17

Fecha de presentación: febrero, 2020
Fecha de aceptación: marzo, 2020
Fecha de publicación: mayo, 2021

CARACTERÍSTICAS
DE LA CONECTIVIDAD A INTERNET EN EL CANTÓN PASAJE
CHARACTERISTICS OF INTERNET CONNECTIVITY IN THE CANTON PASAJE

Kelvin Giovanni Pincay Romero[1]
E-mail: kpincay2@utmachala.edu.ec
ORCID: https://orcid.org/0000-0003-1562-0037
[1] Universidad Técnica de Machala. Ecuador

Cita sugerida (APA, séptima edición)

Pincay Romero, K. G. (2021). Características de la conectividad a internet en el cantón Pasaje. *Revista Universidad y Sociedad*, 13(3), 150-160.

RESUMEN

Con el objetivo de caracterizar la conectividad a Internet en el Cantón Pasaje se desarrolló una investigación de tipo descriptivo con enfoque cuantitativo fundamentada en los métodos de observación científica, analítico-sintético, histórico-lógico y estadístico; además se empleó la técnica de entrevista. Los resultados obtenidos evidencian que las empresas proveedoras de los servicios de Internet cumplen las regulaciones estatales instituidas, el protocolo utilizado es el de la Agencia de Regulación y Control de Telecomunicaciones. Los ataques más frecuentes son el tipo DDoS y los Spam. Se concluye que las características de la conectividad de Internet se basan en la conexión por fibra óptica y el principal dispositivo de seguridad empleado es el firewall de Mikrotik; no tienen diseñados sistemas profundos para garantizar una conectividad más segura.

Palabras clave: Internet, conectividad, sistemas de seguridad, empresas proveedoras.

ABSTRACT

In order to characterize Internet connectivity in the Canton Pasaje, a descriptive research was developed with a quantitative approach based on scientific, analytical-synthetic, historical-logical and statistical observation methods; In addition, the interview technique was used. The results obtained show that the companies that provide Internet services comply with the state regulations established, the protocol used is that of the Telecommunications Regulation and Control Agency. The most frequent attacks are DDoS and Spam. It is concluded that the characteristics of Internet connectivity are based on the fiber optic connection and the main security device used is the Mikrotik firewall; they do not have deep systems designed to ensure more secure connectivity.

Keywords: Internet, connectivity, security systems, supplier companies.

INTRODUCCIÓN

En la actualidad es imposible ya vivir sin los servicios que presta internet, hoy es un hecho irrefutable el uso de esta tecnología para desarrollar el trabajo o simplemente para establecer comunicación con familiares y amigos. Hace más de un lustro que Barber, et al. (2014), señalaban que el 80% de las personas a nivel mundial de un manera u otra empleaban el Internet, cifra que continúa en aumento de manera progresiva y casi universal gracias a los beneficios que representa la conexión a la banda ancha móvil.

En la actualidad las suscripciones a esta banda representa el doble de los contratos a la banda ancha fija (Ecuador. Ministerio de Telecomunicaciones de la Sociedad de la Información, 2019). Basta este ejemplo para comprender la importancia que cada día más adquiere Internet en las relaciones sociales, políticas, económicas, culturales, etc. A tal punto ha llegado su presencia, influencia e impacto en la actual sociedad llamada del conocimiento que, es considerada el soporte de una cultura en ascenso en la búsqueda y construcción colectiva e innovadora del conocimiento, en contraposición al conocimiento individual (Borgia, 2014).

Esta tecnolgía que surgió con fines de inteligencia militar en 1969 bajo el nombre de ARPANET (***Advanced Research Projects Agency Network)*** conectando a tres universidades de California se ha convertido en una herramienta común de connotación social, por ejemplo hoy muchas personas cuentan con una computadora, un tablet o un teléfono inteligente e incluso ya se ha colocado en la preferencia de las personas los relojes inteligentes, dispositivos que disponen de un paquete de navegación de Internet.

Estos avances tecnológicos han propiciado un nuevo concepto de Internet que sa ha dado en llamar el "Internet de las cosas" o "***Internet of Things***" (IoT, en sus siglas en inglés), convirtiéndose en una tendencia tecnológica que estimula cada vez más a las compañías y empresas a la innovación de tecnologícas con acceso a Internet (Borgia, 2014; García, 2019). Se estima que actualmente en cada segundo se conectan 126 nuevos dispositivos a la red (Pisano, 2018), para lo cual es preciso contar con el acceso a Internet, motivando así a los proveedores de los servicios de Internet (ISP) a disponer de una mayor ancho de banda y velocidad que permitan satisfacer las demandas de conectividad a larga distancia de los equipos inalámbricos y la estabilidad de las conexiones .

Realidad no ajena al Ecuador donde el Estado y Gobierno han trazado polítcas públicas encaminadas a incrementar los índices de informatización de la sociedad a través del fortalecimiento de las infraestructuras tecnológicas, sostenidas por una fuerte inversión pública básica; por otro lado, el Plan Nacional de Banda Ancha, han permitido que la población tenga acceso a Internet para satisfacer la demanda de servicios. En este sentido se reporta por la Agencia de Regulación y Control de las Telecomunicaciones que en el mes de marzo de 2019 exisitían 11.148.222 suscripciones a Internet tanto en banda ancha móvil como fija, lo que representa el 62,2% de penetración al servicio de Internet, de estas el 82,1% corresponden a las conexiones móviles (Ecuador. Ministerio, 2019).

Estas políticas públicas diseñadas para el empleo de Internet se centran en: 1) la garantía de acceso a las tecnologías de las telecomunicaciones, lo que requiere de infraestructuras, capacitación y el empoderamiento de la población y la regulación del mercado en busca de la reducción de los precios y favorecer la competencia; 2) fomento de estrategias alternativas de infraestructuras de redes inalámbricas para la gestión comunitaria, 3) la construcción integral de un marco civil y de derechos para la regulación de Internet y 4) la seguridad de las conexiones que, incluye estrategias de seguridad institucionales, encriptación, técnicas de puntos neutros, empleo de estándares abiertos y la participación de la población en el cumplimiento de las normas y medidas en el cumplimiento de las políticas de seguridad (Torres & Vila, 2015).

Sin embargo, en la práctica cotidiana las vulnerabilidades de ciberseguridad, que aún ocurren con frecuencia, son un ostáculo para el logro de una eficiente conectividad a Internet; realidad no ajena a nuestro contexto, lo que motivó el presente estudio con el objetivo de caracterizar la conectividad a Internet en el Cantón Pasaje.

Internet, es la conexión de los dispositivos informáticos por medio de cables físicos o de manera inalámbrica, controlados por protocolos de comunicación, equipos intermedios de comunicación como routers y switches, y proveedores de los servicios constituyen una red de comunicación; estas redes así conformadas se pueden interconectar por medio de cables subterráneos, submarinos y aéreos, y/o satélites formando así una gran red a nivel mundial (Ramírez, 2015). De esta forma, sencilla y resumida se puede explicar en que consiste la red más grande del orbe, denominada Internet; podemos entonces entender que Internet es un conjunto de redes de comunicación heterogéneas más pequeñas interconectadas.

Cabe entonces preguntarse ¿cómo se interconectan estas redes heterogéneas?

Para poder establecer el "diálogo" entre las redes se emplean los protocolos TCP/IP que establecen un "lenguaje común", lo que permite que estas se configuren y

funcionen como una sola red de alcance global, interconectado a todo el planeta.

Además, del TCP/IP que viabiliza la interconexión de todas las redes del mundo, existen otros atributos que distinguen a Intenet, entre los más significativos se encuentran:

- Universalidad, se encuentra extendida por todo el orbe; facilita la interacción con personas de cualquier parte del mundo mediante el correo electrónico, las redes sociales, el chat, la trasferencia de archivos, etc.
- Variedad, ofrece la posibilidad de acceder a una gran gama de información mediante la World Wide Web (WWW) y otros servicios como transferencias de ficheros, mensajería, etc.
- Interactividad, las personas conectadas pueden interactuar, facilitando los espacios colaborativos muy útiles para los negocios, la educación, la participación en las redes sociales, etc.
- Económica, permite economizar los costos por trasferencia de información, correspondencia y otros servicios; asimismo se ahorra tiempo en la consulta de una gran variedad de información.

Para poder entender la evolución de Internet, CISCO Systems (2013), propone cuatro etapas o fases; según el impacto que ha tenido en la sociedad y el mundo empresarial, estas son:

Fase 1. Esta etapa se incia en los años 90 del pasado siglo XX, a la cual se le llama "Era de la conectividad" caracterizada por la búsqueda de contenidos mediante el empleo del navegador web y uso del correo electrónico; lo que permitió que el mundo estuviera más informado y comunicado, elimando las barreras geográficas.

Fase 2. Período denominado "Economía interconectada"; esta etapa inició en los últimos años de la década de los 90. Esta etapa se significa por la digitalización de los procesos mercantiles, se potenció el comercio electrónico, transformando la dinámica de la gestión comercial y mercantil, se facilitó una nueva manera para que las personas realicen sus compras y las empresas accedan al mercado.

Fase 3. Esta esta llamada "Experiencias cooperativas" inció en el año 2000, con el auge de las redes sociales, los servicios de video, el uso de la nube como proveedora de información; las nuevas innovaciones tecnológicas impactaron en las relaciones empresariales y sociales.

Fase 4. Etapa denominada "Internet de Todo" (IdT) o "Internet de las Cosas" (IoT). En esta fase se trasciende de la conectividad entre personas a la interconexión y comunicación entre los procesos, los datos y los dispositivos; esta dinámica ha transformado la concepción inical de Internet, creando novedosas experiencias, capacidades y oportunidades sin precedentes, favoreciendo la calidad de vida de las personas y la gestión de los procesos empresariales en beneficio de la productividad y los valores financieros.

Hoy las conexiones a Internet adquieren un mayor valor, a través de ellas los Sistema de Información brindan la información adecuada y pertinente. Los datos representan no solo la información generada por las personas, sino también de los objetos o dispositivos, que facilitan un mejor procesamiento de la información y resultados, así como la toma de decisiones.

Según Ramírez (2015), ***"la capacidad de IdT puede incluir análisis de datos multidimensionales en tiempo real (Inteligencia de Negocio o BigData), colaboración integrada por video (videoconferencias o telepresencia) y seguimiento remoto de recursos físicos (RFID o GPS)".*** (p. 23)

Estas novedades tecnológicas han sido posible, en gran medida, gracias al desarrollo de la ciencia y la técnica que han permitido una mayor conexión a Internet, en busca de una más amplia cobertura y mejor calidad de los servicios. Actualmente existen diversidad de tipos de conexión que facilitan el acceso desde cualquier zona a donde antes las tecnolgías no podían llegar.

Los ISP utilizan diversas tecnologías para conectar a los usuarios a Internet. Las conexiones de los dispositivos de tecnología informática, como computadoras, tablets, teléfonos móviles, etc. se realizan de diversas maneras, entre ellas están la conexión a través de cables de fibra coaxial y de fibra óptica, línea telefónica (ADSL), telefonía móvil (GSM, GPRS, 4G), vía satelital y las redes inalámbricas o ***wireless*** (LMDS, PLC, WIMAX).

En la tabla 1 se recoge de manera resumida las principales características de algunos de estas vías de conexión a Internet.

Tabla 1. Características de las principales vías de cone-

xión a Internet.

Sistema de conexión	Características
Conexión por cable	Esta tecnología consigue altas velocidades de trasmisión de datos, abandonando la conexión directa punto a punto y adoptando la conexión multipunto donde el cable puede ser compartido por varios usuarios. Cada nodo puede brindar servicio a una cantidad de usuarios entre 500 y 2000, pero para obtener una conexión de calidad la distancia entre el usuario y el nodo no puede ser superior a medio kilómetro y no se puede usar la vía telefónica tradicional de cables de cobre, este debe ser coaxiales, garantizado la longitud necesaria para conectar al usuario. Además, al estar conectados varios usuarios a un mismo nodo la tasa de transferencia se reduce de manera proporcional al número de conexiones.
Conexión de línea telefónica ADSL	ADSL (Asymmetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica), es una tecnología que emplea la línea telefónica de cables de cobre convirtiéndola en una línea de alta velocidad, que supera el obstáculo de la tecnología anterior RTC al poder trasmitir voz y datos de manera simultánea en una misma línea telefónica, gracias al modem ADSL. Para este proceso se establecen dos canales de alta velocidad no asimétricos, uno para el envío de datos y otro para la recepción; el canal de recepción de datos es de mayor velocidad que el de envío y un tercero para el servicio telefónico básico de comunicación estándar de voz.
Conexión satelital	Otra vía también muy utilizada en la actualidad para acceder a Internet es la satelital, permite llegar mediante banda ancha a zonas donde no puede llegar el cable. Solo se necesita contar con una antena, un decodificador y un módem satelital. Esta vía es empleada como alternativa por los ISP para la distribución de contenidos y transferencia de archivos, para así superar la congestión de las redes tradicionales. Generalmente los ISP emplean conexiones híbridas de telefonía y satélite, para lo cual deben contar con antenas parabólicas digitales, modem para acceso telefónico a Internet como el ADSL, el RCT y el RDSI o mediante cable, una tarjeta receptora para PC, programas específicos y estar suscriptos a un proveedor de satélite.
Conexión inalámbrica o wireless	Entre las conexiones más utilizadas actualmente están las inalámbricas como la Wi-Fi, que funcionan mediante un sistema eléctrico de comunicación para conectar los dispositivos a través de ondas electromagnéticas direccionadas a los puertos. Esta tecnología permite el establecimiento de redes locales mediante ondas infrarrojas y de radio de frecuencias de libre empleo, no utiliza ningún tipo de cable. Su mayor dificultad consiste en la disminución de la velocidad según la distancia del punto de acceso. Los sistemas de conexión inalámbrica de banda ancha se denominan Broadband Wireless Systems (BWS), entre ellos los sistemas:. 1. PLC (Conexiones Power Line); convierte a la red eléctrica en una línea digital de gran velocidad, que facilita el acceso a la WWW mediante banda ancha. Siendo una de las más utilizadas. 2. LMDS (Local Multipoint Distribution System); se comporta como acceso inalámbrico mediante el uso de las ondas radioeléctricas a altas frecuencias, configurando un bucle con gran ancho de banda. Su calidad de conexión se iguala a la del cable de fibra óptica y el satélite. Entre sus beneficios están el poder llevar los servicios de Internet a lugares donde el sistema basado en cables no es eficaz y hacer más bajos los costos por concepto de mantenimiento al ser la comunicación por vía aérea. 3. WIMAX (*Worldwide Interoperability for Microwave Access*), tiene una amplia cobertura permitiendo el acceso a sitios a los que no accede adecuadamente la fibra óptica o el ADSL

Fuente: Borgia (2014).

Asimismo, para la implementación de estos sistemas de conexión a Internet se necesita de dispositivos tales como routers y convertidores de señales. Entre los más utilizados podemos señalar el router fabricado por MikroTik; este router permite el monitoreo y administración de la red. Puede configurarse a través de una interfaz de línea de comandos accesible por puerto serie, telnet y Secure Shell (SSH), y a través de una interfaz gráfica de usuario disponible como una interfaz basada en web (WebFig).

También, es frecuente el empleo de Unidad de red óptica (ONU), este dispositivo de red óptica convierte las señales ópticas transmitidas mediante fibra en señales eléctricas. Este hardware facilita la gestión de diferentes tipos de datos, optimizando y reorganizando su flujo para una transportación más eficaz. Una de las ventajas de la ONU es que se pude conectar mediante diferentes tipos de cables (par trenzado de cobre, coaxial y fibra óptica) y también mediante la Wi-Fi. Al igual que el terminal de línea óptica (OLT) que es el dispositivo para conectar un tronco de fibra óptica.

La superautopista de Internet proporciona acceso universal, rápido y económico a una gran cantidad de información diversa de calidad, facilita la gestión en las más diversas esferas de la actividad humana. Siguiendo a Berners-Lee, et al. (1992), encontramos los siguientes servicios:

- Acceso remoto mediante la conexión de ordenadores y dispositivos (TELNET)
- Protocolo de transferencia de ficheros (FTP) entre una computadora local y una computadora remota.
- Protocolo de transferencia de hipertextos (HTTP), permite la lectura de archivos de texto, imágenes, sonidos y vídeos, situados en la WWW.
- Correo Electrónico o e-mail, permiten la comunicación entre las personas sin importar la distancia de manera rápida.
- "News" y los canales de Chat (IRC), permiten establecer la conversación en tiempo real entre personas situadas en diferentes partes del mundo. Además, facilita la participación en conferencias, foros y debates.
- Conectividad entre dispositivos informáticos.

Estas y otras ventajas que ofrecen los servicios de Internet fundamentan la demanda de sus servicios por parte de las instituciones, organismos y empresas; así como por la sociedad en general.

Pero, es necesario también conocer los riesgos que entrañan su empleo regularmente asociado al inadecuado uso que dan los usuarios a sus servicios. Entre los riesgos del empleo de Internet se encuentra la subordinación a su funcionamiento; la interrupción por cualquier motivo provoca el colapso de la red, causando la paralización de los servicios con el consabido atraso de los procesos de la gestión empresarial que acarrea pérdidas económicas. Por otro lado, el uso indiscriminado puede provocar dependencia provocando trastornos de la conducta principalmente entre los jóvenes (Torres & Vila, 2015).

Otro de los potenciales riesgos está dado por su carácter de anonimato y libertad, cualquier persona puede colgar en la red todo tipo de información sin censura bajo el más estricto anonimato, lo que facilita el uso negativo de la Internet y permite conductas antisociales como la divulgación de pornografía, violencia, terrorismo, estafas y fraudes; además, bajo estas condiciones de anonimato y libertad se introducen virus, gusanos informáticos, troyanos, malware, ransomware, spam y phising, entre otros programas malignos. También Internet es susceptible a los ataques DDoS, a los botnet y a los spyware con el propósito de dañar las bases de datos y hardware, robar información, etc. (Román, et al., 2013).

Como vemos la vulnerabilidad de Internet es un hecho que ocurre con mucha frecuencia develando los llamados "huecos de red", que la hace insegura, pues es posible interceptar una comunicación, capturar y/o dañar la información; así como atentar contra los sistemas y hardware, razón por la cual las empresas proveedoras de los servicios de Internet tienen una mayor demanda de sistemas de seguridad que permitan dar protección a la gestión empresarial (Pisano, 2018).

Tal es la relevancia que ha adquirido la seguridad de Internet que se ha derivado como rama particular de la seguridad informática; esta rama se dedica a detectar, prevenir y menguar las amenazas de ataques a la red de redes.

En tal sentido, para el empleo de Internet se han diseñado políticas de seguridad que deben ser cumplidas por los ISP; estas políticas establecen en general tres etapas: preparación, prevención y respuesta.

La etapa de preparación a su vez contempla tres fases: 1) la declaración de los roles y responsabilidades de los usuarios; 2) análisis de los riesgos y 3) establecimiento de la estructura del sistema de seguridad.

La etapa de prevención se orienta a la implementación del sistema de seguridad y sistemático control de la seguridad de la red. Por último, en la etapa de respuesta se detectan los ataques a la red, se activan los métodos y protocolos de seguridad, se restauran las posibles alteraciones a las operaciones y funciones de la red, y se revisan los procedimientos, métodos y protocolos implementados en la política de seguridad, en la búsqueda del perfeccionamiento de estos (CISCO Systems, 2013; y Piñero & Rodríguez, 2020).

Sobre la base de estas políticas los ISP diseñan procedimientos, métodos y modelos de seguridad direccionados a la protección de los protocolos TCP/IP en el cumplimiento de las normas establecidas por las organizaciones internacionales y estatales de cada nación. Entre los recursos para brindar a los usuarios una conexión segura

a Internet los ISP cuentan con diversos protocolos y modelos basados en software y hardware, a saber:

- Protocolo de Seguridad Internet (IPsec)

Este protocolo de protección de la comunicación TCP/IP es un conjunto de extensiones de seguridad diseñado por el ***Engineering Task Force*** (IETF)); está fundamentado en la encriptación de los datos de la capa IP, para ello cuenta con dos procedimientos la ***Authentication Header*** (AH) y el ESP, los que pueden ser utilizados de forma combinada para propiciar una mayor seguridad al IP; además de estos dos protocolos la IPsec cuenta con otros componentes básicos como el ***Internet Key Exchange*** (IKE) para la gestión automática o manual de la red, la asociación de seguridad para la política de gestión y procesamiento del tráfico y los algoritmos de autentificación y encriptación.

- Access Control Lists (ACL).

Mediante esta herramienta se crea una lista de permisos a usuarios de manera individual o en grupos para tener permiso de acceso al FTP, Internet, etc. Por otro lado, permite definir el ancho de banda y horarios.

- Firewalls (Contafuegos)

Este sistema de seguridad es una especie de servidor intermedio entre las conexiones de SMTP y el ***Hypertext Transfer Protocol*** (HTTP), estos pueden ser hardware, software o mixtos que, permite bloquear el acceso no autorizado a un computador o red. Existen diferentes tipos de contrafuegos, entre ellos: de capa de red o de filtrado de paquetes, de capa de aplicación, personales, etc.

Los Firewalls constituyen uno de los sistemas pioneros aplicados para la seguridad de las conexiones a Internet. Los ***firewalls*** facilitan el tráfico en la red, siendo capaces de bloquear el tráfico sospechoso (Bailey, et al., 2007).

Como vemos los ***firewalls*** no solo bloquean el tráfico no autorizado o sospechoso, también puede analizar el tráfico que entra o sale mediante la configuración de filtros que deciden sobre el acceso y salida de la información. Aunque los ***firewalls***, constituyen una capa de seguridad, mal configurados pueden hacer vulnerable la red por algún tipo de malware, por lo que se recomienda combinarlos con un antivirus (Abbes, et al., 2017).

- PRTG Network Monitor

Este software permite el monitoreo de la infraestructura de la red, servidores, sitios web, aplicaciones, etc. (García, et al., 2020).

- Modelos de seguridad

Asimismo, los ISP diseñan y adoptan modelos de seguridad para los servicios de Internet que integran diversos software y hardware; uno de los modelos que con mayor frecuencia se utiliza por las empresas proveedoras de estos servicios es el propuesto por la Organización Internacional para Normalización (OSI). La seguridad de este modelo se organiza en capas: 1) capa física, 2) capa de enlace de datos, 3) capa de red, 4) capa de transporte, 5) capa de sesión, 6) capa de presentación y 7) capa de aplicación. En cada una de estas capas se realiza el control, protección y preservación de integridad de los datos (Bejarano, 2017). Este procedimiento se realiza a la par en las capas correspondientes tanto en el sistema emisor como en el receptor, donde el sistema solicitante verifica y el servidor emisor responde (Olifer & Olifer, 2009).

Ahora bien, entre las primeras medidas para contrarrestar los potenciales riesgos a los que nos exponemos al conectarnos a Internet están las que pueden ser adoptadas por el usuario, como la protección de los ordenadores contra los virus, para ello es necesario contar con programas antivirus, que son el primer filtro de protección de nuestros dispositivos (computadores, smartphones, tablets, etc.) y de la información que atesoramos en ella.

También, es recomendable el empleo de contraseñas, se aconseja utilizar diferentes contraseñas para los distintos servicios de Internet, las que deben ser renovadas frecuentemente, así como no utilizar ninguna que relacione datos personales como fecha de nacimiento o nombre del usuario o familiar; se recomienda emplear cifrados que mezclen números, caracteres y símbolos permitidos que hagan difícil su descifrado por los hackers (Olifer & Olifer, 2009).

Asimismo, es importante la seguridad de los datos, para lo cual se puede emplear memorias externas debidamente protegidas con contraseñas. En este sentido hoy es muy socorrido el empleo de la nube.

Por último, a la hora de navegar en la red es oportuno no visitar las páginas Web sospechosas de ser trasmisoras de virus; las Web seguras son certificadas con el SSL (Se identifican con facilidad pues el URL de acceso a la página Web es un https).

MATERIALES Y MÉTODOS

La investigación llevada a cabo es de tipo descriptiva con enfoque cuantitativo, sistematizada a través de los métodos de observación científica, analítico-sintético, histórico-lógico y estadístico; además se empleó la técnica de entrevista en profundidad para la recolección de la información.

La observación científica realizada en el campo junto a la entrevista aplicada a los funcionarios y empleados de las empresas suministradoras del servicio de Internet en el

cantón facilitaron la determinación de las características de la conectividad que se brinda a los clientes. El método histórico-lógico fue utilizado para el análisis de la evolución de Internet en el tiempo; el estadístico se empleó en la planificación de la investigación, en la recolección de la información, en el procesamiento, codificación y cuantificación de la información, así como para analizar los resultados. A través, del método analítico-sintético se estudiaron y resumieron estos resultados, lo que sirvió para arribar a las conclusiones del estudio.

La entrevista aplicada como instrumento para la recolección de la información sobre las características de los servicios que presentan las empresas proveedoras de los servicios de Internet; contó con 9 preguntas; para su confección se tuvieron en consideración las indicaciones de Espinoza &Toscano (2015):

1. Localización y análisis de instrumentos similares.
2. Validez y contextualización de los instrumentos seleccionados.
3. Confección de una primera versión del instrumento.
4. Validación mediante especialistas.
5. Puesta a punto del instrumento.
6. Prueba piloto.
7. Elaboración de la versión final del instrumento.

En el cumplimiento de los pasos 1 y 2 se analizaron y contextualizaron los cuestionarios validados por García (2019), en su estudio "Análisis de la transmisión de datos y seguridad de la red de proveedor de Internet en la empresa Cybermar, en el recinto Mata de Cacao" y el de Cuzme (2015), utilizado en su tesis de maestría intitulada "El Internet de las Cosas y las consideraciones de seguridad"*, las* que sirvieron como referentes para la concepción de las preguntas de la entrevista aplicada.

Una vez cumplidos los pasos del 1 al 3 la primera versión del instrumento se sometió a la consulta de 3 especialistas en la esfera de los servicios de Internet y dos docentes con experiencia en el tema. Estos expertos evaluaron los siguientes elementos: 1) pertinencia y coherencia de las preguntas en relación con el objeto de estudio, 2) objetividad de las preguntas y 3) adecuación estructural, metodológica y técnica del cuestionario para la obtención de la información.

El instrumento fue perfeccionado teniendo en consideración los criterios y sugerencias de los expertos. Por otro lado, para evaluar su confiabilidad de consistencia interna se utilizó el coeficiente Alfa de Cronbach, que resultó igual a 0,953, valor próximo a 1 que, le otorga alta confiabilidad.

La población estuvo constituida por los 124 funcionarios y empleados de las 12 empresas proveedoras de los servicios de Internet del Cantón Pasaje en la Provincia de El Oro. El tamaño de la muestra se obtuvo mediante la aplicación de la fórmula:

$n=N\ \sigma^2Z_\sigma^{\ 2}/(e^2(N-1)\ +\ \sigma^2Z_\sigma^{\ 2})$, donde n: tamaño de la muestra; N= tamaño de la población; σ= desviación estándar de la población Z=constante correspondiente al nivel de confianza y e=error muestral. Resultando n= 30, para Z =1,96; e= 0.05 y σ=0.16.

Los 30 entrevistados de la muestra se seleccionaron teniendo en cuenta la representatividad de cada una de las doce empresas del cantón, para lo cual se utilizó el muestro estratificado.

RESULTADOS Y DISCUSIÓN

La información obtenida a través de la observación científica directa en el campo y la entrevista en profundidad realizada, después de haber sido procesada, codificada y cuantificada se brinda en las siguientes tablas y gráficos estadísticos.

La Figura 1 ofrece información sobre la cantidad de ISP y usuarios (empresas y personas) a las cuales brindan los servicios de Internet, en el Cantón Pasaje.

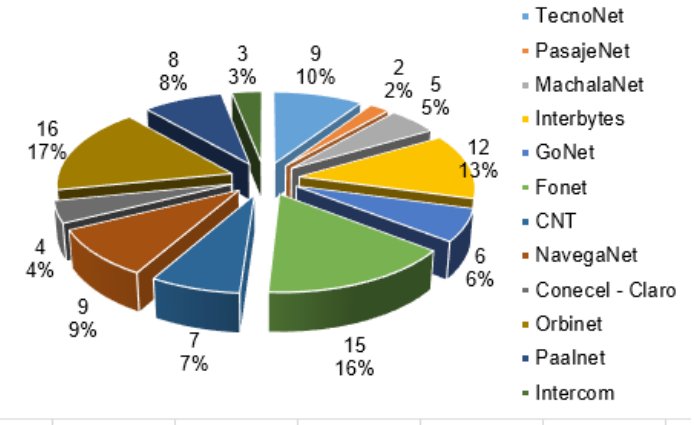

Figura 1. Empresas proveedoras y usuarias de los servicios de internet, cantón Pasaje, noviembre de 2020.

Los datos de la Figura 1 desvelan que en el Cantón Pasaje en el actual año 2020 operan 12 empresas proveedoras de los servicios de Internet que, brindan conexión a un total de 3968 empresas usuarias y clientes naturales.

Sobre las normas empleadas para protocolizar la seguridad de Internet, el 100% de los funcionarios y empleados entrevistados respondieron que utilizan el protocolo de seguridad de la Agencia de Regulación y Control de

Telecomunicaciones (ARCOTEL), de esta forma cumplen las normativas estatales establecidas al respecto.

La respuesta de los entrevistados a esta pregunta se resume en la figura 2.

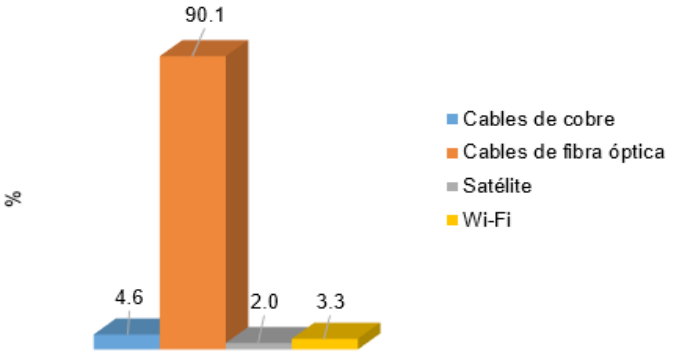

Figura 2. Principales tipos de conexión a internet. Cantón Pasaje, noviembre de 2020.

Los datos 2 evidencian que el 90,1% de los usuarios están conectados a Internet principalmente a través de cables de fibras ópticas y el resto mediante cables de cobre por vía telefónica, Wi-Fi y Satélite.

Al preguntar a los funcionarios y empleados sobre los dispositivos que la empresa utiliza con mayor frecuencia para establecer las conexiones a Internet, se obtuvo la información que se resumen en la stabla 2.

Tabla 2. Dispositivos empleados por las empresas para la conexión a Internet.

Dispositivos	%
Router Micro-Tik	100
Olt	66,7
ONU	90.1
Modem	5.0

Estos datos evidencian que el 100% de las empresas utilizan el ruter fabricado por la compañía MicroTik y un 90,3% de los entrevistados declararon utilizan la ONU para convertir las señales de las fibras ópticas en señales de corriente eléctrica y en menor cuantía se utilizan terminales Olt y modem.

El 100% de los entrevistados reconocen que la red ha sufrido algún tipo de ataque; el 66,6% de estos agregan que la frecuencia de ocurrencia es media, mientras que para el 33,3% restante es considerada de baja.

El nivel de impacto de estos ataques a Internet son estimados de nivel medio por el 50% de los entrevistados, mientras que la otra mitad de la muestra de funcionarios y empleados de los ISP lo consideran bajo.

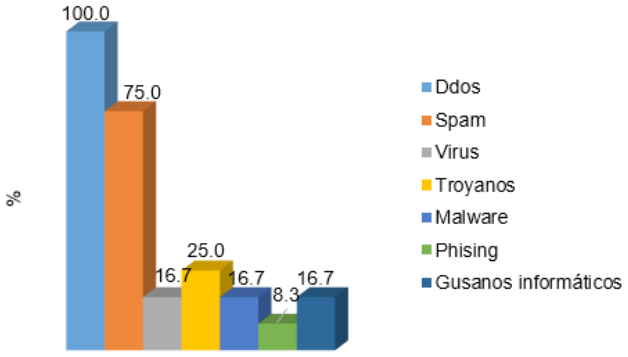

Figura 3. Tipos de ataques a Internet. Cantón Pasaje, noviembre de 2020.

Los datos de la Figura 3 revelan que los ISP del Cantón Pasaje han recibido algún tipo de ataque a Internet siendo el más frecuente el DDoS (100%) y en segundo lugar los Spam (75%), seguidos por los troyanos (25%), los virus, malware y gusanos informáticos (16,7%), y los Phising (8,3%), lo que evidencia que aún existen huecos en la seguridad de la red.

Al cuestionar a los directivos y empleados de las empresas sobre. ¿cuál es el sistema de seguridad que utilizan?, el 100% expresan que 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.

La figura 3 brinda información sobre el tiempo de recuperación después de un ataque a red.

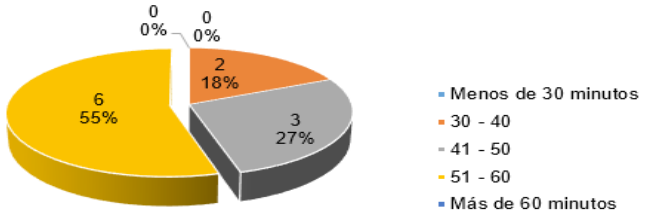

Figura 3. Tiempo de recuperación a los ataques a Internet.

Los datos de la Figura 3 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 y clientes en general.

El 100% de los entrevistados estiman que el mayor uso que se le da a la Internet es el correo electrónico, las redes sociales y la telefonía móvil; el 83% considera que también se emplea en la gestión empresarial y un 75% para el consumo de vídeos.

Los resultados obtenidos a través de la observación directa en los ISP permitieron determinar que en el Cantón Pasaje existen 12 ISP que prestan servicios de Internet a 3968 empresas y usuarios naturales, con un promedio aproximado de 331 usuarios por empresa proveedora y una velocidad media entre 3.5 y 5 megas por cliente. En los últimos cinco años se observa un acelerado crecimiento de los usuarios conectados a Internet.

Los servicios de Internet brindados por los ISP del cantón se caracterizan por el cumplimiento de las regulaciones y normas establecidas por el Estado para la seguridad de las conexiones a la red de redes. Estas empresas se rigen por los protocolos de ARCOTEL, organismo que dictamina el cumplimiento de los planes de seguridad de contingencia en cuanto a los servicios ofrecidos; sin embargo, no establece los mecanismos que se deben utilizar para efectuar 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 adecuados, así como establecer métodos de seguridad en conjunto con el usuario o empresa que recibe el servicio. Los sistemas de seguridad utilizados por los ISP se estructuran sobre la utilización de un firewall como principal medida de control de posibles amenazas.

Las conexiones se establecen generalmente a través de cables de fibra óptica, aunque aún subsisten las líneas de cobre para establecer la conexión a Internet de los domicilios donde cuentan con teléfono fijo y no llega la fibra óptica; estos usuarios se conectan a través de modem. También, en las zonas donde no llega la red de fibra óptica se emplea la Wi-Fi. Otra de las vías empleadas es la satelital para los usuarios que cuentan con antenas satelitales tanto en las zonas rurales como metropolitana. En correspondencia con estas formas de conexión se utilizan los dispositivos Olt y ONU.

Por otro lado, la información recaudada demuestra 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 del sistema mediante la introducción de virus, troyanos, gusanos, etc. Resultados que se corresponden con los estudios de Bejarano (2017), quien alude que, estos son los riesgos más frecuentes de un sistema de seguridad vulnerable. Particularmente Bejarano (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, aplicaciones y equipos de cómputo o partes de estos.

Los ataques recibidos se consideran de frecuencia media con un impacto entre medio y bajo, siendo los de mayor frecuencia los de tipo DDoS y los Spam en ese orden; debido en gran medida a la no existencia de un modelo de seguridad profundo estructurado en capas que permita un mejor filtrado de la información y con ello evitar los ataques por este concepto. Estos ataques pretenden 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. Estos resultados se corresponden con los de Bejarano (2017), quien determinó la frecuencia de la ocurrencia de DDoS en el 68% de los ataques a la red. En tal sentido Pisano (2018), considera 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.

Mediante el análisis de la información obtenida se determinó que el firewall de Mikrotik es utilizado por el 100% de las empresas dada por su flexibilidad para la configuración, aunque no es el de más fácil administración; en tal sentido Tam, 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 una más eficiente visualización del funcionamiento de los dispositivos de red en tiempo real.

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

De igual forma los estudios de Olifer & Olifer (2009); y Bejarano (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.

Asimismo, la información recaudada evidencia que se produce demora en el tiempo de recuperación después de un ataque DDoS, lo que ocasiona retraso en el cumplimiento de las obligaciones contractuales y pérdida de oportunidades en la gestión empresarial u organizacional. En este sentido, CISCO Systems (2013), estima 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 en un breve tiempo la recuperación y la rápida activación y puesta en función de los servicios solicitados por los clientes y para el óptimo desempeño empresarial.

Los usuarios de Internet en el Cantón Pasaje emplean con mayor frecuencia los servicios de redes sociales, correo electrónico y telefonía móvil, la gestión empresarial y el consumo de vídeos, Resultados que se corresponden con los datos ofrecidos por Cuzme (2015), quien considera que aún todas las potencialidades tecnológicas que brinda Internet no son aprovechadas en función de la llamada Internet de las Cosas, lo que requiere además de las políticas de organismos nacionales e internacionales generadas en ese sentido, de la voluntad de los ISP y los usuarios (empresas y población) mediada por el conocimiento de su utilidad.

CONCLUSIONES

Del análisis y discusión de los resultados se pude concluir que la conectividad a Internet en el Cantón pasaje se caracteriza por contar con 12 ISP y 3968 empresas y usuarios naturales, esta última cifra con tendencia a seguir incrementando como en los últimos cinco años; cada cliente cuenta con una velocidad promedio entre 3.5 y 5 megas. Las vías utilizadas para las conexiones son en primer lugar los cables de fibra óptica, seguida por las líneas de cobre para la conexión de los domicilios cuentan con teléfono fijo y donde no llega la fibra óptica; también, se utiliza la Wi-Fi y en menor medida la vía satelital. Se utilizan dispositivos como modem, Olt y ONU en correspondencia con los conectores empleados.

Es significativo el cumplimiento por parte de todos los ISP de las regulaciones y normas establecidas por el Estado para la seguridad de las conexiones a Internet, 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 los modelos de seguridad profunda por capas, como el diseñado por la Organización Internacional para Normalización. Se producen ataques de niveles de frecuencia e impacto entre medios y bajos, lo que evidencia la existencia de "huecos en la red" a través de los cuales se introducen 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.

Las vulnerabilidades más frecuentes son los ataques de tipo DDos y los Spam, que ocasionan el desbordamiento de la capacidad de los ruters, causando demora en el tiempo de respuestas a las necesidades de los usuarios, situación que se agrava por el tiempo de recuperación, que se encuentra entre 30 y 60 minutos, produciendo dilatación en los servicios a los clientes, obstaculizando la gestión empresarial u organizacional y el incumplimiento de las obligaciones contractuales.

Los servicios de Internet que prestan los ISP en el Cantón Pasaje aún se corresponden con los de la etapa de "Experiencias Cooperativas" fundamentada en el empleo de las redes sociales, los servicios de vídeo, la gestión empresarial y el uso de la nube como proveedora de información, pues a pesar del consumo de los servicios de telefonía móvil (smartphones) todavía son insipientes los servicios del Internet de las Cosas.

REFERENCIAS BIBLIOGRÁFICAS

Abbes, T., Bouhoula, A., & Rusinowitch, M. (2017). Detection of firewall configuration errors with updatable tree. ***International Journal of Information Security***, 15(3), 301–317.

Bailey, M., Oberheide, J., Andersen, J., Mao, Z. M., Jahanian, F., & Nazario, J. (2007, septiembre). Clasificación y análisis automatizados de malware de Internet. En, ***Taller internacional sobre avances recientes en la detección de intrusiones.*** (pp. 178-197). Springer.

Barber, B. R., Batlle, A., & Borge, R. (2014). ***Internet, Derecho y Política: Las transformaciones del Derecho y la Política***. Editorial UOC, S.L.

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

Berners-Lee, T., Caillau, R., Groff, J-F. & Pollerman, B. (1992). World-Wide Web: The Information Universe, Electronic Networkin*. Research, Applications and Policy, (1)*2.

Borgia, E. (2014). La visión de Internet de las cosas: características clave, aplicaciones y problemas abiertos. *Comunicaciones informáticas , 54* , 1-31.

CISCO Systems (2013). *Informe Anual de Seguridad de Cisco 2013*. https://www.cisco.com/c/dam/global/es_es/assets/pdf/Cisco_ASR_2012_v2_020813.pdf

Cuzme, R. F. (2015). *El Internet de las Cosas y las consideraciones de seguridad*. (Tesis de Maestría). Pontificia Universidad Católica de Ecuador.

Ecuador. Ministerio de Telecomunicaciones de la Sociedad de la Información (2019). *Libro Blanco de territorios digitales en Ecuador*. Ministerio de Telecomunicaciones de la Sociedad de la Información.

Espinoza Freire, E. E., & Toscano Ruíz, D. F. (2015). Metodología de investigación educativa y técnica. Ediciones UTMach. Universidad Técnica de Machala.

García García, E. (2019). *Análisis de la transmisión de datos y seguridad de la red de proveedor* de Internet en la empresa Cybermar en el Recinto Mata de Cacao. (Tesis de titulación). Universidad Técnica de Babahoyo.

García Roque, D. I., Sosa López, D., & Prieto Santana, B. (2020). ATEL, agente de telecomunicaciones. Una experiencia digital. *Sociedad & Tecnología*, *3*(1), 24–28.

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

Piñero Jiménez, D., & Rodríguez Suárez, Y. (2020). Procesos estratégicos y claves de la ECOING 12 utilizando las tecnologías BPM. *Sociedad & Tecnología*, *3*(2), 27–33.

Pisano, A. (2018). *Internet de las Cosas.* (Tesis de maestría en Gestión de Servicios Tecnológicos y de Telecomunicaciones). Universidad San Andrés.

Ramírez, A. (2015). Desde la conectividad hasta la Internet de Todo (IdT). Universidad San Ignacio de Loyola. *Revista de la Facultad de Ingeniería de la USIL Saber y Hacer*, 2(1), 19-31.

Román, R., Zhou, J., & López, J. (2013). Sobre las características y desafíos de la seguridad y la privacidad en el Internet distribuido de las cosas. *Redes informáticas, 57* (10), 2266-2279.

Tam, K., Hoz Salvador, M. H., Mcalpine, K., Basile, R., Matsugu, B., & More, J. (2015). *Seguridad UTM con Fortinet: Dominando FortiOS*. Elsevier.

Torres, J., &Vila-Viñas, D. (2015). Conectividad. Accesibilidad, soberanía y autogestión de las infraestructuras de comunicación. En, D., Vila-Viñas, y X. E., Barandiaran (Editores), *Buen Conocer - FLOK Society*. (pp. 7181-718). Editorial IAEN / Editorial CIESPAL.