INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año V. Vol V. N°9. Julio – Diciembre. 2023
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

https://doi.org/10.35381/i.p.v5i9.2622

Firewall para la seguridad de la red los laboratorios. Universidad Estatal de Bolívar, Ecuador

Firewall for network security laboratories. Bolivar State University, Ecuador

Xavier Efraín Mullo-Pilamunga
pg.xavieremp74@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-8308-9279

Ariel José Romero-Fernández
ua.arielromero@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0002-1464-2587

Gustavo Eduardo Fernández-Villacres
ua.eduardofernandez@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ambato, Tungurahua
Ecuador
https://orcid.org/0000-0003-1028-1224

Rita Azucena Díaz-Vásquez
ui.ritadiaz@uniandes.edu.ec
Universidad Regional Autónoma de los Andes, Ibarra, Imbabura
Ecuador
https://orcid.org/0000-0003-4183-6974

Recibido: 20 de marzo de 2023
Revisado: 15 de mayo de 2023
Aprobado: 25 de junio de 2023
Publicado: 31 de julio de 2023

INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año V. Vol V. N°9. Julio – Diciembre. 2023
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

RESUMEN

El objetivo de la investigación fue presentar una propuesta para mejorar la seguridad de la red en los laboratorios de la Universidad Estatal de Bolívar. La investigación fue de enfoque cuantitativo y descriptiva. En los resultados se analizaron y estudiaron los mecanismos tanto de hardware como de software que posee actualmente el Laboratorio de Ingeniera en Sistemas en materia de seguridad informática, llegando a la conclusión de que no utilizan un firewall adecuado con las políticas de seguridad de la información. Se puede concluir que con las encuestas realizadas se puede establecer que la mayoría de estudiantes son completamente inconscientes de su seguridad informática, los técnicos no realizan actualizaciones de seguridad de los equipos y tampoco verifican los certificados HTTP en las páginas que frecuentan. Las políticas de seguridad propuestas toman en cuenta una amplia gama de servicios que estarán disponibles para estudiantes internos y externos mejorando la seguridad informática.

Descriptores: Seguridad; informática; técnicos; alumnos; software. (Tesauro UNESCO).

ABSTRACT

The objective of the research was to present a proposal to improve network security in the laboratories of the State University of Bolívar. The research was quantitative and descriptive approach. In the results, the mechanisms of both hardware and software that the Laboratory of Systems Engineering currently has in terms of computer security were analyzed and studied, reaching the conclusion that they do not use an adequate firewall with information security policies. It can be concluded that with the surveys carried out, it can be established that the majority of students are completely unaware of their computer security, the technicians do not carry out security updates on the equipment and they do not verify the HTTP certificates on the pages they frequent. The proposed security policies take into account a wide range of services that will be available to internal and external students by improving computer security.

Descriptors: Security; computing; technicians; students; software. (UNESCO thesaurus).

INTRODUCCIÓN

En la actualidad, cada organización requiere de al menos un Firewall para proporcionar a su arquitectura de red una seguridad adecuada. Los Firewall son el componente central de la seguridad en una red. En los últimos años los riesgos han aumentado de forma significativa, por lo que cada vez es necesario una clase más robusta de cortafuegos.

El alto desarrollo alcanzado en tecnologías de la información a nivel global y el intenso uso por parte de los estudiantes de las mismas han provocado el incremento de los volúmenes de datos que se transportan mediante las redes. (Plasencia Moreno, 2017), esta constante se expresa en gran medida en los centros educativos universitarios, ya que al ser centros de investigación y desarrollo necesitan estar constantemente intercambiando información con el internet.

(North, J. and Pascoe, R, 2016) indican que la ciber-seguridad es un tema de creciente preocupación, especialmente para las empresas del sector privado, pues son ellas las cuales con mayor frecuencia son víctimas de costosos ataques informáticos. En su trabajo ellos resaltan la importancia de concebir la seguridad como un tema de interés para toda la organización, y no solo para el departamento de tecnología.

En las universidades la concientización tiene un rol importante para crear entre los estudiantes una percepción aguda sobre los riesgos de seguridad informática. Ellos son futuros profesionistas que pronto deberán hacer frente a las amenazas informáticas como parte de su vida profesional. Existen investigaciones que han identificado la importancia que la seguridad sea fomentada e investigada desde el ámbito universitario. (Roque Hernández, 2018)

El trabajo de Stanciu y Tinca (2016) destaca la creciente necesidad de implementar procesos y eventos de capacitación y concientización acerca de la seguridad informática, especialmente en las universidades, pues el conocimiento de los estudiantes suele ser más técnico y específico de su campo de estudio y menos orientado hacia aspectos de

seguridad. Se recalca que la actitud de las personas ante lo expuesto en sus ordenadores o dispositivos, asociada a su conducta, anida una debilidad considerablemente grave ante los riesgos informáticos externos.

Aunque este artículo, utiliza la palabra firewall, que en un contexto clásico es una de las tantas herramientas con la que se implementa, la seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software.

La Universidad Estatal de Bolívar fue conformada en 1977 como una extensión de la Universidad de Guayaquil como facultad de Ciencias Administrativas, para 1989 después de muchos y esfuerzos y gestiones fue reconocida como Universidad Estatal de Bolívar; a medida que transcurre el tiempo la universidad no ha dejado de innovar y crecer en el campo educativo, realizando implementación en el área tecnológica, es así que a medida que la tecnología se innova también aparecen nuevas amenazas y ataques contra la seguridad de la información.

En este sentido, en la Universidad Estatal de Bolívar, en varias observaciones técnicas relacionadas con la seguridad informática de la institución y específicamente en los laboratorios de la Escuela de Ingeniería en Sistemas, se pudo apreciar que estos son utilizados por los estudiantes para el acceso a internet, pero estos equipos al estar conectados también a la red interna de la institución son una puerta de acceso a la información institucional la cual corre un peligro inminente, si no se cuenta con un buen sistema de seguridad en la red, lo que puede traer como consecuencia perdida de información y/o alteración de la misma, además del posible acceso de intrusos externos a la red a través de internet.

En el presente artículo lo que se requiere es analizar los mecanismos de software y hardware utilizados para la seguridad de la red en los laboratorios de la Escuela de

Ingeniería en Sistemas, con la finalidad de establecer una propuesta para explotar al máximo los recursos disponibles y adaptarlos a las normativas de seguridad para la protección de la información que se mueve por esta red.

De lo descrito anteriormente se puede apreciar que la problemática existente y como solución a la misma, se plantea el presente trabajo investigativo cuyo objetivo general será: Estructurar la configuración adecuada de un firewall físico para complementar la Seguridad Informática de los laboratorios de la Carrera de Ingeniería en Sistemas pertenecientes a la Universidad Estatal de Bolívar. Previo al planteamiento de una propuesta tecnológica de solución, se desarrolla a continuación el siguiente fundamento teórico:

Firewall: Los firewalls, según López (2016) son esencialmente dispositivos que filtran tramas que tienen como destino las máquinas donde están alojados, así como tramas que se originan en esas máquinas o tramas que están en tránsito, en base a parámetros que se pueden leer en la misma trama, como IP de destino, IP fuente, dirección de red, protocolo, puerto, etc. Al conjunto de especificaciones que filtran el flujo de señal, se denominan políticas, para Baca (2016) una política de seguridad es un conjunto de reglas, así como de prácticas que definen y regulan los servicios de seguridad de una organización o un sistema con el fin de proteger sus recursos críticos y sensibles, en otras palabras, son las reglas de lo que está permitido y lo que no. Es así como los firewalls, esencialmente implementan políticas y las diferencias entre diferentes firewalls, reside en las características del hardware y de la interfaz de estudiantes, que faciliten la escritura de políticas.

En una red informática tradicionalmente la primera línea de defensa contra ataques a la seguridad de la información es un FIREWALL o cortafuegos siendo éste un dispositivo de Hardware o software, que permite gestionar y filtrar la totalidad del tráfico de los paquetes de datos entrantes y salientes que circulan por la red ya sea interna o externa,

en este sentido, Miranda y Ramírez (2016) consideran un firewall o cortafuegos como un elemento de hardware o software que es usado en una red de computadoras con el fin de controlar las comunicaciones, y según sea el caso permitirlas o prohibirlas según las políticas de red que haya definido la organización garante de la red. La manera de controlar el tráfico de los paquetes de datos que navegan por la red es imponer una serie de reglas que permiten que se pueda acceder o salir de nuestra red sin ninguna restricción. Con esto se logra proteger los activos contra las amenazas comunes que supone la internet.

El Firewall controla el tráfico de la red, puesto que es un dispositivo especializado que permite o niega el tráfico según una serie de políticas definidas por el administrador de red. Ahora bien, el Firewall está diseñado específicamente para inspeccionar el tráfico; por lo tanto, es un dispositivo capaz de inspeccionar el tráfico de una red que genera más de mil millones de paquetes trasversales en un periodo de tiempo corto. Al compararlo con un ser humano, es imposible que este interactúe de forma directa con la red, inclusive si se dispusiera de una herramienta para observar el tráfico de forma directa en una red, le resultaría imposible al ser humano decidir qué tráfico es bueno o malo; por lo tanto, debido a que la seguridad de la red es importante y que para un ser humano es imposible procesar los millones de paquetes generados por la red de forma directa, se requiere dispositivos especializados que garanticen la seguridad del tráfico de la red como son los firewalls (Urbina, 2016).

La función principal de un firewall es establecer una barrera de seguridad entre redes informáticas. En este sentido se puede proteger la red o parte de ella, de entornos hostiles que sean una potencial fuente de ataque. Existen actualmente muchas tecnologías y arquitecturas de sistemas de firewall, y cada una tiene su aplicabilidad, ventajas y desventajas. Los firewalls controlan el flujo de red filtrando los paquetes que pasan por ella. Este filtrado puede tener algunos niveles de complejidad y eficiencia. Puede ser un

filtrado sencillo en el que solo se considera la información de las cabeceras de los protocolos principales, hasta sofisticados sistemas de filtrado continuo de contenidos.

Además de filtrar los accesos también altera la conexión en los casos de percibir comportamientos extraños o pocos comunes en los sistemas de comunicación, debido a una señal de un posible ataque o intrusión en la red; también ayuda a calcular datos de la red como, por ejemplo, la velocidad de acceso a internet con la que entran y sales los datos de la red, en otras palabras, el tipo de tráfico que se está generando.

En este orden de ideas, se pueden establecer tres tipos de firewalls: el clásico, el de nueva generación (NGFW) y el UTM (Unified Thread Management) firewalls. Existe una discusión entre los NGFW y los UTM (administración centralizada de las amenazas), en realidad pueden considerarse equipos equivalentes, donde la diferencia, vienen más de las campañas de mercadeo que buscan diferenciar sus productos, algunos fabricantes denominan UTM a sus equipos dirigidos a la PYME, y NGFW a sus equipos de gama alta, dirigidos a las empresas grandes, mientras que otros fabricantes denominan NGFW a todos sus equipos independientes del tamaño de la organización y otros denominan UTM a todos sus equipos no importando la gama de aplicación (Martínez, 2017).

El equipo de administración centralizada de amenazas es un dispositivo que están utilizando actualmente las empresas, las empresas lo conocen como un sistema de gestión unificado de amenazas, el cual es capaz de realizar tareas como detección de intrusos en la red, además de tener antivirus en Gateway (Stallings & Brown, 2014).

Políticas que se deben implementar en un sistema de Firewall: Las características de seguridad según Solano, O. Pérez, D. y Bernal J. (2016) detallan los servicios de seguridad del sistema, se determina que hacer o no hacer con los recursos del sistema, además de quien lo puede hacer, también se hace mención de cómo se implementan dichos servicios. También al configurar un firewall se deben de tomar en cuenta dos

políticas básicas, las cuales se fundamentan en el tipo de seguridad que quiera adoptar la organización. La primera es la política restrictiva, con ella se rechaza el paso de cualquier información, excepto la que está explícitamente autorizada y que consiste en servicios por Internet y de proveedores. Aquí el firewall debe obstruir todo el tráfico y deberá ser analizado y aceptado, caso por caso. La segunda es la política permisiva, que autoriza el paso de toda la información, excepto aquella para la cual está negado.

MÉTODO

La investigación es de enfoque cuantitativo y descriptiva, porque determina la cantidad de alumnos que ingresan al laboratorio diariamente y la razón por la que acceden al mismo, para determinar si los firewalls cumplen su objetivo limitando el acceso a sitios no seguros para la institución**.** La investigación se llevará a cabo en los laboratorios de la escuela de Ingeniería de Sistemas de la Universidad Estatal de Bolívar y la población inmersa en la problemática está definida en el periodo 2018-2019 en un total de 1933 estudiantes de los laboratorios, junto con 4 Técnicos.

RESULTADOS

Análisis de resultados de las encuestas realizadas a los técnicos

Pregunta 1.- El 70% de los técnicos indican que la información no es segura al utilizar el internet en los laboratorios de la universidad

Pregunta 2.- El 61% de los técnicos mencionan que los programas y sistemas operativos que ellos administran no están actualizados y el 39% indica que sí, estableciendo que hay computadoras que si tienen actualizaciones y otras no; siendo éstas vulnerables a pérdidas de información.

Pregunta 3.- En esta tabla se verifica la importancia de asegurar la información, ya que todos los técnicos afirman que debe ser resguardada la información de la universidad.

Pregunta 4.- Los técnicos mencionan que las computadoras del laboratorio presentan infección de virus constantes; el 90% manifiesta que frecuentemente adquieren virus las maquinas.

Pregunta 5.- Los resultados demuestran que el 70% de los técnicos señalan que las computadoras de los laboratorios no cuentan con autentificación e identificación de estudiantes; lo que se evidencia que cualquier persona puede acceder al sistema.

Pregunta 6.- En esta tabla se demuestra que el 95% de los técnicos encuestados consideran que se debe establecer políticas de seguridad en firewall para evitar vulnerabilidad de la información.

Análisis de resultados de las encuestas realizadas a los estudiantes

Pregunta 1.- El 60% de los estudiantes consideran que la información que se comparte por internet al usar los laboratorios no está segura, mientras que el 40% señalan positivamente respecto al tema.

Pregunta 2.- En esta tabla se puede revisar que no es un hábito de los estudiantes revisar que las páginas de internet tengan un protocolo seguro (https), demostrado con el 70% de los encuestados.

Pregunta 3.- Dentro de los resultados se identifica que el 60% de los estudiantes se ve afectado por las páginas invasivas que aparecen en internet, haciendo que su experiencia no sea agradable.

Pregunta 4.- Los resultados demuestran que para el 90% de los estudiantes es importante que la información sea privada y confidencial, aún más si se trata de internet.

Pregunta 5.- En esta tabla se evidencia que el 70% de los estudiantes no ha sido estafado electrónicamente, pero al no contar con controles, están expuestos a robo de información.

Pregunta 6.- De acuerdo a los resultados, el 90% de los estudiantes cree que la información debe ser asegurada para evitar daños en las computadoras y otros tipos de ataques que pueda sufrir el sistema.

DISCUSIÓN

El análisis de los equipos de seguridad que poseen los laboratorios de la Escuela de Ingeniería en Sistemas y de cómo estos no están siendo utilizados como es debido, tuvo el propósito de identificar posibles amenazas o escaso aseguramiento de la información a pesar de ser equipos de última generación. El nivel de control físico es bueno, pero se evidencia un riesgo informático debido a la desactualización del software de los equipos. Debido a las pocas actualizaciones que se realiza en los laboratorios de computación son vulnerables a los ataques, los cuales se pueden transmitir virus, pérdida o robo de información; no solo el cliente puede ser atacado; sino también cuando el cliente se conecta al servidor en el caso de correos electrónicos consumen sus servicios, el servidor puede sufrir un ataque.

Además, si comparamos nuestros resultados con los hallados en otros estudios realizados, podemos ver que dichos resultados tienen semejanzas en cuantas algunas coincidencias en la investigación, ya que el estudiante no tiene una cultura de seguridad informática y tampoco es consciente del peligro de navegar en internet con una escasa seguridad de los servidores.

La implementación de un firewall físico permitirá ser un barrera para evitar que personas no conocidas tengan acceso al servidor; efectuando políticas de restricción y permisibilidad que ayuden a las organizaciones como las universidades sean vulnerables a sufrir problemas de ataques a sus redes informáticas por la cantidad de estudiantes que tienen acceso a las mismas tanto interna como externamente, por esta razón se

adoptan estas políticas, ya que, crean ambientes más flexibles y seguros para los estudiantes de la red (Villalón, 2013).

Aunque, cabe destacar, que las amenazas no sólo provienen de Internet, por lo que es responsabilidad del administrador de la red incrementar la seguridad en todos los otros puntos de vulnerabilidad. La propuesta busca mejorar la protección de las redes en los laboratorios de la Escuela de Ingeniería de Sistemas, de las amenazas externas y agregar protección a las redes del laboratorio de ataques provenientes de las otras redes de la universidad, así como proteger a las otras redes contra ataques desde máquinas del laboratorio.

CONCLUSIONES

Al finalizar la presente investigación, se pueden establecer las siguientes conclusiones:

Se analizaron y estudiaron los mecanismos tanto de hardware como de software que posee actualmente el Laboratorio de Ingeniera en Sistemas en materia de seguridad informática, llegando a la conclusión de que no utilizan un firewall adecuado con las políticas de seguridad de la información. La metodología utilizada para el diseño y desarrollo resultó eficiente ya que permitió obtener información importante y relevante para el proceso de investigación y queda disponible para su utilización en investigaciones similares.

Las políticas de seguridad propuestas para el laboratorio de la Escuela de Ingeniería en Sistemas de la Universidad Estatal de Bolívar toman en cuenta una amplia gama de servicios que estarán disponibles para estudiantes internos y externos mejorando proporcionalmente la seguridad informática de los estudiantes. De las encuestas realizadas se puede establecer que la mayoría de estudiantes son completamente inconscientes de su seguridad informática, ya que, los técnicos no realizan

actualizaciones de seguridad de los equipos y tampoco verifican los certificados HTTP en las páginas que frecuentan.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A los docentes, estudiantes y técnicos de escuela de Ingeniería de Sistemas de la Universidad Estatal de Bolívar del periodo 2018-2019.

REFERENCIAS CONSULTADAS

López C., R. (2016). Diseño de un cortafuegos para bloquear sistemas de evasión de censura de internet basados en proxy. [Design of a firewall to block proxy-based Internet censorship circumvention systems]. *Revista de Investigaciones Altoandinas*(18), 1-10.

Martínez, T. (2017). Diferencias entre UTM y NGFW, las hay? Obtenido de Telequismo Blog personal: Recuperado de: http://www.telequismo.com/2017/07/utm-ngfw.html/

Miranda, Jezreel Mejia, & Ramirez, Heltton. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, (17), 01-15. https://doi.org/10.17013/risti.17.1-15

North, J. and Pascoe, R. (2016). Cyber security and resilence - it's all about governance. *Governance Directions, 68* , 146-151.

Plasencia Moreno, L. &. (2017). Referencial architecture of Big Data for the management of telecommunications. *Revista chilena de ingeniería*, 566-577.

Roque,R. (2018). Concientización y capacitación para incrementar la seguridad informática en estudiantes universitarios. [Awareness and training to increase computer security in university students]. *Revista de tecnología y sociedad PAAKAT, 8*(14). Obtenido de http://dx.doi.org/10.32870/Pk.a8n14

Solano, O., Pérez, D., & Bernal, J. (2016). El sistema de información y los mecanismos de seguridad informática en la Pyme. [The information system and computer security mechanisms in SMEs]. *Revista Punto de Vista,* *7*(11), 77-98. https://dialnet.unirioja.es/descarga/articulo/6121657.pdf

Stallings, W., & Brown, L. (2014). Seguranca de computadores: principios e práticas. [Computer security: principles and practices]. Río de Janeiro: Elsevier Editorial.

Urbina, G. (2016). Introducción a la seguridad informática. [Introduction to computer security]. México: Grupo Editorial Patria.

Villalón, J. (2013). Firewalls transparentes. [transparent firewalls].https://n9.cl/1dcz6

©2023 por los autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones de la licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional (CC BY-NC-SA 4.0) (https://creativecommons.org/licenses/by-nc-sa/4.0/).