán los usuarios según su tipo, de esta forma se evita tráfico de broadcast innecesario.

b. Definición de Direccionamiento IP

A fin de complementar la seguridad en el diseño de direccionamiento IP, se debe subnetear la red de tal manera que cada red se asigne a cada VLAN, la segmentación es otra medida de seguridad para evitar ataques entre usuarios de la red.

Como se puede visualizar las VLAN's, de servicios y de usuarios son de uso general se definen para todos los servicios que se brinda y las de usuarios en base a los diferentes tipos de usuarios.

1.7. Colocar un equipo de DLP (Data Loss Prevention)

Un DLP es un sistema que identifica, monitorea y protege datos en uso, dota en movimiento y datos en reposo por medio de mecanismos de inspección, análisis contextual de transacciones colocación de un DLP entre el core y los routers de los proveedores de servicio de internet, o antes del firewall.

Para regular el tratamiento legítimo de datos confidenciales, controlar e informar sobre el uso responsable de la información. Garantizar la privacidad del contenido de los mismos, esto con la finalidad de observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad. Un DLP nos permite bloquear además los dispositivos que presenten anomalías como por ejemplo spam.

1.8. Firewall perimetral

Finalmente proporcionar protección extra a la red limitando los ataques a puertos con vulnerabilidades de equipos y servidores, los accesos no autorizados, y la mayoría de los códigos maliciosos automatizados.

Para seleccionar los equipos de firewall o DLP más adecuado para la red se debe analizar la cantidad de usuarios simultáneos que atraviesen por estos equipos de tal manera que no degraden el rendimiento de la red.

Se debe considerar la instalación de un IPS como complemento a la seguridad de la red, mismo que puede ser un módulo incorporado al firewall o un módulo adicional que sirve para detectar los ataques que se pueden dar en la red, todos los equipos q forman parte de la red deben tener implementadas políticas de seguridad, se debe considerar deshabilitar puertos innecesarios que se instalan en los equipos (PC, SWITCH CORE, SWITCH DE ACCESO, RED

INHALAMBRICA, CENTRAL IP, VIDEOCONFERENCIA), lo que ayudara a minimizar el riesgo de ataques a la red interna

Finalmente la instalación de un equipo de monitoreo y la designación de un profesional para la detección y evaluación de anomalías que se presenten en la red contribuirá con la solución de seguridad implementada.

2. Evaluación de Resultados

La arquitectura adecuada de seguridad en una red LAN se debe basar en un análisis de riesgos, para realizar un correcto diseño de red que cuente con seguridades cubriendo las necesidades de la Universidad, se deberá invertir en lo necesario, elegir los dispositivos y herramientas óptimas para poder brindar un servicio de calidad a los usuarios adquiriendo un aceptable nivel de prevención de riesgos.

Para poder alcanzar los beneficios de estas buenas prácticas se debe realizar evaluaciones a las herramientas que se ofrecen en el mercado, antes de seleccionar la más adecuada para lograr mitigar los riesgos organizacionales. Las herramientas de bajo costo no siempre ayudan a economizar a una organización no tampoco las más caras pueden llegar a ser la solución técnica-tecnológica que requiera la Universidad.

Para proteger la información que genere la Universidad debería estar determinada a un corto tiempo para poder garantizar un equilibrio financiero y técnico - tecnológico.

Ahora si dentro de las evaluaciones realizadas se logra determinar la existencia de Virus informáticos en los equipos de los usuarios de la red el riesgo de que se pueda contagiar el resto de usuarios es alto, por lo que se debe sugerir la utilización del antivirus comercial porque el impacto sería desastroso, debido a esto también es recomendable establecer y difundir políticas de seguridad para los equipos de cómputo especialmente en el acceso hacia el internet, en la descarga de software no confiable, en los correos maliciosos o a su vez los dispositivos de almacenamiento removibles.

CONCLUSIONES

En trabajos de buenas prácticas de diseño e instalación de seguridades en redes LAN hay que partir de un diseño óptimo para la Universidad y que este tenga un retorno de inversión en el menor tiempo posible de acuerdo a equipos y administradores que estén en el proyecto.

Hay que tener siempre claro cuáles son los riesgos potenciales y de quien nos debemos cuidar, podemos realizar implementación de seguridad sin mayor inversión y con un adecuado diseño de la red, dividido en segmentos de red de acuerdo a los perfiles de usuario.

Con un buen diseño, equipos óptimos y seguridades adecuadas se debe plasmar políticas de seguridad en la red mismas que van desde los dispositivos que se conectan a la red hasta atravesar por cada componente de la misma.

Las políticas de seguridad deben ser cumplidas de la mejor manera, tanto el seguimiento, el monitoreo y la evaluación de la solución implementada por el administrador de red, como por los usuarios que forman parte de ella.

BIBLIOGRAFÍA

Linares, J., Rivera, H., Cubillos, F. y Silva, A. (2013). «Integración del módulo DeviceView que permite gestionar switches multi-vendor al sistema de monitoreo de red Open Source Nagios, para centralizar la administración en redes LAN,» Tekhné, vol. 10, nº 2, pp. 27-32, 2013.

Ferreira, J.C., Acuña, G. (2012). «Análisis sobre el comportamiento del troughput en redes LAN bajo tecnología Power Line Communications,» Iteckne, vol. 9, nº 2, pp. 22-32, 2012.

Bonilla, S.M. y González, J.A. (2015). «Modelo de Seguridad de la Información,» Ingeniería como USBmed, vol. 3, nº 1, pp. 6-14, 2015.

Blanco, H.J., Bohorquez, E.W., Salinas, E.A. (2015). «SIMULACION DE REDES LAN Y WLAN HACIENDO USO DEL SOFTWARE NS-2,» Visión electrónica: algo más que un estado, vol. 8, nº 2, pp. 145-154, 2015.

Puspita, F.M. et al. (2013). Improved models of internet charging scheme of single bottleneck link in multi QoS networks. *Journal of Applied Sciences*, 2013, vol. 13, no 4, p. 572.

Lee, K.II. et al. (2012). *UPnP QoS network system and method for reserving path and resource*. U.S. Patent No 8,135,837, 13 Mar. 2012.

Lin, J. et al. (2015). Performance evaluation of time slot based QoS aware ad hoc network scheme for CBR and TCP flows. En *Network Operations and Management Symposium (APNOMS), 2015 17th Asia-Pacific*. IEEE, 2015. p. 139-144.

An, F.T. et al. (2014). A new dynamic bandwidth allocation protocol with quality of service in ethernet-based passive optical networks. *arXiv preprint arXiv:1404.2413*, 2014.

Zhao, W. (2012). *Methods and apparatus for selecting a wireless network based on quality of service (QoS) criteria associated with an application*. U.S. Patent No 8,214,536, 3 Jul. 2012.