UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ESTUDIO DE FACTIBILIDAD PARA LA IMPLEMENTACIÓN DEL PROTOCOLO DE RED DE CAPA DE TRANSPORTE DNS-OVER-QUIC (DOQ) EN LA UNIVERSIDAD TÉCNICA DE BABAHOYO

ESTUDIANTE:

JEFFERSON JESÚS CAICEDO PAREDES

TUTOR:

ING. WELLINGTON MALIZA CRUZ

AÑO 2022

Planteamiento del Problema

Desde la primera vez que se introdujo el protocolo DNS (Sistema de Nombres de Dominio conocido en inglés como, Domain Name System) en el año 1983, con la finalidad de reemplazar el antiguo método mantenido por la Stanford Research Institute (SRI). El cual almacenaba en un archivo HOSTS todos los nombres de los servidores conectados a internet, método que a medida que se expandía la red, almacenar los nombres en el archivo HOSTS no resultaba conveniente.

Motivo por el cual el sistema DNS llegó para traducir las consultas del usuario, indexando el nombre de dominio con su respectiva dirección IP del servidor.

Sin embargo, las consultas que se realizan a través de internet viajan en texto plano, es decir, no van cifradas y esto implica una falta de seguridad y privacidad de los usuarios en línea. Porque pueden ser víctimas de ataques que operan en la red como typosquatting, secuestro de registros e intoxicación de caché. Desafortunadamente muchas personas se ven afectadas por estas amenazas conocidas también como DNS hijacking.

Eventualmente han ido surgiendo lo que conocemos ahora con el término protocolo de seguridad DNS, cuya función es implementar seguridad al sistema de nombres de dominio DNS encriptando el tráfico DNS del usuario dependiendo del protocolo que se utilice.

Hay diversos protocolos de seguridad DNS, pero los que hoy en día predominan en internet son: DNS-over-HTTPS (DoH) e igualmente DNS-over-TLS (DoT) que hacen uso del protocolo de transporte TCP aprovechando las capas de seguridad de los protocolos HTTPS y TLS para su encriptación. Así mismo DNSCrypt que funciona sobre TCP y UDP implementando seguridad con algoritmo de cifrado y, por último, DNS-over-QUIC (DoQ) el cual hace hincapié en la (relativamente) nueva tecnología QUIC que trabaja sobre el protocolo de transporte UDP.

Debido a que el protocolo de seguridad DNS-over-QUIC (DoQ) se estandarizó oficialmente en mayo de 2021, su adopción en los diferentes servidores DNS públicos de empresas que ofertan su servicio a nivel global es casi nula. No obstante, Google que en un principio desarrolló e implementó la tecnología QUIC en su navegador Google Chrome, posteriormente uniéndose navegadores como Microsoft Edge y Mozilla Firefox (Isaiah, 2020). Fue el comienzo para que la IETF se interesara en QUIC y estandarizaran su versión abriendo la posibilidad a que los principales servidores DNS públicos oferten DNS-over-QUIC (DoQ) en el tiempo que crean pertinente.

A pesar de que DNS-over-QUIC (DoQ) fue estandarizado en 2021, AdGuard, la empresa experta en el bloqueo de publicidad ya había implementado el protocolo en sus servidores DNS públicos desde 2020 ofreciendo así un protocolo de seguridad DNS rápido, seguro y privado (Bagirov, 2020) que cualquier persona puede usar con el software de la empresa u optar por realizarlo manualmente a través de la dirección Upstream DNS: quic://dns.adguard.com.

En este sentido, la creciente aplicación del protocolo no ira sino solo hacia arriba. Por ende, utilizar el protocolo DNS-over-QUIC (DoQ) ayudará a solucionar los problemas que tienen los demás protocolos como DNS-over-HTTPS (DoH), DNS-over-TLS (DoT) y DNSCrypt que al ejecutarse sobre TCP y enviar los paquetes, estos se envían en orden de llegada (RTT) lo que provoca retrasos cuando se sufre la pérdida de un paquete o se realizan varias consultas a la vez. Además de las dificultades que implica la migración de conexiones en TCP.

Abordar todos estos problemas gracias al protocolo DNS-over-QUIC (DoQ) contribuirá a nuestra privacidad, nos mantendrá seguros y nos dará la posibilidad de mejorar la velocidad al navegar por internet.

Justificación

Proteger la privacidad y seguridad cuando realizamos consultas en internet a través de un cliente web es nuestra responsabilidad. En este sentido, mediante la adquisición de conocimiento y posterior evaluación del protocolo DNS seguro DNS-over-QUIC (DoQ). Se anhela demostrar los beneficios que posee y el cómo resuelve los problemas generales que tienen los demás protocolos de seguridad a nivel de DNS como DNS-over-HTTPS (DoH), DNS-over-TLS (DoT) y DNSCrypt.

En adición a lo escrito anteriormente y por medio de los resultados obtenidos del presente estudio de caso. Se prevé determinar la factibilidad que conlleva la implementación del protocolo de seguridad DNS en la Universidad Técnica de Babahoyo, siendo la entidad académica de nivel superior la principal beneficiaria al aportar mejoras de seguridad, velocidad y privacidad en la red a sus estudiantes, docentes y personal administrativo.

Por último, este proyecto de titulación cumple con la finalidad de aportar conocimiento e información de las nuevas tendencias tecnológicas de seguridad que funcionan en la red. Así como la oportunidad de ofrecer alternativas a protocolos recientemente estandarizados y medir en lo posible su aplicación hacia la práctica.

Objetivos

Objetivo General

Determinar la factibilidad del protocolo de red de capa de transporte DNS-over-QUIC (DoQ) para su implementación en la Universidad Técnica de Babahoyo.

Objetivos Específicos

- Analizar la información relacionada con DNS y el protocolo DNS-over-QUIC (DoQ).
- Describir los resultados obtenidos en base a las técnicas aplicadas al caso de estudio.
- Evaluar mediante el desarrollo de la investigación la usabilidad del protocolo DNS-over-QUIC (DoQ).

Línea de Investigación

La línea de investigación del cual se inicia para el desarrollo del caso de estudio es sistemas de información, y comunicación, emprendimiento e innovación. Así mismo, la sublínea de investigación es redes y tecnologías inteligentes de hardware y software.

En relación a las líneas de investigación planteadas anteriormente, el tema a desarrollar del caso de estudio abarca el conocimiento de tecnologías a nivel de red. Una de las cuales es el modelo de interconexión de sistemas abiertos (OSI) que parte como un modelo de referencia para los protocolos de red que permiten la comunicación universal entre las redes de ordenadores. En este caso, vinculado con la familia de protocolos de seguridad a nivel de DNS.

Marco Conceptual

La Universidad Técnica de Babahoyo ubicada en la Av. Universitaria Km 21/2 Av. Montalvo es una institución académica de nivel superior que tiene como propósito generar, aplicar y difundir la formación del talento humano a través del ejercicio docente, la investigación y la vinculación con la comunidad. (UniCarrera, s.f.)

La red de la entidad académica funciona a través de una topología anillo, actualmente construida en un 80% con cable de fibra óptica y 20% con cable de cobre. El proveedor de servicios de internet (ISP) que oferta conexión de internet a la universidad es la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA) que proporciona 2.1 GB de conexión a internet, los cuales se encuentran distribuidos entre la entidad principal y las sucursales extensión Quevedo y Agronomía conectadas por medio de radioenlace punto a punto.

En términos de seguridad en la red, el ISP proporciona un firewall externo para cubrir la protección a nivel de red. No obstante, la Universidad Técnica de Babahoyo opera a nivel de resolución de consultas de dominio DNS con los servidores DNS de Google.

Un sistema de nombres de dominio (DNS) sirve para traducir dominios en direcciones de Protocolo de Internet (IP). Todo dispositivo que disponga de una conexión a internet tiene una dirección IP pública exclusiva que sirve como un identificador. Cualquier equipo puede hacer uso de la IP para localizarlo y establecer una comunicación a través de la red. Conocido universalmente como el directorio telefónico de internet, los servidores DNS facilitan la vida del usuario al no tener que memorizar una sucesión de números administrado por el sistema de redireccionamiento IPv4: 192.168.1.1 (dirección IP privada predeterminada en la mayoría de routers) o el nuevo sistema de redireccionamiento que además de números contiene caracteres alfanuméricos IPv6: 2400:cb00:2048:1::c629:d7a2. (Cloudflare, s.f.)

En este sentido, cuando los usuarios quieren visitar un sitio web en internet necesitan introducir un nombre de dominio que identifica el sitio al cual desean ingresar (como facebook.com). Inicialmente nuestro ordenador verifica si la dirección IP en relación a dicho dominio se encuentra almacenada en el archivo HOSTS o en la caché DNS. Si no es el caso, el ordenador enviará automáticamente la consulta de dominio DNS del usuario a una red de 4 servidores DNS (recursor de DNS, DNS root server, servidor de nombres TLD y servidor de nombres autoritativo) que interactúan entre sí para obtener la dirección IP entendible para el dispositivo (en este caso 31.13.71.36 [IPv4]) que hace referencia al dominio correspondiente.

Debido a que el sistema DNS por defecto no proporciona seguridad en las consultas que se realizan a través de un cliente web, solo era cuestión de tiempo para que personas con malas intenciones aprovechen las vulnerabilidades a nivel de red. En este caso vulnerabilidades que involucran al sistema de nombres de dominio DNS. Generalmente las personas involucradas tienen conocimientos acerca de la tecnología y el cómo se implementa, conocidos como Hackers, Script Kiddies, Cracker, Lamer, Phreakers, etcétera. Cada nombre se encuentra relacionado con el procedimiento antiético que realizan.

A continuación, se describen las principales vulnerabilidades de seguridad a nivel de DNS que constantemente son explotadas perjudicando a los usuarios:

Suplantación de DNS

La suplantación de DNS (o conocido en inglés como DNS Spoofing) consiste en engañar al usuario resolviendo un nombre de dominio con una dirección IP falsa que afirma ser la original. Esta técnica de hacking se puede realizar de varios métodos, pero los más usados son:

- **Man In The Middle (MITM):** conocido en español como un ataque de intermediario, es un término general utilizado para definir cuando un perpetrador se posiciona en una conversación entre un usuario y una aplicación, ya sea para espiar o hacerse

pasar por una de las partes, haciendo parecer un intercambio normal de información. (Imperva, s.f.)

- **Servidor DNS comprometido:** En términos simples se trata de secuestrar el servidor DNS e inyectar direcciones IP maliciosas a la petición del usuario para enviarlo a un sitio web que no es el original.

Ataques de denegación de servicio (DoS)

Un ataque DoS (Denial of Service) consiste en hacer completamente inaccesible un sistema de ordenadores, un servicio o recurso de la víctima.

De acuerdo con Murillo (2020), menciona que “el ataque de denegación de servicio normalmente busca la pérdida de la conectividad con la red donde se encuentran estos recursos, bien por un consumo excesivo del ancho de banda o sobrecarga del sistema atacado”.

Una extensión de un ataque DoS es el ataque de denegación de servicio distribuidos (DDoS) que a diferencia de DoS que genera cantidades masivas de peticiones a través de una dirección IP al objetivo de la víctima. El ataque DDoS consiste en realizar la misma acción, pero a través de diferentes IP (conocidos como bots) que se encuentran en ordenadores alrededor del mundo.

Packet Sniffing

El escaneo de paquetes a nivel de red puede incurrir en problemas graves de seguridad debido a que se puede interceptar varios o todo el paquete que contiene una consulta enviada por el DNS. Además, la información de la consulta va en texto plano sin firmar ni cifrar y sin autenticado, esto hace que sea fácil su manipulación.

Desde el punto de vista de (Ariyapperuma & Mitchell, 2007), indican que “al capturar los paquetes de consulta del DNS, se puede generar una respuesta errónea lo

suficientemente rápido como para llegar al solucionador recursivo antes que la respuesta correcta del servidor de nombres DNS. Comprometer un router en una red de tránsito permite a un atacante capturar el paquete de respuesta DNS del servidor de nombres y modificarlo". (pp. 335-342)

Typosquatting

Un ataque typosquatting, también llamado URL hijacking o fake URL es similar a la suplantación de DNS. Sin embargo, estos ataques se cometen principalmente por error del ser humano, debido a que el usuario ingresa un dominio con un error de ortografía en la barra de direcciones del cliente web e inmediatamente se realizará una consulta DNS hacia el dominio mal escrito registrado por el atacante y solo será cuestión de realizar un ataque de ingeniería social (phishing) hacia la víctima.

Tal y como se mencionó anteriormente, un atacante registra legalmente un dominio con un error ortográfico común para realizar el engaño ej. facebook.com (original), ffacebook.com (falso). Afortunadamente existen herramientas como dnstwist que escanean dominios falsos que pueden llegar a incurrir en ataques de phishing, fraude y espionaje corporativo. (EsGeeks, s.f.)

Seguridad DNS

Inicialmente se pensó en un método que adicione seguridad al sistema de nombres de dominio (DNS) y a raíz de la problemática se desarrolló el método de seguridad DNSSEC.

El acrónimo DNSSEC hace referencia a Domain Name System Security Extensions (conocida por su traducción en español como Extensiones de Seguridad para el Sistema de Nombres de Dominio). Es una capa de seguridad que figura como una extensión del servicio DNS añadiendo métodos de autenticación que benefician la integridad de los datos e impiden la posibilidad de realizar ataques de suplantación o falsificación. (INCIBE, 2019)

DNSSEC crea un seguro sistema de nombres de dominio al agregar firmas criptográficas asimétricas a los registros DNS existentes. Estas firmas digitales se almacenan en servidores de nombres DNS junto con tipos de registros comunes, tales como A, AAAA, MX, CNAME, etc. De esta manera se verifica que la consulta este firmada por un servidor de nombres autoritativo original. (Cloudflare, s.f.)

DNSSEC utiliza el método de clave pública basado en dos claves distintas, una pública que, como su nombre indica, es de dominio público, y otra privada, que únicamente debe conocer su propietario. Mediante el uso de las claves y las firmas generadas a partir de ellas, se puede saber si un mensaje ha sido modificado o no, permitiendo así garantizar la integridad y autenticidad del mensaje. (INCIBE, 2019)

Protocolos de seguridad DNS

Los servidores DNS de Google que utiliza la Universidad Técnica de Babahoyo adicionan seguridad en las consultas de dominio DNS bajo los protocolos que se ejecutan en la capa de transporte del modelo OSI a través de TCP o UDP, los cuales son DNS-over-HTTPS (DoH) y DNS-over-TLS (DoT). Adicional a los dos protocolos descritos anteriormente existen también los protocolos DNSCrypt y DNS-over-QUIC (DoQ).

DNS-over-HTTPS (DoH)

DoH acrónimo para referirse a DNS-over-HTTPS es un protocolo seguro DNS con el objetivo de implementar seguridad por medio del protocolo de Transferencia de hipertexto (HTTPS) a las consultas DNS del usuario.

Como DoH utiliza la capa de seguridad del protocolo HTTPS este se ejecuta sobre el protocolo de transporte TCP en vez de una conexión UDP que es el medio general por el cual se envía información por internet. Así TCP permite establecer un intercambio de datos simultáneos por parte de los dos dispositivos involucrados aprovechando los beneficios que otorga TCP en la trasmisión de datos.

Como DoH funciona por medio del puerto (443) al igual que HTTPS esto incrementa la seguridad dado que las consultas se camuflan como un tráfico HTTPS normal y por ende garantiza que los atacantes no puedan falsificar o alterar el tráfico DNS. (Cloudflare, s.f.)

DNS-over-TLS (DoT)

A diferencia del protocolo DNS-over-HTTPS (DoH) apoyado por grandes empresas tecnológicas como Google, fundación Mozilla y otros proveedores de servidores privados (Digitalguide, 2020). DNS-over-TLS se encuentra defendida por la organización Internet Engineering Task Force (IETF).

Ahora bien, DoT se ejecuta en el puerto 853 creando un túnel TLS encriptado entre el cliente y el servidor. Después, a través de la utilización de certificados PKIX (Public Key Infrastructure X.509) basados en nombres de dominio es como se realiza la autenticación (Porro Sáez, 2019). Pero DoT podría considerarse un protocolo seguro, no tan seguro ya que en su aplicación plantea que se establece una única conexión y por ende un administrador de red podría ver las consultas DNS que se realizan. Como consecuencia, este protocolo de seguridad DNS está enfocado más al ámbito empresarial para monitorear de manera general actividades que se realicen en la internet.

Sin embargo, para hacer uso de DNS-over-TLS el software debe ser compatible tanto del lado del servidor como del cliente para ser funcional. Actualmente, hay varios proveedores de Internet que proporcionan los correspondientes servidores DNS. No obstante, el software requerido puede ser un resolutor de código auxiliar para establecer la conexión TLS. (Digitalguide, 2020)

DNSCrypt

DNSCrypt implementa seguridad al encriptar las consultas DNS a través de algoritmo de cifrado X25519 junto con EdDSA y XSalsa20-Poly1305 o XChaCha20-Poly1305. Su

utilización requiere de un software en el cliente para funcionar e igualmente estar soportado por los resolutores DNS públicos.

Su seguridad radica en la encriptación del tráfico DNS al utilizar HTTPS como método de envío. Motivo por el cual al igual que DNS-over-HTTPS, DNSCrypt se camufla en el tráfico HTTPS anonimizando las consultas de dominio DNS y proveyendo seguridad. Además, DNSCrypt se puede utilizar con los protocolos de transporte TCP y UDP al igual que convive en armonía con DNSSEC.

Sin embargo, el protocolo DNSCrypt nunca fue clasificado como un proyecto en la organización Internet Engineering Task Force (IETF) y, si bien encripta el tráfico DNS, no lo hace de extremo a extremo.

DNS-over-QUIC (DoQ)

El protocolo de transporte QUIC; siglas que hacen referencia a “Quick UDP Internet Connections” o en español “Conexiones UDP rápidas en Internet”. Comenzó con el diseño del ingeniero de software Jim Roskind en el año 2012 mientras era empleador de Google, ampliando su desarrollo en 2013 a los años siguientes.

DNS-over-QUIC se ejecuta en la capa de transporte UDP ofreciendo una mayor velocidad al enviar paquetes a través de una conexión multiplexada en un solo viaje de ida y vuelta (RTT). A diferencia de TPC que envía paquetes en orden de llegada lo que provoca retrasos si se sufre una pérdida de paquete o cuando se realizan varias consultas a la vez. Además, DoQ ofrece la posibilidad de migrar conexiones.

El protocolo fue estandarizado oficialmente en mayo del año 2021 lo que ha provocado su constante crecimiento llegando a ocupar el 7% del tráfico actual de internet antes de su estandarización y se mantiene en crecimiento. (Rüth, 2018)

Si bien DNS-over-QUIC continúa creciendo, todavía, las grandes empresas que proporcionan servidores DNS públicos como Google, Cloudflare, Cisco no han implementado DoQ como una alternativa de protocolo de seguridad DNS público en sus servidores. Actualmente los servidores públicos DNS de AdGuard ya tiene implementado DNS-over-QUIC desde diciembre de 2020 (Bagirov, 2020), uniéndose también el cortafuegos NextDNS. (NextDNS, s.f.)

Características DNS-over-QUIC

Handshake Delay

El protocolo QUIC realiza el Handshake TLS 1.3 mediante 1 sola negociación, lo que reduce a la típica Handshake TLS 1.3 de 2 veces que se realiza con TCP hacia el cliente y servidor. Esto no solo garantiza que la conexión esté siempre autenticada y cifrada, sino que también hace que el establecimiento de la conexión inicial sea más rápido.

Head-of-line Blocking Delay y Migración de conexiones

Gracias a HTTP/2 el usuario cuenta con la disponibilidad de realizar varias consultas a través de TCP, es decir, multiplexar las diferentes solicitudes HTTP ayuda a que se utilice mejor el ancho de banda de la red disponible (Ghedini, 2018). Sin embargo, cuando se produce una pérdida de paquete de datos, se crea un “bloqueo de cabeza de línea” que impide procesar los demás paquetes en cola. Por ende, se ralentiza la red al momento de realizar las solicitudes y respuestas.

QUIC implementa multiplexación a través de UDP con la ventaja de que los flujos de datos no se vean afectados si se incurre en una perdida, los demás paquetes de datos continuaran el camino hasta llegar a su objetivo, los paquetes perdidos de conexión se reanudaran y se enviaran de forma aleatoria.

Factibilidad Técnica

Se relacionan todos los componentes tecnológicos que incurren en la implementación del protocolo DNS-over-QUIC (DoQ) en la Universidad Técnica de Babahoyo.

Descripción	
Computadoras	HP
SO	Variable: Windows, Linux
Servidor	DNS

Elaborado por: Jefferson Caicedo

Nota: La aplicación para el requerimiento de un servidor DNS depende de la institución académica de nivel superior. Debido a que se puede adaptar la tecnología como más le beneficie para usar el protocolo seguro DoQ.

Factibilidad Económica

Debido a que DNS-over-QUIC (DoQ) es un protocolo de seguridad que funciona a nivel de DNS para proteger las consultas de dominio del usuario. Actualmente AdGuard es el único proveedor de servidores DNS públicos que cuentan con DNS-over-QUIC (DoQ). Por ende, cualquiera puede beneficiarse del mismo a través de los diferentes softwares comerciales y libres con los que cuenta la empresa.

No obstante, también se puede implementar manualmente para enviar las consultas de dominio y resolverlas a través de las direcciones de los servidores AdGuard: quic://dns.adguard.com [DoQ]

Tabla 2

Opción 1. Lista de costos que incurre la implementación del protocolo de seguridad DNS-over-QUIC (DoQ), además de la opción manual mediante un servidor DNS privado.

Software	Descripción	Precio
AdGuard Home.	Servicio DNS basado en red.	Gratis
Total		$0,00 dólares

Elaborado por: Jefferson Caicedo

Tabla 2.1

Opción 2. Lista de costos que incurre la implementación del protocolo de seguridad DNS-over-QUIC (DoQ), además de la opción manual mediante un servidor DNS privado.

Software	Descripción	Precio
AdGuard DNS (hoy por hoy, en fase beta).	Servicio DNS basado en la nube.	Gratis
Total		$0,00 dólares

Elaborado por: *Jefferson Caicedo*

Tabla 2.2

Opción 3. Lista de costos que incurre la implementación del protocolo de seguridad DNS-over-QUIC (DoQ), además de la opción manual mediante un servidor DNS privado.

Software	Descripción	Precio
AdGuard.	Ofrece funciones de seguridad web e intermediario con los servidores DNS públicos de la empresa AdGuard.	1 licencia vitalicia: $170,00 (9 dispositivos) **575 dispositivos (Uso Estudiantil y Administrativo) = 64 licencias**
Total		$10.880 dólares.

Elaborado por: Jefferson Caicedo

Los softwares que oferta AdGuard funcionan por medio de diferentes SO gratuitos o comercial, la instalación del mismo incurre en el tipo de SO que se encuentra implementado en los dispositivos informáticos de la Universidad Técnica de Babahoyo. Motivo por el cual la inversión inicial no toma en consideración el SO donde se ejecuta el software.

Factibilidad Operativa

De acuerdo con rvillarroel16 (2017), expresa que “la factibilidad operativa identifica si el proyecto puede ser operado a través de los recursos de la organización, además de los recursos que participaran en el proyecto. Busca la manera de tener la mejor disponibilidad del momento y lugar adecuado, cuando el proyecto se convierta en resultados”.

En este sentido, dado que el uso de DNS-over-QUIC (DoQ) funciona como un protocolo de seguridad a nivel de DNS para proteger las consultas de dominio que realiza el usuario. La Universidad Técnica de Babahoyo puede operar a través de los recursos del mismo.

Por otro lado, se identifican los siguientes recursos humanos que son necesarios:

Tabla 3

Recursos Humanos.

Cantidad	***Función***	***Cargo***
1	*Técnico; Programador*	*Personal técnico con conocimiento a nivel de red.*

Elaborado por: Jefferson Caicedo

Marco Metodológico

La necesidad de describir los beneficios y el continuo crecimiento del protocolo de seguridad DNS-over-QUIC (DoQ) utilizado para proteger las consultas de nombres de dominio que realiza el usuario al navegar por internet. Además de estimar el protocolo para su aplicación en la institución académica de nivel superior de la ciudad de Babahoyo, plantea el ambiente adecuado para enfrentar el presente estudio de caso con la investigación descriptiva.

A través del objetivo planteado del caso de estudio y enmarcado en una investigación descriptiva se prevé analizar la información referente al protocolo del tema investigativo delimitado a una población. Citando a Westreicher (2021), plantea que “la población objetivo es aquel grupo de personas que es de interés de los investigadores en un estudio estadístico, o que se ve (o se verá) afectado por un determinado proyecto”.

En este contexto la población objetivo del presente estudio de caso se encuentra delimitado a las personas que conforman el grupo académico referenciando los indicadores obtenidos desde la página de la Universidad Técnica de Babahoyo que son 461 docentes (titulares & no titulares) y 11.759 estudiantes. Sin embargo, se propuso realizar una muestra dado el tamaño de la población, el tiempo límite, la situación actual que pasa la ciudad de Babahoyo con los cambios meteorológicos y la pandemia COVID-19 que incurren en la falta de comunicación.

Motivo por el cual, la muestra se realizará de 125 personas del ámbito académico entre docentes y estudiantes a través de la aplicación web Google Forms (en español, Formularios de Google).

De igual importancia, se realizó una entrevista semiestructurada para recopilar información en relación a la estructura general de la red universitaria delimitado a personas claves con conocimiento y manejo de tecnología en la Universidad Técnica de Babahoyo.

Resultados

De acuerdo con los resultados obtenidos de la encuesta realizada (Ver anexo 2) delimitada a una muestra de 125 personas pertenecientes al ámbito académico entre ellos docentes y estudiantes de la Universidad Técnica de Babahoyo a través de la aplicación web Google Forms, se planteó 8 interrogantes con la finalidad de determinar el conocimiento y su pensar de los involucrados con relación al tema de investigación.

Manteniendo la objetividad, en la primera pregunta que involucra el conocimiento acerca del sistema de nombres de dominio (DNS) se obtuvo que 49.6% mantiene un claro entendimiento sobre un sistema DNS a diferencia del 33.6% y 16.8% que representan al no y un conocimiento vago del DNS. Sin embargo, en contraste con la siguiente pregunta el 45.6% de las personas no posee conocimiento sobre las amenazas existentes que perjudican a las consultas de nombres de dominio que realiza el usuario en internet y esto conlleva a que puedan ser víctimas de los conocidos ataques DNS hijacking. Un 28% se encuentra a salvo ya que comprenden los riesgos que implican las amenazas a nivel de DNS y un 26.4% podría no estar tan seguro al no comprender muy bien cómo funcionan este tipo de amenazas.

Igualmente, en la pegunta 3 de la encuesta realizada un 44.8% esta errada al pensar que el sistema DNS de manera predeterminada protege las consultas de nombres de dominio que realiza el usuario en internet a través de un cliente web. Debido a que desde su creación el sistema DNS envía dichas consultas en texto plano (sin seguridad), afortunadamente un 30.4% entiende lo antes mencionado y un 24.8% no cuenta con mucho conocimiento para determinar si la pregunta planteada es correcta o no. Por otro lado, un 57.6% opina que es recomendable implementar seguridad en las consultas de nombres de dominio, de tal manera que se mantienen a salvo de las amenazas existentes en la red en comparación con el 26.4% que no lo cree necesario y un 16% que muestra un interés parcial.

Llegando a la pregunta clave un 57.6% no cuenta con conocimiento acerca de los protocolos de comunicación DNS seguros, un grave problema ya que depende de dichos protocolos que el tráfico DNS se mantenga protegido de las amenazas DNS que existen en la red. No obstante, un 42.4% que representa a 53 personas, si entienden que sin los protocolos DNS seguros no obtendríamos mayor privacidad ni seguridad al realizar las consultas de dominio. En relación a ello el 86.8% de las 53 personas sabe sobre la existencia del protocolo de seguridad más común DNS-over-HTTPS (DoH) seguido del 71,7 con DNS-over-TLS (DoT) y curiosamente un 39.6% conoce el protocolo DNS-over-QUIC (DoQ) quedando atrás con menos de 33% DNSCrypt y DNS-over-DTLS.

Sin embargo, el 64% de las personas encuestadas a nivel general no sabe sobre la existencia del protocolo DNS-over-QUIC (DoQ). En base a estos resultados queda claro que el protocolo, aunque es relativamente nuevo no cuenta con una visualización notoria en el conocimiento de las personas. A diferencia de ello un 63.2% cree pertinente que se debería implementar el protocolo de comunicación DNS seguro DNS-over-QUIC (DoQ) para obtener así mejoras de velocidad, privacidad y seguridad en las consultas de nombres de dominio que realiza en usuario mientras esté conectado a la red de la Universidad Técnica de Babahoyo en comparación con el 8.8% que no lo considera una opción viable y un 28% que se muestra indiferente con la implementación.

Por último, en la entrevista realizada al personal objetivo del departamento de sistemas se pudo conocer el equipo con el que cuenta la institución académica de nivel superior e igualmente el funcionamiento general de la red resultando así en una posible adopción del protocolo DNS-over-QUIC (DoQ).

Discusión de Resultados

Mediante el análisis de contenido referente al marco conceptual del tema establecido en el estudio de caso, se expresa de manera congruente y objetiva en primer lugar el funcionamiento del sistema de nombres de dominio (DNS) raíz donde se ejecutan los protocolos de seguridad DNS que sirven para adicionar seguridad a las consultas de nombres de dominio que los usuarios realizan a través de internet, resultando así en una mayor privacidad.

Teniendo en cuenta que DNSSEC solo adiciona autenticación en las consultas de nombres de dominio ayudando a minimizar algunas amenazas que existen en internet, no es suficiente para tener una privacidad al 100%. Por ende, surgieron los protocolos de seguridad DNS siendo el más conocido DNS-over-HTTPS (DoH) seguido de DNS-over-TLS (DoT) y DNSCrypt.

Sin embargo, bajo la investigación realizada al protocolo de seguridad DNS-over-QUIC (DoQ) resaltando sus características se pudo obtener información acerca de los beneficios que aporta superando así a los protocolos ya conocidos DoH, DoT y DNSCrypt. Solucionando los problemas que tienen dichos protocolos debido a su implementación a través de TCP.

En este sentido la aplicación del protocolo de seguridad DNS; DNS-over-QUIC en la Universidad Técnica de Babahoyo ofrecerá todos los beneficios del protocolo al dirigir todas las consultas de nombres de dominio que se realicen en la red universitaria al servidor DNS de AdGuard, debido a que el mismo es actualmente el principal en proveer servidores DNS para la resolución de consultas de dominio con el protocolo seguro DNS-over-QUIC.

No obstante, la empresa AdGuard oferta diferentes softwares, siendo el más recomendable AdGuard DNS Home con el cual se podrá crear un servidor DNS privado para la resolución de consultas en la red universitaria proveyendo diferentes opciones como la

posibilidad de ver el tráfico DNS. Es decir, las consultas de dominio que realicen las demás personas que se encuentren en la red y limitando su contenido. Por supuesto debido a que el software es gratuito no se incurren en costos por parte de la universidad además de la política cero registros al utilizar los servidores DNS de AdGuard. Motivo por el cual se puede tener total seriedad al momento de utilizar dichos servidores. Por otro lado, mediante la factibilidad realizada tanto en la factibilidad técnica y operativa, la universidad tiene los recursos tecnológicos para aplicar la tecnología. Adicionalmente en la factibilidad económica surgen 4 variables disponibles para usar el protocolo DoQ.

La opción 1 (Tabla 2) y la más recomendable es la utilización de AdGuard DNS Home ya que crearemos un servidor DNS privado en la red y por ende al agregar todos los dispositivos en el software estos se beneficiarán del protocolo. La opción 2 (Tabla 2.1) es actualmente no recomendable ya que se encuentra en fase beta lo que significa que habrá errores en la utilización del mismo, pero no se cierra la posibilidad de que en un futuro sea estable y funcional. La opción 3 utiliza el software comercial de AdGuard por ende se debe realizar una inversión inicial (Tabla 2.2) que incurre en un gasto por parte de la Universidad.

La opción 4 es la manual ya que AdGuard proporciona las direcciones de los servidores DNS Upstream con los diferentes protocolos de seguridad DoH, DoT, DNSCrypt y DoQ. Solo será cuestión de utilizarlos en un servidor DNS privado para administrar las consultas de nombres de dominio con el protocolo DNS-over-QUIC.

Algo muy importante a tener en cuenta es que la Universidad Técnica de Babahoyo utiliza los servidores DNS de Google para manejar las consultas de dominio. Debido a que Google actualmente no proporciona el protocolo de seguridad DNS-over-QUIC, adaptar dicho protocolo en la red universitaria incurre en la necesidad de reemplazar los servidores DNS de Google con los servidores DNS de AdGuard que si oferta dicho protocolo. Por supuesto la realización del mismo se hará solo con el permiso de la universidad basada en su política.

Conclusiones

En este estudio de caso se logró comprender los beneficios que aporta el protocolo DNS-over-QUIC, que funciona en el sistema DNS adicionando velocidad, seguridad y privacidad cuando el usuario realiza consultas de nombres de dominio en la internet. Determinando así su funcionalidad, siendo mucho mejor que los protocolos DNS-over-HTTPS, DNS-over-TLS y DNSCrypt debido a que su ejecución en la capa de transporte UDP es superior a la capa TCP que es donde corren los 3 protocolos descritos anteriormente.

Por medio del análisis de factibilidad se determinó que el protocolo DNS-over-QUIC puede implementarse en la Universidad Técnica de Babahoyo por 4 variables distintas. Asimismo, como se explicó en la discusión de resultados la adopción del protocolo en la entidad académica de nivel superior es solamente y único privilegio de la misma decidir aplicar los cambios necesarios para la adopción del protocolo en la red universitaria, trayendo consigo los beneficios descritos en el primer párrafo para el personal administrativo e igualmente para los docentes y estudiantes que mostraron su entusiasmo mediante la encuesta realizada si se llegara a implementar el protocolo.

Recomendaciones

A través de la investigación que se llevó a cabo se pudo conocer el protocolo DNS-over-QUIC e igualmente evidenciar los beneficios del mismo. Sin embargo, se recomienda investigar más sobre dicho protocolo para enriquecer el conocimiento debido a la temprana edad que tiene desde su estandarización. Al mismo tiempo, nos damos cuenta que los protocolos de seguridad a nivel de DNS ayudan a combatir los ataques que diariamente se realizan en internet, de modo que al optar por aprender más sobre dichos protocolos y el cómo implementan seguridad, estaremos protegidos ya que conoceremos como enfrentar las amenazas y pon ende salvaguardar nuestra información personal.

Por otro lado, aunque el caso de estudio está enfocado en la factibilidad que conlleva su aplicación en la Universidad Técnica de Babahoyo, es recomendable utilizar dicho protocolo o cualquier otro que adicione seguridad y se ajuste a nuestras necesidades, para mantener seguras y privadas las consultas de nombres de dominio que realicemos en cualquier red a la cual estemos conectados.

Referencias

B., G. (9 de Febrero de 2022). *¿Qué es DNS y cómo funciona?* Recuperado el 13 de Marzo de 2022, de Hostinger: https://www.hostinger.es/tutoriales/que-es-dns

Bagirov, V. (15 de Diciembre de 2020). *AdGuard DNS-over-QUIC*. Obtenido de AdGuard: https://adguard.com/en/blog/dns-over-quic.html

Cloudflare. (s.f.). *¿Cómo funciona DNSSEC?* Recuperado el 14 de Marzo de 2022, de Cloudflare: https://www.cloudflare.com/es-la/dns/dnssec/how-dnssec-works/

Cloudflare. (s.f.). *DNS sobre TLS vs. DNS sobre HTTPS | DNS seguro*. Recuperado el 15 de Marzo de 2022, de Cloudflare: https://www.cloudflare.com/es-es/learning/dns/dns-over-tls/

Cloudflare. (s.f.). *What is DNS? | How DNS works*. Recuperado el 12 de Marzo de 2022, de Cloudflare: https://www.cloudflare.com/es-es/learning/dns/what-is-dns/

Cloudflare. (s.f.). *What Is The OSI Model?* Recuperado el 15 de Marzo de 2022, de Cloudflare: https://www.cloudflare.com/es-la/learning/ddos/glossary/open-systems-interconnection-model-osi/

Digitalguide. (9 de Julio de 2020). *DNS over HTTPS: más seguridad en la red*. Recuperado el 16 de Marzo de 2022, de IONOS: ionos.es/digitalguide/servidores/know-how/dns-over-https/

Digitalguide. (7 de Febrero de 2020). *DNS over TLS: un protocolo más seguro*. Recuperado el 16 de Marzo de 2020, de IONOS: https://www.ionos.es/digitalguide/servidores/seguridad/dns-over-tls/

EsGeeks. (s.f.). *TYPOSQUATTING: EXPLICACIÓN Y ESQUEMA DE ATAQUE PHISHING*. Recuperado el 14 de Marzo de 2022, de EsGeeks: https://esgeeks.com/typosquatting-ataque-hacking/

Ghedini, A. (26 de Julio de 2018). *The Road to QUIC*. Obtenido de Cloudflare: https://blog.cloudflare.com/the-road-to-quic/

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la Investigación* (Sexta ed.). México: McGraw Hill. Obtenido de https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Imperva. (s.f.). *Man in the middle (MITM) attack*. Recuperado el 14 de Marzo de 2022, de Imperva: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/

INCIBE. (11 de Julio de 2019). *DNSSEC, asegurando la integridad y autenticidad de tu dominio web*. Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/dnssec-asegurando-integridad-y-autenticidad-tu-dominio-web

Isaiah, M. (10 de Octubre de 2020). *Google Chrome browser is rolling out HTTP/3 via IETF QUIC*. Obtenido de TechSpot: https://www.techspot.com/news/87058-google-chrome-browser-rolling-out-http3-ietf-quic.html

Murillo, O. (5 de Noviembre de 2020). *¿Qué es una ataque de denegación de servicio (DoS)?* Obtenido de Sarenet: https://blog.sarenet.es/ataque-de-denegacion-de-servicio/

NextDNS. (s.f.). *What is DNS over TLS (DoT), DNS over Quic (DoQ) and DNS over HTTPS (DoH & DoH3)?* Recuperado el 16 de Marzo de 2022, de NextDNS: https://help.nextdns.io/t/x2hmvas/what-is-dns-over-tls-dot-dns-over-quic-doq-and-dns-over-https-doh-doh3

Porro Sáez, I. (4 de Julio de 2019). *Protege tus peticiones DNS con DNS over TLS*. Obtenido de INCIBE: https://www.incibe-cert.es/blog/protege-tus-peticiones-dns-dns-over-tls

Rüth, J. (15 de Mayo de 2018). *How much of the Internet is using QUIC?* Obtenido de APNIC: https://blog.apnic.net/2018/05/15/how-much-of-the-internet-is-using-quic/

rvillarroel16. (20 de Enero de 2017). *Factibilidad Operativa*. Obtenido de PORQUERIA: https://ingenieriadesoftwareutmachala.wordpress.com/2017/01/20/factibilidad-operativa/

Solano, J. (s.f.). *EL MODELO OSI*. Recuperado el 15 de Marzo de 2022, de Departamento de Informática y Sistemas | Web Personal: Juan Antº López Quesada: http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/index.html

UniCarrera. (s.f.). *Universidad Técnica de Babahoyo UTB*. Recuperado el 17 de Marzo de 2022, de UniCarrera: http://unicarrera.com/universidad/universidad-tecnica-de-babahoyo-utb/

Westreicher, G. (12 de Marzo de 2021). *Población objetivo*. Recuperado el 18 de Marzo de 2022, de Economipedia.com: https://economipedia.com/definiciones/poblacion-objetivo.html

Ariyapperuma, S., & Mitchell, C. J. (2007, April). Security vulnerabilities in DNS and DNSSEC. In *The Second International Conference on Availability, Reliability and Security (ARES'07)* (pp. 335-342). IEEE. Obtenido de https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.7046&rep=rep1&type=pdf

Kosek, M., Doan, T. V., Granderath, M., & Bajpai, V. (2022). One to Rule them All? A First Look at DNS over QUIC. *arXiv preprint arXiv:2202.02987*. Obtenido de https://arxiv.org/pdf/2202.02987.pdf

Batenburg, B. (2022). *Performance of DNS over QUIC* (Bachelor's thesis, University of Twente). Obtenido de http://essay.utwente.nl/89441/1/Batenburg_BA_eemcs.pdf

Langley, A., Riddoch, A., Wilk, A., Vicente, A., Krasic, C., Zhang, D., ... & Shi, Z. (2017, August). The quic transport protocol: Design and internet-scale deployment. In *Proceedings of the conference of the ACM special interest group on data communication* (pp. 183-196). Obtenido de https://dl.acm.org/doi/pdf/10.1145/3098822.3098842

Anexos

Anexo 1: Entrevista

Entrevista realizada al Ing. Luis Alberto Alcibar Torres, director del departamento de sistemas de la Universidad Técnica de Babahoyo.

Entrevistador: ¿Como está estructurada la red de la universidad Técnica de Babahoyo?

Entrevistado: La red está en una estructura anillo, en donde aquí, la estructura principal Data Center de donde llega la fibra óptica del proveedor de internet, un 80% está distribuida a cada departamento. En las sucursales como Agronomía y Extensión Quevedo que son la parte de los campos externos, el proveedor facilita un enlace de radio debido a la distancia y así mismo como está estructurada la red general, se encuentra estructurada la red de los campos. El 20% restante se maneja con cable de cobre hasta que se readecue la fibra con un proveedor externo para que el enlace sea con una capacidad de 10GB LAN a través de fibra.

Entrevistador: ¿Como se llama el ISP y cuál es la velocidad de internet que oferta?

Entrevistado: La empresa que oferta internet a la Universidad Técnica de Babahoyo se llama CEDIA (Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia), el cual proporciona 2.1GB de internet a partir de noviembre de 2021. 1.4GB se distribuye a en la universidad principal, 500 en la extensión Quevedo y Agropecuaria. CEDIA también le proporciona a la universidad varios servicios adicionales además de proporcionar conexiones de backup si se incurre en un fallo por parte de la red principal.

Entrevistador: Usted menciona que el ISP provee servicios adicionales, en esos servicios ¿Puede haber un servicio de seguridad a nivel de red?

Entrevistado: La red CEDIA tiene un firewall externo que proporciona seguridad a la red.

Entrevistador: ¿La Universidad Técnica de Babahoyo administra algún servidor DNS?

Entrevistado: La Universidad Técnica de Babahoyo administra un servidor DNS privado para manejar las consultas que contienen información de carácter sensible.

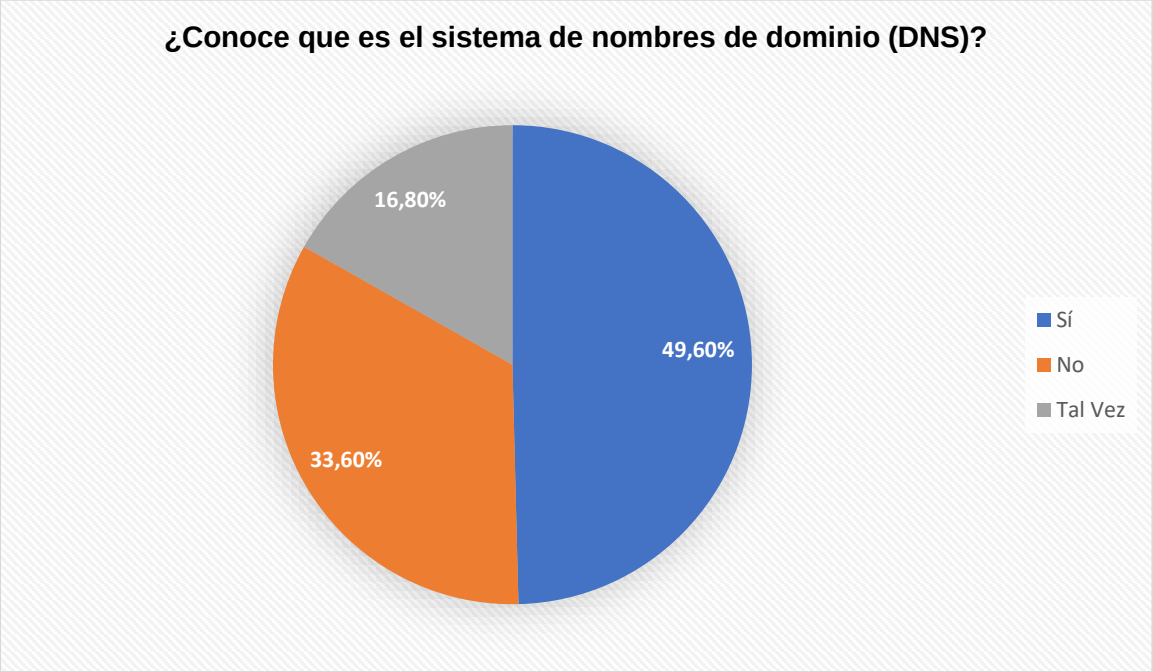
Entrevistador: ¿Cómo se divide el personal del departamento de sistemas?

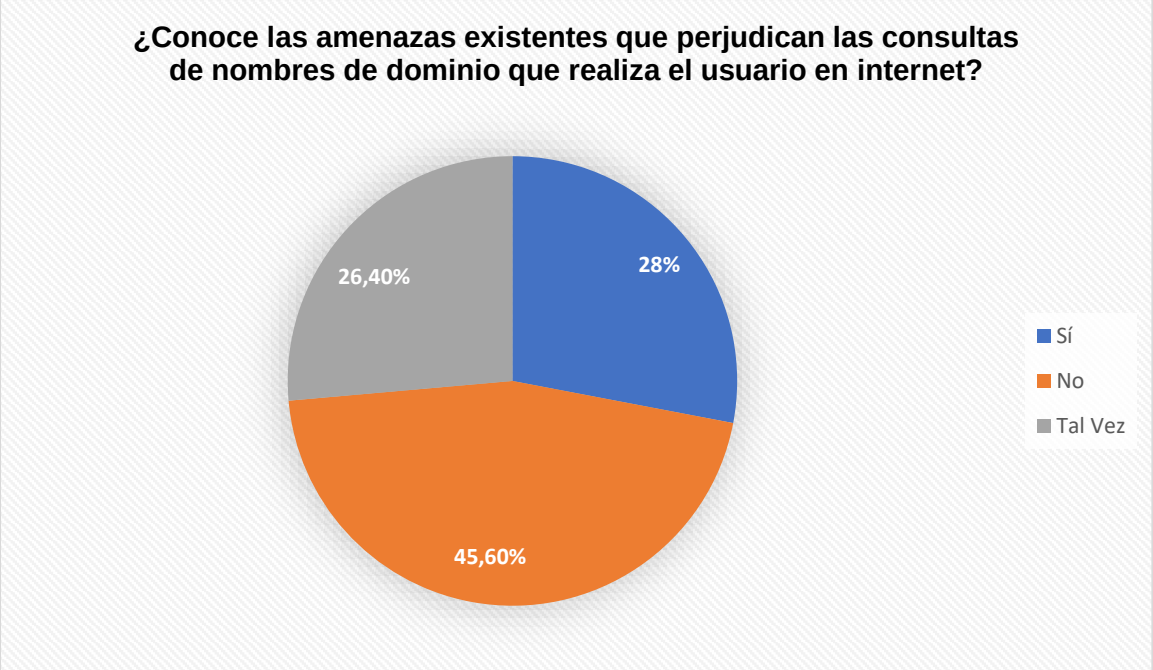
Entrevistado: El personal se divide en dos áreas, software y hardware. Por ende, existe personal a nivel técnico que resuelve los problemas relacionados con el hardware y el personal con conocimientos de programación al encargarse de la parte de software.

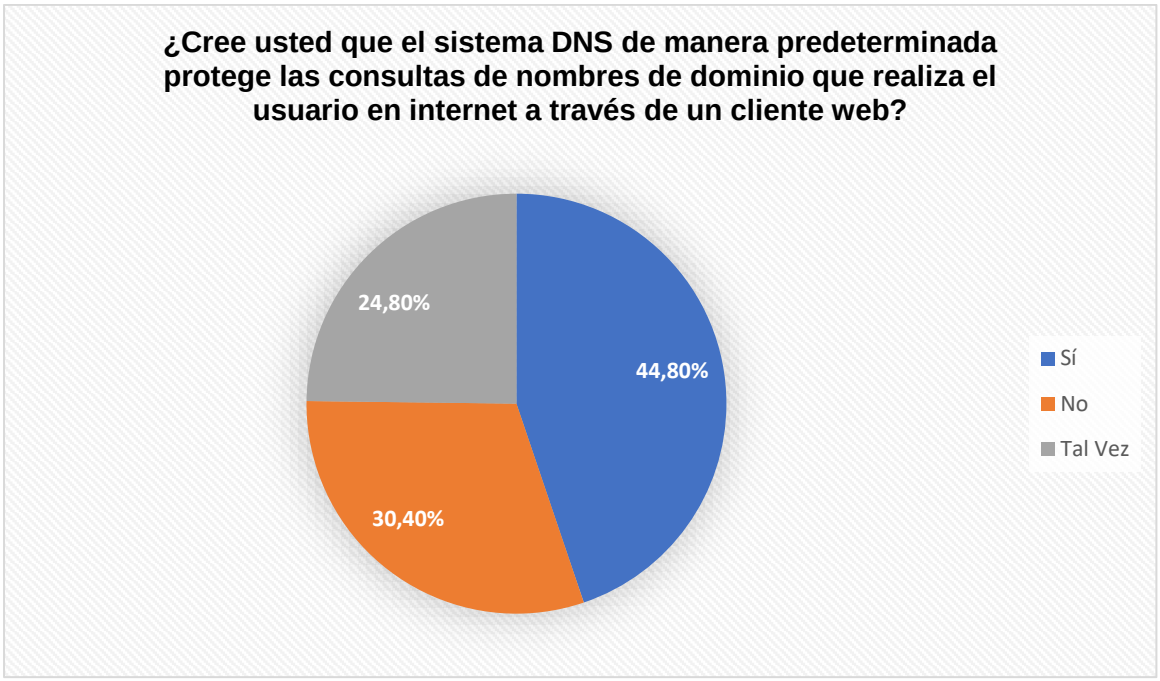
Entrevistador: ¿La Universidad Técnica de Babahoyo utiliza servidores DNS de alguna empresa?

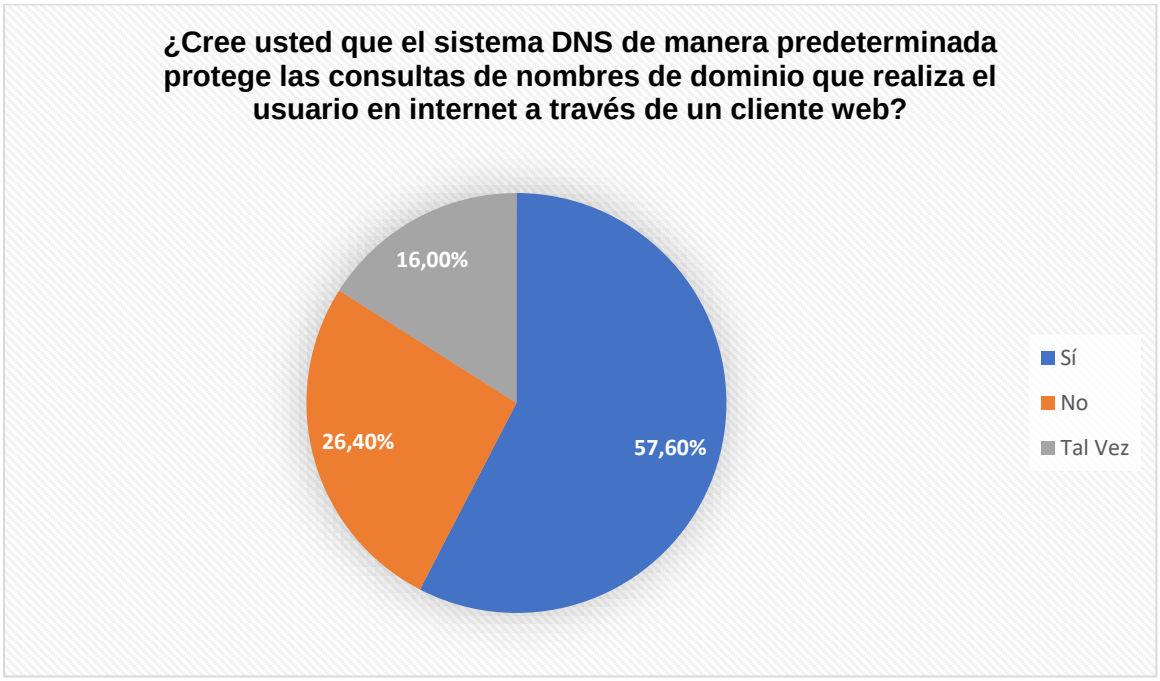
Entrevistado: Haciendo una búsqueda a través de una página web se pudo observar que la universidad resuelve las consultas de nombres de dominio (obviando el servidor DNS privado) con los servidores DNS de Google proporcionando seguridad DNS-over-HTTPS y DNS-over-TLS, protocolos que fueron adaptados por Google para proporcionar seguridad a nivel de DNS. Google también proporciona varios servicios a nivel académico para la universidad.

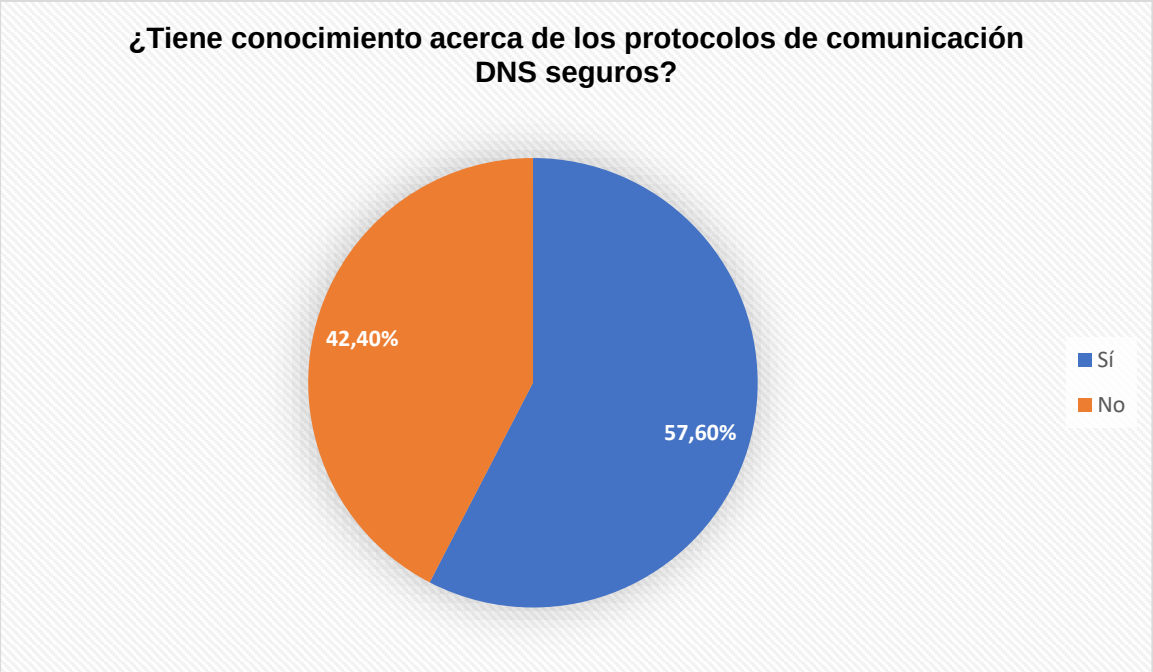
Anexo 2: Encuesta

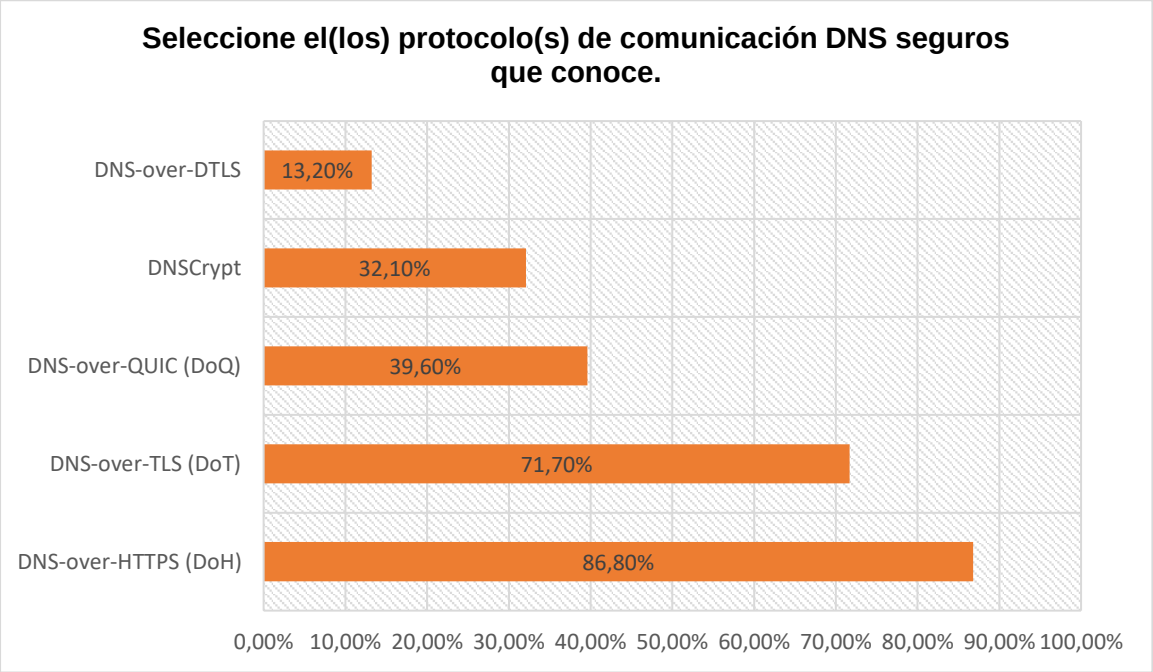


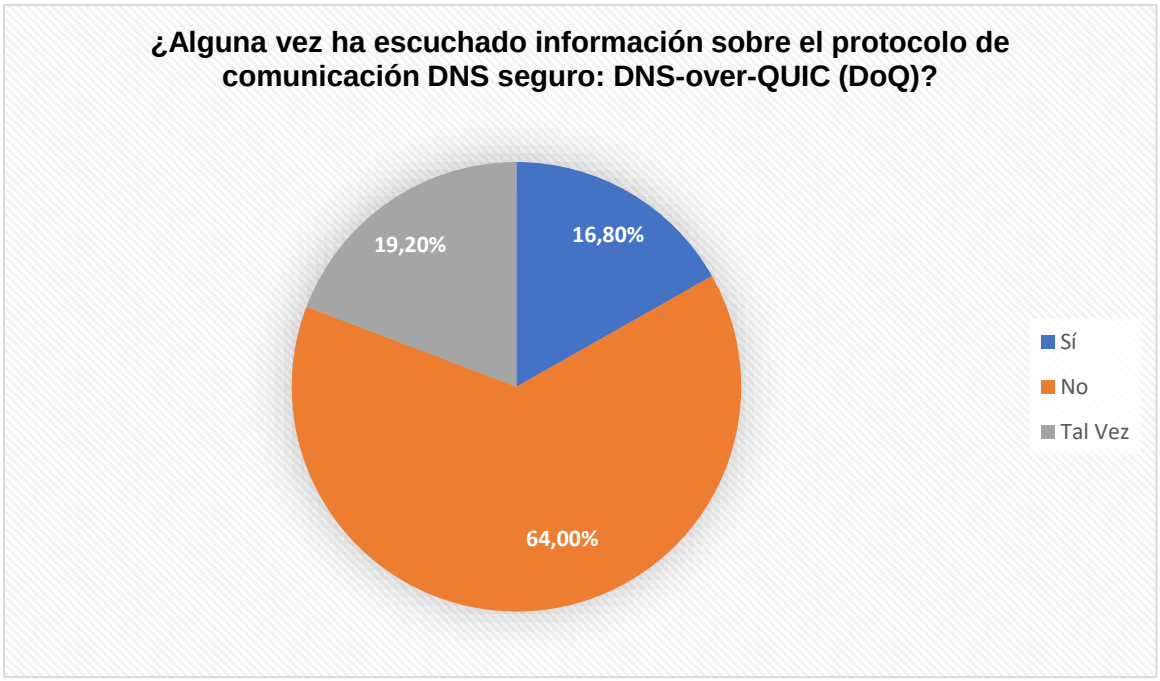


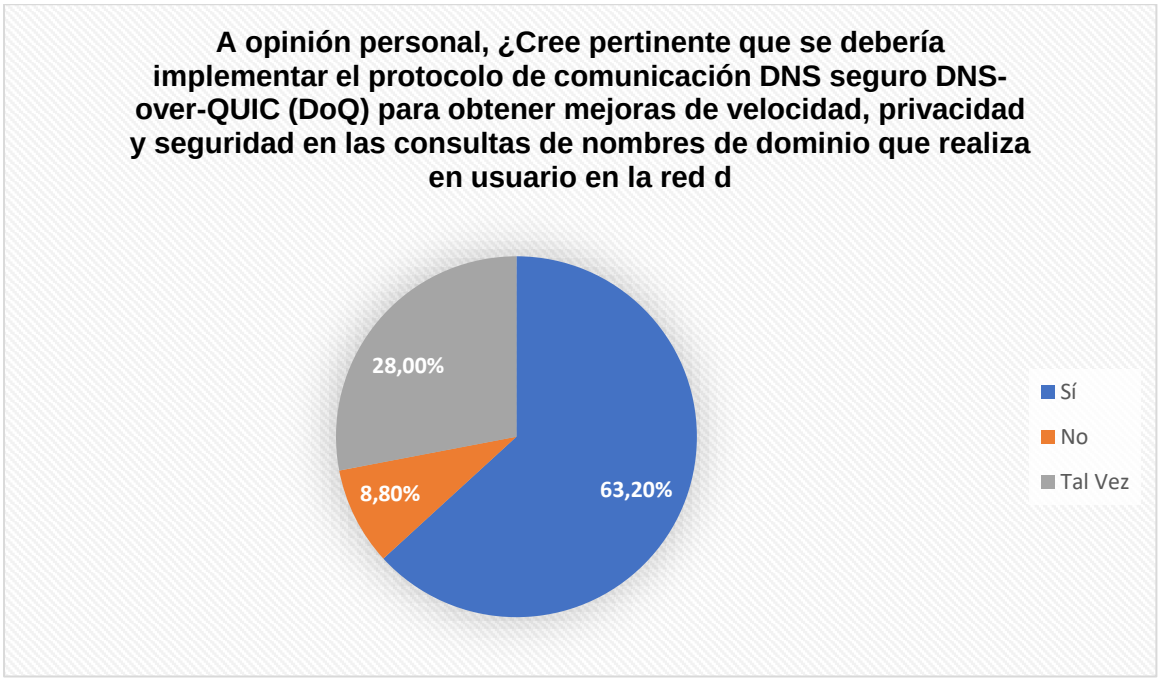

¿Cree usted que el sistema DNS de manera predeterminada protege las consultas de nombres de dominio que realiza el usuario en internet a través de un cliente web?
24,80%
44,80%
30,40%
Sí
No
Tal Vez


¿Cree usted que el sistema DNS de manera predeterminada protege las consultas de nombres de dominio que realiza el usuario en internet a través de un cliente web?
16,00%
26,40%
57,60%
Sí
No
Tal Vez


¿Tiene conocimiento acerca de los protocolos de comunicación DNS seguros?
42,40%
57,60%
Sí
No


Seleccione el(los) protocolo(s) de comunicación DNS seguros que conoce.
DNS-over-DTLS
13,20%
DNSCrypt
32,10%
DNS-over-QUIC (DoQ)
39,60%
DNS-over-TLS (DoT)
71,70%
DNS-over-HTTPS (DoH)
86,80%
0,00% 10,00% 20,00% 30,00% 40,00% 50,00% 60,00% 70,00% 80,00% 90,00% 100,00%

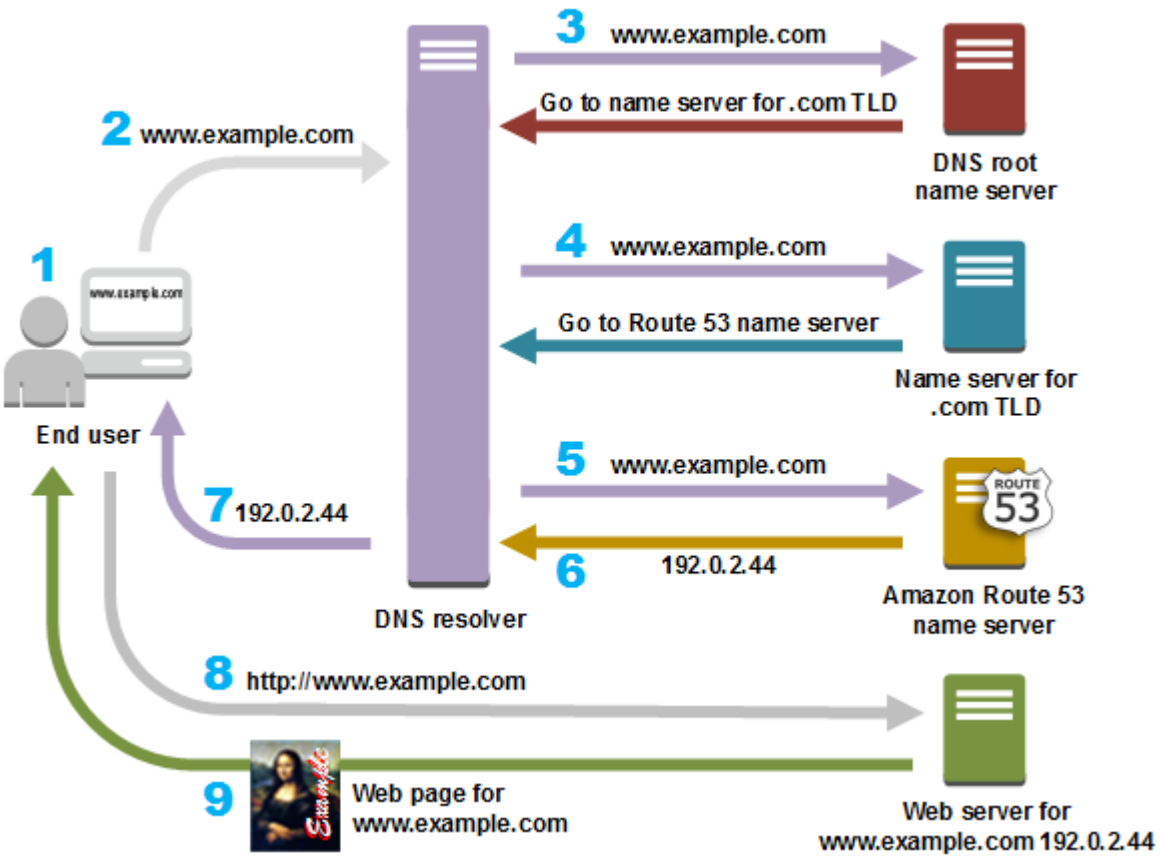

¿Alguna vez ha escuchado información sobre el protocolo de comunicación DNS seguro: DNS-over-QUIC (DoQ)?
16,80%
64,00%
19,20%
Sí
No
Tal Vez


A opinión personal, ¿Cree pertinente que se debería implementar el protocolo de comunicación DNS seguro DNS-over-QUIC (DoQ) para obtener mejoras de velocidad, privacidad y seguridad en las consultas de nombres de dominio que realiza en usuario en la red d
63,20%
8,80%
28,00%
Sí
No
Tal Vez

Anexo 3: Infografías – Marco Conceptual

Figura 1

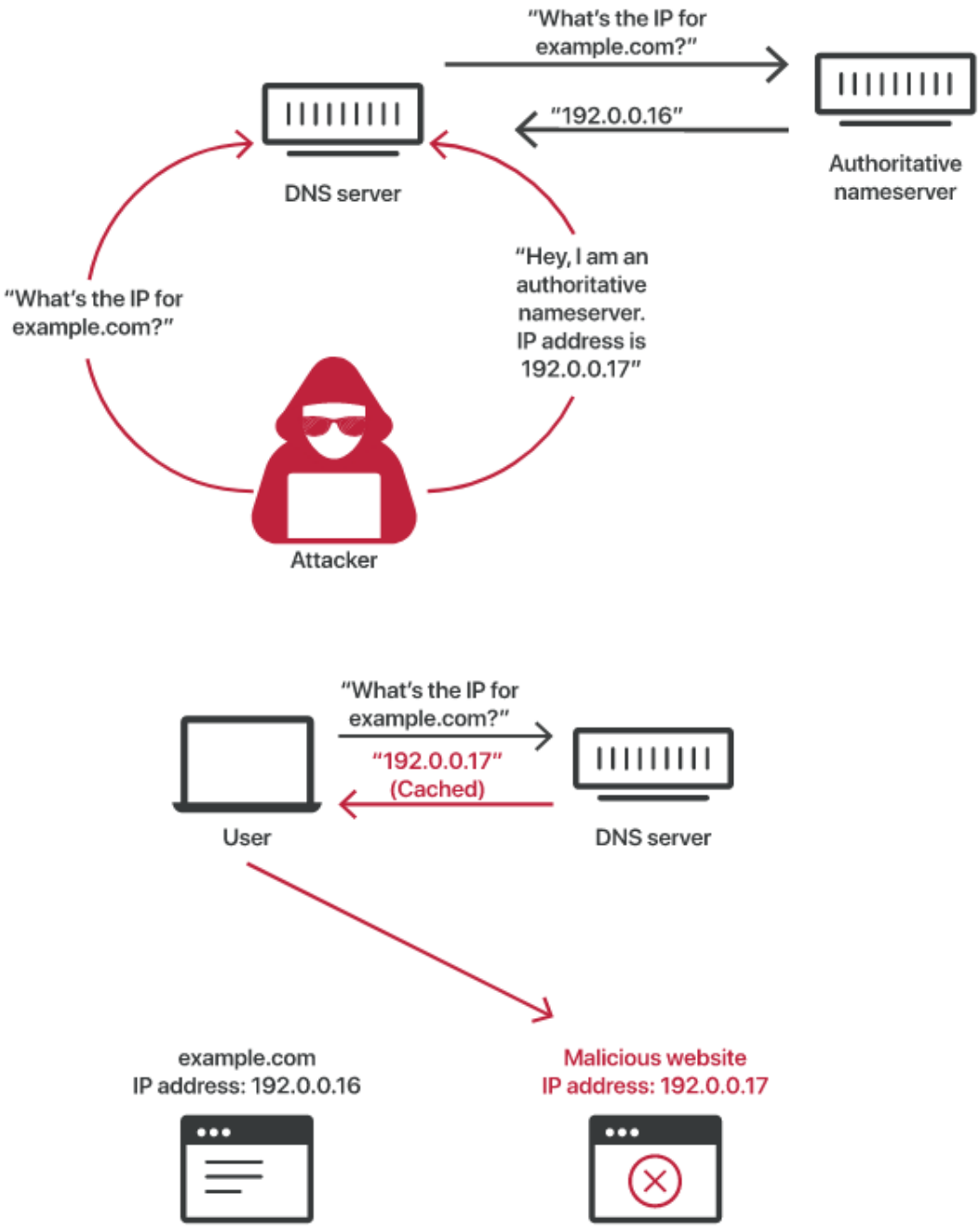
¿De qué manera un DNS dirige Tráfico hacia su Aplicación Web?



Nota. Tomada de *¿Qué es DNS?* [Infografía], Amazon Web Services, Inc., s.f., https://aws.amazon.com/es/route53/what-is-dns.

Figura 2

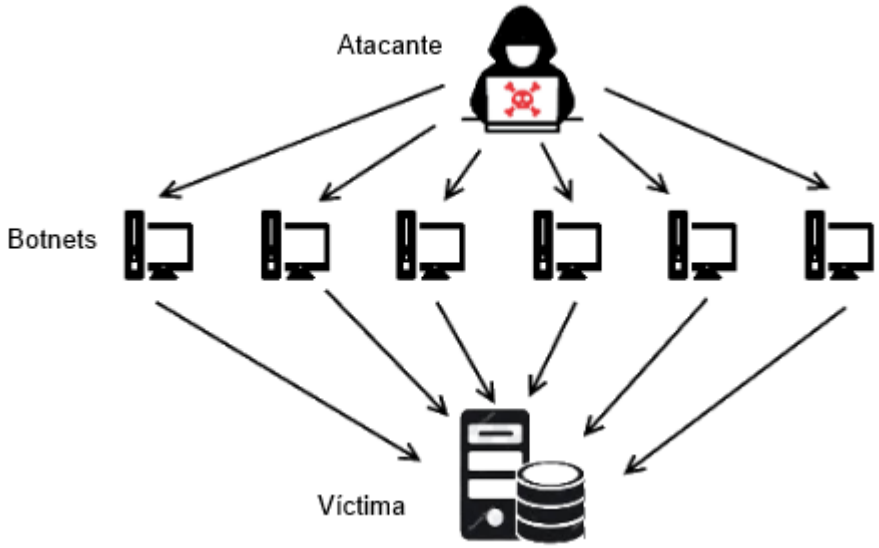
Envenenamiento de caché DNS (Suplantación de DNS)



Nota. Tomada de *¿Qué es el envenenamiento de caché DNS? | Suplantación de DNS* [Infografía], Cloudflare, Inc., s.f., https://www.cloudflare.com/es-es/learning/dns/dns-cache-poisoning.

Figura 3

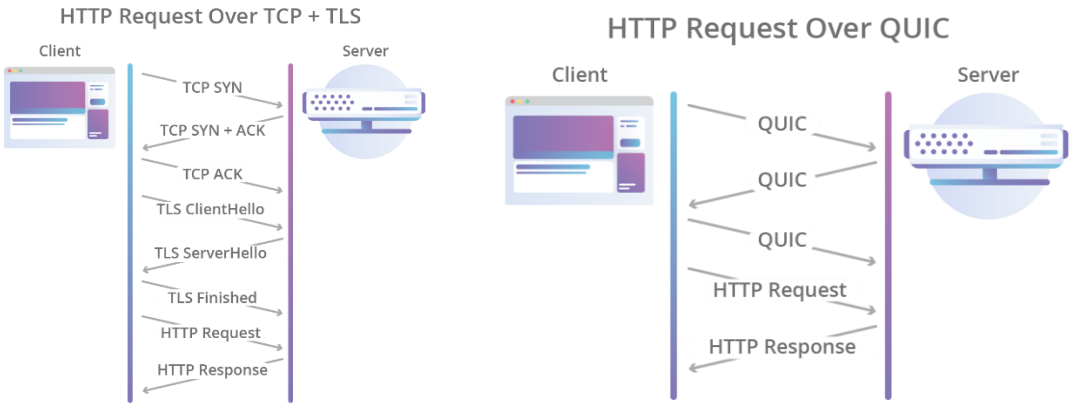
Ataque de Denegación de Servicio Distribuido (DDOS)



Nota. Tomada de *Denegación de Servicio (DoS)* [Infografía], Segurísimos en la Web, s.f., https://segurisimosenlaweb.com.ar/denegacion-de-servicio-dos.

Figura 4

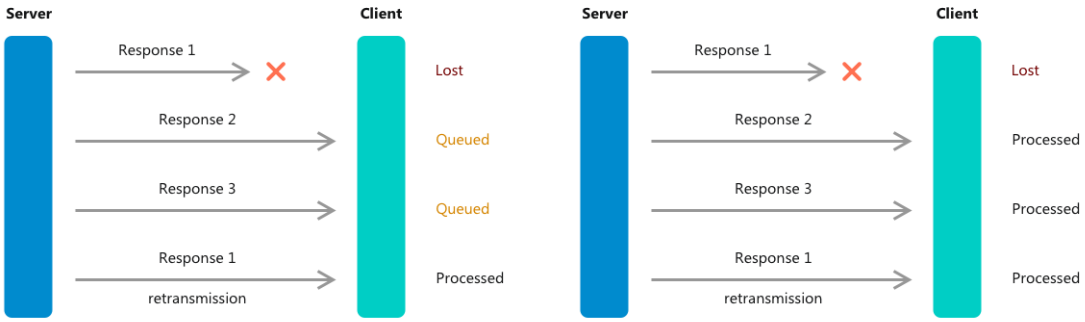
Funcionamiento de Handshake en TCP+TLS vs QUIC



Nota. Tomada de *The Road to QUIC* [Infografía], Cloudflare, Inc., 2018, https://blog.cloudflare.com/the-road-to-quic.

Figura 5

Funcionamiento de Head-Of-Line Blocking (Bloqueo de cabecera de línea) en TCP vs QUIC



Nota. Tomada de *AdGuard DNS-over-QUIC* [Infografía], AdGuard, 2020, https://adguard.com/en/blog/dns-over-quic.html.