ISSN: 2773-7349

Sociedad & Tecnología

Revista del Instituto Tecnológico Superior Jubones

2021
Volumen / 4
Número / 2
Mayo / Agosto

Fecha de presentación: 29/01/2021, Fecha de Aceptación: 17/03/2021, Fecha de publicación: 1/05/2021

Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje

Effectiveness and efficiency of the security of LAN networks. Canton Pasaje

Nelly Victoria Ley Leyva[1]
E-mail: nley@utb.edu.ec
ORCID: https://orcid.org/0000-0003-2296-7354
Diana María Granda Ayabaca[2]
E-mail: dgranda@institutojubones.edu.ec
ORCID: https://orcid.org/0000-0001-7433-2225
Cristian Rafael Benítez Flores[2]
E-mail: cbenitez@institutojubones.edu.ec
ORCID: https://orcid.org/0000-0003-4109-0973
Verónica Jacqueline Guamán Gómez[2]
E-mail: vguaman@institutojubones.edu.ec
ORCID: https://orcid.org/0000-0001-9284-5040
[1]Departamento de idiomas de la Universidad Técnica de Babahoyo, Babahoyo, Ecuador.
[2]Instituto Tecnológico Superior Jubones, Pasaje, Ecuador

Cita sugerida (APA, séptima edición)

Ley Leyva, N. V., Granda Ayabaca, D. M., Benítez Flores, C. R. & Guamán Gómez, V. G. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. *Revista Sociedad & Tecnología*, 4(2), 205-222.

RESUMEN

Con el objetivo de analizar la efectividad y eficacia de la seguridad de las redes LAN brindadas por las empresas proveedoras de los servicios de internet del Cantón de Pasaje se desarrolló un estudio descriptivo sistematizado mediante los métodos de revisión bibliográfica, analítico-sintético, estadístico y triangulación de datos, así como por la técnica de encuesta. El instrumento de recogida de la información se aplicó a 18 directivos de empresas proveedoras de los servicios y a 1000 funcionarios de las entidades usuarias. Los principales resultados señalan que se cumple con las normas estatales establecidas, para lo cual se implementan los protocolos de la Agencia de Regulación y Control de Telecomunicaciones con el empleo del firewall de Mikrotik; los ataques a las LAN se producen con una frecuencia e impactos negativos medios, con un tiempo de recuperación entre 30 y 60 minutos, siendo el más recurrente el DDoS. Las empresas proveedoras no utilizan modelos de seguridad profunda más confiables como el de la Organización Internacional para Normalización. Se concluye que los sistemas de seguridad de las redes LAN utilizados en el Cantón Pasaje no son plenamente eficientes y eficaces.

Palabras claves:

eficacia, eficiencia, modelos de seguridad, LAN

ABSTRACT

In order to analyze the effectiveness and efficiency of the security of the LAN

networks provided by the companies that provide internet services in the Canton of Pasaje, a systematic descriptive study was developed through the methods of bibliographic, analytical-synthetic, statistical and triangulation review. Data, as well as by the survey technique. The information collection instrument was applied to 18 managers of service provider companies and 1,000 officials of user entities. The main results indicate that the established state standards are met, for which the protocols of the Telecommunications Regulation and Control Agency are implemented with the use of the Mikrotik firewall; Attacks on LANs occur with medium frequency and negative impacts, with a recovery time of between 30 and 60 minutes, the most common being DDoS. Provider companies do not use more reliable deep security models like the International Organization for Standardization. It is concluded that the security systems of the LAN networks used in the Pasaje Canton are not fully efficient and effective.

Key words:

efficacy, efficiency, security models, LAN

INTRODUCCIÓN

El avance científico y tecnológico experimentado desde mediados del pasado siglo XX han revolucionado las formas de actuación de la sociedad; como resultado de este desarrollo y de la convergencia de las tecnologìas de la telecomunicación y la informática nacen las redes de comunicación que, constituyen un hito del desarrollo humano, facilitando el intercambio de información en tiempo real desde cualquier parte de la geografía del orbe, propiciando el fenómeno de la globalización.

En este contexto, el mundo moderno precisa de una gestión de la información ágil, eficiente, eficaz y segura que, facilte la toma de decisiones (del Pino & Fernández, 2021). En este sentido las empresas depositan su confianza en las redes de comunicación; por lo que, las empresas proveedoras de los servicios de Internet deben garantizar la integridad de la información que fluye a través del intercambio de mensajes, datos, recursos, archivos, etc. entre computadoras interconectadas en una red de área local (LAN), para lo cual emplean modelos de seguridad.

Sin embargo, los ataques a estas redes ocurren con mucha frecuencia; cada año las empresas a nivel mundial reportan pérdidas millonarias por concepto de vulnerabilidad y fallos de seguridad (Muñoz & Rivas, 2015), falencias motivadas en gran medida por la falta de implmentación de modelos de defensa en profunidad, realidad que se agraba aún más, pues la tecnología de los sistemas de protección no se desarrollan a la par de los métodos para atacar las redes (Cisneros, 2017); cada vez son más los programas malignos creados; entre ellos, por solo citar algunos ejemplos, están los virus que afectan el sector de arranque (BOOT) y los archivos ejecutables o provocan el desbordamiento de la capacidad de respuesta de las redes; asimismo se encuentran los virus de macro, malware, gusanos, troynos, dialers, adwares, spyware, bacterias, bombas de tiempo y rootkits; muchos de ellos han sido diseñados para que tengan la capcidad de autopropagarse a través de las redes posiconándose en los sistemas operativos (Romero et al., 2018; Benítez et al., 2019).

Estos programas malignos junto a la incorrecta manipulación de la información por parte de los usuarios y de la no aplicación de sistema de seguridad profundos son aprovechados por los ciberdelicuentes para atacar las redes, frente a esta realidad las empresas proveedoras de los servicios de Intenet buscan altenartivas de aseguramiento de manera tal que las vulerabilidades sean prevenidas y en caso de producirse contrarrestarlas y disminuir el tiempo de recuperación, de esta forma se procura evitar el daño y pérdida de la información que, puede causar graves consecuencias

económicas a las empresas usuarias (Robayo López & Rodríguez Rodríguez, 2015; Guijarro Rodríguez et al., 2018).

Realidad no ajena a las empresas, instituciones y organismos del Cantón de Pasaje, pues a pesar de la existencia de información y protocolos para la seguridad de las redes de comunicación, aún se producen vulnerabilidades en las redes LAN, lo que se traduce en la práctica empresarial, institucional y organizacional en retraso en los servicios, demora a las demandas de los usuarios, incumpliendo de las obligaciones contractuales, pérdida de intenciones de negocios, etc. Situación que motivó el presente estudio con el objetivo de analizar la efectividad y eficacia de la seguridad a redes LAN brindadas por los proveedores de internet del cantón.

MARCO TEÓRICO REFERENCIAL

Antes de cualquier analisis es necesario logarar un acercamiento a la noción de redes LAN, mediante la respuesta a la siguiente pregunta: ¿Qué son las redes LAN?

Las redes LAN son consideradas eficientes recursos tecnológicos que permiten el intercambio de información entre equipos de cómputo interconectados entre sí: son un conjunto de dispositivos interconectados que ocupa un lugar físico, como una oficina de una empresa o una habitación en el hogar; estas pueden ser grandes o pequeñas, y puede ir desde la conexión de un usuario a la red doméstica hasta miles que estén conectados a la red de una empresa, institución, organismo o corporación (Jamieson & Low, 1990).

Las LAN están divididas en cinco áreas principales de aplicación; informática distribuida, sistemas de oficina, redes de terminales, sistemas de fábrica y micro redes; son redes privadas de acceso múltiple y de alta velocidad, que transfieren millones de bits/s mucho mejor que los sistemas ordinarios de comunicación (Olifer & Olifer, 2009), lo que las convierte en un poderoso instrumento de trabajo en el ámbito empresarial; pero al estar conectadas a la Internet existe el potencial peligro de sufrir ataques cibernéticos por parte de delincuentes con diferentes propósitos: tener acceso a información, robar datos, introducir diferentes tipos de malware a los equipos, dañar los sistemas, interrumpir u obstaculizar el funcionamiento de la red, etc. (Wright & Harmening, 2009; Moya, 2017).

Estos riegos que acarrea la interconexión de las redes de comunicación, deben ser asumidos con responsabilidad por las empresas, pues la gestión empresarial requiere de esos recursos tecnológicos para lograr el éxito y la permanencia en el mercado.

Por lo que, para lograr la seguridad de las redes LAN hay que tener presente el control y las medidas de seguridad, aspectos que deben ser tenido en consideración desde la propia planificación y creación de la red.

Planificación adecuada de la red

La planificación y creación de una red dependerá de las necesidades de la organización o empresa y se deberán tener en cuenta ciertos factores como la topología, el hardware, el software y el método de transmisión de la red en función a los servicios y actividades internas que realiza para la gestión del proyecto organizacional o empresarial. En este sentido es fundamental contar con el apoyo de la gerencia del proyecto, que es la que demanda los servicios (CISCO, 2007).

Además, durante esta etapa de planificación se debe elegir al personal encargado de la asesoría de seguridad. Este personal puede ser consultores de red, así como oficiales de seguridad y auditoría; así como diseñar el nivel de servicios de los usuarios de dicha red (Baluja García & Anías Calderón, 2006).

Nivel de servicio

El nivel de servicio comprende los permisos de usuario en la red LAN; estos tienen como propósito evitar problemas de pérdida de

datos, otorgando distintos permisos según el nivel de acceso a los servicios de cada usuario. Asimismo, un aspecto necesario a considerar dentro del nivel de servicios de usuarios de la red es el mantenimiento periódico a dichos permisos para mantenerlos al día junto a las claves de cada usuario. De igual forma, es importante considerar software, hardware y servicio de seguridad, que formarán parte de la red.

Software de red

La calidad del software de red repercute en la funcionalidad, las fallas, la instalación correcta y modificación del mismo, elementos inherentes a la seguridad de los servicios que presta, de ahí la imperiosa necesidad de elegir el software según los requerimientos de la organización (Cornelius et al., 2018).

Hardware de red

Otro elemento de suma importancia, si de seguridad de la red se trata, es la calidad del hardware de red, este repercute en la compatibilidad, falla del equipo de red, confiabilidad y respaldo de información del mismo. En la selección del hardware se ha de tener en consideración la compatibilidad con el estándar LAN y la planta de cable seleccionado; además, se debe tomar en cuenta ciertas especificaciones como el rendimiento máximo más bajo que el previsto (Tarek et al., 2017).

Para lograr un buen servicio de seguridad de la LAN se deben considerar tres aspectos: control de acceso, confiabilidad o privacidad y conexiones externas.

Control de acceso

El control de acceso se realiza mediante un grupo de tecnologías que, implementa una infraestructura de red para cumplir con las políticas de seguridad, para así solucionar los problemas ocurridos en las empresas y proteger a todos los dispositivos conectados a dicha red que, pueden ser afectados, de esta forma se evita o limita el posible daño causado por las amenazas contra la seguridad de la misma (Salles & Carvalh, 2015).

Confidencialidad o privacidad

Para garantizar la confidencialidad o privacidad en una red se debe implementar una tecnología de red que permita una conexión segura de una red LAN sobre una red pública, mediante una red privada virtual (Da et el., 2014).

Conexiones externas

Las conexiones externas se realizan a través de una red de área amplia denominada WAN (*Wide Area Network)* que comunica dos o más redes LAN mediante una conexión remota que implemente protocolos como TELNET o SSH, lo que acarrea un menor rendimiento en la transmisión de datos por las largas distancias entre el servidor y el punto de sesión (Kenneth et al., 2015). De todos estos elementos dependerá en gran medida la integridad de los datos.

Integridad de datos

Como ya hemos mencionado los servicios de seguridad de una red incluyen la protección de la información ante los posibles accesos no autorizados (Jamieson & Low, 1990). Este servicio es conocido como integridad de datos, o sea asegurar que los valores correspondientes a cada dato no sean modificados de manera errónea; para lo cual el sistema debe proteger el acceso y gestión de los mismos por parte de individuos no autorizados, evitando que modifiquen o eliminen los valores de manera malintencionada (Olifer & Olifer, 2009).

El análisis de la integridad de datos en una red se puede orientar a través de dos enfoques: conexión e integridad. El enfoque de conexión alude a la garantía del recibo de los mensajes y paquetes tal y como fueron enviados, aspecto que abarca las interrupciones de servicio; mientras que, el enfoque de integridad sin conexión garantiza únicamente mensajes individuales protegiéndolos de las posibles modificaciones (Olifer & Olifer, 2009); para alcanzar esta integridad de los datos existen diversos recursos tecnológicos.

Recursos tecnológicos para la protección de las LAN

Los ciberataques a las redes LAN en gran medida son el resultado de una mala gestión de protección de las conexiones con redes exógenas como Internet; luego para la protección de las redes LAN es necesario que las empresas y organismos a la hora de contratar los servicios de Internet, que brindan las empresas proveedoras. Deben tener presente aspectos tales como:

1) Los protocolos de seguridad específicos: WPA, WPA2o y WPA3 que permiten el tráfico de Internet solo bajo el cifrado de contraseñas (González Paz et al., 2016).

2) Los mecanismos de seguridad: SSH, HTTPS y SSL que sirven para asegurar la comunicación a través del acceso web entre servidor y cliente, utiliza la autentificación que facilita que mediante un plugin para Firefox se puedan monitorear los datos transferidos entre servidores web y clientes. El protocolo Secure Shell (SSH) posibilita el acceso a equipos remotos empleando el cifrado a través de un canal SSH, de esta forma un hacker no puede detectar el usuario y contraseña, ni nada que se escriba durante el proceso de conexión al servidor (González Paz et al., 2016).

3) El servicio de autenticación orientado a prevenir el acceso a los datos a usuarios no autorizados, evitando el uso de los mismos para ataques o modificaciones malintencionadas. Un método común y con gran aplicación es el método de autenticación mediante firma digital (Olifer & Olifer, 2009).

   Al igual que en cualquier sistema de seguridad, la autenticación consiste en garantizar que el acceso de los verdaderos usuarios de la red; se trata de asegurar que el host receptor sea el correcto, y que el host que emite el mensaje sea válido. El proceso se basa en dos aspectos, 1) asegurar que las entidades sean auténticas durante la conexión, y 2) la conexión no sea interferida por un tercero. Para ello se definen dos tipos de autentificación: 1) autentificación de entidades, que asegura que los hosts de origen y de destino sean correctos, para posteriormente establecer la conexión y 2) autentificación del origen de los datos, que consiste en asegurar la fuente de origen de un paquete o dato enviado.

4) Access Control Lists (ACL). Este recurso permite establecer una lista de permisos a usuarios y grupos de ellos para acceder a FTP, Internet, etc. Asimismo, facilita la definición del ancho de banda y horarios.

5) El empleo de un sistema o mecanismo de seguridad como el *firewall.* Este dispositivo de seguridad permite el monitoreo del tráfico entrante y saliente de la red. Este mecanismo es quien permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad (Cornelius et al., 2018).

   No obstante, a la innegable importancia que tiene el *firewall* dentro de una red de computadoras, Tarek et al. (2017) alertan sobre las configuraciones incorrectas del *firewall* que pueden causar graves infracciones de seguridad y hacer vulnerable la red, por lo que, se debe tener mucho cuidado con el sistema a implementar.

6) Spiceworks, software que permite el monitoreo de la red desde un panel de control desde cualquier lugar y en tiempo real (Magoni, 2018).

7) Tecnologías de "túnel" como VPN (González Paz et al., 2016).

8) EventSentry es un software que permite el monitoreo de cualquier dispositivo SNMP (ruters, servidores de Linux, interruptores que usan SNMP (Magoni, 2018).

9) PRTG Network Monitor, este software de forma asequible y fácil monitorea todos los elementos de una infraestructura de red, servidores,

sitios web, aplicaciones, etc. Esta herramienta evalúa el estado y último acceso de cualquiera de los dispositivos conectados en tiempo real (Magoni, 2018).

Modelos de seguridad

En la actualidad existe una tendencia a la implementación de modelos de seguridad que integran varios de estos recursos para un control efectivo y eficaz de la red y así lograr altos estándares de seguridad. Entre estos modelos se encuentran el de Fortinet, compañía pionera en integrar varias funciones juntas en una sola plataforma, la *Unified Threat Management* (UTM), incluyendo firewall, VPN, control de aplicaciones, prevención de intrusos y filtrado web, ofreciendo protección total de contenidos (Kenneth et al., 2015).

De igual forma, está el modelo de la Organización Internacional para Normalización (OSI) estructurada en capas: física, enlace de datos, de red, de transporte, de sesión, de presentación y de aplicación. Este sistema por capas busca la seguridad de la información, mediante el control de los datos, cada capa cumple la función de analizar y remover la información de control de dichos datos, protegiéndolos y preservando su integridad (Bejarano, 2017; Moya, 2017); este proceso se produce en las capas pares del sistema instalado en los equipos emisores y receptores; proceso que requiere de una verificación por parte del cliente que emite una solicitud, y por parte del servidor que responde a la misma; a nivel de enlace de datos cuando dos dispositivos establecen una sesión de comunicación (Olifer & Olifer, 2009).

Políticas de seguridad

A pesar de que las redes LAN presentan un menor rango de problemas de seguridad que las redes inalámbricas, por el simple hecho de ser estructuras de datos cableadas; existen algunos ataques o inconvenientes, como ya se apuntó anteriormente, que los administradores de red deben considerar posibles y en consecuencia implementar mecanismos y políticas que permitan contrarrestar estos problemas de seguridad (Baluja-García & Anías- Calderón, 2006).

En tal sentido CISCO (2007), propone como buena práctica para la implementación de políticas de seguridad las etapas de preparación, prevención y respuesta.

Etapa de preparación. Dentro de esta etapa se implementan tres actividades previas a la creación de las políticas de seguridad, analizando el entorno y los riesgos que se presentan: 1) declarar las políticas de uso en donde se describan las responsabilidades y roles que interpretarán cada uno de los usuarios; 2) realizar un análisis de los posibles riesgos que se pueden presentar en la red que afecten a los recursos y a los datos; 3) establecer una estructura de equipo de seguridad.

Etapa de prevención. Esta etapa contempla dos actividades fundamentales: 1) la implementación de cambios en la seguridad de los equipos de red, y 2) el monitoreo de la seguridad en la red, determinando las violaciones de seguridad.

Etapa de respuesta**.** Durante esta etapa se realizan las siguientes acciones: 1) detección de la vulneración de seguridad de la red, 2) implementación de métodos de seguridad, 3) una vez que se detecta la violación se ejecuta la restauración de las operaciones, de manera que se pueda asegurar la disponibilidad de la red, y 4) revisión de lo implementado y se asegura que la política de seguridad se mantenga.

Siguiendo este orden de ideas, Baluja-García y Anías-Calderón (2006), estiman como elemento importante los mecanismos de los administradores de las redes para cumplir las políticas de seguridad establecidas, como lo son: 1) los cortafuegos, garantizando una zona confiable para la transmisión de datos resguardado por servidores proxy; 2) los monitores de seguridad también conocidos como detectores de vulnerabilidad de la red, que son empleados con el propósito de

verificar si los dispositivos de la red son vulnerables o no, similares a los sistemas de detección y de prevención de intrusiones (IDS/IPS), las cuales se enfocan en la detección y prevención de los intentos de intrusión en una red, o en una zona de la red; 3) la encriptación para proteger la confidencialidad, integridad y autenticidad de la información y 4) los sistemas antivirus para la eliminación de programas malignos que pueden terminar en robo de información.

Por último, para hablar de eficiencia y eficacia de la seguridad de los servicios de la LAN es necesario referirse a las métricas de rendimiento.

Métricas de rendimiento

Entre los procesos esenciales para mantener una buena operatividad en la red se presentan el monitoreo, y la verificación del desempeño de la misma, verificando el estado de los servicios que ofrece la red. Cuando se analiza el rendimiento, se evalúan indicadores como la latencia de paquetes, el tiempo de respuesta y el cifrado de sobrecarga que se efectúa en la red (Tarek et al., 2017).

En esta misma línea de análisis, Linero et al. (2015), en su investigación consideran el rendimiento de una red como el tráfico de red que, ha de estar en correspondencia al tamaño de carga útil expresada en bytes; es decir, se analiza la cantidad de información que es posible enviar en un determinado periodo de tiempo. En base a lo mencionado, se pueden definir dos métricas relevantes para evaluar el rendimiento de la red y los servicios que esta presta; el tiempo de respuesta y la disponibilidad a la medida.

El tiempo de respuesta es el lapso que se requiere para poder enviar tramas de datos de un origen a un destino; consiste en la suma del tiempo máximo de espera en la capa física y la capa MAC. Según CISCO (2007) es importante medir el tiempo de respuesta de usuario/aplicación, ya que para muchos usuarios esto es considerado como un factor de éxito en cuanto a la eficiencia del rendimiento de la red que se encuentra brindándole servicios. Se puede definir al tiempo de respuesta como el tiempo que se necesita para que los paquetes viajen de un punto a otro.

La disponibilidad de la medida es considerada como el tiempo en el cual una red o servicio se encuentra disponible para que el usuario pueda acceder a ella; pero, al hablar de una red de datos, la disponibilidad de la medida hace referencia a la confiabilidad de los componentes individuales que se emplean dentro de la topología de la red. Dentro de esta métrica se considera la redundancia de red, ya que es un factor que ayuda a evitar la degradación del servicio.

Como mencionan Da et al. (2014) y Kenneth et al., (2015), con respecto a la seguridad, la detección de URL maliciosas es una tarea esencial en la inteligencia de seguridad de la red y para ello Fortinet destaca aspectos fundamentales como mayor seguridad para contrarrestar las amenazas más desarrolladas, mayor control y mayor inteligencia con ajustes automáticos de políticas basadas en roles para usuarios e invitados en función de su ubicación y perfil de aplicación.

MATERIALES Y MÉTODOS

Para dar cumplimiento al objetivo del estudio se desarrolló una investigación descriptiva con enfoque cuantitativo, sustentada en los métodos revisión bibliográfica, analítico-sintético, estadístico y triangulación de datos, así como en la técnica de encuesta.

A través de la literatura especializada en el tema se realizó la fundamentación teórica del estudio y argumentación de los resultados. El método analítico-sintético facilitó el desglose de la información sobre el objeto de estudio para su análisis por partes y su posterior integración y resumen, lo que permitió la comprensión de los procedimientos de seguridad brindados por las empresas proveedoras e identificación de vulnerabilidades que se

generan en las organizaciones e instituciones.

Mediante el método estadístico se planificó, recolectó, proceso y analizó la información de carácter cuantitativo para medir el nivel de eficacia y eficiencia de la implementación de los sistemas de seguridad en una LAN recolectada a través de la encuesta aplicada a las empresas proveedoras y usuarias de servicios de internet en el Cantón Pasaje. Los datos así obtenidos se resumieron en frecuencias absolutas y relativas, y representados en tablas y gráficos estadísticos.

El mismo instrumento fue aplicado a las empresas proveedoras y usuarias de los servicios de Internet, lo que facilitó la triangulación de los datos y la disminución del sesgo de la información.

El cuestionario aplicado como instrumento para la recolección de la información sobre la seguridad de las redes LAN contó con indicadores cuantificables para medir los índices eficiencia y eficacia que en ese sentido brindan las empresas proveedoras de servicios de Internet.

Partiendo de la conceptualización de la eficacia como los resultados obtenidos en relación con el objetivo propuesto o grado en que el servicio brindado puede lograr el mejor resultado posible (Otero 2001); que en nuestro caso es la seguridad de la red LAN; y entendida la eficiencia en relación con el uso racional de los recursos para alcanzar ese propósito (Jiménez, 2004); o sea, lograr la máxima seguridad de la red tanto en el orden cualitativo como cuantitativo se confeccionó el instrumento para medir la eficacia y la eficiencia.

El instrumento contó con un total de 11 preguntas, de ellas 8 cerradas con escalas linker y 3 abiertas. Las preguntas abiertas permitieron caracterizar la gestión de seguridad de la red en cuanto a tipo de ataque más frecuente, software utilizados para controlar o contrarrestar los ataques y tiempo de recuperación; mientras que las cerradas estuvieron direccionadas a determinar el nivel de eficacia y eficiencia de esta gestión.

La eficacia es operacionalizada a través de los indicadores; frecuencia de ataques a la red, impacto generado por estos ataques y, grado de control y respuesta a los ataques, para lo cual se utilizó una escala de alto, medio, bajo, nunca.

Mientras que la eficiencia fue medida mediante los indicadores: normas de seguridad, uso de hardware, empleo de software, atención a las necesidades de los usuarios y tiempo de respuesta, para lo cual se empleó una escala de malo, regular, bueno, muy bien y excelente.

La elaboración de los instrumentos se realizó siguiendo la metodología propuesta por Hernández (2014), que cuenta con los siguientes pasos:

1) Análisis de instrumentos similares aplicados en otras investigaciones.

2) Evaluación de la validez y contextualización del instrumento.

3) Elaboración de la escala para medir las respuestas de las preguntas.

4) Elaboración de la primera versión de los instrumentos.

5) Validación a través de especialistas. (Talleres de socialización).

6) Puesta a punto del instrumento.

8) Prueba piloto.

9) Elaboración de la versión final de los instrumentos.

Una vez confeccionado fue validado a través da talleres de socialización, según metodología de Rué (2018). Se llevaron a cabo dos sesiones con la participación de tres especialistas en el área de seguridad tecnológica y dos docentes de alta cualificación y experiencia en el tema. Los aspectos valorados fueron:

1) Concreción en la práctica de los referentes teóricos sobre la eficiencia y eficacia de seguridad de las redes.
2) Estructura y coherencia de las preguntas en correspondencia con el objeto de análisis.

3) Adecuación de la escala según las preguntas.
4) Concepción metodológica y técnica para facilitar la recolección de la información.
5) Efectividad del instrumento para medir la eficacia y eficiencia de la seguridad de las redes LAN del cantón Pasaje.

Las sugerencias y recomendaciones dadas por los espacialitas permitieron perfeccionar el instrumento. Además, se aplicó el coeficiente Alfa de Cronbach para estimar la confiabilidad de consistencia interna del instrumento, resultando los valores siguientes:

Cuadro 1. Confiabilidad del instrumento

Preguntas	**Categoría**	**Coeficiente Alfa de Cronbach**
Cerradas	Eficacia	0.933
	Eficiencia	0.936
Abiertas		0,932

Población y muestra

La población estuvo constituida por los directivos de las 51 empresas proveedoras de servicios de Internet y de las 3580 entidades usuarias de esas prestaciones, ubicadas en el Cantón Pasaje de la Provincia de El Oro. El tamaño de la muestra fue calculado con el empleo de la fórmula: $n=N\ \sigma^2Z_\sigma^2/(e^2(N-1) + \sigma^2Z_\sigma^2)$.

Dónde: n: tamaño de la muestra; N= tamaño de la población; Z=constante correspondiente al nivel de confianza (1,96); e=error muestral (0.05) y σ= desviación estándar de la población. En el caso de las empresas proveedoras de los servicios de Internet σ=0.12 y para las entidades usuarios σ= 0.95.

De esta forma la muestra quedó formada por 18 directivos de las empresas proveedoras y 1000 de las entidades usuarias; la selección se realizó a través del muestreo aleatorio.

RESULTADOS

Los resultados obtenidos en las encuestas a las diferentes empresas proveedoras y usuarias de servicio de internet en el Cantón Pasaje se resumen en las siguientes tablas.

3.1. Resultados de la encuesta aplicada a los directivos de las empresas proveedoras de los servicios de Internet en el Cantón Pasaje

La **tabla 1** recoge de manera sintética los resultados de la encuesta aplicada a los directivos de las empresas proveedoras de los servicios de Internet, referentes a la eficiencia de la gestión de seguridad de la LAN.

Tabla1. Resultados de la encuesta a las empresas proveedoras de los servicios de Internet sobre la eficiencia de la seguridad de las LAN del Cantón Pasaje

Preguntas	M	%	R	%	B	%	MB	%	E	%
1. ¿Qué tan eficientes son las normas de seguridad impuesta por el Estado?	0	0	0	0	0	0	12	66.7	6	33,3
2. ¿Qué tan eficiente es el sistema de seguridad implementado en cuanto a hardware?	0	0	0	0	9	50,0	9	50.0	0	0
3. ¿Qué tan eficiente es el sistema de seguridad implementado en cuanto a software?	0	0	0	0	15	83,3	3	16,7	0	0
4.¿Cómo es la atención a las necesidades de los usuarios?	0	0	0	0	15	83,3	3	16,7	0	0
5. ¿Cómo es el tiempo de respuesta a los usuarios?	0	0	0	0	15	83,3	3	16,7	0	0

Leyenda: M: Malo; R: Regular; B: Bien; MB: Muy Bien; E: Excelente
Fuente: Encuesta a directivos de las empresas proveedoras de los servicios de Internet

Análisis estadístico

El 100% de los encuestados valora entre Muy Bien y Excelente la eficiencia de las normas impuestas por el Estado, las que son cumplidas a través del empleo del protocolo de seguridad de la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL).

Respecto a qué tan eficiente es el sistema de seguridad implementado en cuanto a hardware; el 100% de los encuestados de forma tácita confirman tener implementado un sistema de este tipo al ser considerado como Muy Bueno o Bueno por el 50% respectivamente.

De igual forma el 100% de las empresas tienen implementado un sistema de software y su nivel de eficiencia fue evaluado de Bueno por el 83,3% de los encuestados, de Muy Buena por el 16,7%.

Por otra parte, el 83,3% estima de Buna la atención a las necesidades de los usuarios y de igual forma evalúan el tiempo de respuesta.

En la siguiente **tabla 2** se resume la información brindada sobre la eficacia de la gestión de seguridad de la LAN brindada por las empresas proveedoras de servicios de Internet.

Tabla 2. Resultados de la encuesta a las empresas proveedoras de los servicios de Internet sobre la eficacia de la seguridad de las LAN del Cantón Pasaje

Preguntas	Alta	%	Media	%	Baja	%	Nunca	%
6. ¿Con que frecuencia se producen los ataques a la red local?	0	0	15	83,3	3	16.7	0	0
7. ¿Cuál fue el impacto generado por el ataque a la red local?	0	0	12	66,6	6	33.3	0	0
8. ¿Con qué grado de eficacia se puede controlar o contrarrestar este tipo de ataques en una posible implementación dentro del Cantón de Pasaje?	3	16.7	15	83,3	0	0.0	0	0

Fuente: Encuesta a directivos de las empresas proveedoras de los servicios de Internet

Análisis estadístico

Los datos de la tabla 2 desvelan que el 100% de las empresas han sufrido algún tipo de ataque a la red local, que es considerado con una frecuencia media por el 83,3% de los encuestados. Asimismo, el 66,6% de los directivos estima que el impacto generado por esos ataques ha sio medio; lo que evidencia la existencia de "huecos en la red", aunque estos no sean considrados de un nivel alto.

De igual forma, el 83,3% de los encuestados considera que estos ataques pueden ser controlados o contrarrestados desde el cantón con un nivel de eficacia media, sólo uno considera puede ser alto.

Por último, se analizan los resultados de las preguntas abiertas a las empresas proveedoras de los servicios de Internet sobre la seguridad de las LAN del Cantón Pasaje.

Pregunta 9. ¿Cuál es el sistema de seguridad que utilizan?

Análisis estadístico

Al cuestionar a los directivos de las empresas sobre. ¿cuál es el sistema de seguridad que utilizan? estos declararon que el 100% de los proveedores de Internet usan el Firewall de Mikrotik debido a su flexibilidad en su configuración; además, porque las funciones de estas empresas se rigen bajo las normativas impuestas por la Agencia de Regulación y Control de Telecomunicaciones.

Pregunta 10. ¿Qué tiempo de recuperación se requiere después de un ataque a la LAN?

Análisis estadístico

El **gráfico 1** brinda información sobre el tiempo de recuperación después de un ataque a la LAN.

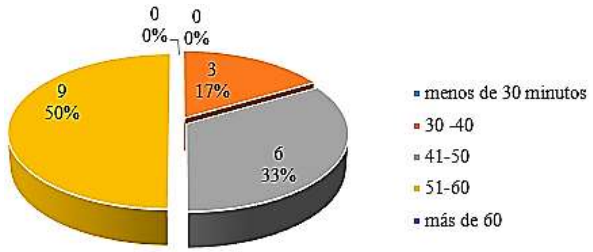

Gráfico 1. Tiempo de respuesta a los ataques a la LAN
Fuente: Encuesta a directivos de las empresas proveedoras de los servicios de Internet

Los datos del gráfico 1 revelan que el tiempo de recuperación después de un ataque cibernético a la red se encuentra entre 30 a 60 minutos; se significa que un 50% de los encuestados estima que se requiere entre 51 a 60 minutos, lo que debe ser tomado en consideración, para disminuir el tiempo, pues en este lapso obstaculiza los servicios que demandan los usuarios, lo que puede ocasionar graves problemas en la gestión de las empresas.

Pregunta 11. ¿Cuál es el ataque más frecuente a la red?

Análisis estadístico

El 100% de los encuestados coincidieron en considerar que el ataque más común hacia la red es el tipo DDoS, cuyo fin es sobrecargar la capacidad del servidor ocasionando que las respuestas a las solicitudes de los usuarios sean más lentas o que simplemente no sean atendidas, lo cual genera un retraso en los servicios que se brindan.

3.2. Resultados de la encuesta aplicada a los directivos de las empresas usuarias de los servicios de Internet en el Cantón Pasaje

En la **tabla 3** se resume cuantificada la información brindada por los directivos de las empresas usuarias sobre la eficiencia de la gestión de seguridad de la LAN por parte de la empresa proveedora.

Tabla 3. Resultados de la encuesta a las empresas usuarias de los servicios de Internet sobre la eficiencia de la seguridad de las LAN del Cantón Pasaje

Preguntas	M	%	R	%	B	%	MB	%	E	%
1. ¿Qué tan eficientes son las normas de seguridad impuesta por el Estado?	0	0	0	0	252	25,2	748	74.8	0	0
2. ¿Qué tan eficiente es el sistema de seguridad implementado en cuanto a hardware?	0	0	0	0	285	28,5	632	63,2	83	8,3
3. ¿Qué tan eficiente es el sistema de seguridad implementado en cuanto a software?	0	0	29	2,9	651	65,1	320	32.0	0	0.0
4.¿Cómo es la atención a las necesidades de los usuarios?	0	0	0	0	734	73,4	266	26,6	0	0.0
5. ¿Cómo es el tiempo de respuesta a los usuarios?	0	0	32	3,2	588	58,8	380	38,0	0	0.0

Leyenda: M: Malo; R: Regular; B: Bien; MB: Muy Bien; E: Excelente
Fuente: Encuesta a directivos de las empresas usuarias de los servicios de Internet

Análisis estadístico

El 74,5% de los encuestados valora de Muy Bien y el resto de Bien la eficiencia de las normas implementadas por el Estado, para lo cual emplean el protocolo establecido por la Agencia de Regulación y Control de Telecomunicaciones (ARCOTEL).

Sobre la eficiencia del sistema de seguridad implementado en cuanto a hardware; los directivos de las empresas usuarias lo consideran entre Buena y Excelente. Sin embargo, en relación con el software evalúan este nivel de eficiencia entre Regular y Muy Bueno, con predominio del criterio de Bueno (65,1%).

El 73,4% estima que la atención a sus necesidades como usuarios es Buena y el 26,6% la considera Muy Buena; sin embargo, 32 entidades clientes son del criterio que el tiempo de respuesta a los usuarios es Regular.

En la siguiente **tabla 4** se resume la información brindada por los directivos de las empresas usuarias sobre la eficacia de la gestión de seguridad de la LAN brindada por las empresas proveedoras.

Tabla 4. Resultados de la encuesta a las empresas usuarias de los servicios de Internet sobre la eficacia de la seguridad de las LAN del Cantón Pasaje

Preguntas	Alta	%	Media	%	Baja	%	Nunca	%
6. ¿Con qué frecuencia se producen los ataques a la red local?	0	0	1000	100	0	0	0	0
7. ¿Cuál fue el impacto generado por el ataque a la red local?	85	8,5	884	88,4	31	3,1	0	0,0
8. ¿Con qué grado de eficacia se puede controlar o contrarrestar este tipo de ataque en una posible implementación dentro del Cantón de Pasaje?	0	0	891	89.1	109	10.9	0	0,0

Fuente: Encuesta a directivos de las empresas usuarias de los servicios de Internet

Análisis estadístico

Al analizar los datos de la tabla 5 se evicencia que el 100% de las empresas de la muestra que cuentan con los servicios de Internet han sufrido algún tipo de ataque a LAN; estiman que estos se producen con uma frecuencia media y la mayoría estima que el impacto que generan es medio; aunque 85 clientes lo considreran de alto y 31 de bajo.

Estos datos también develan que el 89,1% de los directivos de las empresas y

organismos encuestados son de la opinión que el nivel de eficacia de las acciones que se pueden acometer desde el municipo para controlar y contrarrestar el impacto generado puede ser medio.

A continuación se analizan los resultados de las preguntas abiertas a las empresas usuarias de los servicios de Internet sobre la seguridad de las LAN del Cantón Pasaje.

Pregunta 9. ¿Cuál es el sistema de seguridad que utilizan?

Análisis estadístico

El 100% de los clientes declaran que el sistema de seguridad utilizado por las empresas proveedoras es el Firewall de Mikrotik, lo que coincide con la información obtenida de estas últimas.

Pregunta 10. ¿Qué tiempo de recuperación se requiere después de un ataque a la LAN?

Análisis estadístico

De igual forma el 100% de los encuestados consideran que el tiempo de respuesta está entre los 30 a 60 minutos.

Pregunta 11. ¿Cuál es el ataque más frecuente a la red?

Análisis estadístico

También, en esta respuesta el 100% declara que el ataque más frecuente es el DDoS, lo que dificulta las operaciones de la empresa al desbordar la capacidad del servidor.

DISCUSIÓN DE LOS RESULTADOS

Al triangular los datos obtenidos de las encuestas aplicadas a los directivos de las empresas proveedoras y usuarias se evidencia que en sentido general existe correspondencia entre los criterios, pudiéndose determinar que:

Las empresas proveedoras de servicios de Internet cumplen las regulaciones y normas establecidas por el Estado para la seguridad de las LAN del cantón. Los sistemas de seguridad se estructuran sobre la utilización de un firewall como principal medida de control de posibles amenazas. Estas empresas se rigen por los protocolos de ARCOTEL, este organismo dictamina que deben cumplir con un plan de seguridad y un plan de contingencia en cuanto a los servicios ofrecidos; sin embargo, no establece los mecanismos que se deben utilizar para cumplir dicha ordenanza; por tal razón las empresas que proveen el servicio de Internet tienen la flexibilidad de configurar o usar un sistema de seguridad según sus criterios sobre los que son más adecuado, así como establecer métodos de seguridad en conjunto con el usuario o empresa que recibe el servicio.

Mediante el análisis de la información extraída de las empresas encuestadas se determinó que el firewall de Mikrotik es el más utilizado por su flexibilidad en su configuración, aunque no es el de más fácil administración; en tal sentido Da et al. (2014) y Kenneth et al. (2015) consideran que existen otros sistemas que deben ser explorados como es el firewall de Fortinet que ofrece una mejor capacidad de administración por permitir la visualización del funcionamiento de los dispositivos de red en tiempo real.

Al respecto existen investigaciones como la de Kenneth et al. (2015), quienes estiman que en el tema de seguridad de redes debe tenerse presente los modelos de seguridad como el de la propia compañía Fortinet estructurado en la plataforma *Unified Threat Management* soportada en el sistema operativo FortiOS.

De igual forma los estudios de Olifer y Olifer (2009), Bejarano (2017) y Moya (2017) abundan sobre las bondades del modelo de la OSI estructurado en capas de alto estándar de seguridad e integridad de los datos. Este modelo permite que la información transferida desde una computadora hacia otra sea filtrada por cada una de las capas en ambos dispositivos; este intercambio de información ocurre entre capas OSI pares, de forma tal que cada una de las capas del sistema fuente u origen añade información de control al dato, y cada una de las capas del sistema receptor (destino) examina,

analiza y remueve la información de control del dato en cuestión.

Por otro lado, los datos sobre el nivel de eficiencia demuestran que aún existen huecos en la red a través de los cuales se producen ataques informáticos que vulneran la integridad de los datos; además, existe la potencial amenaza de daños a los software y hardware hardware del sistema mediante la introducción de virus, troyanos, gusanos, etc. Resultados que se corresponden con los estudios de Wright y Harmening (2009), Bejerano (2017) y Moya (2017) quienes aluden a los riesgos más frecuentes de un sistema de seguridad vulnerable. Particularmente Bejerano (2017) enfatiza en los llamados "huecos de la red" a través de los cuales se puede robar, dañar o borrar la información; así como en las infecciones producidas por virus que pueden causar daños en los sistemas operativos, archivos y aplicaciones, así como en los equipos de cómputo o partes de estos.

Asimismo, la información evidencia que a pesar que no existen serias dificultades en cuanto a la atención a las necesidades de los usuarios, si se produce demora en el tiempo de respuestas, lo que ocasiona retraso en el cumplimiento de las obligaciones contractuales y pérdida de oportunidades en la gestión empresarial u organizacional.

Al respecto CISCO (2007), Linero et al. (2015), Tarek et al. (2017), estiman que un factor vital para considerar a una red eficiente el tiempo de respuesta a los usuarios estrechamente relacionado con el rendimiento de la red. En los estudios realizados por CISCO (2017) las limtaciones en cuanto al tiempo de respuesta están dadas con mayor frecuencia en las aplicaciones de voz, pues el tiempo de espera afecta la fluctuación y la calidad de la llamada por voz. Algunos de los factores que conspiran contra el tiempo de respuesta son la congestión de la red, los dispositivos de red infra motorizados, las fallas de red, ruidos o errores CRC, entre otros.

Relativo a la información brindada por los indicadores para medir la eficacia se observa correspondencia entre la información brindada por los proveedores y usuarios, así con los datos relativos a la eficiencia, lo que evidencia la existencia de huecos en la red, pues los encuestados perciben la ocurrencia de los ataques con una frecuencia media, al igual que su nivel de impacto. De igual forma consideran como un nivel medio el grado de eficacia para controlar o contrarrestar los ataques.

En este sentido, Baluja-García y Anías-Calderón (2006) estiman que los ataques a la red pueden ser controlados y menguados mediante la implementación de políticas de seguridad, a través de las cuales se puede lograr la eficacia de los mecanismos de seguridad para asegurar la disponibilidad de la red. Estas políticas deben abarcar desde la evaluación del riesgo hasta la implementación de equipos de respuesta; solo desde estas consideraciones será posible lograr los objetivos de seguridad de la red controlando y contrarrestando las posibles vulnerabilidades, lo que permitirá un breve tiempo de recuperación que, permita la rápida activación y puesta en función de los servicios necesarios para el óptimo desempeño empresarial.

Entre los ataques a la LAN recibidos el de mayor frecuencia es el DDoS debido en gran medida a la no existencia de un modelo de seguridad que permita visualizar en tiempo real el funcionamiento de los dispositivos de red. En este sentido, la inclusión del firewall de Fortinet facilitará el monitoreo sistemático del funcionamiento de los dispositivos de red mediante gráficos, de esta forma se sabría con exactitud cuándo se está realizando un ataque de DDoS, permitiendo bloquear la entrada de las continuas solicitudes que saturan la capacidad del router.

Estos resultados se corresponden con los de Villa (2017), quien determinó la frecuencia de la ocurrencia de DDoS en el 68% de los ataques a una red LAN. En tal sentido Romero et al. (2018) consideran que, para contrarrestar y minimizar el impacto de este tipo de ataque se deben

implementar modelos que utilicen balanceadores de carga de tráfico como parte del sistema de seguridad.

CONCLUSIONES

El análisis de la información obtenida a través de los métodos e instrumentos de recolección de empleados permiten concluir que:

- Las empresas proveedoras de servicios de Internet cumplen las regulaciones y normas establecidas por el Estado para la seguridad de las LAN del cantón, mediante la implementación de los protocolos de ARCOTEL, utilizando el firewall de Mikrotik por su configuración flexible, pero no se tienen en cuenta otras posibilidades como la visualización del funcionamiento de los dispositivos de red en tiempo real, lo que facilitaría prevenir con mayor eficacia los ataques a las redes LAN.
- La seguridad que brindan las empresas proveedoras de servicios de Internet no utilizan sistemas de seguridad profunda de las redes LAN totalmente eficientes y eficaces, toda vez que existen "huecos en la red" a través de los cuales se producen ataques informáticos mediante virus, troyanos, gusanos, etc. que vulneran la integridad de los datos; además, de la potencial amenaza de daños a los software y hardware de los sistemas informáticos.
- Entre los ataques el más recurrente es el DDoS que desborda la capacidad de ruters, causando demora en el tiempo de respuestas a las necesidades de los usuarios.
- El tiempo de recuperación de los ataques a las redes LAN se encuentra entre 30 y 60 minutos, lo que repercute desfavorablemente en la gestión de las entidades usuarias.
- Las empresas proveedoras no utilizan modelos de seguridad más confiables como el diseñando por la Organización Internacional para Normalización; lo que, permitirá el cumplimiento de las obligaciones contractuales y la gestión empresarial u organizacional de manera más eficiente y eficaz.

De lo anteriormente señalado se deduce que los sistemas de seguridad de las redes LAN utilizados en el Cantón Pasaje no son plenamente eficientes y eficaces.

REFERENCIAS BIBLIOGRÁFICAS

Baluja-García W., & C. Anías-Calderón, C. (2006). Amenazas y defensas de seguridad en las redes de próxima generación. *Ingeniería y competitividad,* 8(2). 7-16.

Bejarano, F. E. (2017). Seguridad en redes. Unidad 2. Herramientas de control y seguimiento de accesos. Bogotá D.C.: Fundación Universitaria del Área Andina.

Benítez Flores, C. R., Granda Ayabaca, D. M., & Jaramillo Alba, J. A. (2019). La computación en la nube en los espacios educativos. *Sociedad & Tecnología*, *2*(1), 51–58. https://doi.org/10.51247/st.v2i1.67.

Cornelius, D., Lars, H ., Julius, M., Maximilian, H., & Georg, C. (2018). Verified iptables Firewall Analysis and Verification, *Journal of Automated Reasoning,* 61(1-4), 191–242.

CISCO (2007). Administración de rendimiento: Informe oficial de mejores prácticas. https://www.cisco.com/c/es_mx/support/docs/availability/high-availability/15115-perfmgmt.html

Cisneros, C. I. (2017). Modelo de seguridad de defensa en profundidad para los GADS (Gobiernos Autónomos Descentralizados) Municipales del Ecuador con base en el sistema de gestión de información. (Tesis de maestría). https://1library.co/document/yevjd8ez-seguridad-profundidad-gobiernos-autonomos-descentralizados-municipales-gestion-informacion.html

Da, H., Kai, X., & Jian, P. (2014). Malicious URL detection by dynamically mining patterns without pre-defined elements, *World Wide Web,* 17(6), 1375–1394.

del Pino Sarduy, J. A., & Fernández Álvarez, D. (2021). GPLAN: Sistema Informático para la gestión de los Planes de Desarrollo Individual. *Sociedad & Tecnología*, *4*(1), 23–30. https://doi.org/10.51247/st.v4i1.72

González Paz, A., Beltrán Casanova, D., & Fuentes Gari, E. R. (2016). Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos. Universidad y Sociedad 8 (4), 130-137.

Guijarro Rodríguez, A., Yepez Holgin, J., Tania J. Peralta Guaraca, J., & Ortiz Zambrano, M. (2018). Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios, 39 (42).

Hernández, S., R., Fernández, C. C., & Baptista, L. P. (2014). *Metodología de la Investigación* (6ta edición). México: McGrauHill.

Jamieson, R., & Low, G. (1990). Local area network operations: a security, control and audit perspective, *Journal of Information Technology,* 5, 63-72.

Jiménez R. E. (2004). Indicadores de calidad y eficiencia de los servicios hospitalarios. Una mirada actual. Rev Cubana Salud Pública, 30(1). http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864 34662004000100004&lng=es&nrm =iso>. ISSN 0864-3466.

Kenneth, T., Martín, S., Ken, M., Rick, B., & Bruce, M. (2015). Seguridad UTM con Fortinet: Dominando FortiOS, Newnes.

Linero-Ramos, R., Camargo-Ariza, L., & Medinadelgado, B. (2015). Análisis del rendimiento de redes basadas en el estándar IEEE 802.15.4. Universidad Industrial de Santander Bucaramanga, Colombia. *Revista UIS Ingenierías,* 14(1), 71-79. http://www.redalyc.org/articulo.oa?id=553756867006

Magoni, V. (2018). Los 5 mejores software de monitoreo de red en 2017.*Tanaza*. https://medium.com/tanaza/los-5-mejores-software-de-monitoreo-de-red-en-2017-f1f3adc6a962

Moya, S. (2017). Modelo de Referencia OSI para Redes de Comunicación. https://www.isamex.org/intechmx/index.php/2017/08/07/modelo-de-referencia-osi-para-redes-de-comunicacion/

Muñoz, M., & Rivas, L. (2015). Estado actual de equipos de respuesta a incidentes de seguridad informática. *RISTI-Revista Ibérica de Sistemas e Tecnologías de Informação,* 1-15.

Olifer, N., & Olifer, V. (2009). *Redes de computadoras.* Mexico: Mc Graw Hill.

Otero, M. J. (2001). *Eficiencia y eficacia.* http://www.gerenciasalud.com/art05.htm

Robayo López, J., & Rodríguez Rodríguez, R. (2015). Aseguramiento de los sistemas computacionales de la empresa. *Sitiosdima. Net.*

https://repository.unad.edu.co/handle/10596/3818

Romero, C. M., Figueroa, M. G., Vera, N. D., Álava, C. J., Parrales, A. E., Álava, M. C., Murillo, Q. A., & Castillo; M. M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: Editorial Área de Innovación y Desarrollo, S. L. DOI: http://dx.doi.org/10.17993/IngyTec.2018.46

Rué, J. (2018). *Talleres, ¿actividad o proyecto?* Universidad Autónoma de Barcelona. http://www.ugr.es/~fjjrios/pce/media/7-Talleres ActividadProyecto.pdf

Salles, R. M., & Carvalho, J. M. A. (2015). An Architecture for Network Congestion Control and Charging of Non-cooperative Traffic, *Journal of Network and Systems Management,* 19(3), 367–393.

Tarek, A., Ade, l. B., & Michaël, R (2017). Detection of firewall configuration errors with updatable tree, *International Journal of Information Security,* 15(3), 301–317.

Villa, J. (2017). Seguridad de la red LAN. *Asociación Colombiana de Ingeniería de Sistemas. ACIS*. https://acis.org.co/archivos/Conferencias/2017/Conferencia1312.pdf

Wright, J., & Harmening, J. (2009). "15" Computer and Information Security Handbook. Morgan Kaufmann Publications Elsevier Inc.

Síntesis biográfica de los autores

Nelly Victoria Ley Leyva

Master en Ciencias de la Educación, profesora ocasional de la Universidad Técnica de Babahoyo.

Diana María Granda Ayabaca
Ingeniera en Sistemas Informáticos, Magister en sistemas computacionales, vicerrectora académica del Instituto Tecnológico Superior Jubones.

Cristian Rafael Benítez Flores
Ingeniero en Sistemas Informáticos, docente investigador del Instituto Tecnológico Superior Jubones.

Verónica Jacqueline Guamán Gómez
Licenciada en ciencias de la educación, magister en ciencias pedagógicas, docente investigador del Instituto Tecnológico Superior Jubones, doctorante por el Instituto Central de Ciencias Pedagógicas de la Habana.