Implementación de protocolos de seguridad en redes usando tecnologías Cisco

Paola Andrea Realpe Zambrano[1]

Jhonatan Franky Ñañez Muñoz[2]

Nelson Sebastián Barón Orteaga[3]

Cítese como: Realpe-Zambrano, P. A., Ñañez-Muñoz, J. F. y Barón-Orteaga, N. S. (2023). Implementación de protocolos de seguridad en redes usando tecnologías Cisco. En H. Juajibioy-Otero, J. A. Oviero, H. D. Huertas-Moreno, N. S. Gallego-Eraso, F. C. Gómez-Meneses y O. A. Bernal-Ortiz (comps.), *Investigar e innovar en ambientes diversos con sustento en el desarrollo humano sostenible* (pp. 62-68). Editorial UNIMAR. https://doi.org/10.31948/editorialunimar.172.c251

Resumen

Esta idea de investigación se enfoca en la implementación y gestión de un buen protocolo de seguridad en las redes, teniendo en cuenta una recolección de información sobre las múltiples amenazas, la tecnología Cisco, las partes y componentes que conforman una red, al igual que su funcionamiento general. Por lo tanto, este proyecto se basa en la búsqueda de información útil para evitar o mitigar las incidencias de inseguridad en el país, debido al aumento de los ciberataques a compañías, hecho que ha dejado consecuencias negativas, ya sea el daño de datos importantes o la pérdida económica masiva. El principal objetivo fue analizar las implementaciones actuales en los protocolos de seguridad en las redes, haciendo uso de los dispositivos Cisco, para poder preservar la seguridad, privacidad e integridad de los datos, indagando en los distintos problemas presentes, en la infraestructura y mantenimiento en las redes, además de identificar la configuración en los dispositivos y proponer una estrategia que brinde una solución aceptable que contribuya de manera significativa a la conectividad. Por último, fue necesario apropiarse de conocimientos con relación a las redes, con el fin de buscar soluciones innovadoras que aporten a la nueva era del desarrollo en el campo de la ingeniería de sistemas.

Palabras clave: tecnología; seguridad; protocolos; redes; Cisco.

[1]Universidad Mariana, Programa de Ingeniería Sistemas, Semillero ELITE. Correo electrónico: parealpe@umariana.edu.co
[2]Universidad Mariana, Programa de Ingeniería Sistemas, Semillero ELITE. Correo electrónico: jhonanez@umariana.edu.co
[3]Universidad Mariana, Programa de Ingeniería Sistemas, Semillero ELITE. Correo electrónico: nbaron@umariana.edu.co

Implementation of security protocols in networks using Cisco technology

Abstract

This research idea focuses on the implementation and management of a good security protocol in networks, taking into account a collection of information on multiple threats, Cisco technology, the parts and components that make up a network, as well as its general operation. This project is based on the search for useful information to avoid or mitigate insecurity incidents in our country due to the increase in cyberattacks against companies, which have produced many negative consequences, either the damage of important data or massive economic loss. The main objective was to analyze the current implementations of network security protocols, making use of Cisco devices, to preserve the security, privacy, and integrity of the data, investigating the different problems present in the infrastructure and maintenance in networks, in addition to identifying the configuration in the devices and proposing a strategy that provides an acceptable solution that contributes significantly to connectivity. Finally, it was necessary to appropriate knowledge related to networks, for finding innovative solutions that contribute to the new era of development in the field of systems engineering.

Keywords: Technology; security; protocols; networks; Cisco.

Introducción

En Colombia, existen actualmente varias empresas y compañías que contribuyen constantemente a la economía del país; sin embargo, esto ha generado un incremento, en los últimos años, de los ataques cibernéticos, un ejemplo claro de este hecho es que, en el año 2021, hubo aproximadamente mil millones de intentos de ciberataques, que fueron confirmados por el empresa de ciberseguridad Fortiner; esto evidencia un aumento de malware en las redes, debido a la técnica de phishing, por lo cual, el 19 % de las empresas se han visto afectadas en estos últimos 12 meses (Semana, 2021a).

Por esta razón, se ha evidenciado la necesidad de una mejora en los protocolos y sistemas de seguridad en las redes, con base en una investigación profunda sobre los temas de este proyecto, así como también un seguimiento de las diferentes actividades de investigación que involucran datos continuos y discontinuos, para tener un mejor panorama de las circunstancias que vive el país en relación con su seguridad.

Por lo tanto, el objetivo de este proyecto es dar una solución o mitigar los posibles daños que pueden causar el robo o la modificación de la información de forma ilegal, por medio de la implementación de un protocolo de seguridad y haciendo uso de los diferentes dispositivos, con el fin de aportar un enfoque de defensa que se centre en las amenazas, y así evitar que se o se ponga en riesgo los recursos de la red; para ello, se tendrá en cuenta los flujos y configuraciones de un entorno empresarial.

En relación con los objetivos específicos de este proyecto, lo primero que se realizará es una revisión documental para identificar y conocer el funcionamiento a profundidad del manejo de las redes y las posibles soluciones usando dispositivos Cisco, también se analizará los distintos problemas de seguridad informática dirigidos hacia los activos de información en una red informática; se aplicará una configuración avanzada en las tecnologías Cisco para

mitigar los problemas de seguridad informática; finalmente, se propondrá una guía de buenas prácticas de seguridad basada en una implementación avanzada de las tecnologías Cisco.

En la primera fase se realiza la investigación de diferentes recursos, incluyendo la biblioteca de la universidad, el laboratorio de redes y otras fuentes confiables para el estudio de los dispositivos como módems, puentes, *switch*, routers, puntos de acceso inalámbricos y servidores. De igual manera, es necesario enfocarse en los conocimientos de los tipos de redes: LAN, WLAN, MAN WAN, entre otras, que ofrecen servicios a un servidor para transmitir y procesar datos.

En la segunda fase se realiza un análisis con base en la investigación de los casos y problemas ocurridos en las redes en la actualidad, además del uso del laboratorio de Alvernia para hacer las distintas prácticas de diagnóstico, con el fin de afrontar nuevos desafíos con ayuda del desarrollo tecnológico, además de brindar la información correcta en la implementación de mejora, para poder preservar la seguridad en redes y mantener la privacidad, integridad, disponibilidad, con el propósito evitar vulnerabilidades que se presentan en la red.

En la última fase, se desarrolla un informe con todo lo que se ha abordado; también se incluirá las posibles soluciones a la vulnerabilidad de la red; finalmente, se dará a conocer el análisis y los resultados.

Cabe señalar que, el trabajo hace parte del paradigma cuantitativo, empírico analítico, de tipo aplicado, debido a que el objetivo general del proyecto busca la implementación de un protocolo que garantice un alto porcentaje en la seguridad de las redes y su información privada y sensible por medio de dispositivos CISCO. Por lo tanto, se necesita una investigación que vaya desde el funcionamiento, las características, hasta las posibles vulnerabilidades de la red, con el propósito de buscar una solución que se base en los dispositivos de seguridad aplicados a una infraestructura, ya sea una corporación o una institución que maneje datos importantes.

Una vez se termine este proyecto, se espera complementar sobre temas que abarquen la seguridad a nivel municipal, departamental y nacional, de esta manera, contribuir con la nueva generación de la tecnología.

Planteamiento del problema

En Colombia, recientemente se han presentado cifras alarmantes en cuanto a ataques cibernéticos, con un número aproximado de 23.000 noticias sobre estos crímenes, que violan la integridad y seguridad de los datos (Semana, 2021b). Teniendo en cuenta que, durante estos dos últimos años, se presentó la problemática de la pandemia por el covid-19, que afectó a todos los países del mundo, tanto de forma social, económica, política como empresarial, se ha recurrido a la tecnología para emprender y administrar los negocios; por lo tanto, en estas situaciones, el uso y almacenamiento de datos y redes es de suma importancia, teniendo en cuenta las cifras de afectación por las vulnerabilidades en la red que pueden producir consecuencias negativas, por ejemplo, en Bogotá, ya se han registrado 8.355 casos de ataques cibernéticos; en Medellín, aproximadamente 1.664 casos, y en Cali, 1.569.

Por lo anterior, se evidencia la necesidad de una seguridad de calidad, donde se tenga en cuenta todas las formas de acceso a la red, ya que existen diferentes puntos críticos que los hackers aprovechan para encontrar vulnerabilidad en los dispositivos, un ejemplo es el rúter, que es el encargado de controlar el acceso, en otras palabras, es un elemento crítico del cual se necesita la asignación de una seguridad avanzada para reducir la posibilidad de un ataque infiltrado.

Por otra parte, se conoce que los switches son atacados, con la diferencia de que estos no dan acceso, pero su desventaja es que no se ha hecho pública la información sobre los riesgos de seguridad que pueden presentarse como también de las posibles soluciones en caso de un daño colateral.

En conclusión, la realización de este proyecto es importante porque puede ser una solución fiable para evitar las consecuencias de los constantes robos de información y vulnerabilidades que se presentan en la actualidad, es decir, la implementación de un protocolo de seguridad puede llegar a mitigar o minimizar los daños de un ataque a las redes ya sea virtual o físico.

¿Cómo se implementan protocolos de seguridad en redes informáticas, usando tecnología CISCO?

Actualmente, existen un conjunto de reglas y lineamientos que siguen los protocolos de seguridad, que están presentes entre dispositivos en las comunicaciones que se realizan por medio de una red; la función principal de estas normas es clasificar si los datos son rechazados o recibidos, pero la decisión depende de los posibles errores o ataques que puedan presentarse, por lo que existen diversos protocolos que son utilizados a nivel internacional para configurar y mantener el orden y la integridad de los datos que manejan. Algunos de los ejemplos de protocolos son los siguientes: internet protocol, transmission control protocol, internet control message, entre otros.

El impacto que podría traer el estudio de esta problemática a la comunidad académica, a las instituciones y a la sociedad es un aumento de seguridad en los datos privados y confidenciales, evitando la pérdida y desarrollando respaldos de seguridad, debido a los altos riesgos que se presentan en la actualidad. En este sentido, la implementación de un protocolo de seguridad es muy útil y necesaria actualmente, cuando estamos en medio de una constante evolución en relación con el software y hardware.

Fundamentación teórica

La idea y el objetivo principal planteados para este proyecto es analizar todo el proceso en la implementación de protocolos de seguridad para poder prevenir cualquier tipo de vulnerabilidad como virus, troyanos, sniffers y todo tipo de ataques maliciosos en las redes informáticas; para lograr esto, se utilizará la tecnología CISCO, con el fin de preservar la seguridad en redes y mantener la privacidad y un sistema seguro. La idea principal se la llevará a cabo mediante una revisión documental de los antecedentes, por ejemplo, cada día hay más ataques informáticos, se crean nuevos virus, aumentan los ciberdelincuentes; cada día la tecnología avanza más y también debe aumentar su seguridad. Por lo anterior, se utilizará la tecnología CISCO, ya que cuenta con protocolos avanzados de seguridad para poder prevenir cualquier tipo de ataque informático.

Una vez se haga la revisión documental, se procederá a caracterizar y conocer el funcionamiento a profundidad del manejo de las redes, sus protocolos para poder estar prevenidos ante cualquier tipo de ataque y saber identificar qué tipo de ataque informático es. También, se indagará acerca de los distintos problemas que se presentan en la infraestructura de las redes, por ejemplo, la gran cantidad de ataques a los bancos mundiales, qué tipo de virus utilizaron para poder vulnerar el sistema, ataques informáticos a grandes compañías como la Nasa para poder adquirir información confidencial, la innumerable cantidad de cuentas, tarjetas de crédito, páginas web, servidores web e información robada por ciberdelincuentes.

Ante eso, se busca posibles soluciones mediante CISCO, así, el proyecto se lo desollará a través del uso del laboratorio de Cisco de la Universidad Mariana y asesoría continua del profesional encargado de la administración del espacio de la universidad durante los últimos semestres para el desarrollo del proyecto.

Asimismo, se buscará ejemplos de protocolos de varias empresas que buscan una seguridad de calidad para evitar el robo o la configuración de información privada y sensible de su base de datos; también, se llevará a cabo un análisis en relación con los recursos que se van a utilizar, el tiempo, las fases, los procedimientos y posibles percances que pueden presentarse, con el fin de estar preparados para realizar un planteamiento del proyecto adecuado y permitir su correcto emprendimiento a lo largo del proceso.

Metodología

De acuerdo con todo el material de consulta, se observa la necesidad de la creación de una fuente de información confiable sobre el conocimiento de redes y estudio de infraestructura.

Primera fase

Esta fase se llevará a cabo por medio de la investigación, mediante el uso de espacios de la Universidad Mariana como la biblioteca, laboratorio de redes y otras fuentes de información confiables para el estudio de dispositivos de red: módems, puentes, switches, rúteres, puntos de acceso inalámbricos y servidores, con el objetivo de adquirir los conocimientos en el manejo de redes por medio de la tecnología CISCO para la implementación de protocolos, estándares con los se va a trabajar; los distintos tipos de topologías que existen en las networking que permiten definir la forma como están conectadas las PC y otros dispositivos, también es necesario conocer el tipo de red con la que se trabajará, que pueden ser las siguientes: LAN, W LAN, MAN, WAN, entre otras; además, cómo es una red punto a punto, redes cliente servidor y así realizar distintas pruebas en el desarrollo del proyecto; para la transmisión datos se hará uso de distintos cables o medios inalámbricos.

Además de incluir protocolos y modelos lógicos de red, se trata de conocer las actualizaciones de hardware de los distintos componentes de las redes, lo que es la instalación, la configuración de servidores, la solución de problemas, mantenimientos preventivos y todo el conocimiento sobre software con la que trabaja la tecnología CISCO.

Segunda fase

En esta fase se llevará a cabo el análisis de la información para observar la mejor metodología de implementación de protocolos de seguridad en las redes informáticas por medio de dispositivos CISCO. Todo esto se llevará a cabo con el estudio de casos y problemas ocurridos, además de contar con el apoyo de sitios oficiales de confianza que brindan información verídica; se hará uso del laboratorio de redes de la Universidad Mariana para la realización de pruebas prácticas con el fin de diagnosticar los distintos problemas a investigar, lo que permitirá afrontar nuevos desafíos con la ayuda del desarrollo tecnológico; de igual forma, se obtendrá información correcta en la implementación de mejora para poder preservar la seguridad en redes y mantener la privacidad, integridad y disponibilidad, con el propósito evitar las vulnerabilidades que se puedan presentar en la red.

Tercera fase

Una vez realizada toda la investigación y apropiación de todos los conocimientos necesarios en el área, se dará a conocer los problemas encontrados y las posibles soluciones para mitigar los problemas de seguridad informática, cómo se llevará a cabo por medio de una guía y un informe que abarque todas las buenas prácticas de seguridad basada en la configuración avanzada por medio de las tecnologías CISCO. Por último, se dará a conocer los diferentes análisis y resultados por medio de una presentación digital según el evento propuesto.

Discusión de resultados

El trabajo hace parte del paradigma cuantitativo, empírico analítico de tipo aplicado, esto se debe a que el objetivo general del proyecto busca la implementación de un protocolo que garantice un alto porcentaje en la seguridad de las redes y su información privada y sensible por medio de dispositivos CISCO, por lo cual se necesita una investigación que vaya desde el funcionamiento, las características hasta las posibles vulnerabilidades de la red, con el propósito de buscar una solución que se base en los dispositivos de seguridad aplicados a una infraestructura ya sea una corporación o una institución que maneje datos importantes.

En consecuencia, se desea desarrollar o implementar un protocolo seguro en la infraestructura de las redes para disminuir el riesgo de las posibles afectaciones cuando se presenta un virus o un hackeo de la información, por lo tanto, este proyecto puede ser considerado como una idea de innovación que busca un beneficio relacionado con las empresas o corporaciones que trabajan con datos sensibles.

- Generación de nuevos conocimientos avanzados en relación con la infraestructura y los protocolos en las redes.
- Fortalecimiento de saberes en cuanto a la tecnología y a la seguridad para evitar el robo de los datos.
- Aumento de conocimientos sobre las aplicaciones de la tecnología de las redes en Colombia, como también las posibles consecuencias al realizar un mal uso en estas o no tener un protocolo de seguridad establecido.
- Análisis de las características disponibles de configuración avanzada a la seguridad de los dispositivos Cisco, entre ellos: rúter, switches, para salvaguardar la comunicación en una networking de datos.
- Implementación de un protocolo de seguridad adecuado por medio de los diferentes dispositivos CISCO.

Conclusiones

En la actualidad se ha presentado un aumento en el porcentaje de ciberataques en el país, hecho que ha producido grandes pérdidas económicas en las empresas, por lo tanto, se resalta la importancia de implementar un protocolo de seguridad adecuado.

Con la apropiación de todos los conocimientos adquiridos en la investigación, además de analizar, plantear y buscar soluciones e implementar la innovación tecnológica en la nueva era de desarrollo, se logrará la formación de profesionales idóneos en el campo de la Ingeniería de Sistemas.

Se necesitan varias prácticas y pruebas para conseguir los resultados deseados, que permitan salvaguardar los datos y mitigar los posibles daños y pérdidas, aplicando un protocolo de seguridad con base en la tecnología Cisco.

Al analizar todas las posibles vulnerabilidades en los dispositivos de red, los hackers suelen utilizar las diferentes aberturas que presentan los switches y los routers para realizar los ataques y el ransomware.

Se implementarán protocolos de seguridad en redes para llevar una privacidad, integridad, autenticidad y disponibilidad en las redes que usen la tecnología CISCO.

Referencias

En el primer trimestre del 2021, Colombia tuvo 1.000 millones de intentos de ciberataques. (2021a, 21 de junio). *Semana*. https://www.semana.com/tecnologia/articulo/en-el-primer-trimestre-del-2021-colombia-tuvo-1000-millones-de-intentos-de-ciberataques/202157/

El año de los ciberataques en Colombia, estas son las alarmantes cifras. (2021b, 2 de julio). *Semana*. https://www.semana.com/economia/empresas/articulo/el-ano-de-los-ciberataques-en-colombia-estas-son-las-alarmantes-cifras/202125/