Pontificia Universidad Católica del Ecuador

SEDE ESMERALDAS

ESCUELA DE SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

AMENAZAS A LAS PLATAFORMAS INFORMÁTICAS BAJO EL CONTEXTO DE LA CIBERSEGURIDAD EN EL E-COMMERCE

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR:

BRIAN EMYR ROBLES BERNAL

ASESOR

MGT. CESAR GODOY ROSERO

Esmeraldas, 2018

Trabajo de tesis aprobado luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grado de la PUCESE previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

Presidente Tribunal de Graduación

Lector
Mgt. Gustavo Chango Sailema

Lector
Mgt. Juan Casierra Cavada

Asesor
Mgt. César Godoy Rosero

MGT. XAVIER QUIÑONEZ KU
Director de la Escuela de Sistemas y Computación

Esmeraldas, 22 de septiembre del 2018

AUTORÍA

Yo, **Brian Emyr Robles Bernal**, portador de la cédula de identidad No. **080292449-8,** declaro que la presente investigación enmarcada en el actual trabajo de tesis es absolutamente original, auténtica y personal.

En virtud que el contenido de esta investigación es de exclusiva responsabilidad legal y académica del autor y de la PUCESE.

Brian Emyr Robles Bernal,

C.I.: 0802924498

CERTIFICACIÓN

Mgt. Cesar Godoy, docente investigador de la PUCE-Esmeraldas, certifica que:

La tesis de grado realizada por BRIAN EMYR ROBLES BERNAL, bajo el título "AMENAZAS A LAS PLATAFORMAS INFORMÁTICAS BAJO EL CONTEXTO DE LA CIBERSEGURIDAD EN EL E-COMMERCE", reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargado de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, 22 de septiembre del 2018.

Mgt. Cesar Godoy Rosero
Asesor de Tesis

AGRADECIMIENTO

A mis padres Pedro Bernal Ruperty y Esmeralda Perdomo Rodríguez por todo su amor y apoyo incondicional a lo largo de mi vida, muchas gracias queridos padres, este triunfo es de ustedes.

A todos mis familiares que estuvieron conmigo desde niño y contribuyeron en mi formación personal y profesional, muchas gracias por todo querida familia.

Gracias totales, este logro es fiel testimonio de mi total gratitud hacia ustedes.

DEDICATORIA

El presente trabajo de investigación está dedicado a mis padres que siempre me apoyaron en todo para poder lograr este objetivo, todos mis logros son de ustedes.

A mi familia, que siempre supo apoyarme y han servido de motivación para seguir adelante.

Brian Robles Bernal

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La presente investigación se realizó con la finalidad de analizar amenazas en plataformas informáticas bajo el contexto de la ciberseguridad en el e-commerce en Ecuador. Las fuentes de información que nutrieron este estudio tienen un enfoque cualitativo, la metodología aplicada se basó en contrastar las referencias teóricas y antecedentes realizados con los resultados obtenidos en las pruebas de laboratorio aplicado. De esto modo, se logró la identificación de las principales amenazas contra plataformas informáticas de e-commerce permitiendo describir su funcionamiento y establecer métodos de prevención que incrementen la seguridad de los datos de los usuarios en el comercio electrónico. En un ambiente de prueba, mediante un ataque de sniffing desde una red local, se extrajo información personal de la cuenta de un cliente en el proceso de compra, capturada por la herramienta wireshark en esta red local.

Palabras clave: amenazas en e-commerce, ciberseguridad, ciberataques.

ABSTRACT

This research was carried out with the purpose of analyzing threats in computer platforms in the context of e-commerce cybersecurity in Ecuador. The sources of information that nourished this study have a qualitative approach, the methodology applied was based on contrasting the theoretical references and background information with the results obtained in the laboratory tests applied. In this way, it was possible to identify the main threats against e-commerce computer platforms and to describe how they work and to establish prevention methods that increase the security of users' data in e-commerce. In a test environment, through a sniffing attack from a local network, personal information was extracted from a customers account in the purchasing process, captured by the wireshark tool on this local network.

Keywords: E-commerce, cyberspace, cybersecurity, computer fraud, computer platforms, threats, vulnerabilities, cyber attacks.

INTRODUCCIÓN

Presentación del tema de investigación

En la actualidad, el ser humano experimenta intensamente el fenómeno de la globalización, consistido en el arte de integrar información de todo tipo y servicios asociados a éstas, dichos servicios son los encargados de dar soporte a los usuarios para la realización de operaciones de todo tipo en el ámbito de las telecomunicaciones.

El área del "e-commerce" o también llamado "comercio electrónico", consiste en la venta de productos o servicios a través de internet, siendo cada vez más demandada, y, por ende, ha sufrido una notable expansión debido a que cada vez son más los cibernautas que se integran al ciberespacio.

Mejoramiento en la infraestructura de redes y telecomunicaciones, incremento salarial, mejora en el sistema educativo, influencia externa, entre otros, son los factores asociados al notable incremento de personas con acceso a internet a nivel mundial.

El aumento en el número de cibernautas genera un volumen de transacciones cada vez mayor, dando por hecho que, en un futuro no muy lejano, casi todos los pagos tendrán que realizarse a través de internet, esto ha ocasionado que el ciberespacio se vuelva un lugar no tan seguro para usuarios nuevos o inexpertos en realizar compras en internet, y que ciertos sitios web, se conviertan en objetivos de ciberatacantes o asociaciones dedicadas al ciberdelito.

La identificación, estudio y gestionamiento de las amenazas a los sitios web dedicados al e-commerce, permitirá incrementar la ciberseguridad de estos notoriamente, garantizando la seguridad y resguardo de la información de los usuarios finales, además de prevenir ciberataques y evitar que ciberatacantes logren explotar vulnerabilidades en sitios web de comercio electrónico.

Este proyecto de investigación consta de tres capítulos los cuales serán descritos a continuación:

El capítulo I consiste en el desarrollo del marco teórico donde se detallan y explican los diferentes términos y componentes teóricos necesarios para el desarrollo de la presente

investigación, considerando definiciones elementales como plataformas informáticas, amenazas, ciberterrorismo, ciberespacio, e-commerce y, además, las correspondientes bases legales que incluyen la legislación ecuatoriana y la de organismos internacionales.

El capítulo II describe la metodología empleada para el desarrollo de esta investigación, detallando aspectos fundamentales como instrumentos metodológicos utilizados, tipo de investigación y la población empleada en este proyecto.

El capítulo III presenta todos los resultados obtenidos a partir de las tres fuentes de información de la cual se alimenta esta investigación. Establece métodos de prevención para mitigar el riesgo de ser víctima de ciberestafa y además describe una serie de elementos de configuración en el servidor que deben ser tomados en cuenta a la hora de poner en servicio un aplicativo web de e-commerce.

El capítulo IV contrasta los resultados obtenidos por esta investigación con el de investigaciones anteriores, permitiendo así al autor del presente proyecto, afirmar los resultados obtenidos y a su vez negar o actualizar cierta información en materia de ciberseguridad y métodos de prevención para mitigar el riesgo de ciberestafa en sitios web de e-commerce.

El capítulo V y el capítulo VI presentan las conclusiones y recomendaciones obtenidas en base a los objetivos planteados en esta investigación, identificando las principales amenazas a sitios web de e-commerce, describiendo su funcionalidad, estableciendo métodos de prevención contra ciberestafas y sintetizando los resultados obtenidos en las pruebas de laboratorio que fueron realizadas.

Planteamiento del problema

Desde el surgimiento de sistemas informáticos orientados al almacenamiento masivo de datos, se han desarrollado y evolucionado nuevas técnicas, amenazas y herramientas que permiten al o los atacantes (usuarios no deseados) acceder a datos privados de vital importancia para individuos o empresas.

Estos sistemas han venido en auge desde la innovación del concepto del computador personal y el desarrollo de videojuegos en las primeras consolas que salieron al

mercado. Estos dos elementos guardan una estrecha relación entre sí: "La inteligencia artificial"

Pero ¿Cómo interviene la inteligencia artificial en amenazas o vulnerabilidades orientadas a la ciberseguridad? ¿Qué es una amenaza? ¿Qué es una vulnerabilidad? ¿Cuándo estamos en condiciones de catalogar a una determinada acción o evento en un sistema informático bajo la etiqueta de "amenaza a la ciberseguridad del mismo"?

A manera de aclaración y planteamiento del desarrollo de este proyecto, las amenazas y vulnerabilidades tratadas en el presente problema están asociadas a los sistemas de información (SI). Un sistema de información es aquel que está orientado al almacenamiento de información de diversos tipos, su clasificación y procesamiento.

Según Navarro (2009), una vulnerabilidad en la seguridad de un sistema es aquello que compromete la seguridad de todo el sistema en general. Estas vulnerabilidades surgen a partir de diversos elementos que forman un sistema, como, por ejemplo: Un error de codificación, mala asignación de permisos y roles de usuario a un determinado nivel de la aplicación, error en la implementación de nuevos módulos del software, errores en el diseño, fallos en la política de seguridad empresarial, entre otros. Los diversos tipos de vulnerabilidades existentes dan origen a diversos de ataques, pero ¿qué es un ataque? Shirey, R. (2000) define un ataque como: "Una agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema".

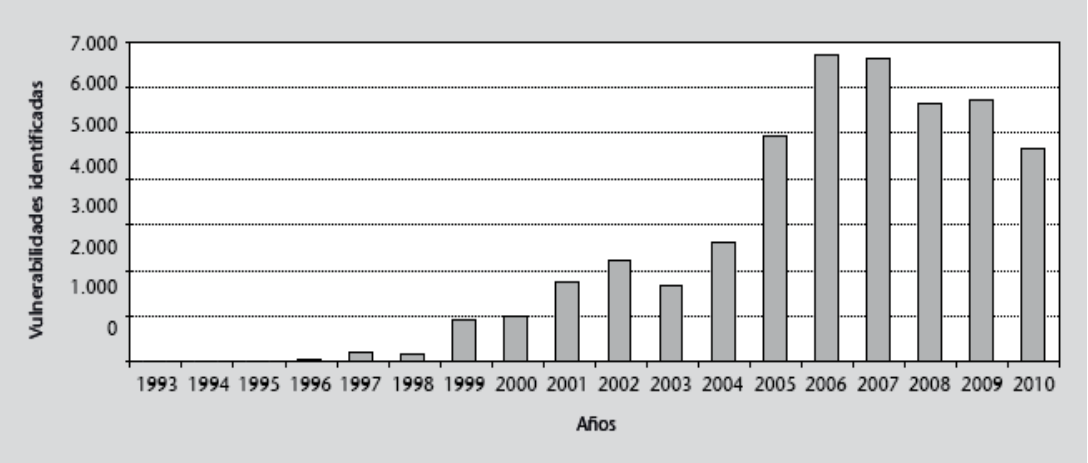


Ilustración 1 Diagrama de número de vulnerabilidades diferentes por año.
Fuente: National Vulnerability Database.

La política de seguridad es un conglomerado de todas las normativas y procedimientos que se tienen que utilizar a la hora de implementar o ejecutar un servicio. Toda acción que atente o suponga una violación a las normativas que rigen la política de seguridad, es considerado como incidente de seguridad (Navarro, 2009).

Para combatir y tratar de evitar estas vulnerabilidades de sistema, los organismos internacionales que rigen todo lo relacionado a amenazas y vulnerabilidades tienden a almacenar dichos procesos maliciosos, identificarlos, clasificarlos, publicarlos y de ser posible, solucionarlos. Una de varias empresas encargadas al almacenamiento y reconocimiento de amenazas y vulnerabilidades es National Vulnerability Database; estas empresas u organismos internacionales suelen avisar días anteriores a la fecha de la publicación sobre una determinada vulnerabilidad identificada a las empresas regentes de dicho software para evitar altercados.

Habiendo aclarado conceptos tales como: Vulnerabilidad de un sistema, sistema de información, política de seguridad e incidentes de seguridad, se puede dar pauta a continuar con las amenazas de un sistema, estas son todas las acciones, eventos o procesos potenciales de violar la política de seguridad de un sistema.

Actualmente, existen diversos tipos de software maliciosos desarrollados con el fin de obtener información confidencial o accesos a sistemas de información. En ciberseguridad, a uno de los tantos tipos de softwares encargados del robo de información a usuarios o sistemas de información se los conoce como botnets. Un botnet o software zombi es un software considerado como inteligencia artificial debido a que no solamente obtiene accesos para el robo de información, sino que también tiene como principal tarea la comunicación entre otros botnets, recibe órdenes desde una central y está en capacidad de incrustarse en el core de cualquier sistema y pasar desapercibido (Navarro, 2009). A lo largo de esta investigación se referenciarán dichas botnets con procesos y servicios más complejos.

Sintetizando lo anteriormente mencionado, la problemática de la investigación contempla amenazas a las plataformas informáticas que aplican e-commerce, su identificación y comportamiento en contra de usuarios finales, para su posterior gestión y ofrecimiento de soluciones a los problemas que éstas ocasionan a los cibernautas y empresas que realizan procesos e-commerce en el ciberespacio, proponiendo así

métodos de prevención que mitiguen los riesgos de ser víctima de ciberestafa, tanto del lado del cliente, como del servidor.

Justificación

Desde el surgimiento de los Sistemas de información (SI) hasta la actualidad, los avances tecnológicos han representado grandes ventajas y desventajas en función de la ciberseguridad, generándose así nuevas formas de estafa y robo de información hacia los usuarios y empresas. Dichas acciones son llamadas "delitos informáticos" y buscan la obtención de datos privados para tener, ya sea mediante la extorción o robo directo de cuentas bancarias, el dinero o algún tipo de beneficio de los usuarios.

En los últimos años, el ciberespacio se ha convertido en un sitio lleno de dinamismo y poblado de transacciones de todo tipo, útiles a la hora agilizar transacciones ligadas al comercio electrónico y propagación de la información. El proceso de globalización en el que se ha visto inmerso el ser humano, a más de ser positivo, lleno de cambios y auges en los ámbitos políticos, sociales, económicos y culturales, ha sido contaminado con las estafas en el ciberespacio, y es que son éstas nuevas facilidades de contacto, provistas por herramientas de comunicación de magnitud mundial, las que permiten a los ciberatacantes realizar estafas y ciberataques de cualquier tipo a determinados grupos de cibernautas que se conectan desde cualquier parte del mundo.

La presente investigación busca identificar los diversos tipos de amenazas a la ciberseguridad orientada al comercio electrónico (e-commerce) existentes en la actualidad, comprender qué es una amenaza, cómo surgen y cómo contrarrestarlas, abarcando también conceptos tales como vulnerabilidades en sistemas de información y métodos de robo de información (phising, ingeniería social, dns spoofing, etc.).

Esta investigación es importante porque al identificar cuáles son las amenazas más recurrentes a plataformas informáticas de e-commerce, se permite establecer métodos de prevención que permitan mitigar el riesgo de ciberestafas en el ciberespacio e incrementar el nivel de seguridad en los servidores que alojan estas plataformas.

Entre los principales beneficiarios de esta investigación estarán los usuarios de los sitios web e-commerce, el autor del presente estudio y la comunidad de e-commerce, que será

beneficiada con las conclusiones y recomendaciones otorgadas por la presente investigación, a manera de feedback.

Objetivos

Objetivo general:

- Analizar amenazas en plataformas informáticas bajo el contexto de la ciberseguridad del e-commerce en Ecuador.

Objetivos específicos:

- Identificar las principales amenazas de ciberseguridad producidas en sitios de e-commerce.
- Describir la funcionalidad de amenazas y vulnerabilidades de los sistemas de e-commerce.
- Establecer métodos de prevención para incrementar la seguridad de los datos de los usuarios.
- Determinar las vulnerabilidades en sitios web de e-commerce mediante la ejecución de ciberataques.

CAPÍTULO I

1. MARCO TEÓRICO

1.1 Antecedentes

El concepto de seguridad, del latín securitas (Real Académica Española s.f.), referencia la palabra al afianzamiento o indemnización a favor de un servicio o de una persona en específico. En el mundo moderno, la seguridad en el ámbito de la informática no deja de ser algo muy ambiguo, sin embargo, es destacable la reacción de individuos, empresas y organizaciones, por pretender garantizar la seguridad de los usuarios en la web.

Mendoza (2015) establece que: En la actualidad, un término ampliamente utilizado es "ciberseguridad", que puede asociarse con otras palabras como ciberespacio, ciberamenazas, cibercriminales u otros conceptos compuestos. Aunque se tiene una percepción general sobre lo que representa, en ocasiones puede utilizarse como sinónimo de seguridad de la información, seguridad informática o seguridad en cómputo -pero esta idea no es del todo correcta. La disyuntiva se presenta cuando es necesario aplicar de manera adecuada los conceptos, de acuerdo con las ideas que se pretenden expresar. Si bien existen distintas definiciones para la ciberseguridad, es importante conocer cuándo se utiliza de forma correcta de acuerdo con el contexto, e identificar sus diferencias con los otros términos -por ejemplo, el de seguridad de la información.

Con el avance tecnológico reciente, cada vez es más notorio el incremento en nuevas, técnicas, tipos de ataques y vulnerabilidades que amenazan a la ciberseguridad en nuestros días, pretendiendo de manera maliciosa, violentar servicios o sistemas de tal manera que se obtenga la información privada de los usuarios, es por eso que Navarro (2009) afirma que: Actualmente, nadie duda de la importancia que tiene la seguridad informática en nuestras vidas. Se vive, cada vez más, rodeados de dispositivos informáticos que nos facilitan el día a día. Reservar entradas o realizar la compra por Internet, un coche con un alto grado de automatización y capacidad de comunicación, un teléfono móvil en el que hablar parece una función secundaria, la digitalización de prácticamente todos los datos relacionados con nosotros (desde la Administración pública, las empresas, o nuestros datos personales, como agenda, correo electrónico,

documentos, etc.), son cosas con las que nos hemos acostumbrado a vivir. De la misma manera, también hemos empezado a percibir la importancia de la seguridad informática. Hoy en día son frecuentes las noticias en la prensa no especializada sobre incidentes de seguridad en el mundo digital, como robo de tarjetas de crédito, suplantación de identidad, robo de datos confidenciales, o incluso ataques dirigidos sobre infraestructuras críticas.

Existen diversos tipos de vulnerabilidades en los sistemas de información y métodos de pago online, es difícil de estimar de manera concreta, cuán grande y devastador puede llegar a ser el daño que puede llegar a causar un virus informático, es decir, se tiene una determinada empresa con millones de usuarios y de cada usuario se poseen registros con informaciones bancarias, datos privados, entre otros. Actualmente están muy de moda los virus informáticos que realizan un tipo de "chantaje electrónico" a los usuarios, Cid (2017) narra cómo estos virus se han hecho con el dominio de empresas que manejan cantidades masivas de información de usuarios y describe que: Quizá 2017 sea el año en el que más ciberataques graves recordaremos. Desde WannaCry a Petya, estos virus poténtisimos ya se han hecho un hueco en nuestra memoria y en el de miles de empresas afectadas en todo el mundo afectadas. Pero es solo el comienzo.

Recientemente, los principales expertos mundiales en ciberseguridad y 'hackers' se han reunido en Las Vegas en la convención Black Hat para hablar de lo que ha ocurrido y, sobre todo, de lo que viene. Y las noticias no son esperanzadoras. Por eso hemos seguido, más atentos que nunca, la nueva edición del evento de hackers más grande del mundo, el Black Hat USA.

Realizando una proyección más cercana al e-commerce y dejando de lado ejemplos de ransomware, existen modalidades que de manera conceptual no han variado a lo largo de los últimos años, aquí es donde se empieza a hacer referencia al "phising", "spoofing", "pharming", entre otros.

En el estudio realizado por (Landaburro, 2017), se determinó que la aplicación de medidas de prevención tecnológicas favorece la evasión de ciberestafas en los sitios web donde fueron aplicadas, entre algunas de estos métodos de prevención se destacan los siguientes:

- Implementación de software de bloqueo.

- Aseguramiento de puertos.
- Estandarización y aplicación de políticas de seguridad de la empresa.
- Desarrollo del sitio web empleando tecnologías y estándares internacionales ya testeados por expertos.
- Ofrecimiento de un manual de usuario para el público en general, entre otras.

1.2 Bases teóricas-científicas

1.2.1 Plataformas Informáticas

Según Binstock (2012) una plataforma informática es el entorno de ejecución de un software, puede llegar a ser el hardware o el sistema operativo (SO), incluso un navegador web u otro software subyacente, siempre que se ejecute el código del programa. Las plataformas informáticas tienen diferentes niveles de abstracción que incluyen una arquitectura de computadora, un sistema operativo o bibliotecas de tiempo de ejecución; también se las conoce como la etapa en la que se pueden ejecutar los programas informáticos.

Para esta investigación en particular, la orientación del uso, comprensión y manejo de plataformas informáticas estará principalmente basada hacia entornos web, la infraestructura de servidores y derivados de ambos.

El área de e-commerce es amplia y abarca muchos temas de investigación que permiten evaluar sus beneficios, desventajas y su estructura que consta del software a utilizarse y el hardware que lo contiene. Unificando términos y haciendo referencia al tema de investigación, es posible plantearse varias interrogantes en cuanto a hardware se refiere, por ejemplo: ¿Es posible encontrar vulnerabilidades a nivel de hardware? ¿qué tipo de infraestructura deberá manejar todo servidor que aloje servicios de e-commerce?

1.3 Infraestructura de Servidores

En la ilustración 2 se representan elementos básicos que conforman la infraestructura de cualquier tipo de servicio online, incluyendo la del e-commerce (a menor escala). Esta estructura está organizada de manera jerárquica, asignando roles a cada elemento.

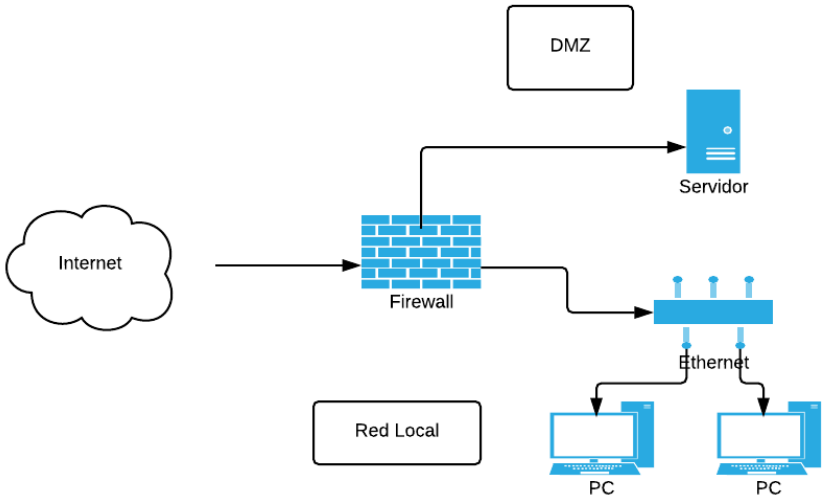


Ilustración 2 Diagrama básico de red.
Fuente: Elaboración propia.

En la ilustración 3 se muestra una infraestructura tipo IAAS (Infraestructure as a Service) o también llamada infraestructura como servicio. Este tipo de infraestructura de red busca crear soluciones económicas y fáciles de ampliar, donde el usuario final posea un servicio virtualizado que se pague por consumo de recursos del servidor en la nube.

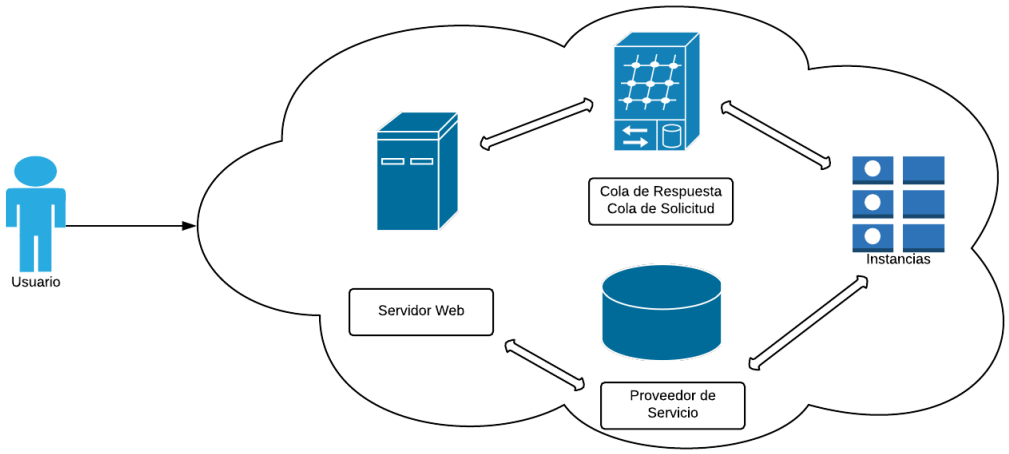


Ilustración 3 Infraestructura como Servicio.
Fuente: Elaboración propia.

1.4 Vulnerabilidades físicas y a niveles de Hardware

Según González, García Perellada, Vigil Portela, y Garófalo Hernández (2013), se considera vulnerabilidad física o de hardware a cualquier vulnerabilidad presente en el ambiente de ejecución del software, estas vulnerabilidades se componen básicamente de malas instalaciones de redes, uso inadecuado de cualquier dispositivo que pertenezca a la infraestructura de trabajo, carencias en la política de seguridad empresarial, falta de elementos de seguridad (extinguidores contra incendios, elementos de limpieza, etc.), ventilación del lugar, entre otros.

Si un atacante llegase a tener acceso a las características de las instalaciones donde se encuentra alojado el servicio web a violentar, podría atentar así a la disponibilidad de la información, es por ello que muchas empresas suelen establecer como reservada o área restringida sus instalaciones, de tal manera de revelar posibles vulnerabilidades o tipo de sistema de almacenamiento y arquitectura de red que la empresa o institución.

(González et al., 2013) también afirman que posibles defectos en la fabricación del hardware o sencillamente una mala manipulación o una aplicación de sus configuraciones, por parte del personal de la empresa encargado de la administración de redes y servidores, ya son considerados como vulnerabilidades a nivel de hardware.

Existen otros elementos ajenos al equipo de trabajo, por ejemplo, la carencia de soporte que recibe el hardware por parte de las empresas desarrolladoras, la falta de actualizaciones de software vuelve al hardware obsoleto y vulnerable, permitiendo posibles manipulaciones de bloques de memoria, insertar valores y demás acciones hostiles hacia el servidor.

La ciberseguridad busca evaluar estos parámetros anteriormente mencionados para poder contemplar si el hardware que se usa está al nivel del software requerido y viceversa.

1.4.1 Cálculo de requerimientos de Hardware

El aseguramiento de niveles óptimos de desempeño pasa por la reservación de una mayor cantidad de recursos físicos para la virtualización, o sea, "mientras más, mejor".

Además, el uso de los recursos virtuales debe estar entre el 60 y 80% de los físicos, para evitar tanto su infrautilización, como su explotación excesiva. (Pol et al., 2013)

Un manifiesto de vulnerabilidad es la carencia de recursos físicos para que el software logre ejecutarse de forma óptima.

(Pol et al., 2013) manifiestan y hacen hincapié en la importancia de contar con el hardware adecuado para el alojamiento y ejecución de máquinas virtuales en servidores.

Wolf y Halter (2005) en su investigación establecieron una ecuación que permite determinar la cantidad de núcleos que los servidores físicos pueden ofrecer a las máquinas virtuales que van a hospedar, estableciendo así el número de procesadores como principal variable a la hora de calcular el hardware necesario para la ejecución de una máquina virtual, la fórmula es: Cantidad de núcleos para las máquinas virtuales = (# de procesadores de la máquina hospedera)*(# de núcleos lógicos de cada procesador) – 1.

Wolf y Halter (2005) también establecieron una ecuación para determinar la cantidad necesaria de memoria RAM, donde las principales variables son la capacidad y la velocidad del bus de memoria, la ecuación es: Capacidad de RAM disponible para las máquinas virtuales = Capacidad de RAM de la máquina hospedera - Capacidad de RAM necesitada por el SO hospedero - Capacidades de RAM necesitadas por los SOs invitados - 1 GB.

Cabe destacar que aquel GB de memoria en la ecuación representa el uso exclusivo que requiere la máquina virtual para ejecutarse por sí sola.

El almacenamiento es otro elemento de vital importancia en cuanto a manejo de servidores se refiere, esta variable representa del conglomerado de todo el espacio requerido por el software para su ejecución. (Wolf et al, 2005) establecieron una ecuación que determina el espacio necesario para que un servicio virtualizado se ejecute en óptimas condiciones, la cual está dada por:

Espacio en disco disponible para las máquinas virtuales = Espacio en disco de la máquina hospedera - Espacio de intercambio de la máquina hospedera y las máquinas virtuales - Espacio de discos fijos de la máquina hospedera y sus máquinas virtuales - Espacio para expandir los discos dinámicos de las máquinas virtuales - Espacios

requeridos por los sistemas operativos de las máquinas virtuales - Espacio requerido por el sistema operativo hospedero - Espacio para salvar el estado de las máquinas virtuales (igual a la capacidad de las memorias RAM de todas las máquinas virtuales hospedadas).

1.4.2 Tipos de Sistemas de Almacenamiento

Existen diversos sistemas de almacenamiento, no solamente para virtualización sino también para incorporar servicios en la nube. (Alejandro et al., 2012) afirman que más del 40% del presupuesto de infraestructura de una empresa, está orientado al almacenamiento, hecho que se debe al incremento en la información debido al volumen de usuarios que manejan las nubes hoy en día.

"En la actualidad, los SAs básicamente empleados en Centros de Procesamiento de Datos (CPDs), son: Almacenamiento Directamente Conectado (DAS6), NAS y las SAN." (González, 2012).

Según González (2012) el almacenamiento directamente conectado (DAS), es aquel tipo de almacenamiento donde los dispositivos de almacenamiento forman parte de la estación de trabajo y están directamente conectados a un servidor y su usabilidad radica en la conexión directa a este.

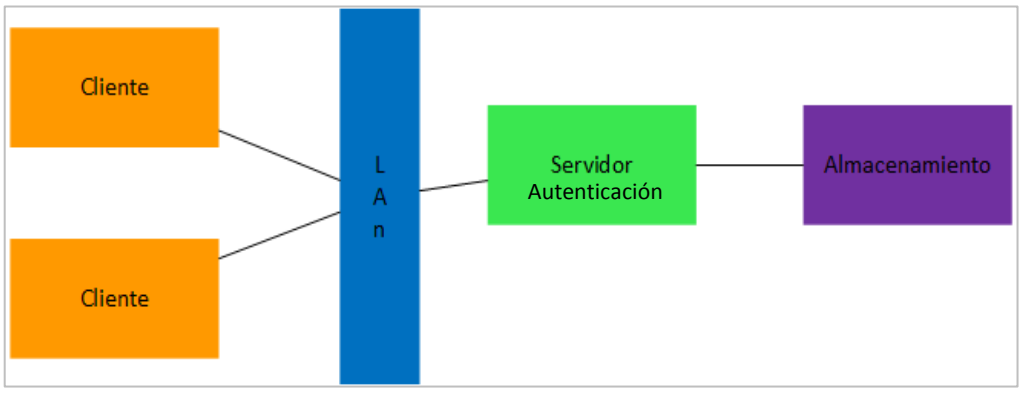


Ilustración 4 Almacenamiento directamente conectado.
Fuente: Elaboración propia.

El manejo de este tipo de sistema es sencillo, pero a su vez ofrece una gran desventaja, debido a que al estar conectados los dispositivos de almacenamiento directamente al servidor, si este falla, provocará una caída general del servicio, lo cual puede ser considerado como un tipo de vulnerabilidad en el diseño de dicho sistema, sin embargo, los bajos costos, su accesibilidad, rapidez y sencilla configuración lo convierten en un

buen candidato pese a sus elevados costos de mantenibilidad debido a que la información se encuentra dispersada por toda la organización, complicando así su gestionabilidad.

González (2012) describe el almacenamiento conectado a la red (NAS) como la solución a los problemas presentados en el DAS. Los dispositivos NAS se conectan directamente a la red de área local, ofreciendo como principal ventaja el servicio "plug-and-play", requiriendo solamente de conexión a la red para su directo funcionamiento ya que estos dispositivos al conectarse, obtienen de forma automática una dirección ip y son reconocidos como un nuevo almacenamiento digital, eliminando así las sobrecargas sobre el sistema operativo, sin embargo, al ser un servicio que utiliza la red para propagación y obtención de datos, puede llegar a sobre utilizar el ancho de banda de la red local, causando así aumento en el tráfico.

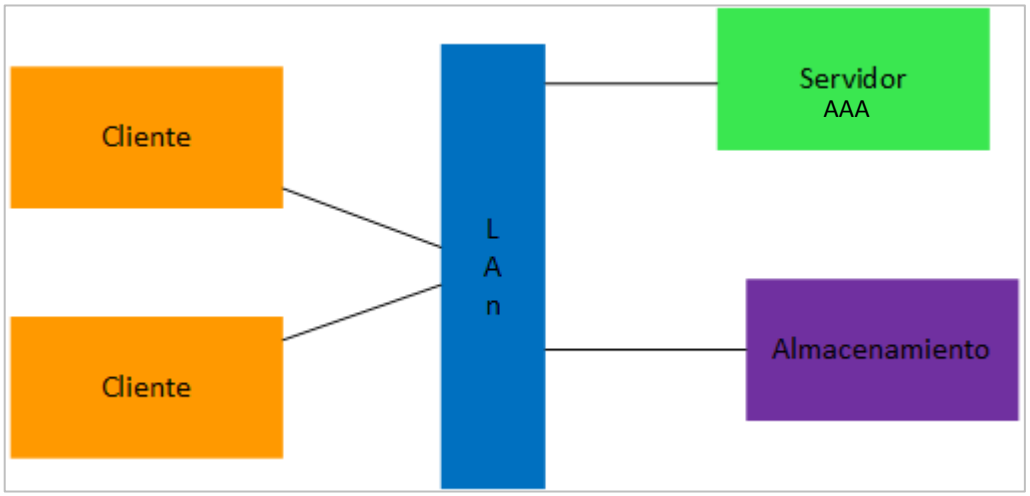


Ilustración 5 Almacenamiento conectado a la red.

Fuente: Elaboración propia.

Red de área almacenamiento (SANs)

Las SANs son redes especializadas cuyo propósito fundamental es la transferencia de datos entre sistemas de cómputo y dispositivos de almacenamiento. Siendo así, una SAN comprende: la infraestructura de comunicación que provee conexiones físicas y una capa de gestión encargada de organizar las conexiones, elementos de almacenamiento y sistemas de cómputo, de manera tal que la transferencia sea robusta y segura. (González, 2012).

Su desarrollo nace a partir de la necesidad de solventar el problema de tráfico y latencia de red presentes en las NAS, ya que este tipo de sistema destina el tráfico de almacenamiento de red a una sola red y no por toda la red de área local, convirtiéndose así en una solución versátil y muy popular en la actualidad para solventar problemas de almacenamiento en la nube.

Por último y no menos importante, se ha considerado al almacenamiento dedicado (AU) como otra opción perfectamente viable para implementar en un servicio de almacenamiento en la nube. Según González (2012) el AU es un sistema integrado de almacenamiento que permite incorporar un sistema basado en el uso de las NAS basado en ficheros y SAN basado en bloques de memoria, reduciendo así el número de implementaciones tecnológicas requeridas para soluciones de almacenamiento, de esta forma se permite la liberación de sobrecargas, tanto en la red de área local como el sistema operativo ya que la transferencia de almacenamiento de un sistema a otro es factible en este modelo de almacenamiento.

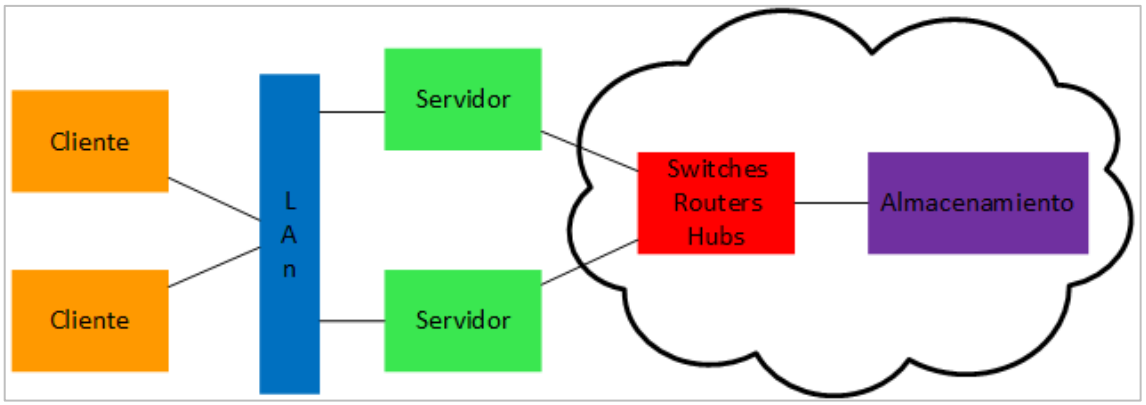


Ilustración 6 Red de Área de almacenamiento.

Fuente: Elaboración propia.

El tipo de sistema de almacenamiento que se maneje, el hardware y el software requerido para la obtención de un funcionamiento óptimo de la nube y servicios virtualizados, el personal capacitado y las condiciones de las instalaciones de trabajo, son elementos básicos dentro cualquier tipo de sistema informático que deben estar bien establecidos, dando prioridades de tal manera que un óptimo rendimiento sea un producto final garantizado. La ausencia de uno o varios de estos elementos ya mencionados conlleva a una sobrecarga de cualquier tipo que desemboca en vulnerabilidad, que puede ser explota de diversas maneras dada su naturaleza inicial.

1.4.3 Ciberseguridad y ciberdefensa

1.4.3.1 Ciberseguridad

Sancho (2017) en su artículo científico denominado "Ciberseguridad. Presentación del dossier Cybersecurity" publicado en la revista URVIO de la Flacso, describe a la ciberseguridad como una condición que permite a los usuarios beneficiarse del intercambio de información y relaciones sociales formadas dentro del ciberespacio, dicha condición se ve representada como la garantía que todo usuario en el ciberespacio debe tener a la hora de realizar cualquier tipo de acción.

1.4.3.2 Ciberespacio

Según el Departamento de Defensa de los Estados Unidos (2017), el ciberespacio es un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio). Pese a aquella descripción, cabe destacar que el ciberespacio no está excelso de daño físico, ya que, al componerse principalmente de una red lógica de nodos que interactúan entre sí, aquel sistema lógico está compuesto por un cableado físico, dependiente de electricidad, condiciones meteorológicas, etc.

La ciberseguridad debe su origen a la creciente ola de usuarios en la web, incrementando de sobremanera el volumen de información disponible en la actualidad, con ello se dio origen al big data, jugando así la ciberseguridad un papel trascendental dentro de esta nueva era tecnológica, de este modo, la necesidad de navegar con seguridad en internet, y, de poder consumir recursos de este con total naturalidad, llevó a la creación de la ciberseguridad, definiéndose ésta como el conjunto de herramientas tecnológicas, políticas y sociales que garantizan la seguridad de la información de los usuarios y todo tipo de dispositivo que interactúe con el ciberespacio.

1.4.4 Ciberdelito

1.4.4.1 Factores de riesgo en el ciberespacio

En el año 2015, La Unión Internacional de Telecomunicaciones (UIT), determinó que la cantidad de usuarios de internet es un estimado del 40% de la población mundial, cerca de 3000 millones de personas, son cifras alarmantes si se considera que estas personas están generando nuevos paquetes de datos constantemente.

Se ha observado que los usuarios de nivel educativo más alto suelen ser más propensos a recibir ataques o ser víctimas de fraude por internet, debido a que las acciones que realizan son complejas en comparación a los usuarios promedio, es por ello que, tan solo la conexión a internet no debe ser suficiente por parte de las autoridades pertinentes de un país o una determinada institución, sino que también se deberán incorporar políticas que garanticen la seguridad de la información en el ciberespacio y que aquellas garantías se vean reflejadas en leyes y estatutos de cada entidad, institución o país.

Autoría	Objetivos	
	Gobierno	Sector Privado
Ataques patrocinados por otros Estados	Espionaje, ataques contra infraestructuras críticas, amenazas persistentes avanzadas (APT, por sus siglas en inglés)	Espionaje, ataques contra infraestructuras críticas, APT
Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, extremismo político e ideológico	Ataques contra redes y sistemas; contra servicios de Internet; infección con *malware*; contra redes, sistemas o servicios de terceros	Ataques contra redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivistas	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros
Ataques de personal con accesos privilegiados (*Insiders*)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes y sistemas, ataques contra servicios de Internet, infección con malware, ataques contra redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT
Impacto	**Alto**	
	Medio	
	Bajo	

Ilustración 7 Factores de riesgo en el ciberespacio.
Fuente: Instituto de Ciberseguridad de España (2012).

1.4.4.2 Tipos de Malware involucrados en el ciberdelito

Con la creciente demanda de servicios en la web, el volumen de usuarios cada vez es más notable y, por ende, al ser internet un servicio de fácil acceso en casi todo el mundo, es notable también la cantidad de ciberdelitos que se cometen a cada instante, es por ello que Sancho (2017) afirma que los gobiernos no solamente deben preocuparse

de dar a la población el acceso a internet, sino también de dotarla de leyes que garanticen la seguridad de la información y capacitaciones constantes para prevenir ciberdelitos, técnicas de ingeniería social, "phising", "farming" y el muy de moda "ransomware", son métodos de obtención de información personal y de chantaje hacia los usuarios, en las que muchas ocasiones es pedida una recompensa por la desinfección del equipo afectado por un malware determinado y dicha recompensa usualmente suele ser pedida en bitcoins (moneda virtual).

Familia de Malware	Descripción
KEYGEN	Genera números de serie para entrar a los programas que requieren números de serie válidos para que los programas funcionen completamente
DUNIHI	Esta Familia de malware normalmente es malware VBS ofuscado que es capaz de propagarse infectando unidades removibles; puede llegar como archivo anexo del correo no deseado.
ACTIVATOR	Quiebra la aplicación y el usuario puede instalarla mutualmente. Sus rutinas le permiten a los usuarios evadir las técnicas de registro y protección de las aplicaciones. Esto les permite utilizar la versión registrada de las aplicaciones.
DOWNAD/ Conficker	Esta explota una vulnerabilidad del servicio del servidor que, cuando es explotada, permite que un usuario remoto ejecute el código arbitrario en el sistema infectado para propagarse a las redes.
CONDUIT	Se incluye en los paquetes de malware como un componente de malware, como un archivo entregado por otro malware, o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
PRODUKEY	Una aplicación que muestra la identificación del producto y la clave del CD de cierto software si se instala en el sistema afectado. Esta herramiento de hackeo puede ser instalada manualmente por el usuario.
SAFNUT	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que lo usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
AGENT	Normalmente trae consigo cargas o realiza otras acciones maliciosos, que van moderando desde moderadamente molestas hasta las irreparablemente destructivas. También pueden modificar las configuraciones del sistema para que se inicie automáticamente. Para restaurar los sistemas afectados podrían requerirse.
CROSSRDR	Se incluye en los paquetes de malware como un componente de malware. Llega al sistema como un archivo entregado por otro malware o como un archivo que los usuarios descargan sin darse cuenta cuando visitan sitios maliciosos.
FAKEAV	Crea carpetas en los sistemas afectados y entrega varios archivos, incluyendo una copia de sí mismo y un archivo malicioso. Realiza varios cambios al registro, uno de los cuales permite que se ejecute cada vez que el sistema arranca.

Ilustración 8 Principales tipos de malware hasta el año 2014.
Fuente: (*Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas*, 2015)

La figura 8 presenta los diversos tipos de malware existentes y su accionar frente a los usuarios y empresas.

1.4.5 Ciberguerra

Considerando el creciente volumen de usuarios y la diversidad de malware existente hasta la fecha, Sancho (2017) hace hincapié en reconocer la importancia de garantizar la seguridad en el ciberespacio asumiendo su complejidad, de tal manera que, los usuarios,

instituciones y países sean capaces de hacer frente a toda esta marea de malware que desemboca en todo tipo de ciberdelitos en el ciberespacio.

Fecha	Denominación	Resumen
1982	Explosión en el sistema de distribución de gas (Unión Soviética)	Los servicios de inteligencia estadounidenses introdujeron una *bomba lógica* en un software de control de infraestructuras gasísticas que había sido robado por espías soviéticos a una empresa canadiense.
2003 2005	Titan Rain	Conjunto de ataques coordinados contra empresas estratégicas e instituciones estadounidenses presumiblemente procedentes de China.
2007	Ciberataque contra Estonia	La retirada en este país de una estatua del período soviético desencadena un conjunto de graves ataques procedentes de Rusia que afectan a las instituciones estatales, bancos y medios de comunicación.
2007	Ciberataque contra Siria	La aviación israelí bombardea una instalación nuclear secreta. El ataque aéreo fue precedido de un ciberataque que engañó a los sistemas de defensa aérea e impidió detectar la incursión de los aviones en el territorio sirio.
2008	Guerra en Osetia del Sur	De manera paralela al conflicto hubo ciberataques coordinados desde Rusia contra sitios gubernamentales de Georgia que quedaron inutilizados y tuvieron que ser reubicados en servidores de otros países.
2010	Stuxnet	Un troyano provoca la destrucción de maquinaria del programa nuclear iraní.

Ilustración 9 Momentos destacados de ciberguerra.
Fuente: (Torres, 2013).

Resulta urgente la formulación de políticas públicas y/o estrategias nacionales de ciberseguridad que sistematicen los principales objetivos nacionales e internacionales en la materia, explicitar las acciones que permitirán alcanzarlos y las metas que permitirán constatar su logro. En efecto, los gobiernos de los países son responsables de elaborar políticas que promuevan y garanticen adecuados niveles de ciberseguridad según estándares internacionales, especialmente en lo que dice relación con la protección de la infraestructura crítica de la información a nivel nacional. (Sancho, 2017)

En su publicación, la OEA (2015) a través del Comité interamericano contra el terrorismo (CICTE), aborda los asuntos de Seguridad Cibernética planteándose entre estados miembros de este organismo, los siguientes objetivos:

- Establecer grupos nacionales de alerta, vigilancia y prevención (CSIRT).
- Crear una red de alerta Hemisférica que proporciona formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas.

- Promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética.
- Fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el hemisferio.

Ante toda esta arremetida de ataques, creación de malware e incluso, atentados terroristas contra estados soberanos, nace la necesidad de definir cuándo una actividad en el ciberespacio es considerada ciberdelito y cómo actuar ante ellas, es por eso que Pons (2017) describe al ciberdelito como toda acción hostil de carácter ilícito que atenta la seguridad de los usuarios al momento de utilizar el ciberespacio.

Zunzunegui e Ignacio (2008) plantean la existencia de 4 rasgos característicos de los ciberdelitos:

- Se cometen fácilmente.
- Requieren escasos recursos en relación con el perjuicio que causan.
- Pueden cometerse en una jurisdicción sin estar físicamente en el territorio sometido a la misma.
- Se benefician de lagunas de punibilidad que pueden existir en determinados Estados, los cuales han sido denominados paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

El planteamiento de estos 4 rasgos característicos en los ciberdelitos es muestra de cuan expuestos están los usuarios, instituciones y estados en el ciberespacio; la razón radica en lo desproporcionada que se encuentra la franja entre avance tecnológico y ciberseguridad. Sencillamente, el mundo moderno pese a poseer un aumento considerable en herramientas tecnológicas orientadas al uso de transacciones online y compras mediante e-commerce, no se encuentra preparado, ni mucho menos capacitado para enfrentar esta creciente ola de amenazas de cara a la utilización de servicios en la nube.

Grupos delictivos	2011	2012	2013	2014	2015
Acceso e interceptación ilícita	1.492	1.701	1.805	1.851	2.386
Interferencia en los datos y en el sistema	228	298	359	440	900
Falsificación informática	1.860	1.625	1.608	1.874	2.361
Fraude informático	21.075	27.231	26.664	32.842	40.864
Delitos sexuales	755	715	768	974	1.233
Contra la propiedad industrial/intelectual	222	144	172	183	167
Contra el honor	1.941	1.891	1.963	2.212	2.131
Amenazas y coacciones	9.839	9.207	9.064	9.559	10.112
Total	**37.412**	**42.812**	**42.403**	**49.935**	**60.154**

Ilustración 10 . Principales tipologías penales que se comenten en esta nueva era tecnológica. Fuente: Ministerio del Interior, España (2016).

En la figura 10 se logra evidenciar con datos reales, el número de incidencias ciberdelictivas registradas en los últimos años, son cifras que evidencian lo preparados que están los usuarios, instituciones y estados en cuanto a ciberdefensa se refiere.

Otra característica importante en el incremento de ciberataques, a más de la falta de conocimiento a la hora de navegar por el ciberespacio, es la confianza que poseen los ciberatacantes en el momento de su accionar, elementos tales como el anonimato, carencias constitucionales a nivel legislativo de cada estado, país o región, y a su vez, la no exposición física al momento de cometer ciberdelitos, brindan a los ciberatacantes la sensación de comodidad en la realización de sus actos, haciendo que esta, sea una actividad cada vez más popular en la actualidad.

1.4.6 Procesos penales en la cibercriminalidad

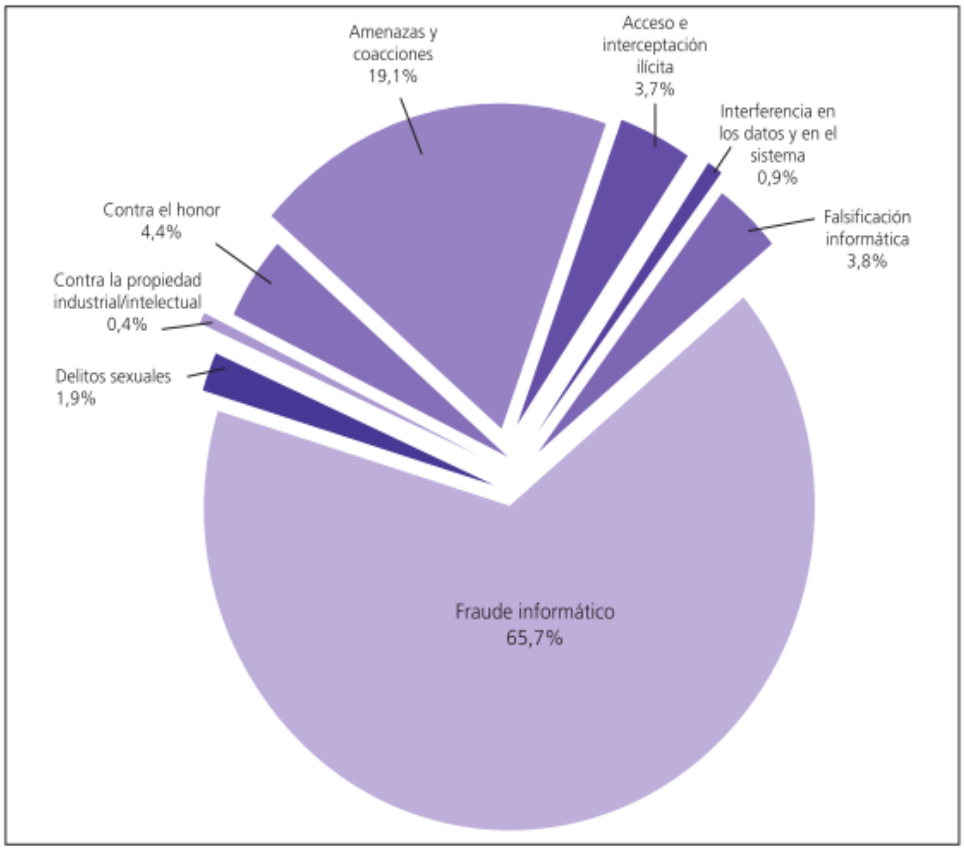


Ilustración 11. Tipología de procesos penales de la cibercriminalidad en España (2015). Fuente: Ministerio del Interior, España (2016).

La figura 11 presenta porcentualmente, los diversos tipos de ciberdelitos cometidos en España durante el año 2015, de los cuales, el fraude informático o popularmente conocido como "phishing" fue aquel que se impuso sobre los demás, dato que no sorprende si se conoce que este tipo de ciberdelito va de la mano con e-commerce y big data, siendo las redes sociales y las páginas de comercio electrónico, las principales víctimas a la hora de "pescar" posibles víctimas para el robo de su información personal.

Según Centeno (2015) y el último informe de la Agencia europea para la Seguridad de las Redes y de la Información (ENISA), las amenazas a la ciberseguridad más destacadas son:

- Malware.
- Ataques basados en el uso de la web.
- Ataques basados en aplicaciones web.

- Denegación de servicio (DDoS, Denial of service).
- Botnets.
- Phishing.
- Correo basura (spam).
- Ransomware.
- Amenaza interna.
- Daños físicos.
- Robos o pérdidas.
- Kit de explotación de vulnerabilidades.
- Violación de datos,
- Robo de identidad.
- fuga de información.
- Ciberespionaje.

1.4.6.1 Malware

Pons (2017) define al malware como el conjunto de softwares maliciosos (gusanos, troyanos, etc.) que afectan al contenido del sistema informático a acceder.

Debido a su diversidad, el campo de acción de los denominados malwares es muy amplio, comprendiendo desde troyanos básicos, simples virus que afectan los pendrives de los usuarios, hasta la obtención y robo de contraseñas mediante el uso de keyloggers o algún tipo de virus adquirido mediante la visita a una maliciosa página web, además de ser capaces de no solamente causar perjuicios a nivel de usuario, sino que también pueden llegar a causar la caída de servicios por la generación de tráfico basura y el incremento de latencia en una red de área local.

Los ataques por denegación de servicio (DDoS, Denial of service) hacen que sea imposible el acceso a los propios recursos y servicios de una organización o empresa y posteriormente solicitan un rescate para detener los ataques. El "bot" es otro programa malicioso utilizado para tomar el control de un equipo informático, sin que sea detectado fácilmente. El phishing es el término informático que se utiliza cuando el atacante intenta suplantar la identidad de cualquier víctima para adquirir su información confidencial. (Pons, 2017).

El tipo de amenaza más controversial y popular en los medios hasta el momento es el denominado "ransomware", (Pons, 2017) lo describe como un software malicioso que se apodera de los equipos de las víctimas, bloqueándolos, encriptando sus archivos y otorgando al atacante un control total o parcial de los dispositivos infectados.

Los ciberatacantes suelen pedir recompensas económicas a manera de "rescate" a cambio del desencriptamiento de sus archivos, dichas recompensas son pedidas en bit coins para mayor comodidad y seguridad del atacante.

Habiendo analizado las amenazas a la ciberseguridad con un enfoque minimalista y orientado a instituciones y personales naturales, se procederá a describir el ciberterrorismo y sus principales rasgos característicos.

Chicharro (2009) y Pons (2017) hablan sobre el ciberterrorismo y lo describen como el abuso de nuevas herramientas informáticas con fines perjudiciales en contra de un estado o país, atentando contra la soberanía de este.

Los terroristas acuden al ciberterrorismo para manipular redes de datos, robo de información, daño de redes físicas y realizar atentados de todo tipo, cabe destacar que en esta nueva era tecnológica casi todos los objetos cotidianos ya poseen conexión a internet, convirtiéndolos en vulnerables y manipulables.

Una clara expresión del ciberterrorismo es la manipulación de medios de comunicación públicos para la propagación masiva de un mensaje o como lo acontecido en Alemania en el presente año.

Graham (2017) describió lo acontecido como:" La red ferroviaria de Alemania cayó en un caos el viernes por la noche cuando cayó víctima del ciberataque que sacudió al mundo entero."

El ransomware, llamado "WannaCry" encriptó los datos de navegación de los trenes de la Deutsche Bahn, haciendo imposible el uso de dicho servicio, además exigían de pagos de $ 300 a $ 600 para restaurar el acceso.

Analizando las ciberamenazas terroristas, se presupone que las consecuencias más significativas de este tipo de delitos son económicas y de imagen, aunque por supuesto, no debemos quitar importancia a los relacionados con el contenido. Los ataques son

cada vez más sofisticados y afectan redes informáticas que en teoría disponen de niveles de seguridad extremos, es entonces cuando a este análisis de las implicaciones de los ciberataques (Pons, 2017).

El ciberespionaje sigue los principios y lineamientos que caracterizan al ciberterrorismo, sin embargo, no comprende tan solo a las naciones, un claro ejemplo de ello es cuando los ciberespías buscan hacerse con los datos de multinacionales para vender esta información a empresas competidoras, de tal manera que quienes obtengan dicha información lograrán obtener una ventaja económica y comercial en el mercado.

1.4.7 E-commerce

El comercio electrónico es el intercambio de productos o servicios a través de medios electrónicos (Laudon y Traver, 2011).

El comercio electrónico constituye una gran ventaja en el mundo moderno, permite ahorrar tarifas de transporte, pago por el mantenimiento de un local y optimiza la forma en cómo los usuarios adquieren los servicios mediante en el uso de transacciones online.

Existen diversos prototipos de e-commerce, entre ellos encontramos: empresa – empresa (B2B), empresa – administración (B2A) y empresa – cliente (B2C).

La categoría (B2B) hace referencia a las transacciones comerciales entre mayoristas y minoristas, la (B2A) hace referencia a las transacciones comerciales entre empresas y organismos gubernamentales y el (B2C) es aquel referente a las transacciones comerciales entre empresas y clientes, este último fue elegido para realizar esta investigación, debido a que se busca analizar amenazas que atenten al e-commerce pero que a su vez, incidan en el usuario final, quienes son los más perjudicados en cuanto estafas y ciberdelitos se refiere.

Miles de millones de US$

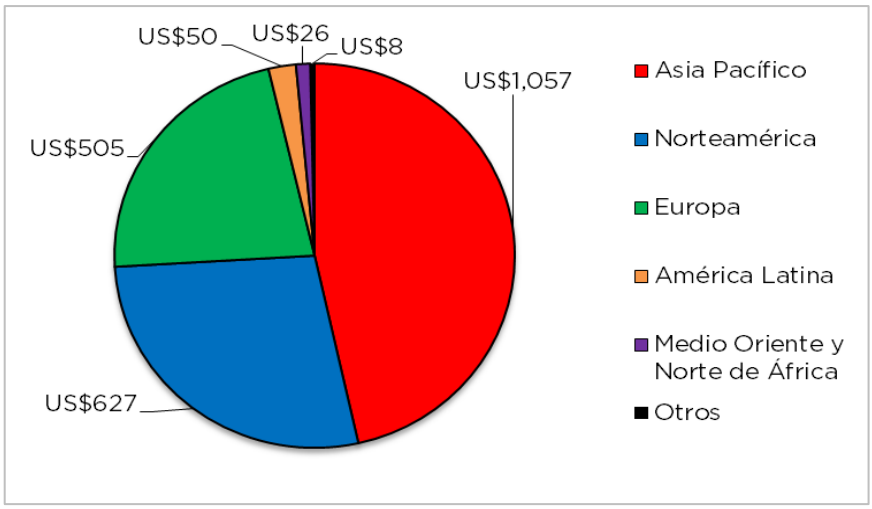


Ilustración 12 Valor del comercio electrónico B2C, 2015
Fuente: (BID - INTAL, 2016).

En la figura 12 se puede apreciar que, latinoamérica, a diferencia de los demás continentes del mundo, no es un lugar donde el comercio electrónico tenga principal acogida por parte de los usuarios, esto pone al descubierto y evidencia la falta preparación de infraestructura tecnológica y organismos que velen y garanticen la seguridad de los usuarios a la hora de utilizar la red.

En miles de millones de dólares, 2014-2015

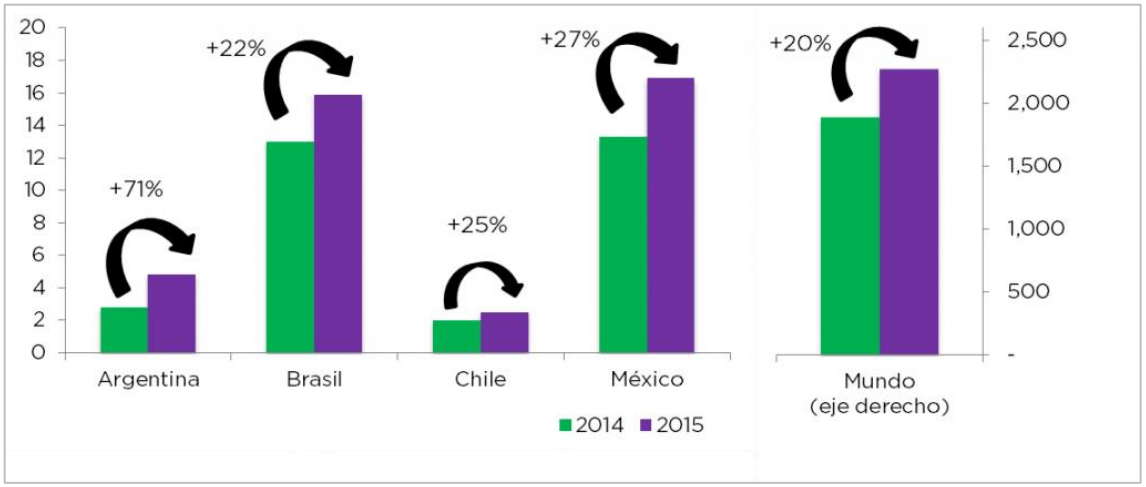


Ilustración 13 Valor y tasas de crecimiento del comercio electrónico B2C en economías latinoamericanas seleccionadas y el mundo.
Fuente: (BID – INTAL, 2016)

1.4.8 Ciberataques a sitios web de e-commerce en el Ecuador

El ciberataque perpetrado por la organización ciberdelictiva Petya ocurrido en mayo del año 2017 también tuvo consecuencias en el Ecuador. Medina (2017) expone que los primeros reportes de tres empresas dedicadas a la ciberseguridad en el país señalaron que al menos unas 15000 personas y 27 empresas fueron amenazadas e infectadas por el virus WannaCry.

Las principales ciudades afectadas fueron Quito, Guayaquil y Manta, ciudades donde el volumen de transacciones electrónicas realizadas por día es considerable, perjudicando de este modo a empresas ligadas a e-commerce en ese año, por su parte, Dmitry Bestuzhev, director del equipo global de investigación y análisis de Kaspersky Lab en América Latina, advirtió que Ecuador fue el tercer país más vulnerado por WannaCry a nivel regional.

Para lograr plasmar el impacto entre incidencias y volumen de usuarios en la red, es necesario conocer indicadores de desempeño del e-commerce.

Tabla 1 Indicadores de desempeño del e-commerce

	EIU	***A.T. Kearney***	***UNCTAD***
Objetivo	Medir el grado en el que los países fomentan el comercio electrónico transfronterizo a través de políticas, regulación e infraestructura	Clasifica los países según el atractivo potencial para el desarrollo de la venta minorista en línea.	Evaluar el grado de preparación de los países para el comercio electrónico.
Tipo de comercio electrónico	Sin especificar	B2C	B2C
Cobertura geográfica	19 países	30 países	137 países
Países de América Latina incluidos	Argentina, Brasil y México	Argentina, Brasil, Chile, México y Venezuela	Argentina, Brasil, Bolivia, Chile, Colombia, Costa Rica, El Salvador, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana y Venezuela

Actualización y disponibilidad de serie histórica	Única medición en 2014	Disponible desde 2012, se actualiza anualmente. Último disponible: 2015.	2014 y 2016
Nro. De subíndices que lo componen	40 indicadores agrupados en cinco categorías: clima de inversiones, entorno de Internet, ambiente para el comercio internacional, marco regulatorio y legal, y medio para pagos electrónicos.	Cuatro métricas: tamaño del mercado en línea; adopción de tecnologías y comportamiento del consumidor (calculados con base en tres indicadores); infraestructura financiera y logística; y potencial de crecimiento.	Cuatro indicadores: Penetración del uso de Internet, servidores seguros por millón de habitantes, uso de tarjetas de crédito y una medida de confianza sobre los envíos postales.

Fuente: (Michalczewsky, 2016).

Resumen de la tabla: Indicadores de desempeño del e-commerce según el grado de fomentación, preparación y, atractivo potencial de países hacia sus usuarios finales.

1.5 Bases legales

Problemática de ciberdefensa y ciberseguridad en el Ecuador.

En el Ecuador, los delitos cibernéticos se incrementan conforme avanza el tiempo, dándose de este modo, su propio espacio en el ámbito local.

Según estadísticas del Instituto Nacional de Estadísticas y Censo (INEC 2016), en el año 2012 la población ecuatoriana con acceso a internet comprendía el 22,5% del total, mientras que en el 2015 se llegó al 32,8%, es decir que, hasta ese año, el Ecuador ya contaba con 6283268,915 cibernautas, según cifras del Banco Mundial.

La creciente ola de nuevos cibernautas en el Ecuador se debe a muchos factores, uno de ellos es la incorporación de nuevos servicios proveídos por empresas y el mismo gobierno al ciberespacio (facturación electrónica, matriculación y asignación de cupos en colegios y universidades, etc.), es por ello que, el gobierno ecuatoriano se vio en la obligación de enfatizar esfuerzos que garanticen la ciberseguridad en el país.

Un claro manifiesto por parte del gobierno ecuatoriano para garantizar la ciberseguridad fue la conformación de un Centro de Operaciones Estratégico Tecnológico, que tenía la finalidad de monitorear varias instituciones públicas y alertar en caso de ciberataques.

A continuación, se presentan proyectos, acuerdos ministeriales y demás herramientas legales que operan en el Ecuador, penando las amenazas a la ciberseguridad:

- Implementación de Ecucert, proyecto sobre el tratamiento de ciberincidentes.
- Acuerdo Ministerial No. 166, emitido por la Secretaría Nacional de la Administración Pública, que obliga a las instituciones públicas (dependientes de la función ejecutiva) a la implementación del Esquema Gubernamental de Seguridad de la Información (Ecuador Universitario 2012).
- Uso obligatorio de las Normas Técnicas Ecuatorianas para la Gestión de Seguridad de la Información.
- Incorporación del objetivo: “Incrementar los mecanismos de ciberseguridad para los sistemas de comunicación estratégicos del estado y la integridad de la información” en su Plan Estratégico Institucional 2015-2017 Secretaría de Inteligencia.

A pesar de todos los esfuerzos, Ecuador no trabaja en ciberseguridad de manera sistemática con políticas definidas, no tienen un plan de acciones para todas las entidades del país y que todas las decisiones de qué hacer en ciberseguridad recaen en el administrador del sitio web (Delgado, 2014).

COIP

Artículo 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre

bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

CAPÍTULO II

2. METODOLOGÍA

2.1 Descripción del lugar

La presente investigación fue orientada hacia el análisis de amenazas a plataformas informáticas que manejen tecnología e-commerce, es decir, amenazas que afectan directamente a sitios webs ligados al comercio electrónico, considerando referentes de gran escala y de repercusión internacional como lo son amazon e eBay, además, abarcando el estudio de webs dedicadas al e-commerce dentro del Ecuador y proveedores de servicio de hosting de los cuales se pueda analizar datos.

2.2 Tipo de investigación

Se determinó que el tipo de investigación sea cualitativo, debido a que través del uso de entrevistas y obtención de material teórico que vaya en lineamiento con los objetivos a lograr por esta investigación, se busca la correcta interpretación de la información y así poder determinar cuáles son las principales amenazas que atentan a la ciberseguridad de las plataformas informáticas dedicadas al e-commerce y toda la comunidad de usuarios que está detrás de ellas.

Esta investigación incluye un proceso narrativo-descriptivo que es otorgado por la información recolectada a través de las entrevistas y la técnica de la observación. Para este caso práctico, se buscará determinar cuáles son las amenazas más recurrentes a las plataformas informáticas que manejen procesos e-commerce.

La investigación es descriptiva debido a que, conforme se obtienen los datos, se realiza el respectivo análisis para determinar causas, vulnerabilidades, amenazas y víctimas de ciberdelito en el ámbito del e-commerce.

2.3 Métodos y técnicas

Debido a la orientación y manejo de datos, la presente investigación es de carácter analítico-sintético, ya que se busca ir de lo más general hacia lo específico, además va en concordancia con el objetivo y lineamiento principal de la investigación, el análisis de amenazas a la ciberseguridad de plataformas informáticas en el e-commerce.

Las técnicas a usarse fueron la entrevista y la observación para la obtención de datos.

La entrevista consistió en una charla orientada a desarrolladores de sitios web ligados a procesos e-commerce, el objetivo de dicha charla fue la obtención de experiencias que ellos como desarrolladores han vivido por culpa de vulnerabilidades explotadas en sus sistemas. En relación a la observación, se buscó estar en constante reflexión de los datos que se obtuvieron, explorando así nuevos escenarios posibles dentro de la investigación.

2.4 Población y muestra

Para el desarrollo de esta investigación, la población fue establecida como un dominio y hosting propio donde se procedió a realizar pruebas para determinar las amenazas a la ciberseguridad de aquel servicio e-commerce. Además, los desarrolladores de sitios web ligados a procesos e-commerce, quienes fueron los proveedores de experiencias adquiridas en el backend de los sitios y empresas donde trabajan.

También se tomaron referencias de First Affiliates, un sitio web que recibe amenazas y vulnerabilidades que acontecen a diario, destacando así entre sus sitios asociados compañías de renombre como IT-ISAC, TeleTtrust, OASIS, entre otras.

2.5 Descripción del instrumento

Los instrumentos de investigación para la obtención de datos en este plan fueron los siguientes:

- Ficha técnica: Documento generado con el objetivo de describir la información recolectada a través de la aplicación de entrevistas a desarrolladores de sitios web ligados a procesos e-commerce.
- Diseño de entrevista: La entrevista fue un cuestionario personalizado en el cual constaron preguntas con el objetivo de facilitar la obtención de testimonios, historias y descripciones personales acontecidas en empresas que manejen procesos e-commerce, vivencias en manejo de ataques y vulnerabilidades explotadas, ciberseguridad, etc.

2.6 Descripción de las técnicas de procesamiento y análisis

El proceso de obtención de datos se originó del constante abastecimiento de material bibliográfico, los nuevos reportes extraídos de sitios webs que gestionan amenazas y vulnerabilidades, y, además, la realización y comprensión de entrevistas a través de la aplicación de una ficha técnica, instrumento encargado de parametrizar la información obtenida de éstas.

Los datos extraídos de las entrevistas serán sometidos a un análisis cualitativo para su posterior comprensión, es decir, de cada entrevista, extraer la información más relevante e incluirla en investigación.

La técnica de la observación consistió en comprender y describir procesos, material bibliográfico, situaciones y vivencias de personas ligadas a empresas que manejen procesos e-commerce.

2.7 Normas éticas

Para la realización de la entrevista se solicitaron datos personales de los entrevistados, sin embargo, no se pretende revelar la información personal de los clientes que acceden a servicios e-commerce, la información fue tratada desde un enfoque cualitativo y sujeto a contraste con las demás entrevistas a realizarse.

Para la realización de esta investigación se trabajó con valores éticos, tales como: Justicia, tolerancia, solidaridad, libertad y responsabilidad.

Las citas expuestas en esta investigación se han realizado tomando en cuenta la normativa APA y son de exclusiva responsabilidad del investigador.

CAPÍTULO III

3. RESULTADOS

A lo largo de la investigación se obtuvieron los datos de discusión a través de tres tipos de fuentes:

- Bibliográfica
- Aplicación de Entrevistas
- Pruebas reales a un servidor E-commerce

3.1 Análisis Bibliográfico

Resulta interesante observar la relación directa entre países con mayor cantidad de transacciones E-commerce realizadas y países que ya están en un proceso de crecimiento en cuanto a materia de comercio electrónico se refiere, debido a que, entre mayor sea el mercado, mayor será el riesgo de convertirse en cibervíctima.

En esta investigación, empleando un estudio bibliográfico recopilatorio de diversas fuentes a nivel mundial, se ha logrado identificar que de todos los ciberdelitos que se conocen hasta la fecha, el fraude informático se alza de entre los demás con un 65% en relación con todos los ciberdelitos acontecidos hasta el momento en el ciberespacio.

El fraude informático está orientado mayormente hacia los cibernautas, por lo que lamentablemente en la mayoría de los casos, no está al alcance de las empresas responsables de las aplicaciones web con E-commerce contrarrestar el arsenal de ciberataques dirigidos hacia sus usuarios finales. En atribución a lo anteriormente mencionado, en la mayoría de los países con un creciente volumen de comercio electrónico, se evidenció la escaza legislación que penalice el fraude informático, ciberdelito y ciberdelincuencia en general, creando de este modo, el ambiente propicio para que los ciberdelincuentes puedan obrar con mayor seguridad.

Las principales formas de fraude informático se manifiestan a nivel de usuario empleando diversos métodos de robo de información y suplantación de identidad, dichos métodos son vías para la ejecución de ciberataques aplicando la ingeniería social, los más recurrentes

son el phising y el pharming que en la mayoría de los casos, tienen como objetivo la obtención de la información de pago del usuario final.

A nivel de aplicación, manejo y control de servidores, se logró identificar que aquellos sitios web E-commerce que no poseían certificados y medidas para incrementar la seguridad de la aplicación, eran más propensos a recibir ciberataques con el fin de vulnerar dichas aplicaciones web, es decir que, los sitios web en general, se encuentran en un constante bombardeo de ciberataques por parte de organizaciones ciberdelictivas que están a la espera de poder violentar una brecha de seguridad por más mínima que esta sea, además, a nivel de comunidad E-commerce, se ha logrado un consenso global que busca la publicación y pronta solución de las diversas vulnerabilidades acontecidas hasta fecha de hoy, por lo que, está en manos de quienes administran estos sitios web E-commerce, el poder incrementar la seguridad de su sitio y a su vez brindar asesoría y la información pertinente a manera de feedback para que sus usuarios no sean presa fácil de organizaciones ciberdelictivas y se conviertan en una estadística más de fraude informático.

3.2 Análisis de las entrevistas

Se aplicó una entrevista a tres empresas que realizan E-commerce en el Ecuador con el fin de conocer y evidenciar la situación en materia de ciberseguridad en este campo a nivel nacional, y a su vez, para la obtención de datos que alimenten y respondan a los objetivos de esta investigación, las empresas fueron:

3.2.1 Yaesta.com

Es un sitio web de E-commerce el cual comercia productos de diferentes proveedores en un mismo sitio a manera de mercado, promueve el pago seguro a través de la aplicación de diferentes métodos de pago y facilidades al cliente.

3.2.2 Mi Tienda SA.

Es una plataforma en línea multiestablecimiento que ofrece productos de diferentes marcas y proveedores, emulando así un centro comercial y permitiendo la creación de mini tiendas a partir de la tienda principal.

3.2.3 Ikiam

Es una empresa pública que oferta servicios de asesoría y desarrollo de tecnologías a nivel nacional. En su página web ofertan cursos relacionados a diversos campos de investigación, debido a que cuenta con el aval de la Universidad Regional Amazónica IKIAM.

Las respuestas de los entrevistados develaron datos significativos en materia de seguridad de servidores mediante el uso de certificados, métodos de pago seguro, legislación nacional e internacional, control de la información privada de usuarios y referencias internacionales provenientes de expertos y comunidades E-commerce.

Los entrevistados afirmaron haber estado bajo ciberataques al menos una vez durante su vida empresarial, sin embargo, dichos ciberataques no llegaron a tener mayores repercusiones ya que ellos afirman haber solucionado las vulnerabilidades explotadas a tiempo, además, mediante la utilización de aportes otorgados por expertos a nivel mundial y la participación activa en comunidades E-commerce, han logrado mitigar el riesgo de explotación de vulnerabilidades aún más, es por ello que priorizan y centran su atención en la comunicación cliente-servidor, debido a que las empresas mediante la contratación de agentes externos, certificados e innovación en seguridad propia, están en capacidad de mitigar ese riesgo, sin embargo, del lado del cliente las tres empresas entrevistadas afirmaron contundentemente que no es el caso.

A nivel local mostraron su desconformidad con las normativas que rigen al país debido a que existe, pero no es tan completa, por lo que ciertas acciones ciberdelictivas llegan a quedar en el anonimato, sin embargo, afirmaron que del lado del servidor la protección al cliente contra el fraude es positiva ya que emplean prácticas internacionales para mitigar ese riesgo.

Afirmaron también regirse a estándares de seguridad internacionales como por ejemplo el pago seguro, la encriptación de paquetes de información y el no almacenamiento de la información de compra de los usuarios por lo que todas las transacciones son privadas mediante la utilización de pasarelas de pago seguro emitidas por las instituciones financieras.

Por último, afirmaron que el Ecuador aún no se encuentra preparado para afrontar la creciente ola de nuevas transacciones de comercio electrónico, sin embargo, esto no implica que no existan expertos ni empresas a nivel local capaces de mitigar riesgos y promover el uso de aplicaciones web E-commerce en el Ecuador.

3.3 Análisis en un servidor E-commerce mediante la ejecución de ciberataques.

Para la realización de esta práctica se utilizaron diversas herramientas de análisis de aplicativos web y modelos de ciberataques con la finalidad de comprender el comportamiento que tienen las aplicaciones web bajo este tipo de amenazas, entre ellas se utilizaron:

- Kali Linux 2.0 2018
- Owasp Mantra
- Owasp Zap
- Sqlmap
- Ettercap
- Sqlmap

Las pruebas fueron realizadas en un servidor Centos 7.5 1804 debido a que ofrece gran seguridad y estabilidad en ambientes empresariales, además de contar con una garantía de siete años aproximadamente.

Se utilizó el CMS Magento en su versión 2.2.5 ya que está orientado en su totalidad al E-commerce y posee gran aceptación por parte de la comunidad, además de ser uno de los más seguros y estables en el mercado hasta el momento. Se trabajó empleando dos escenarios, el primero consistía nada más en poseer las dependencias necesarias y el ambiente idóneo para que magento funcionase de manera óptima, obviando el aspecto de la seguridad del sitio, dicho ambiente empleaba los siguientes elementos.

- Apache 2.4

- Php 7.1
- Mysql 15.1

En este primer ambiente se realizaron pruebas a nivel local debido a que el servidor no poseía los certificados de seguridad correspondientes y se consideró además la vulnerabilidad del acceso no autorizado a la red por parte de ciberatacantes o personal no autorizado, estas pruebas consistieron en el uso de la aplicación Ettercap empleando el modelo de ataque man in the middle, el cual consiste en interceptar la información de compra que envían los clientes hacia el servidor al momento de realizar una transacción.

En el segundo ambiente se utilizó el servicio de hosting de la empresa ecuaweb, el cual contaba con soporte para comunicaciones SSL, protección de un firewall e IPS sobre aplicaciones web, balanceo de carga del servidor y mejor configuración del mismo a. En este ambiente se ejecutaron ciberataques empleando la herramienta Sqlmap que consiste en realizar ataques de inyección sql a urls vulnerables.

También se emplearon las herramientas Mantra y Zap pertenecientes al proyecto de seguridad de aplicaciones web abiertas (OWASP) las cuales sirvieron para analizar el sitio web en busca de vulnerabilidades de todo tipo a nivel de aplicación. El análisis que brindó Zap demostró que un sitio web puede ser vulnerable aún aplicando medidas de seguridad debido a que se encontraron vulnerabilidades de nivel medio y bajo a nivel de sesión y de caché del sitio web.

Establecer métodos de prevención para incrementar la seguridad de los datos de los usuarios.

Esta propuesta de intervención consiste en brindar señales y buenas prácticas a nivel de aplicación y de usuario con el fin de mitigar el riesgo de fraude informático.

Establecer métodos de prevención para incrementar la seguridad de los datos de los usuarios.

3.3.1 A nivel de servidor y aplicación web:

- Balancear riesgo y usabilidad: Está claro que a medida que se incremente el nivel de complejidad de la aplicación será más difícil para los ciberatacantes encontrar vulnerabilidades en el sistema, sin embargo, también puede resultar molesta la

acción de autenticarse de diversas maneras y demasiadas veces para los usuarios finales, es por ello por lo que se debe mantener un equilibrio entre riesgo y usabilidad.

- Conocer el origen y destino final de los paquetes de datos: En la actualidad resulta imprescindible conocer y comprender dónde se originan los datos, hacia dónde van y quién o qué los está enviando, a nivel de aplicativo web, es posible distinguir todos estos aspectos de tal manera que se permita un filtrado de la información que facilite a los administradores del sitio web un estándar que clasifique los paquetes de datos entre confiables o no, en adición a todo esto, a nivel de servidor y en php, existen métodos que permiten la identificación de los de datos de los clientes de forma clara, como por ejemplo los arreglos $_GET, $_POST, $_COOKIE **y** $_SESSION.
- Exposición de credenciales de acceso: En muchas ocasiones los programadores no suelen tener mayor cuidado con los archivos que contienen las credenciales para acceder a la base de datos, esta información es de vital importancia para la aplicación web en cuestión y puede desembocarse en muchos problemas si llega a caer en manos equivocadas, es por ello que se debe configurar el servidor para rechazar peticiones de recursos que no deben ser accesibles.
- Configuración, mantenimiento y actualizaciones periódicamente: El mundo moderno se encuentra en todo el apogeo del avance tecnológico, por lo que en su mayoría todo hardware y software posee una vida útil de dos años aproximadamente, transcurrido ese tiempo ya se considera vulnerable y poco eficiente, es por ello que se deben realizar tareas de revisión y mantenimiento de la aplicación y servidor de forma periódica, de tal manera que se eviten o mitiguen riesgos, además de incluir buenas prácticas a nivel de seguridad del servidor en sus configuraciones mediante la instalación de certificados de seguridad y un debido hardening a los servidores.
- Comunicación constante con los usuarios: A lo largo de esta investigación se han estudiado diversas formas de cometer fraude informático y una de las más populares es el pharming, por lo que resulta de vital importancia establecer canales de comunicación seguros e informar a la comunidad en general sobre medios oficiales que posea la empresa para realizar diversos tipos de anuncios, por ejemplo, url oficial del sitio web en cuestión, correos oficiales que informen a los

usuarios de eventos o noticias, etc. De no informar debidamente a los usuarios se incrementa el riesgo que organizaciones ciberdelictivas o personas malintencionadas envíen correos fraudulentos solicitando información privada de los **usuarios** o reenviándolos a un sitio web que es una copia del original para obtener información bancaria o ser víctimas de extorción.

3.3.3.1 A nivel de usuario:

- Utilizar sitios web seguros (protocolo https): Un sitio web seguro es aquel que cuenta con los debidos certificados de seguridad, brindando confianza al usuario y evitando ser víctima de diversos tipos de fraude informático y robo de su información.
- Verificar la conexión: No se recomienda realizar transacciones online desde dispositivos ajenos al usuario y tampoco desde redes públicas, debido a que probablemente exista otra persona interceptando la información que es enviada a la aplicación web al momento de realizar la compra.
- Mantener el antivirus actualizado: A nivel de usuario promedio, puede marcar una gran diferencia tener un buen y actualizado antivirus, mucho mejor si este cuenta con un módulo avanzado de bloqueo de sitios web fraudulentos y de malware que se descarga automáticamente cuando se visita determinados sitios web.
- Seguridad en las contraseñas: Se debe evitar usar la misma contraseña en varios sitios web y además que esta no lleve información personal del usuario, debido a que puede llegar a ser fácilmente descifrable al poseer datos conocidos por los ciberatacantes (año de nacimiento, nombres, apellidos, etc.).
- Ser cautelosos con la información que llega a los correos electrónicos: No se debe enviar información a remitentes desconocidos y mucho menos acceder a links enviados por ellos debido a que pueden reenviar a sitios web fraudulentos o contener algún tipo de malware, por ello se debe tener conciencia sobre qué se hace con la información ya que esta es una de las principales formas de estafa existentes en el ciberespacio.

- Incrementar la seguridad en redes locales: En el Ecuador existe una gran vulnerabilidad en los routers de la empresa cnt, debido a que todos poseen las mismas claves de acceso y estas son de conocimiento público, por lo que cualquier persona con acceso a la red está en condición de alterar las dns del router y redireccionar a los usuarios de dicha red a sitios web fraudulentos que lucen exactamente iguales a los originales, esta vulnerabilidad ya fue estudiada y publicada por CEDIA en el año 2015, por lo que se debe crear conciencia en los usuarios finales sobre qué tan seguros están al utilizar su propia red local y a su vez cuestionarse qué tan seguro es el servicio de internet están utilizando.

CAPÍTULO IV

4. DISCUSIÓN

A lo largo del desarrollo de esta investigación se han podido comprobar el estudio realizado por Mendoza (2015) como tendencia global y herramienta principal para etiquetar, clasificar, definir al ciberespacio y a todo los elementos y acciones que lo acontecen, de tal forma que se permita la obtención de avances y actualizaciones de contenido más fácilmente, dicho estilo de referencia es el más aceptado y es aquel se ha utilizado en el transcurso de esta investigación, usando el prefijo "ciber" y generando términos tales como "ciberespacio", "ciberataques", "ciberdelincuencia", "cibercrimen", etc.

El uso de artefactos y servicios que manejan IOT ha pasado de ser un lujo para convertirse en una necesidad, es por ello que por donde se observe, existen puntos de vulnerabilidad tecnológica latentes en el diario vivir de la sociedad actual. Navarro (2009) hizo hincapié sobre ello y resaltó la importancia de la ciberseguridad como principal agente rector de dichas acciones y nuevas costumbres ahora "cotidianas" en el mundo moderno.

Cid (2017) y la convención mundial del Black Hat USA afirmaron que el año 2017 sería uno de los más recordados en materia de ciberataques debido a la gran variedad de virus y nuevos métodos de robo de información más recientes hasta la fecha, sin embargo, el escenario que se describía no era muy alentador, dando a entender que la brecha entre ciberseguridad y ciberdelitos iba a ser cada vez mayor, describiendo así al ciberespacio de los próximos años como un sitio totalmente inseguro y vulnerable ante cualquier tipo de ciberataque.

Esta investigación ha encontrado muchas opiniones divididas al respecto, donde algunas instituciones afirman cuan inseguro es el ciberespacio y otras rechazan fervientemente la idea de que se tenga que vivir con temor de usarlo, sin embargo, el desarrollo de este proyecto basado en estudios bibliográficos, entrevistas realizadas a empresas ligadas al E-commerce y experimentación consistente en prácticas realizadas

de laboratorio en materia de ciberseguridad, ha puesto en manifiesto la tendencia positiva que se tiene en cuanto al incremento de la ciberseguridad de estos aplicativos, donde, a más del desarrollo tecnológico necesario para combatir al cibercrimen, se tienen también leyes y organismos internacionales que identifican este tipo de acciones, de tal manera que el mismo escenario global que ofrece el anonimato y la ejecución de ciberataques a estas organizaciones ciberdelictivas, también está en calidad de mitigar el riesgo, condenándolas y penalizando todo su accionar afirmando así la investigación realizada por Landaburro (2017).

El planteamiento de esta investigación está orientado al análisis de amenazas en plataformas informáticas bajo el contexto de la ciberseguridad en el e-commerce en Ecuador, mediante el uso de fuentes bibliográficas, comunidades E-commerce, aplicación de entrevistas a expertos o gente relacionada a tecnologías ligadas a comercio electrónico y la ejecución de ciberataques y análisis de vulnerabilidades en un servidor propio.

Según datos estadísticos a nivel global y local, sumándose a las palabras de Navarro (2009), la tendencia sobre el incremento en los ciberdelitos está en constante crecimiento, por lo que las opiniones respecto a que tan seguros son los sitios web están divididas, mucho más si se considera un mayor grupo de ciberdelitos, sin embargo, las comunidades de E-commerce, de ciberseguridad y hacking ético están empleando cada vez más esfuerzos en la publicación y solución de posibles vulnerabilidades en diversos tipos de sistemas, esta reacción ha surgido como la necesidad que se tiene a nivel global en materia de ciberseguridad de subsanar y contrarrestar la industria del ciberterrorismo y la ciberdelincuencia.

Por otra parte, el Ecuador no es indiferente a lo que se vive en otros países, debido a que considerando el volumen de empresas E-commerce existentes hasta la fecha a nivel nacional, se puede considerar que la industria ecuatoriana no está preparada con totales garantías, sin embargo, se esfuerzan constantemente para lograrlo, aplicando estándares de seguridad y calidad a sus sistemas web mediante la utilización de buenas prácticas en materia de ciberseguridad.

CAPÍTULO V

5. CONCLUSIONES

Sintetizando los datos obtenidos a lo largo de esta investigación, se puede evidenciar que los objetivos de la misma han sido concretados, habiéndose nutrido de diferentes fuentes bibliográficas y canales de información, como también mediante la aplicación de técnicas de recopilación de datos, análisis de los mismos, y a su vez mediante prácticas que sumadas a lo anteriormente citado, proporcionaron la información necesaria para la identificación de las principales amenazas a plataformas informáticas que manejen procesos E-commerce y su debida propuesta de intervención tanto del lado del cliente como del servidor.

Las principales amenazas de ciberseguridad producidas en sitios web de e-commerce son aquellas que atentan contra la integridad de los datos de los usuarios, debido a que son los usuarios finales quienes más riesgos presentan en relación a las vulnerabilidades que pueda poseer la aplicación y el servidor web que la aloje, esto se debe principalmente a que los fallos a nivel interno son totalmente mejorables hasta el punto de poder llegar a un estado óptimo en el sistema, todo esto empleando técnicas y estándares internacionales fácilmente accesibles en esta era globalizada, sin embargo, los ciberatacantes se aprovechan del desconocimiento que posee la mayoría de cibernautas, empleando así, métodos y técnicas de robo de información y suplantación de identidad.

Las amenazas a nivel de sistemas e-commerce se enfocan en el servidor que aloje el aplicativo web y explotan estas vulnerabilidades a través del uso de xploits, malas configuraciones en el servidor y carencia de las seguridades correspondientes para un aplicativo web de e-commerce en general.

Se debe mitigar el riesgo de fraude informático mediante la generación de campañas de concientización sobre el uso que se le da a la información personal en internet, de tal manera que se obtenga un nuevo modelo de usuario promedio que esté en calidad de distinguir y elegir de manera sabia, cuándo realizar una transacción y entregar su información de pago y cuando no.

Una vez se tenga una correcta configuración de la aplicación web de e-commerce y el servidor que la aloja, se deberá también manejar una correcta política de seguridad dentro de la empresa para evitar vulnerabilidades a nivel local.

CAPÍTULO VI

6. RECOMENDACIONES

Se recomienda a los administradores de sitios web de e-commerce mejorar la seguridad de los sitios web de e-commerce mediante la instalación de certificados de seguridad, de tal manera que sean fácilmente distinguibles de los sitios fraudulentos en internet.

Estar en constante retroalimentación a base de papers y participación activa dentro de una comunidad e-commerce que publique nuevos tipos de amenazas y posibles vulnerabilidades a explotar en cms y otras tecnologías ligadas al comercio electrónico.

Establecer de forma clara la comunicación con los usuarios, de tal manera que estos sepan de lo aconteciente en la empresa de e-commerce por medio de emails y boletines de prensa que informen cualquier anomalía, promociones y novedades dentro de la compañía.

Establecer una correcta política de seguridad dentro de la empresa, de tal manera que la red y el servidor en cuestión no sean vulnerados por accesos no autorizados, permitiendo así ataques tipo sniffing dentro de la red local.

REFERENCIAS

GLOSARIO

Ciberseguridad: Protección de la infraestructura computacional y toda la información que esta almacena.

Ciberespacio: Lugar no físico de intercambio de información de manera virtual.

E-commerce: Comercio electrónico, transacciones realizadas de manera electrónica.

Plataformas Informáticas: Sistema que tiene por objetivo hacer funcionar módulos de software o de hardware de forma integrada.

Amenaza informática: Todo aquello que atente contra la seguridad de un sistema informático.

Vulnerabilidad informática: Debilidad en un sistema informático.

Fraude Informático: Toda aquella acción delictiva cometida a través de vías informáticas.

REFERENCIAS BIBLIOGRÁFICAS

Alejandro, I., González, S., Lilia, I., García, R., Abel, C. A., & Hernández, G. (2012). Nubes Privadas Que Soporten Infraestructura Como Servicio (Iaas1), *11*(3).

BID – INTAL. (2016). *Valor y tasas de crecimiento del comercio electrónico B2C en economías latinoamericanas seleccionadas y el mundo*.

Binstock, A. (2012). Dr. Dobb's The World of Software Development. Retrieved from http://www.drdobbs.com/web-development/googles-redefinition-of-the-browser-as-p/240003086?itc=edit_stub

Centeno, U., & Javier, F. (2015). Ciberataques, la mayor amenaza actual, 4–5. Retrieved from http://www.ieee.es/Galerias/fichero/docs_ opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Chicharro, A. (2009). La labor legislativa del consejo de Europa frente a la utilización de internet con fines terroristas. *Revista de Internet, Derecho Y Política 9*, 1–4. Retrieved from https://dialnet.unirioja.es/ servlet/articulo?codigo=3101795

Delgado, A. (2014). Gobernanza de Internet en Ecuador: Infraestructura y acceso. Retrieved from www.repositorio.educacionsuperior.gob.ec/ handle/28000/1579

E., C., & Center, L. (2017). Introduction to cyberspaceoperations.

Graham, C. (2017, May 13). The Telegraph. *Cyber Attack Hits German Train Stations as Hackers Target Deutsche Bah*. Retrieved from http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackers-target-deutsche/

González, A. G., García Perellada, L. R., Vigil Portela, P. E., & Garófalo Hernández, A. A. (2013). PROPUESTA DE LAS ARQUITECTURAS DE SERVIDORES, RED Y VIRTUALIZACIÓN DE UNA NUBE PRIVADA QUE BRINDE INFRAESTRUCTURA COMO SERVICIO (IAAS1). *Revista Telem@tica*.

Labdaburro, L. (2017). Ciberseguridad. *Red Latinoamericana de Análisis de Seguridad Y Delincuencia Organizada (RELASEDOR) FLACSO Sede Ecuador*, (20).

Laudon, K., & Traver, C. (2011). E-Commerce. *Prentice Hall*.

Medina, F. (2017, May 17). El ciberataque global impactó en Ecuador. *El Comercio*. Retrieved from https://www.elcomercio.com/actualidad/ciberataque-wannacry-impacto-ecuador-hackeo.html

Michalczewsky, K. (2016). Conexion Intal. Retrieved from http://conexionintal.iadb.org/2017/03/08/el-comercio-electronico-y-los-factores-de-su-desarrollo/

Pons, V. (2017). Ciberseguridad, (20). Retrieved from www.flacso.edu.ec

Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. (2015).

Sancho, C. (2017). Ciberseguridad, (20). Retrieved from www.flacsoandes.edu.ec

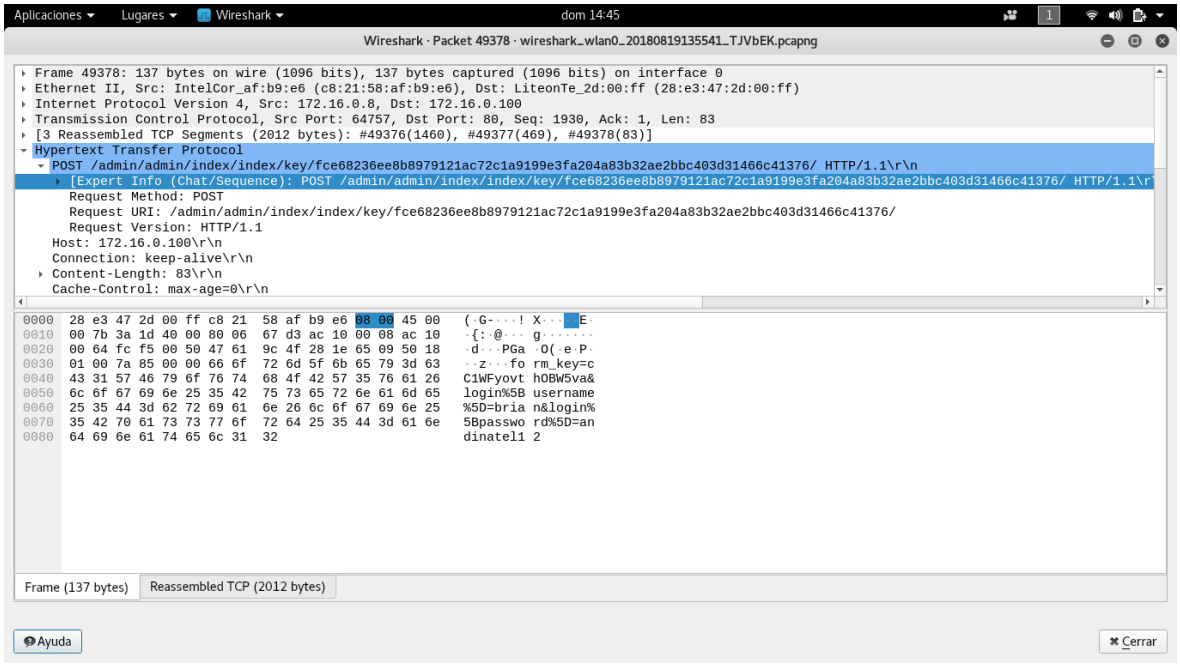
Torres, M. (2013). Ciberguerra. *Manual de Estudios Estratégicos Y Seguridad Internacional, Coordinado Por Javier Jordán*, 329–348.

Reporte de Seguridad Cibernética e Infraestructura Crítica de las Américas. (2015).
Torres, M. (2013). Ciberguerra. *Manual de Estudios Estratégicos y Seguridad Internacional, Coordinado Por Javier Jordán*, 329–348.

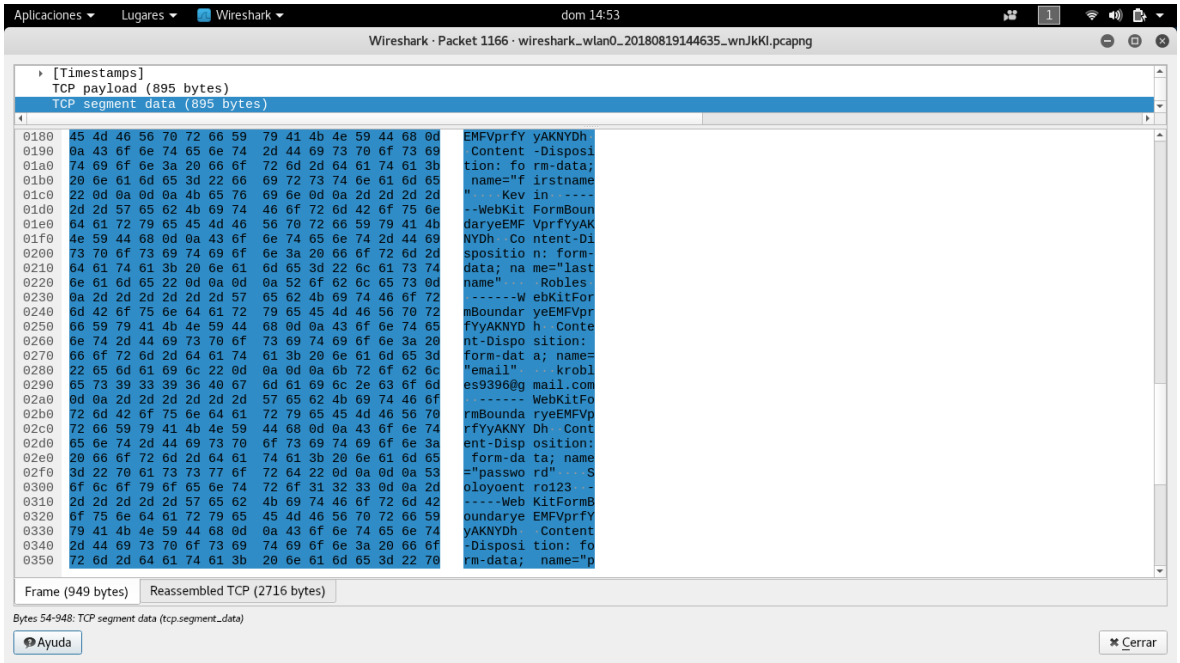
Wolf, C., & Halter E.M. (2005). *Virtualization: From the Desktop to the Enterprise*.

Zunzunegui, S., & Ignacio, J. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore*, 169–187. Retrieved from http://www.ehu.eus/documents/1736829 /2176658/08+Subijana.indd.pdf

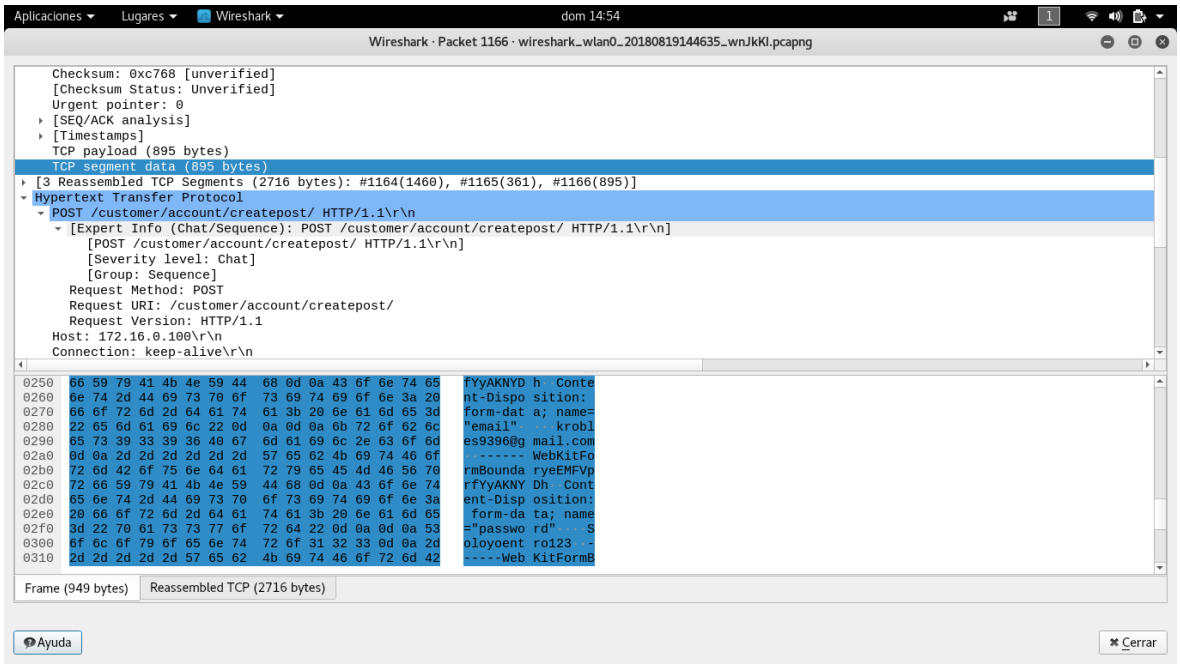
ANEXOS



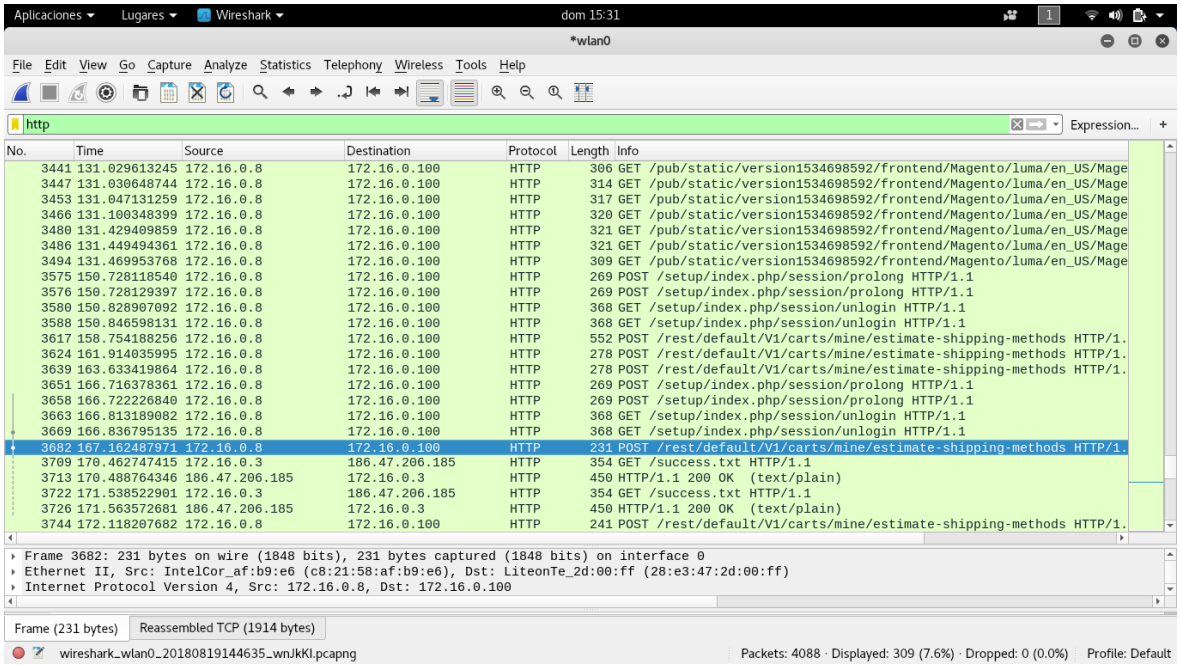
Anexo 1. Capturando usuario administrador utilizando la herramienta Wireshark.



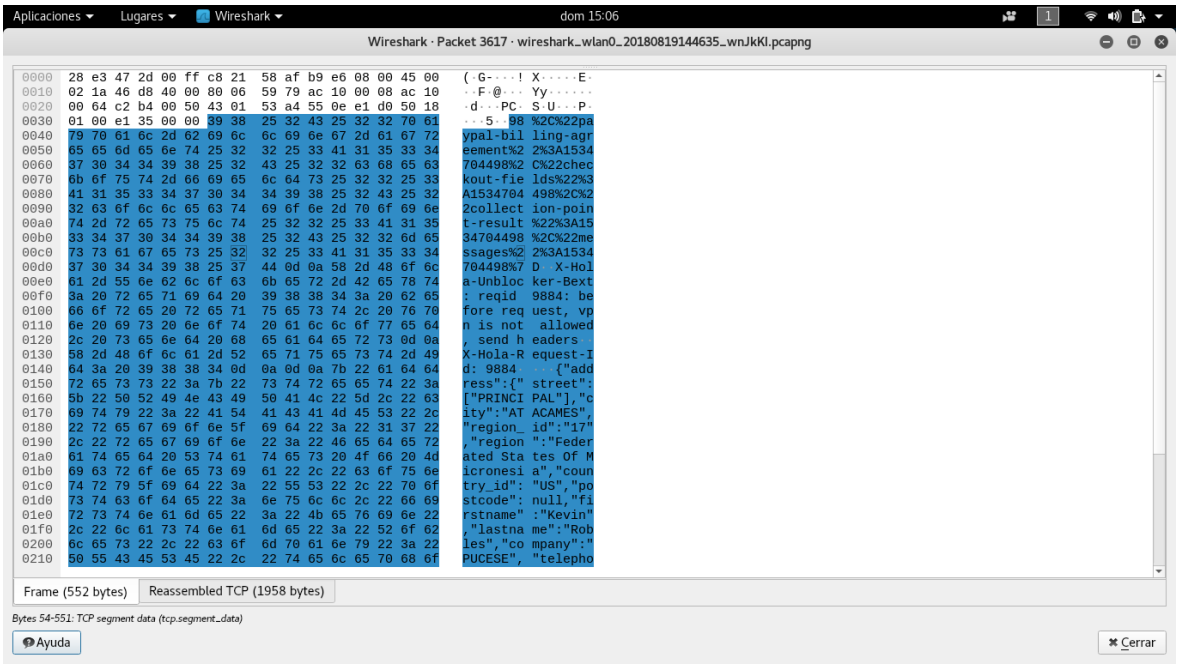
Anexo 2. Capturando Información de compra del cliente utilizando la herramienta Wireshark.



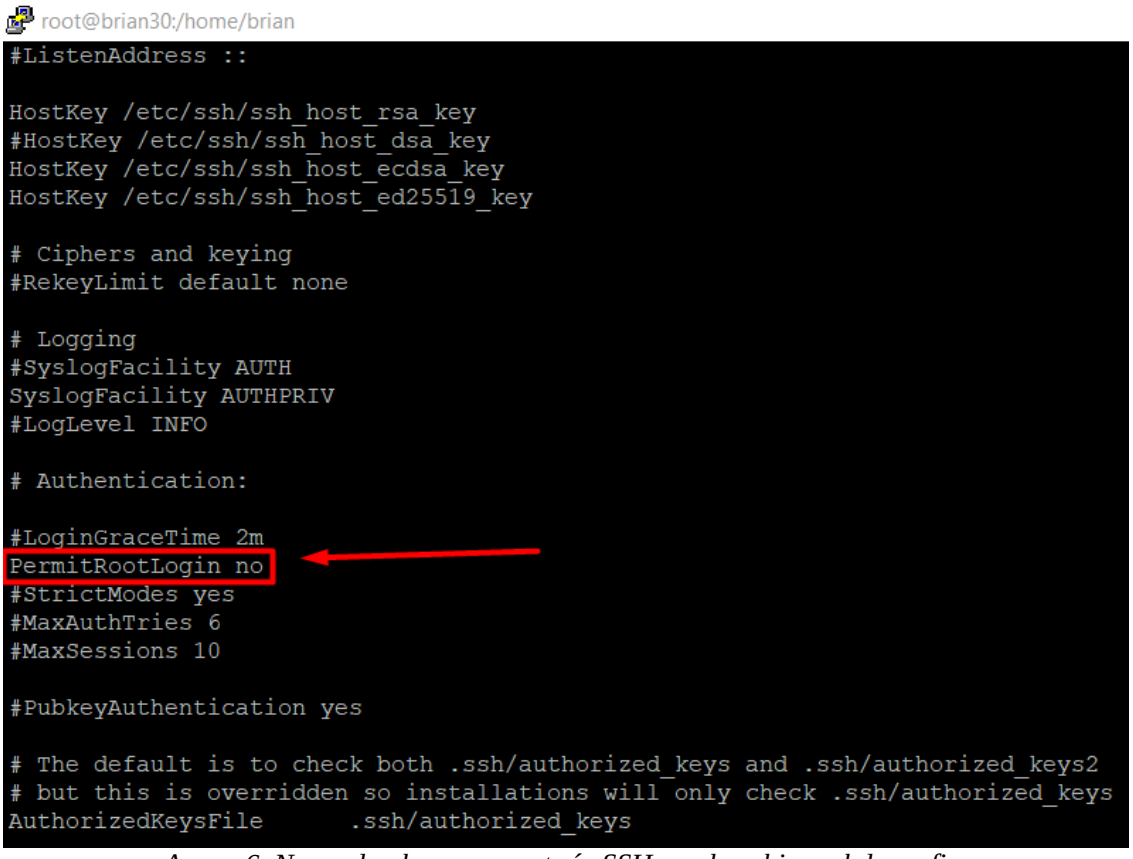
Anexo 3. Capturando información personal del cliente utilizando la herramienta Wireshark.



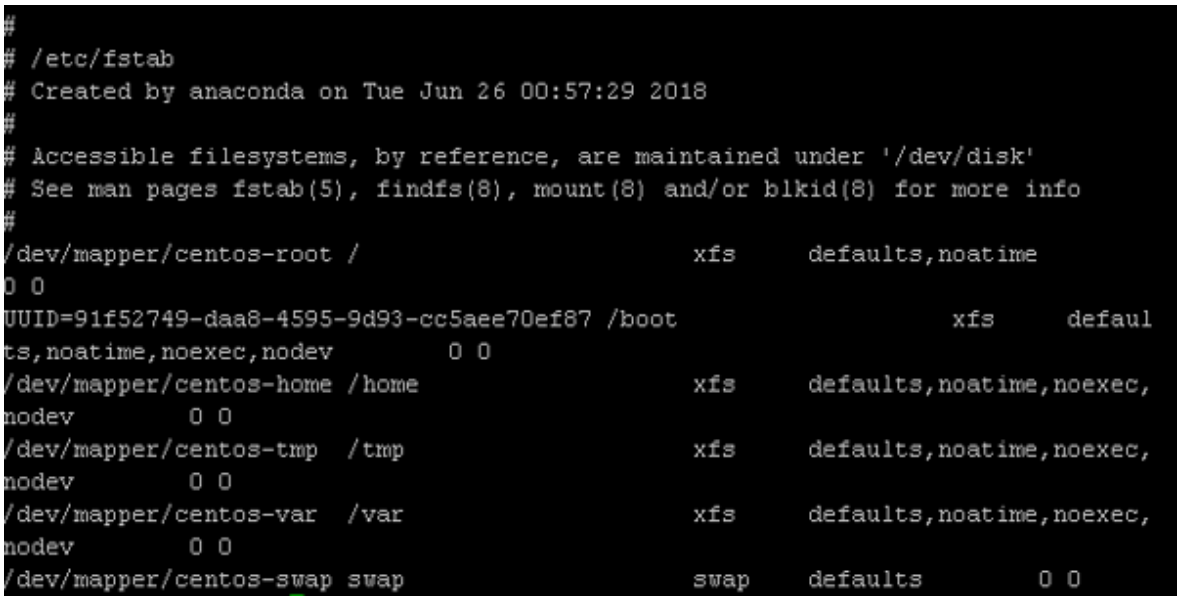
Anexo 4. Tráfico capturado utilizando la herramienta Wireshark.



Anexo 5. Capturando información de compra del cliente a detalle utilizando la herramienta Wireshark.

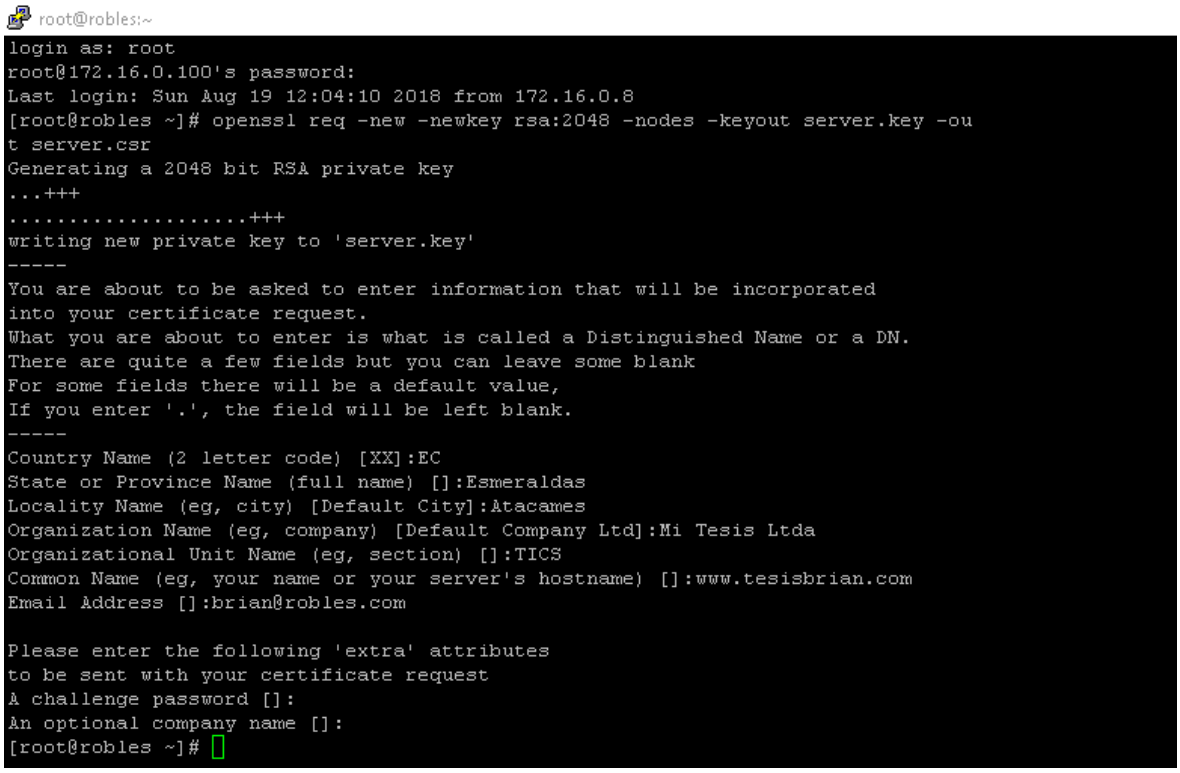


Anexo 6. Negando el acceso root vía SSH en el archivo sshd_config.

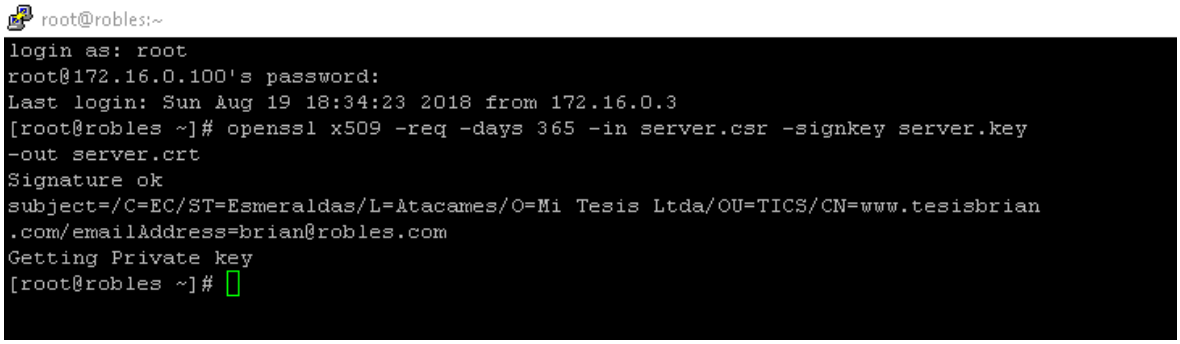


Anexo 7. Formato de almacenamiento recomendado para incrementar la seguridad del servidor.

Anexo 8. Añadiendo excepciones en el firewall de http y https.



Anexo 9. Generando clave privada y solicitud de certificado usando openssl.



Anexo 10. Generando certificado SSL propio usando open ssl x509.

root@robles:~

```
[root@robles ~]# ls
anaconda-ks.cfg  openscap_data  server.crt  server.csr  server.key
[root@robles ~]# cat server.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIC4DCCAcgCAQAwgZoxCzAJBgNVBAYTAkVDMRMwEQYDVQQIDApFc211cmFsZGFz
MREwDwYDVQQHDAhBdGFjYW11czEWMBQGA1UECgwNTWkgVGVzaXMgTHRkYTENMAsG
A1UECwwEVE1DUzEbMBkGA1UEAwwSd3d3LnR1c2lzYnJpYW4uY29tMR8wHQYJKoZI
hvcNAQkBFhBicmlhbkByb2JsZXMuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAprmILfJxhuJt+fR6CRWftaGn8SwOHO9qP7pcz91OHqk/GTily/H7
ueaVF5brHMLMz3Ij5E5QAyqgBpyPfiF5v242XzoeGL161ind+KDR76DUxtcXw3eI
Ayts4nLIXI3sPt1H6qIVHsasum6eoSl2UoSNtGcRuOr1jJusCJY/moio4YHKMiwI
uLwfAHOvqqfD8hsI4S44uIn/qNfRm5DvN7LICX3Viv9QOGg9TLko3Vpxjop216Ys
45HfrIIMcQpc8NslaBNAu3LOXt3ZZ/9JpI1LM9UGPj9oOmw92trUVSI+2z7BvkAy
7cFabC/IDCHjxTdm6EHypzmS2NAoGOsZpQIDAQABoAAwDQYJKoZIhvcNAQELBQAD
ggEBAGrBp1IHjfd9P3vc4V2t/uEwCpZukxiJBc+9cdv+xBkjhaCYlsHXveMRUSW5
doDEzULOFNtJMRHjbEfSFWfJB2ZkwVfMG9O8LnFqHGI895JFIwV7sSDco96FlQEk
HQQe3hKG9ybQusYHqilrQsFE/KtvHo/Rt2H5pvXSfooSy4Ajl6LP58dzlzPitgxf
3wycL/BJnmPlOIBzdcdQTd9wDQt11uoAs7kx6Ml4UT5PAtgPhNF2ShApWhH5CfEv
1LBMFbKnJTz+HSNkGfQoG6JyK2BOwDmodjnpdmkgKl+RCP1msNdOY1WxJQ9xUtIp
eB/Uz8rVmgydlo+Mkz6D3XNuzYo=
-----END CERTIFICATE REQUEST-----
[root@robles ~]#
```

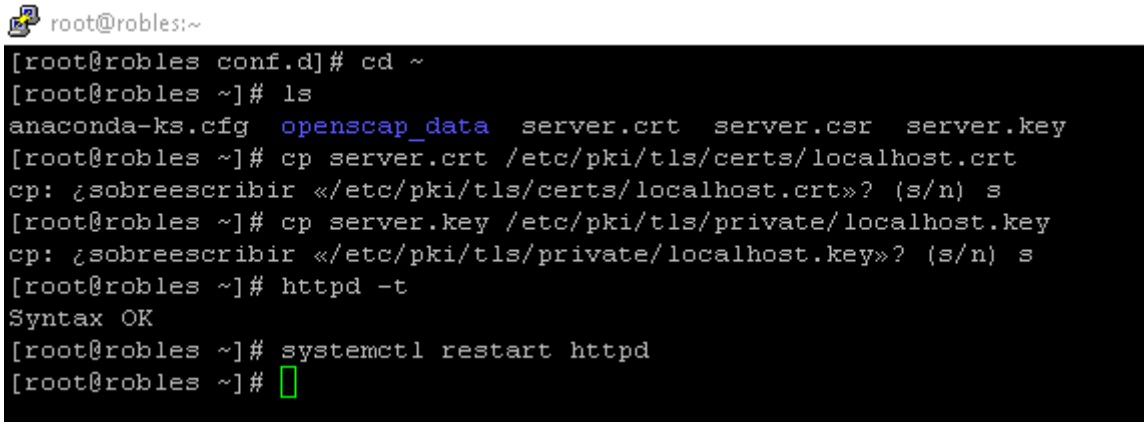
Anexo 11. Mostrando solicitud de certificado.

root@robles:~

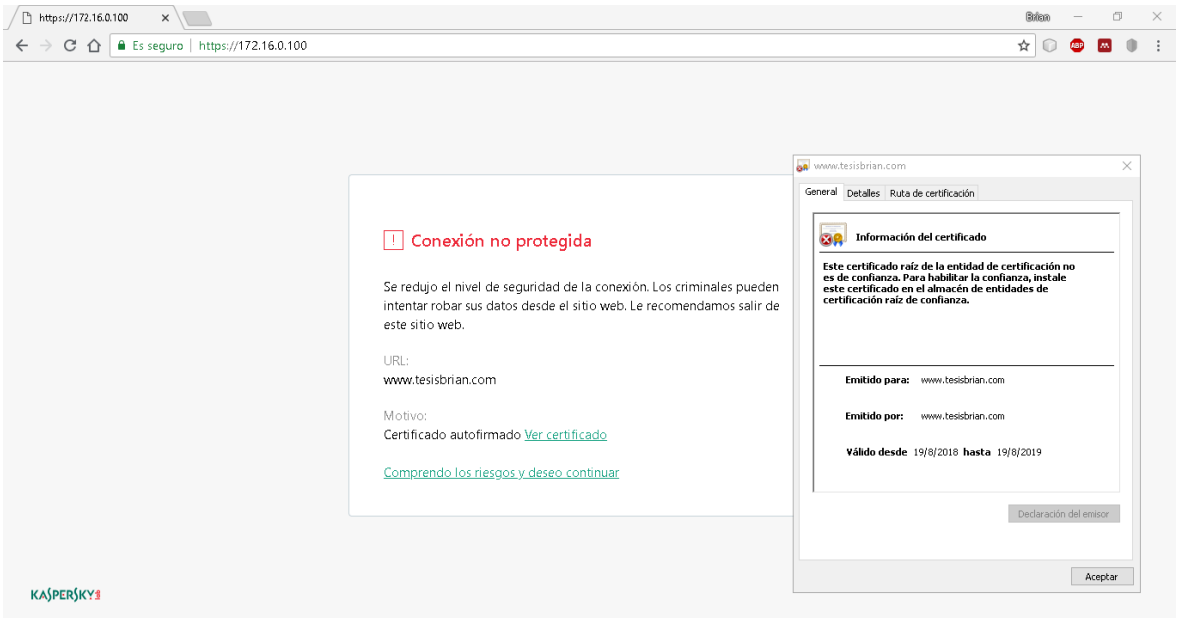
```
[root@robles ~]# ls
anaconda-ks.cfg  openscap_data  server.crt  server.csr  server.key
[root@robles ~]# cat server.key
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBKkwggS1AgEAAoIBAQCmuYgt8nGG4m35
9HoJFZ+1oafxLA4c72o/ulzP3XQeqT8ZOKXL8fu55pUXluscwszPciPkTlADKqAG
nI9+IXm/bjZfOh4YuXrWKd34oNHvoNTG1xfDd4gDK2zicshcjew+3UfqohUexqy6
bp6hKXZShI2OZxG46vWMm6wIlj+aiKjhgcoyLAi4vB8Ac6+qp8PyGwjhLji4if+o
19GbkO83ssgJfdWK/1A4aD1MuSjdWnGOinbXpizjkd+sggxxClzw2yVoEOC7cvRe
3dln/OmkjUsz1QY+P2jSbD3a2tRVIj7bPsG+QDLtwVpsL8gMIePFN2boQfKnOZLY
OCgY6xmlAgMBAAECggEABO184ebFhjgRCg84wCX8d3DUtuMXc7F7OXBfp+EiunlE
HSm4dMOtLfxrsavLPSlgxkzYVLofOUgkPK3J6+9vWsIWJ1BfbVmmEMhiACQ4sD1v
rITU9fkFcxqIeFTuKRYkwmL16kBqIWO73TLBy3+fOKckTQ2yz2VaZpJ/Ti2qqZWO
MjQ1AWvcVzPJ89qgXCkfom8GS8HfB4+gLbBSnebowQkPQdUPS2XOWF2U3aDMGjgL
yR9HCcG68xxUosooy4HtBp/CeaAqkNfqOAOj4HvbzKhI9nIVhxLr3EtA8OOuXqQX
m5Rh88oFtLXrgAdWtwGxeE7Og6HvCr4ipAluPav/QQKBgQDdnBtHB/Fjs/Ct/wIF
UCOtO5daDxRByaNIMku8yIsHM2f210XqOuTWQ66JVOvSjSPTR/cg53NWIAlmYnqD
12kDIHi8hi1N8RfPvxYuflQdxnD1OiqMOyciOspdj8Lo6+arAhOL+t20z4+iudnJ
hfx3EPGOPgdFxBx+/uQnJhN5kQKBgQDAmQGk6ml2OYK7MkSRzKQZaitNL1RG1bQh
8evb9ubkuFK1UvP33/vZNAqOZYvFMjFUxU/Hdj4ckSRT3wEdDIzLiKXulKFUlwNg
5l+rbM825rCruDoCYjFlOcgJ+8c2G1Pc2IJeDN7sxhdBOFu2DY85bLxrkoNGoroJ
YzreTu2O1QKBgQDLen21T7697EeOi7pARKAtfKzw3S2dZlZNgRj3oy+8kd/gzzL8
dV32urhOlLoi/sMpSUfJZ5sINmxLHRse3pRmcZdKiuzoRvm1H+BvGkGEAWRQ4gN9
NQcur8qF8+1kTs5CsKpf+hO92uMo5/rnxeXVMbKKB7xHu9TqaoHOzEpPcQKBgQCQ
bm3QOcZK1YgXT/QiDoAFWxwL7jFfSYWjayPAOiEe5qeHuSSh/4ODeEZuUPKHOEPM
WYehgifEDohaqULRgQbY36noB+gQYoszELAwAxJGDqvwquA9x1tZmQJNklXrWoUC
eg8R7r8Ceu8X+OO9299LZiLK3P27a+7teU+9RR133QKBgQCvAdNxvv7ipNfJUedJ
t2Xp/qdr7IwLCOGAoIzXd48j912qaBgVke1dp8vd6+/Rzpo1qUmjp+BDImCP23Lz
odFoG7HfaNzR62yzMJ+WLgwZdK36SaztSFmnZjUep6u5TkF7EVwTrvzk5bZOAAK6
PcnmyvTQU+qvWQzEqkS1weAC3A==
-----END PRIVATE KEY-----
[root@robles ~]#
```

Anexo 12. Mostrando Clave privada.

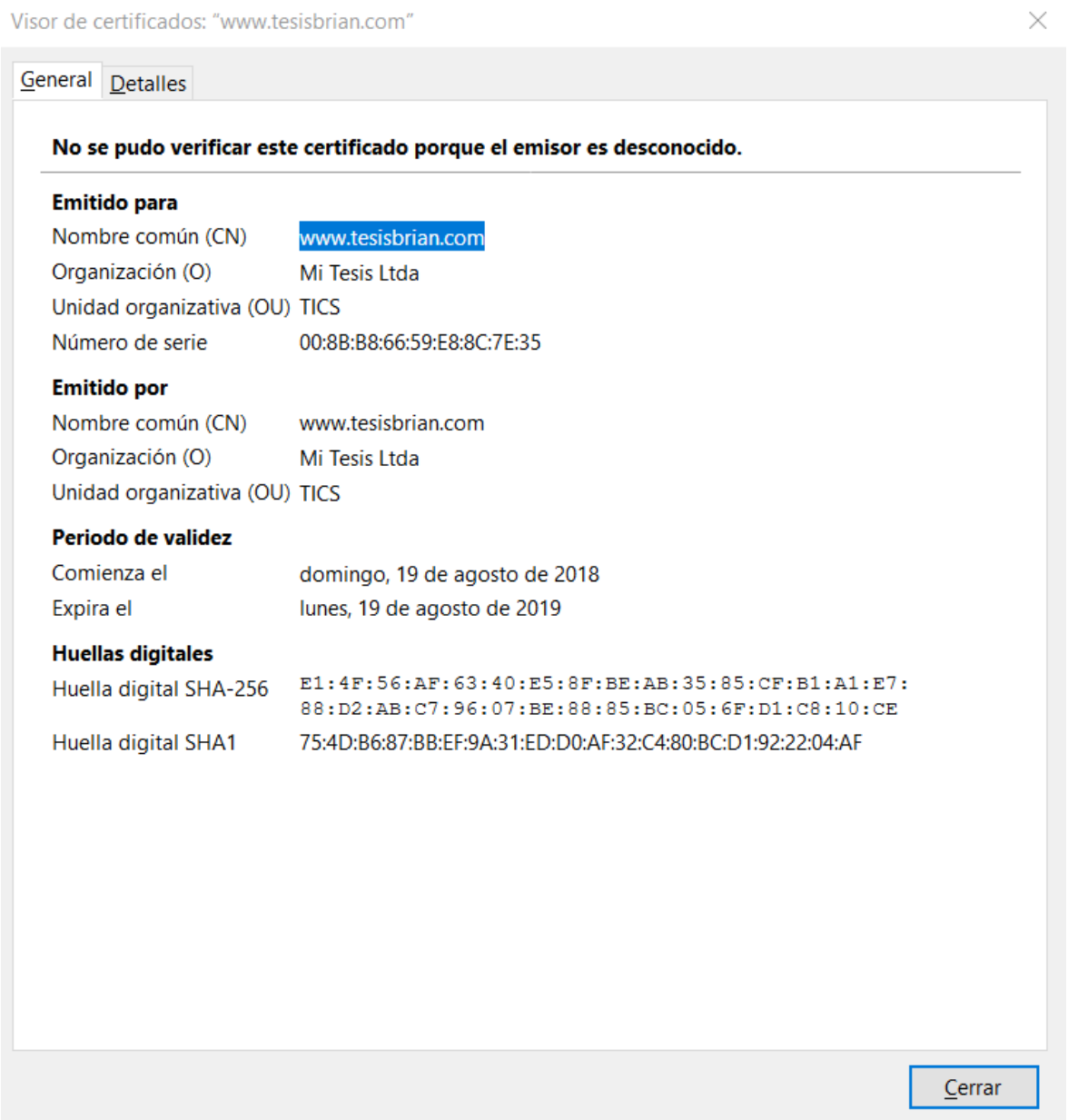
Anexo 13. Mostrando Certificado generado.



Anexo 14. Copiando certificados en los directorios certs y private.



Anexo 15. Comprobando certificado en el navegador.



Anexo 16. Huellas digitales.

https://www.youtube.com/watch?v=xxirxAbWDsE

Anexo 17. Video demostrativo de instalación de certificados (vía youtube).

https://www.youtube.com/watch?v=CG6yUUyV9hs

Anexo 18. Video demostrativo de técnicas de Hardening al servidor (vía youtube).

AMENAZAS DE CIBERSEGURIDAD EN EL E-COMMERCE

Autor: Brian Robles Bernal.

brian.robles@pucese.edu.ec

PUCESE

Entrevista para tesis de grado orientada a gerentes y desarrolladores de sitios web ligados a procesos E-commerce.

***Obligatorio**

Nombre Completo *

Nombre de la Empresa o Compañía a la que pertenece *

Cargo o posición en la compañía *

¿Alguna vez ha sido infectado su sistema E-commerce por algún malware o virus informático? ¿De qué forma se logró identificarlo y corregirlo a tiempo? *

¿Consideraría usted que el avance tecnológico perjudica el correcto funcionamiento de su sitio web gracias a la creciente ola de nuevas técnicas en materia de ciberataques? ¿Por qué? *

¿Cuáles considera usted que son las amenazas más recurrentes contra sitios web ligados al E-commerce? *

¿De qué manera se gestiona la información personal de los usuarios que realizan transacciones en su sitio web de E-commerce? *

¿Considera usted que las empresas son conscientes de la creciente ola ciberataques e invierten lo suficiente en materia de seguridad? ¿Por qué? *

¿De qué manera influye el comportamiento de los usuarios en la

explotación de vulnerabilidades en los sitios web de E-commerce? *

¿Qué repercusiones trae consigo el desconocimiento de medidas preventivas y formas de estafa por parte de los usuarios de E-commerce? *

¿De qué forma se garantiza la ciberseguridad de su sitio web? (Manejo de sistemas de seguridad, normativas, etc.) *

¿Utiliza aportes realizados por expertos provenientes de comunidades e-commerce para su sitio web? *

¿De qué manera inciden las normativas de seguridad en la disminución de ciberataques a su sitio web de E-commerce? *

¿Están preparadas las empresas en materia de ciberseguridad para afrontar el creciente volumen de usuarios e-commerce en el Ecuador? *

¿Con qué frecuencia recibe ciberataques su sitio web de e-commerce? *

¿Qué tan preparada considera que está la industria e-commerce en el Ecuador para repeler ciberataques? *

¿Qué tipo de certificados recomienda usar en un servidor que aloje un sistema E-commerce? *

Describa características y elementos que considere necesarios para un correcto funcionamiento y seguridad de un servidor que aloje sitios web E-commerce. *

Recomendaciones o datos que considere importantes mencionar en materia de ciberseguridad

Anexo 19. Formato entrevista.