UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS ECONÓMICAS
DOCTORADO

TESIS

VULNERABILIDADES EN LA SEGURIDAD DE LAS TRANSACCIONES INTERACTIVAS DE COMERCIO ELECTRONICO A TRAVES DE LA WEB

Alumno: Ruben Jorge Fusario
Director de Tesis: Maria Jose Bianco
Miembros del Tribunal de Tesis:
Maria Teresa Gasparri, Javier Garcia Fronti, Dario Piccirilli.
Fecha de la defensa de la Tesis: 25 de octubre 2017

Nullius in verba

(…no hay palabras finales…)

Lema de la Royal Society (1660)

"El conocimiento tiene el carácter de la provisionalidad y está abierto a refutaciones, cada nueva refutación significa un avance en la ciencia y en el conocimiento".

(Karl Popper)

Capítulo 3. La encuesta a futuros profesionales de TIC

Agradecimientos

A la Facultad de Ciencias Económicas de la Universidad de Buenos Aires por brindarme la oportunidad de culminar mi carrera profesional y docente con la participación en el Doctorado.

A la Dra. María Teresa Casparri que con entusiasmo y dedicación conduce la Secretaria de Doctorado y Posdoctorado de la Facultad, alentando permanentemente a los doctorandos.

A mi Directora de Tesis Dra. María José Bianco por sus valiosos consejos y recomendaciones, sin los cuales, no habría culminado el trabajo de Tesis.

Al Dr. Javier García Fronti, por su invalorable aporte profesional y experiencia en el Doctorado que me orientaron eficazmente desde un comienzo.

A los estudiantes que completaron la encuesta, pertenecientes a las carreras de la Licenciatura y de la Ingeniería en Sistemas de Información, futuros profesionales de TIC, por su valiosa colaboración.

Ruben Jorge Fusario

Resumen

En la actualidad nuestra vida depende de manera creciente de los sistemas informáticos a los cuales accedemos a través de la red Internet. Especialmente ha cobrado suma importancia la adquisición de productos y la contratación de servicios mediante operaciones de comercio electrónico. De esta forma muchas empresas y usuarios en general, han expandido su campo de acción sin tener en cuenta las limitaciones territoriales.

Para implementar el comercio electrónico se utiliza la red Internet. Si bien es evidente que existe inseguridad en ella, el público en general continúa utilizándola para realizar transacciones cada vez más sofisticadas, básicamente por la comodidad que brinda hacerlo desde el hogar o la oficina y no concurrir a las entidades bancarias y/o negocios, evitando de esta manera el traslado, las interminables colas y las esperas innecesarias.

Con respecto a la sensación de inseguridad que se genera al operar en este sistema, Wright (2002) afirma que la falta de conocimiento por parte de los usuarios de los procesos involucrados en el comercio electrónico origina, en muchos casos, la desconfianza y la reticencia al empleo del mismo.

Al respecto, en la Encuesta Global sobre Delitos Económicos 2016 (PWC Argentina 2016) se expresa que no son frecuentes las evaluaciones de riesgo de fraude por parte de las empresas. La manera más frecuente de detectar un fraude es a través del aviso informal de un empleado. Por otro lado, también indica que los delitos informáticos se consolidan como el segundo tipo de fraude más reportado (33%). En el 2014, el 21% de los casos reportados se correspondía con este delito y el 50% de las empresas consultadas temía sufrir un ataque informático en los próximos 24 meses. No obstante, solo el 30% de los encuestados disponía de un plan de respuesta a un incidente.

Son numerosas las aplicaciones que se desarrollan para ser utilizadas a través de la red Internet. Específicamente en el área comercial, las transacciones que tradicionalmente se realizaban manualmente hoy tienden decididamente hacia un ambiente informático con sistemas conectados a la red. Esta circunstancia generó un gran desafío y la aparición de situaciones desconocidas especialmente en las áreas operativas, técnicas y sobre todo en el ámbito de la seguridad informática.

Respecto de los sistemas de pago empleados en el comercio electrónico, Sumanjeet (2009) sostiene que los mismos se pueden clasificar en cuatro categorías: pago online mediante

tarjetas de crédito, pago online mediante moneda electrónica o *electronic cash*, sistema de cheque electrónico y sistema de pago electrónico basado en tarjetas inteligentes.

En el trabajo de tesis solo consideraremos los sistemas de comercio electrónico trazable no anónimos, que son aquellos en los cuales se identifica unívocamente el origen y destino de la transacción, como así también, su trazabilidad a través de la red Internet. No se considerarán los sistemas no trazables que operan con moneda electrónica, los cuales ameritan un tratamiento diferente debido a las características particulares que involucra su implementación y funcionamiento.

Definiremos como vulnerabilidades de los sistemas de comercio electrónico, a las deficiencias o debilidades que afectan exclusivamente la seguridad de dichos sistemas, por lo tanto, quedan excluidas en este trabajo de tesis las fallas que alteran el funcionamiento del sistema ocasionadas por deficiencias en el diseño, implementación, programación y/o configuración del mismo.

El origen de estas vulnerabilidades en la seguridad responde a numerosas causas, una de ellas es la demanda imperiosa de la sociedad y el comercio en general, de nuevas aplicaciones informáticas. Esto ha ocasionado que frecuentemente los programadores de software releguen la prioridad del tratamiento de la seguridad del sistema, en función de un desarrollo informático más rápido. Ante esta falta de seguridad, que en algunos casos es real y en otros aparente, se detectan vulnerabilidades en redes y sitios web que generan incertidumbre en el usuario cuando debe efectuar operaciones en el sistema.

En consecuencia, la investigación de esta tesis permite relevar y analizar las vulnerabilidades del sistema de comercio electrónico según la evaluación efectuada por estudiantes universitarios, pertenecientes a las carreras de Ingeniería y Licenciatura en Sistemas de información, los cuales a su egreso, se convertirán en futuros profesionales de la Tecnología de la Información y la Comunicación (TIC).

El diseño metodológico escogido es empírico y cuantitativo a efectos de estudiar la relación entre variables cuantificadas inherentes a la seguridad en el sistema de comercio electrónico. Se emplea el método de la estadística descriptiva para realizar el relevamiento de los datos cualitativos y su correspondiente análisis posterior. La encuesta incluye exclusivamente estudiantes de los últimos años de las carreras universitarias mencionadas, que de acuerdo al plan de estudios disponen de la capacitación técnica adecuada para evaluar las vulnerabilidades que generan falencias en la seguridad del sistema.

La opinión técnica de dichos estudiantes es relevante, dado que serán profesionales que eventualmente podrían entender e intervenir en las modificaciones a las políticas y procedimientos de seguridad, como así también, en el diseño de las aplicaciones informáticas que forman parte del sistema de comercio electrónico.

Palabras Clave: vulnerabilidades, comercio electrónico, protocolo TCP, sitio web, protocolo SSL/TLS.

Introducción General

El comercio electrónico (en inglés *Electronic Commerce*, o también *e-Commerce*) es la actividad que permite la adquisición de bienes y servicios mediante el empleo de técnicas y herramientas electrónicas que al efectuarse online[1] posibilitan automatizar el proceso de compra, reduciendo los costos y el tiempo requerido para concretar las operaciones. También se denomina comercio electrónico a la realización de transacciones financieras por medio de información electrónica, que se transmite a través de las redes de telecomunicaciones. Valle (2002)

Al respecto, Dolder (1999) afirma que "La Economía en Red asociada con la actual red informática pública Internet está transformando progresivamente la organización social de los países conduciendo, en los primeros años del siglo XXI, a una Sociedad en Red." (pág.10)

Laudon & Traver (2013) definen al comercio electrónico como "El uso de Internet, la Web y aplicaciones de software para hacer negocios. Dicho de otra manera, más formal, comprende las transacciones comerciales digitales que ocurren entre organizaciones, entre individuos, y entre organizaciones e individuos." (pág.12)

En el Estudio Especial de la Organización Mundial del Comercio (OMC) sobre Comercio Electronico (2012) ésta lo define como "la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones." (pág.1)

Este trabajo de tesis investiga las vulnerabilidades en la seguridad de las transacciones interactivas de comercio electrónico trazable a través de la web y pretende responder el siguiente interrogante; ¿Qué componente del sistema de comercio electrónico trazable presenta mayor nivel de vulnerabilidad para la seguridad del sistema, y cuál es el orden de importancia de los factores que afectan dicha seguridad, según la evaluación efectuada por futuros profesionales de TIC?

Para resolverlos, es necesario responder algunas preguntas específicas, que contribuirán a aproximarnos al problema planteado:

[1] ONLINE: En línea, los datos se procesan en forma interactiva a diferencia de lo que sería un proceso batch o de procesamiento diferido.

¿Cuáles son los elementos componentes y los requerimientos mínimos de seguridad inherentes a una operación de comercio electrónico?

¿Qué protocolos se emplean en la red de área local (LAN)[2], en la red de área extensa (WAN)[3] y en la red Internet para una comunicación confiable y segura entre el equipo del usuario y el sitio web del proveedor?

¿Cuál es el componente en el cual reside la vulnerabilidad principal de la seguridad del comercio electrónico?

¿En qué orden de importancia es posible ubicar los principales factores de vulnerabilidades para la seguridad del sitio web[4] participante de una transacción de comercio electrónico?

La elección del tema de tesis se fundamenta en la importancia creciente y sostenida del comercio electrónico en la sociedad en general, y en el incremento y sofisticación de los ataques a la seguridad del sistema, en especial sobre aquellos aspectos relativos a las vulnerabilidades que afectan al usuario, a la red y al sitio web del comerciante o proveedor.

Asimismo, ha contribuido para la elección del tema la experiencia obtenida por el autor, a través de una extensa actividad profesional y docente en carreras de grado y posgrado, en el campo de la seguridad informática y de las redes de datos.

Con respecto a la inseguridad del sistema y en particular a la evolución del fraude en el comercio electrónico en América Latina, Souza (2017) a cargo del área "*Merchant Specialized Sales* Visa América Latina & Caribe" dice:

> El rápido crecimiento posiciona a América Latina como una de las regiones más atractivas del mundo para el desarrollo del *e-Commerce* pero también para los ataques de los defraudadores. Hacia fines de 2016, en el marco de volumen de ventas, el *e-Commerce* en América Latina habrá representado un aproximado de US$ 66.700 millones. (pág.3)

Otro de los factores que confirman la relevancia del tema es que la misma fuente mencionada sostiene que el fraude con tarjetas de crédito en línea se estima en alrededor de 0,6 %, de todas las transacciones realizadas con tarjetas; esto implica que para el 2016 se

[2] LAN: Local Area Network.
[3] WAN: Wide Area Network.
[4] SITIO WEB: Es un conjunto de páginas web a las cuales se accede desde un mismo dominio o subdominio de la web.

experimentó un perjuicio aproximado de 400 millones de dólares para el área de América Latina.

El incremento de los ataques, es en la actualidad de tal magnitud que para combatir las transacciones fraudulentas, el comercio en EEUU está dejando atrás la tradicional banda metálica en favor de circuitos integrados o chips[5] incrustados en las tarjetas. A partir de octubre de 2016, los bancos de ese país hacen responsable directamente a los comerciantes y proveedores por las compras con tarjetas de crédito falsas, y esto ha ocasionado que muchos comerciantes pasaran a utilizar las tarjetas con chips.

En el comercio electrónico, un aspecto esencial es la confianza de los usuarios y proveedores para concretar las operaciones. A su vez, esa confianza está basada en la ausencia de incidentes de seguridad[6], que ocurren cuando se presentan vulnerabilidades en la seguridad de la aplicación informática del sitio web, en la estación del usuario y/o en las redes LAN e internet que las vinculan.

Dado que las causas que originan inseguridad en la operación son múltiples, resulta relevante conocer los factores determinantes y la valoración de los mismos por parte de estudiantes universitarios de las carreras de Ingeniería y Licenciatura en Sistemas de Información, que serán futuros profesionales de TIC, y por lo tanto, se ocuparán de tareas tales como el desarrollo de aplicaciones informáticas, administración de redes, dirección de las áreas de sistemas, consultorías de sistemas, seguridad informática, control de calidad, etc. De esta forma, entenderán e intervendrán desde dichas áreas, respecto al modo de acción que se implementarán para contrarrestar la inseguridad en el sistema.

El tema de la inseguridad del comercio electrónico ha sido estudiado y analizado en diferentes periodos e instituciones y, si bien se han elaborado hasta el presente numerosas encuestas a usuarios, comerciantes y empresarios que operan frecuentemente transacciones de comercio electrónico a través de la web, las mismas tienden a reflejar la percepción subjetiva que dichos agentes tienen al respecto, basadas en las experiencias personales y/o ajenas, exitosas o no, y no se fundamentan en un análisis profesional acerca de los factores determinantes que condicionan la seguridad del sistema.

[5] CHIPS: Componente de algunos milímetros cuadrados de superficie, compuesto por sílice, sobre el cual se construyen circuitos electrónicos.
[6] INCIDENTE DE SEGURIDAD: Ataque a la seguridad del sistema que ocasiona un fraude y/o robo de datos.

Es por ello que planteamos en la investigación el objetivo general de identificar, según la evaluación efectuada por futuros profesionales de TIC, el componente del sistema de comercio electrónico trazable a través de la web, que presenta mayor nivel de vulnerabilidad para la seguridad y determinar para dicho componente, el orden de importancia de los factores que afectan la seguridad del mismo. Para alcanzar este objetivo general debemos previamente plantear los siguientes objetivos específicos:

- Identificar los principales componentes que intervienen en una transferencia online de comercio electrónico trazable a través de la web y detallar los requerimientos mínimos de seguridad que debería tener la trasferencia
- Determinar los protocolos que se emplean en las redes LAN, WAN e Internet para una comunicación confiable y segura entre el equipo del usuario y el sitio web
- Determinar el componente en el cual reside la vulnerabilidad[7] principal de la seguridad del comercio electrónico
- Determinar el orden de importancia de los principales factores de vulnerabilidad en la seguridad del sitio web empleado en las transacciones de comercio electrónico

Analizaremos los objetivos planteados considerando que, desde un punto de vista técnico, una transacción de comercio electrónico es una actividad que requiere una serie de operaciones previamente programadas para actuar sobre los registros de una base de datos, de forma tal de efectuar consultas, introducir, modificar o eliminar datos. Esta actividad está estrechamente vinculada a la evolución de la informática, que experimenta avances tecnológicos relevantes en el hardware y el software que la componen. Sin embargo Tirante (2006) señala que:

> No obstante día a día con el avance tecnológico aparecerán situaciones nuevas, dignas de investigarse, donde quizá en los primeros momentos no tengamos las respuestas adecuadas, pero el hombre, el ser realmente inteligente, no podrá ser superado por las maquinas, y seguramente las hallará. (pág.97)

Con respecto al auge de la informática Lechtaler & Fusario (1999) agregan que "el fenómeno informático es la expresión de un crecimiento acelerado de la capacidad de procesar información por parte del género humano. Esta capacidad de procesamiento es la que convierte a la información en conocimiento." (pág.5)

[7] VULNERABILIDAD DE LA SEGURIDAD: Deficiencias o debilidades del sistema que afectan la seguridad del comercio electrónico.

Es por ello que la revolución informática, como una parte sustancial de la revolución de las nuevas tecnologías, es sólo la cobertura tecnológica de un proceso mucho más amplio y definitorio: el desplazamiento de la humanidad hacia la sociedad del saber (Drucker, 1993).

Por otro lado, según opina Lussato (1982), todo proceso exponencial, como el inherente a la informática, entraña algo de catastrófico, aun cuando no fuese más que por el mero hecho de que no es controlable; por tal motivo produce intranquilidad el desarrollo vertiginoso de la informática dado que se ignora si el desarrollo será a la postre benéfico o maléfico.

Como se mencionó anteriormente, un factor importante en el desarrollo del comercio electrónico es la confianza de los usuarios y de los comerciantes. Sin embargo, existen numerosos incidentes de seguridad en dicho ámbito, como también en la banca electrónica o *home banking*. La mayoría de ellos se producen debido a lo vulnerable que es el ser humano, por ejemplo, con la seguridad de sus claves y datos confidenciales -a veces tentado por algún premio- y en otras oportunidades, debido a la ingenuidad del usuario.

Al respecto, citaremos un incidente de seguridad en el ámbito bancario, ocurrido en Mar del Plata en el año 2002 durante el feriado de Semana Santa. El lunes posterior a esa fecha, numerosos empleados bancarios no pudieron ingresar al *home banking* por tener la clave bloqueada. Una vez desbloqueada la cuenta por parte del banco, los empleados se dieron cuenta que no les faltaba dinero. Sin embargo, otros que sí pudieron ingresar, porque no tenían bloqueada la cuenta, se anoticiaron que éstas habían sido vaciadas o habían sufrido extracciones importantes. Por tratarse de bancos, y ante el temor al desprestigio, mantuvieron en un primer momento el tema en reserva.

No obstante, al comunicarse entre sí los encargados de la seguridad informática se comprobó que el incidente había afectado a numerosos bancos y empleados. La investigación, basada en la dirección IP, dio como resultado que los ingresos a los sitios web de los bancos se efectuaron desde un locutorio de Mar del Plata. Por otro lado, se verificó que las cuentas que no se bloquearon tenían claves muy simples - como 1234, números del DNI o nombres de los hijos/esposa, etc.- mientras que las que se bloquearon tenían claves mucho más complejas, por lo cual se dedujo que el tercer intento de

introducir una clave errónea bloqueó la cuenta. Se comprobó también que el dinero fue transferido a cuentas de usuarios de muy bajos recursos, quienes en 2001 por disposiciones del Ministerio de Economía debieron gestionar las tarjetas de débito y que posteriormente, por necesidad económica, las vendieron a desconocidos, conjuntamente con las *passwords* correspondientes. A través de estas tarjetas de débito, el atacante retiró el dinero de los cajeros automáticos, por aquel entonces sin cámaras de seguridad.

Con referencia a la vulnerabilidad del sistema de comercio electrónico, Callegari (2017) sostiene que el usuario debe recordar siempre que al utilizar los servicios de comercio electrónico se están realizando transacciones comerciales a través de medios virtuales, y a pesar que esta situación puede generar en él una sensación de menor riesgo que en una transacción comercial física, en ambos casos se encuentra involucrado el dinero.

El sistema de comercio electrónico abarca diferentes módulos componentes, desde la computadora del cliente, pasando por las redes de comunicaciones: la red LAN del usuario, y la internet, los protocolos de comunicación y seguridad involucrados, y finalmente el sitio web del proveedor. Al respecto, debemos determinar en primer lugar los componentes del sistema de comercio electrónico que presentan mayor nivel de vulnerabilidad respecto de la seguridad del sistema. Una vez identificados se deben hallar los factores que inciden en forma determinante sobre la inseguridad en dichos componentes. La encuesta posibilita cumplimentar estas actividades y corroborar en forma total o parcial la siguiente hipótesis:

- Se espera que los futuros profesionales de TIC, determinen que el componente de mayor nivel de vulnerabilidad para la seguridad del comercio electrónico trazable se centraliza en el sitio web del proveedor, y ponderen el orden de importancia de los principales factores que afectan dicha seguridad.

Por otro lado, como hipótesis específicas se consideran las siguientes:

- El sistema de comercio electrónico trazable tiene como principales componentes: el host del cliente y su navegador web; las redes LAN e Internet, los protocolos de comunicaciones y de seguridad que brindan una conectividad confiable y segura; el sitio web del vendedor y entidades intermedias.

- Los requerimientos mínimos de seguridad de toda operación online de comercio electrónico deben ser: autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto de los datos intercambiados, el no repudio que garantiza que la transacción es consentida por cada uno de los participantes y la disponibilidad de los datos y del sistema.

Por otro lado se estima que, si se verifica que la transferencia de datos entre el host del usuario y el sitio web se efectúa a través de redes LAN e Internet mediante protocolos de comunicaciones con calidad de servicio -como el Protocolo para el Control de las Transmisiones (TCP)[8] que brinda confiabilidad- y con protocolos que brindan seguridad -como el protocolo Nivel de Puertos Seguros/Nivel de Transporte Seguro (SSL/TLS)[9] que autentica y encripta la comunicación- la vulnerabilidad principal en la seguridad del comercio electrónico no se produce en el transporte de datos entre el usuario y el sitio web del vendedor, sino que se origina en el sitio web del vendedor.

Por último, se considera que la vulnerabilidad en la seguridad del sitio web del vendedor se debe a los factores siguientes, en orden de importancia decreciente: el sitio no está respaldado por una autoridad certificante; el acceso directo al sitio se efectúa sin el empleo de una contraseña seguras ni se efectúa la prueba de Turing para diferenciar ordenadores de humanos (CAPTCHA)[10]; no se emplean los servicios de un firewall para limitar e inspeccionar el tráfico entrante y saliente del sitio; existencia de sitios web falsos que utilizan el método de *phishing*[11] que posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito; falta de actualización permanente del software utilizado en el sitio web; no se registran en el sitio las acciones de los usuarios en bitácoras[12] adecuadas; falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario; falta de validación de los datos, antes de almacenarlos en el servidor de la empresa; seguridad física del servidor insuficiente; deslealtad del personal que opera la plataforma de *e-commerce* del sitio; falta de realización de pruebas de vulnerabilidad y de cumplimiento de las normas y estándares de la industria; y por último, el sitio web del vendedor no emplea

[88] TCP: Transmission Control Protocol.
[9] SSL/TLS: Secure Sockets Layer/ Transport Layer Security
[10] CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart.
[11] PHISHING: Adquisición fraudulenta de datos confidenciales mediante suplantación de identidad.
[12] BITACORAS: Son archivos o bases de datos en los cuales se graba secuencialmente todos las acciones y eventos que se requieran registrar para su posterior análisis.

el protocolo Plataforma de Preferencias de Privacidad (P3P)[13] para el control, por parte de los usuarios, del uso que el sitio efectúa sobre sus datos personales.

La inseguridad del comercio electrónico, cuando se materializa en la captura de información confidencial de los usuarios, también ha dado lugar a un comercio paralelo: la venta de dicha información en la web conocida como el cibermercado negro de datos robados. De este modo los datos de la tarjeta de crédito de un usuario pueden venderse entre 2 y 90 dólares, dependiendo del patrimonio y solvencia financiera del usuario; los datos de la cuenta bancaria entre 80 y 700 dólares; cuentas de correo electrónico entre 5 a 12 dólares, según datos de Panda Security (2012), Danchev (2011) y Symantec Inc. (2010 y 2011).

La problemática de la inseguridad en el comercio electrónico ha dado lugar a numerosos estudios y publicaciones al respecto Traver (2014) dice:

> ¿Qué es una transacción comercial segura? Cada vez que usted entra en un mercado se expone a riesgos, incluyendo la pérdida de su privacidad (información acerca de lo que compro). Su principal riesgo como consumidor es no obtener aquello por lo que pago. De hecho, ¡podría pagar y no recibir nada! O peor aún, ¡que alguien le robe su dinero mientras esta en el mercado! Como un comerciante en el mercado, su riesgo es que no reciba el pago de lo que vende. Los ladrones toman mercancía y luego escapan sin pagar nada, o le pagan con un instrumento fraudulento, una tarjeta de crédito robada o dinero falsificado. (pág. 265)

En seguridad informática existe un concepto básico que indica que la seguridad de cualquier sistema teleinformático[14] puede ser quebrantada si se utilizan los recursos y el tiempo suficiente. Podemos decir entonces que no existe la seguridad absoluta y esto es aplicable también al caso del comercio electrónico. No obstante, sí se pueden obtener diferentes niveles o estados de seguridad de los sistemas.

Por lo expuesto, el concepto de seguridad es relativo y al respecto Cano (2013) advierte que ésta "es subjetiva y será diferente para diferentes personas, pues cada una de ellas determina su nivel de riesgo y evalúa sus estrategias compensatorias (*trade – off*) frente a los controles."(pág.26).

[13] P3P: Platform for Privacy Preferences.
[14] SISTEMA TELEINFORMATICO: Sistema compuesto por componentes informáticos y de comunicaciones.

En el caso particular del comercio electrónico, el evento más temido es el robo de los datos de la tarjeta de crédito. Muchos usuarios evitan realizar compras online por temor a que la información de sus tarjetas de crédito se vea comprometida. En EEUU el consumidor está asegurado contra pedidas gracias a la ley federal, que limita la responsabilidad de los individuos a 50 dólares por tarjeta de crédito robada. Para montos superiores a 50 dólares, la compañía que expide la tarjeta es la que por lo general paga el monto defraudado. En algunos casos, se declara responsable al comerciante por no verificar la cuenta ni consultar la lista de tarjetas inválidas publicadas.

En la actualidad, el robo de datos de tarjetas de crédito se produce debido al *hackeo* sistémico de las bases de datos de los sitios web de los proveedores. Es así, como en marzo del 2010 Albert González fue condenado a 20 años de prisión por organizar el mayor robo de números de tarjetas de crédito en la historia estadounidense. Junto con otros dos cómplices rusos, González irrumpió en los sistema informáticos centrales de TJX, BJs, Barnes & Noble y otras compañías, y robo más de 160 millones de números de tarjetas de crédito, provocando a estas empresas pérdidas por más de $ 200 millones de dólares. (Traver, 2014, pág. 280)

Dada la amplia gama de posibilidades del comercio electrónico, el estudio de la tesis sólo analizará las operaciones trazables realizadas mediante tarjetas de crédito, y no se incluyen las transacciones efectuadas por pago electrónico.

Un caso particular de comercio electrónico es el pago electrónico. Un protocolo de pago electrónico consiste en una serie de transacciones al final de las cuales, se ha realizado un pago mediante el uso de un testigo que ha sido acuñado por una entidad autorizada. (Valles, 2002).

El comercio electrónico constituido por los sistemas de pagos electrónicos (EPS)[15], en el cual se realiza la transferencia del dinero entre compradores y vendedores a través de una entidad financiera autorizada por ambos y las tarjetas de crédito, facilita las transacciones financieras a través de la red Internet, que de este modo resultan rápidas y de bajo costo.

En Argentina el incremento del comercio electrónico es incesante y solo presenta en la actualidad una limitación en el aspecto logístico, para la distribución del bien en tiempo y forma al usuario comprador.

[15] EPS: Electronic Pay Systems.

Según la Cámara Argentina de Comercio Electrónico (2017), el *e-Commerce* en Argentina creció 61,7% en 2014, 58% en 2015 y 51,0 % en el 2016. La tendencia en preferencias en la región, se ha inclinado hacia los envíos a domicilio y el mercado argentino no es la excepción: el 73% de los compradores consultados eligieron esa modalidad, un 59% retiró el producto en el punto de venta y el 30% lo buscó en una sucursal del correo.

Asimismo, el diario Bae Negocios (2017) señala:

> Más allá del efecto inflación, la facturación del comercio electrónico en la Argentina volvió a incrementarse durante el año pasado. El alza fue del 51%, aún más importante que la suba de precios que sufrió el país durante 2016. Según los resultados del estudio anual que Kantar TNS realiza para la Cámara Argentina de Comercio Electrónico (CACE), los $ 102.000 millones de facturación corresponden a 47 millones de órdenes de compra, un 24% más que en 2015. Durante 2016 el ticket promedio de compra fue de $ 2.185 y en ese periodo se comercializaron 75 millones de productos, casi el doble que en el año anterior. (diariobae.com, 2017, pág. 16).

Para el desarrollo del tema de la tesis se han considerado en primer lugar los tipos de transacciones online de comercio electrónico, sus componentes, y el tratamiento de la información teniendo en cuenta la seguridad en el traslado de la misma desde el momento de carga de datos por parte del usuario, la transferencia a través de la web y su almacenamiento en los servidores finales.

Al referirse a las transacciones online Lechtaler & Fusario (1999) afirman:

> Se dice que un proceso teleinformático se ejecuta en la modalidad en línea cuando los datos de entrada pasan directamente desde el lugar de origen al lugar de utilización y, viceversa, cuando los datos procesados se envían directamente desde el computador al usuario. (pág.19)

Debemos diferenciar entre comercio electrónico (*e-Commerce*) y los negocios en línea (*e-Business*); el primero incluye transacciones que trascienden las fronteras de la empresa, mientras que el segundo se trata de tecnologías informáticas aplicadas a procesos que ocurren dentro de la empresa. No obstante, algunos autores como Rayport & Jaworski (2003) consideran que el comercio electrónico abarca toda la infraestructura del sistema de

información de la empresa, como así también los diferentes tipos de intercambio comercial de la misma.

El trabajo de tesis comprende tres capítulos; los dos primeros constituyen el marco teórico que da sustento a los conceptos técnicos incluidos en la encuesta, y en el tercero se evalúan los resultados de la misma a tenor de los objetivos e hipótesis planteados.

En el capítulo uno se describe la estructura del comercio electrónico trazable, a efectos de definir sus características principales, la arquitectura de la red Internet que da soporte de comunicaciones al comercio electrónico a través de los sistemas autónomos[16] y *routers* de borde[17] que conforman dicha red.

Se detalla la evolución del comercio electrónico, su impacto en las actividades que acompañan el crecimiento del comercio global y se presentan y analizan sus principales modalidades. Definido el tipo o modelo de comercio electrónico considerado en la tesis, se describen sus componentes principales y características.

Un aspecto relevante del comercio electrónico son los medios de pagos, que se analiza en lo que concierne a esta tesis donde se ha considerado el empleo de tarjetas de crédito, por constituir un método trazable de pago y por tratarse del medio más difundido.

Una vez definida la estructura del comercio electrónico, se describen los principales aspectos inherentes a la seguridad informática, como también los ataques y amenazas más frecuentes que experimentan las aplicaciones en la web, que pueden afectar la seguridad del comercio electrónico. Se detallan los aspectos que hacen a la seguridad de una transacción comercial a través de la web y los principales riesgos que tienen los usuarios cuando operan para realizar dichas transacciones.

Concluye este capítulo con las principales técnicas para la protección de datos en Internet, basadas en métodos criptográficos y esteganográficos y su factibilidad de empleo en el proceso de comercio electrónico para dotar al mismo de un determinado grado de seguridad[18] para la información inherente a la operación.

[16] SISTEMAS AUTONOMOS: Conjunto de redes y routers que son administrados por una única autoridad.
[17] ROUTERS DE BORDE: Equipo enrutador de paquetes ubicado a la entrada/salida de los sistemas autónomos en Internet.
[18] GRADO DE SEGURIDAD DE LA INFORMACION: No existe la seguridad absoluta en informática por lo cual se consideran grados o niveles de seguridad.

En el capítulo dos se completa el marco teórico que brinda sustento a la encuesta, se evalúan las vulnerabilidades de la seguridad en la web puestas de manifiesto a través de los delitos cibernéticos y se detallan aspectos sobresalientes de la guerra cibernética[19] que se libra en la red Internet y que también afectan al comercio electrónico.

Dado que el delito cibernético tiene diferentes variantes y la mayoría de los ataques se llevan a cabo mediante el denominado código malicioso o *malware*, se analizan ~~las~~ diferentes amenazas como ser: virus informáticos[20], gusanos[21], troyanos[22], *crackers*[23], hackers[24], PUPs[25], *botnets*[26], *ramsonware*[27], etc.

Constituye un caso especial el fraude que se realiza con tarjetas de crédito, que como se indicó anteriormente es el medio de pago considerado en la presente tesis y el más difundido para operar en comercio electrónico.

Por otro lado, también se analizan los dos protocolos que brindan confiabilidad y seguridad a las transacciones de comercio electrónico que se realizan a través de la red Internet, el protocolo TCP de la familia TCP/IP[28] que posee calidad de servicio y por esta razón brinda confiabilidad para la comunicación, y el protocolo SSL/TLS que ofrece seguridad en las transacciones, con sus fortalezas y debilidades.

En relación a los protocolos de comunicaciones Forouzan (2006) afirma:

> Un protocolo es un conjunto de reglas que gobiernan la comunicación de datos. Un protocolo define que se comunica, como se comunica y cuando se comunica. Los elementos claves de un protocolo son su sintaxis, su semántica y su temporización. (pág. 18)

[19] GERRA CIBERNETICA: También conocida como guerra informática o guerra digital.
[20] VIRUS INFORMATICO: Software malicioso que reemplaza archivos ejecutables por otros para alterar el funcionamiento del equipo informático.
[21] GUSANOS: Software malicioso que aparentemente para el usuario es inofensivo, pero que al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
[22] TROYANOS: Software malicioso que aparentemente para el usuario es inofensivo, pero que al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.
[23] CRACKERS: Atacantes de sistemas informáticos que violan la seguridad del sistema y toman el control de éste, obtiene información, borran datos, etc.
[24] HACKERS: Desde el punto de vista de la seguridad informática es un atacante que descubre las debilidades de un computador o de una red informática y ataca la confidencialidad y/o integridad de los datos.
[25] PUPs: Potentially Unwanted Programs
[26] BOTNETS: Red de robots informáticos o bots.
[27] RAMSONWARE: Programa informático que encripta, sin autorización del usuario, archivos del sistema infectado y pide un rescate para desencriptarlos.
[28] TCP/IP: Transmission Control Protocol / Internet Protocol.

Para poder desafectar la red que comunica el host del usuario[29] con el servidor del proveedor, como causa principal de la vulnerabilidad en la seguridad del sistema, se deben analizar los servicios brindados por ambos protocolos y determinar si son suficientes para asegurar confiabilidad y seguridad en la comunicación.

Complementado el análisis de los protocolos que ofrecen seguridad en la web también se detallan brevemente las características de los IPSEC[30], SSH[31], 3D secure[32], iKP[33] y SET[34].

Se analizan también las principales amenazas y ataques que enfrenta el sitio web del vendedor. Primero por ser una aplicación informática más, que opera en la insegura red Internet y segundo porque se trata de un sistema que gestiona recursos monetarios, bienes y servicios, lo que implica una atracción permanente para los delincuentes cibernéticos. Dichos factores se incorporan en la encuesta para su evaluación por parte de los estudiantes en lo que concierne a su importancia relativa respecto de la seguridad del sitio web.

Cabe aclarar que no se incluyen en la encuesta los factores que afectan la seguridad del host del usuario en su conexión con la red Internet, debido a que las alternativas de implementación son numerosas y en general, son las mismas que puede experimentar cualquier computador conectado a la red Internet. Se espera que se incorpore en estudios posteriores el host del usuario, como posible fuente de vulnerabilidad en la seguridad del comercio electrónico.

En el capítulo tres se encara la tarea de evaluar la ponderación técnica de los futuros profesionales de TIC respecto de las vulnerabilidades en la seguridad del sistema de comercio electrónico, a través de una encuesta confeccionada a tal efecto.

Se analizan las respuestas de estudiantes universitarios de los dos últimos años de la carrera de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires, y de Ingeniería en Sistemas de Información de la Facultad Regional Buenos Aires, de la Universidad Tecnológica Nacional.

[29] HOST DEL USUARIO: Comprende la PC y el navegador correspondiente.
[30] IPSEC: Internet Protocol Security
[31] SSH: Secure Shell
[32] 3D SECURE: Sistema de pago seguro con tarjeta.
[33] ikP: Internet Keyed Payment Protocols
[34] SET: Secure Electronic Transaction

En particular se evalúan las percepciones que dichos estudiantes consideran relevantes respecto del componente que presentan mayor nivel de vulnerabilidad en la seguridad del comercio electrónico, como así también, el orden de importancia que ellos otorgan respecto de los factores determinantes que afectan esa seguridad, en particular, los correspondientes al componente del sistema con mayor nivel de vulnerabilidad.

La investigación es empírica[35] y cuantitativa a efectos de estudiar la relación entre variables cuantificadas inherentes a la seguridad en el comercio electrónico. Asimismo, al realizar una investigación cuantitativa se fue posible analizar los datos de manera numérica desde el campo de la estadística.

En el marco teórico se consideran los conceptos y factores determinantes relativos a la seguridad en comercio electrónico, que son evaluados por los estudiantes de sistemas a fin de priorizar su incidencia en las vulnerabilidades del comercio electrónico.

Hurtado & Toro (2001) afirman que la investigación cuantitativa tiene una concepción lineal, es decir que existe claridad entre los elementos que conforman el problema, que lo define y limita y permite saber con exactitud dónde éste se inicia y qué tipo de incidencia existe entre sus elementos.

Para la investigación desarrollada, y a efectos de dar respuesta a las preguntas que motivan la misma, se emplea estadística descriptiva que permite presentar los datos, destacar su estructura y organizar los mismos en gráficos para detectar las características sobresalientes y las inesperadas.

La elaboración de gráficos posibilita analizar los datos e identificar sus características sobresalientes. Dado que éstos se obtienen a partir del estudio prospectivo, son de tipo cualitativos y dicotómicos.

Respecto del método estadístico Orellana (2001) afirma:

> La ventaja de los métodos estadísticos es que aplicados sobre datos obtenidos a partir de muestras aleatorias permiten cuantificar el error que podemos cometer en nuestra

[35] INVESTIGACION EMPIRICA: La Investigación empírica está basada en la observación para descubrir algo desconocido o probar una hipótesis y se fundamenta en la acumulación de datos que posteriormente se analizan para determinar su significado.

> estimación o calcular la probabilidad de cometer un error al tomar una decisión en un test de hipótesis. Finalmente, cuando existen datos para toda la población (censo) no hay necesidad de usar métodos de estadística inferencial, ya que es posible calcular exactamente los parámetros de interés. (pág. 2)

Como se señaló la población está conformada por estudiantes universitarios de sistemas de información seleccionados a través de una muestra aleatoria constituida por ciento diez (110) estudiantes de los últimos años de las carreras de Ingeniería en Sistemas de Información de la UTN - FRBA[36] y de la Licenciatura en Sistemas de Información de la UBA FCE[37]. Al respecto, (1972) afirma que "una población es el total de las observaciones concebibles de un tipo particular. Una muestra es un número limitado de observaciones de la población, escogidas de tal modo que permita que todas las observaciones posibles tengan la misma probabilidad de presentarse." (pág. 49)

Con respecto al analisis de las estadisticas Freund, Miller, & Miller (2001) afirman "tradicionalmente, los problemas de inferencia estadística se dividen en problemas de estimación y pruebas de hipótesis, aunque en realidad todos son problemas de decisión." (pág. 322)

Podemos concluir que el trabajo de tesis centra el problema de la seguridad del comercio electrónico trazable en el sitio web del proveedor. De este modo descarta la inseguridad en el transporte de los datos entre el host del usuario y el sitio web, debido al empleo del protocolo Nivel de Puertos Seguros / Nivel de Transporte Seguro (SSL/TLS) que encripta y autentica eficazmente la comunicación, siempre que éste se encuentre actualizado y correctamente implementado. Por otro lado, la confiabilidad en la comunicación está garantizada por el protocolo de nivel de transporte TCP.

El protocolo SSL/TLS utiliza los certificados digitales para autenticar al sitio web y eventualmente al proveedor. Al respecto en el sitio Certsuperior, Noriega (2014) dice:

> Tampoco podemos perder de vista que los certificados SSL/TLS harán las empresas más productivas porque ahorrará muchos pasos de la compra y venta de los productos. En la actualidad muchos de los posibles clientes lo que buscan es la inmediatez, la

[36] UTN FRBA: Universidad Tecnológica Nacional – Facultad Regional Buenos Aires.
[37] UBA FCE: Universidad de Buenos Aires – Facultad de Ciencias Económicas.

> compra instantánea, la garantía de no tener que trasladarse de un lugar a otro para obtener lo que quieren, con los certificados SSL/TLS podrán estar seguros de que pueden dar sus datos de tarjetas de crédito o débito sin riesgo alguno. (Noriega, 2014)

Por otro lado, definir desde un punto de vista profesional dichas vulnerabilidades, es la base para investigaciones futuras, que en función de las nuevas tecnologías emergentes en seguridad informática, desarrollarán nuevas estrategias destinadas a contrarrestar las vulnerabilidades halladas. De esta forma, se avanzará en el conocimiento sobre las posibles debilidades en la seguridad del comercio electrónico y su correspondiente tratamiento.

Por último, se justifica la selección del universo en la idoneidad de los estudiantes que participan de la encuesta para detectar y evaluar en su magnitud real las debilidades en la seguridad del sistema de comercio electrónico, debido a lo avanzado en la carrera universitaria en la cual se encuentran, que les posibilita comprender la operatoria inherente a las transacciones comerciales online, conocer en detalle los procesos que se presentan desde el mismo instante en el cual se ingresan los datos a través del host del usuario y luego se efectúa la transferencia de éstos por las redes LAN e Internet hasta su almacenamiento y procesamiento en los servidores y bases de datos del sitio WEB del proveedor.

<u>Capítulo 1.</u> Estructura del comercio electrónico y requerimientos de seguridad en la red Internet.

Introducción

En este capítulo se describe la estructura y características del comercio electrónico trazable[38], los alcances y límites del mismo en lo que concierne al desarrollo del trabajo de tesis. Asimismo, se analiza la estructura de la red Internet que da soporte de comunicaciones al comercio electrónico a través de los sistemas autónomos[39] que conforman dicha red.

Se detalla la evolución del comercio electrónico y su impacto en actividades que acompañan el crecimiento del comercio global como son: la publicidad en tiempo real, el almacenamiento en la denominada computación en la nube que permite guardar el contenido (datos) y el software de los consumidores en servidores de Internet a los cuales se pueden acceder desde dispositivos móviles o no. También nos detendremos en la acumulación de volúmenes crecientes de información por parte de las empresas que "registran" las numerosas interacciones online que ocurren en la web dando origen al denominado "Big Data", que en general se analiza mediante sofisticados paquetes de software para identificar patrones de conducta y preferencias de los usuarios.

Se presentarán los principales modelos de comercio electrónico: B2C (*business to consumer)*, B2E (*business to employee*), B2B (*business to business*), C2C (*consumer to consumer*), G2C (*goverment to consumer*), C2B (*consumer to business*) y M2B (*movile to business*). Cabe aclarar, que en este trabajo de tesis se considera el modelo B2C, por constituir el más frecuente en el mercado. Una vez definido el modelo de comercio electrónico seleccionado, se describen sus componentes y características principales.

Un aspecto relevante del comercio electrónico son los medios de pagos, los cuales se describen, en lo que concierne a sus principales características, comenzando por el tradicional contra reembolso, y continuando por cargos en cuenta bancaria, tarjetas de crédito, intermediarios electrónicos, tarjetas inteligentes, micro pagos o monederos virtuales y terminal de punto de venta virtual. Para este trabajo se ha considerado el empleo

[38] COMERCIO ELECTRÓNICO TRAZABLE: La trazabilidad se refiere a la posibilidad de determinar el origen y destino de la transacción comercial.
[39] SISTEMA AUTONOMO: Conjunto de redes y routers administrados por una única autoridad.

de tarjetas de crédito, por constituir un método trazable de pago y además ser el más difundido.

Definida la estructura del comercio electrónico se analizarán los principales aspectos inherentes a la seguridad informática, y los ataques y amenazas más frecuentes que experimentan las aplicaciones en la web, los cuales, también pueden afectar la seguridad del sistema de comercio electrónico.

La determinación de las amenazas y ataques que eventualmente puedan afectar la seguridad del modelo seleccionado posibilitará elaborar la encuesta. Ésta, orientada a estudiantes de los últimos años de las carreras de Licenciatura e Ingeniería en Sistemas de Información, permitirá reflejar la opinión técnica de estos futuros profesionales respecto de la pertinencia y grado de importancia de dichos ataques para la seguridad del comercio electrónico. Para ello deberán evaluar los aspectos que hacen a la seguridad de una transacción comercial a través de la web y los principales riesgos que tienen los usuarios cuando operan para realizar dichas transacciones.

Por último, se describirán las principales técnicas para la protección de datos en Internet, basadas en métodos criptográficos y esteganográficos, y su factibilidad de empleo en el proceso de comercio electrónico para dotar al mismo de un determinado grado de seguridad que resulte aceptable tanto para los usuarios, como así también, para los proveedores.

1.1. La red Internet y el comercio electrónico

La actividad del comercio electrónico se efectúa a través de transacciones digitales entre organizaciones, entre individuos, y entre organizaciones e individuos. Estas transacciones se realizan mediante la web y las aplicaciones de software móvil y de escritorio correspondientes. Por lo tanto, la red Internet es la estructura de comunicaciones fundamental que posibilita concretar las operaciones. La aparición de esta red en la década del 80 ha generado una verdadera revolución en todas las ciencias; las llamadas duras como así también las ciencias sociales, podemos afirmar que existe un antes y un después de la creación de la red Internet. Al respecto Valles (2002) afirma que nuestra forma de relacionarnos está cada vez más ligada a las redes de ordenadores y en particular a Internet.

La evolucion de la informática y de las telecomunicacuiones dió lugar a una nueva disciplina la teleinformatica, con respecto al proceso evolutivo de esta ultima Lechtaler & Fusario (2015) afirman:

> El proceso ha sido secuencial. Primero los cambios comenzaron con el desarrollo de la computadora. Luego continuaron cuando se llegó a un punto en el que ellas podían ser operadas por personas de todas las edades, y especialistas; después aparecieron los cambios que se generaron mediante su uso como herramienta. Así es que facilitaron, entre otras cosas, la construcción de equipos de comunicaciones inteligentes. Estos a su vez, permitieron digitalizar prácticamente toda la red mundial de telecomunicaciones, cambiando además la forma de planificar, diseñar y operar. Por último, apareció la idea genial de la red Internet como herramienta de interconexión de computadoras de consumo masivo. Todo ello revoluciono al mundo. Ya nada es igual a como lo fue hace solo veinte años. (pág. 40)

En la práctica tanto el usuario del comercio electrónico como el proveedor se encuentran conectados a redes LAN. Estas a su vez, se vinculan a través de la red Internet.

> Podemos definir una red LAN como una red de computadoras (dispositivos o nodos) ubicados en un área reducida, interconectados entre sí por un medio de comunicaciones que, mediante un software de red apropiado, se comunican para compartir recursos informáticos e información. (Fusario, 2006, pág. 9)

Cabe aclarar que, aunque se utilizan indistintamente los términos Internet y web, éstos no son lo mismo. Internet es una red global (GAN)[40] de alcance mundial constituida por numerosos sistemas autónomos (AS)[41]. En el sistema autónomo se combinan las redes LAN y los *routers*[42], administrados por una única autoridad, que fija la política de enrutamiento de los datagramas IP[43] para todas las redes y *routers* del sistema. El término internet se puede emplear para identificar a la red global que lleva ese nombre o puede también significar conectividad entre redes, como es en el caso del protocolo IP, el cual fue establecido con anterioridad a la aparición de la red Internet.

[40] GAN: Global Area Network.
[41] AS: Autonomous Systems.
[42] ROUTERS: dispositivo de red que se encarga de encaminar los paquetes de datos.
[43] IP: Internet Protocol.

En la figura 1 se observa un ejemplo imaginario del esquema típico de conectividad en el cual el sistema autónomo de una Organización X, denominado AS[44] 812, se comunica con la red Internet mediante los sistemas autónomos de los proveedores de servicios en Internet (ISP)[45] Y y Z. Con el proveedor Y mediante el sistema autonomo147, y con el proveedor Z a través del sistema autónomo 504. Cabe aclarar que los tres sistemas autónomos mencionados también forman parte de la red Internet. Los *routers* A y B del sistema autónomo 812 de la Organización X se denominan *routers* de borde y son los que se comunican con los otros *routers* de borde de los sistemas autónomos pertenecientes a los proveedores Y y Z.

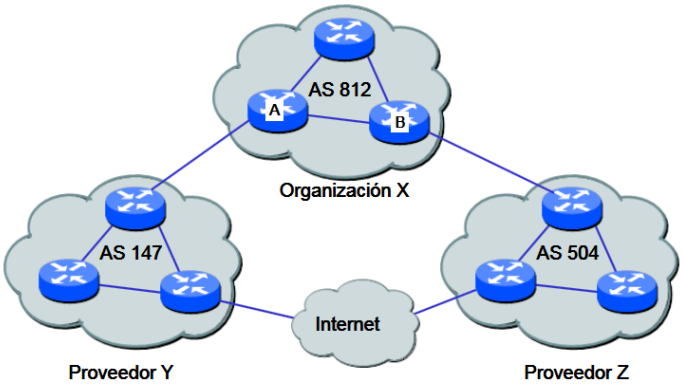


Figura 1 Esquema de conectividad entre sistemas autónomos.
Fuente: (Montañana, 2017)

Con respecto a los terminales comúnmente empleados para la conexión con la red Internet se comenzó con el tradicional computador o PC y luego se extendió, especialmente a partir de la primera década del siglo XXI, con notebooks y comunicaciones móviles compuestas por iPad, iPhones, BlackBerrys, y otros teléfonos inteligentes que irrumpieron en el mercado y comenzaron a competir con las computadoras personales en la realización de transacciones comerciales.

En la actualidad, el 85% de las empresas que operan en la Argentina ya cuenta con *e-Commerce.* De hecho, en promedio, el 21% de la facturación de aquellas compañías que implementaron esta herramienta provino de diferentes dispositivos móviles. En cuanto a las búsquedas, por primera vez se revirtieron las proporciones, ya que el año pasado, el 60% de las sesiones llegaron desde los aparatos móviles. (Bae Negocios, 2017).

[44] AS 812: Sistema Autónomo número 812. Los sistemas autónomos se identifican por su numeración.
[45] ISP: Internet Service Provider.

No solo se trató de una evolución de la tecnología de los equipos terminales móviles sino que también se expandió el crecimiento del ancho de banda, especialmente por la aparición de la tecnología 4G[46].

> En telecomunicaciones, 4G son las siglas utilizadas para referirse a la cuarta generación de tecnologías de telefonía móvil. Es la sucesora de las tecnologías 2G y 3G, y que precede a la próxima generación, la 5G. La tecnología 4G está basada completamente en el protocolo IP, siendo un sistema de sistemas y una red de redes, que se alcanza gracias a la convergencia entre las redes de cables e inalámbricas. Esta tecnología podrá ser usada por módems inalámbricos, smartphones y otros dispositivos móviles. La principal diferencia con las generaciones predecesoras es la capacidad para proveer velocidades de acceso mayores de 100 Mbit/s en movimiento y 1 Gbit/s en reposo, manteniendo una calidad de servicio de punta a punta de alta seguridad que permitirá ofrecer servicios de cualquier clase en cualquier momento, en cualquier lugar, con el mínimo coste posible. (Movistar, 2013)

En el periódico Bae Negocios (2017) se afirma que:

> Según los resultados del estudio anual que Kantar TNS realiza para la Cámara Argentina de Comercio Electrónico (CACE), los $102.000 millones de facturación corresponden a 47 millones de órdenes de compra, un 24% más que en 2015. Durante 2016 el ticket promedio de compra fue de $2.185 y en ese período se comercializaron 75 millones de productos, casi el doble que en el año anterior. Los rubros que impulsaron el crecimiento fueron artículos para el hogar (muebles, construcción, decoración), con una suba del 124%; cosmética y perfumería, con un alza del 104% y accesorios para autos, motos y otros vehículos, que duplicó las ventas. (Bae Negocios, 2017)

Por otro lado, Gustavo Sambucetti, presidente de CACE afirmo en Infosertec, en septiembre del 2016, que actualmente estamos viendo la segunda revolución del *e - Commerce* donde la omnipresencia del consumidor, los *marketplaces* y el uso de múltiples dispositivos traen nuevas oportunidades y retos para el comercio de bienes y servicios. Además, agrega que el estado de la Argentina en comercio electrónico es más que positivo

[46] 4G: Tecnología empleada en comunicaciones de teléfonos móviles de cuarta generación, también denominada LTE, permite el acceso a Internet.

debido a su crecimiento que en el año 2016 fue 60% superior al año anterior. (Arielmcorg, 2016)

El comercio electrónico ha experimentado un desarrollo exponencial, al respecto Traver (2014) señala:

> En 1994, el comercio electrónico no existía como ahora lo conocemos. En 2012, menos de 20 años después, se esperaba que aproximadamente 150 millones de consumidores estadounidenses gastaran cerca de $362 mil millones, y las empresas más de $ 4.1 billones, comprando bienes y servicios en línea o a través de un dispositivo móvil. Una historia similar ocurrió en todo el mundo. Y en este corto periodo, el comercio electrónico se ha reinventado no una, vez sino dos. (pág. 7)

Según el informe de la Cámara Argentina de Comercio Electrónico, compraron online en el 2016 alguna vez, 17,8 millones de personas, lo cual equivale a un 17% más que en el 2015. Además, más del 90% de los adultos están conectados a Internet. (Camara Argentina de Comercio Electronico, 2017)

Otros fenómenos que acompañan el crecimiento del comercio electrónico son: la publicidad en tiempo real, el almacenamiento en la denominada computación en la nube que permite guardar los datos y el software de los consumidores en servidores de Internet a los cuales se pueden acceder desde dispositivos móviles o fijos. En igual sentido se produce la acumulación de volúmenes crecientes de información por parte de las empresas que registran las numerosas interacciones online que ocurren en la web dando origen al denominado Big Data. Éste, se analiza mediante software especializado que posibilita identificar patrones de conducta y preferencias de los usuarios.

En el sitio el Economista.es (2014), Carlos Lopez Lopez, director de operaciones de IMC Group, afirma que:

> Denominamos Big Data a la gestión y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos (…) El objetivo de Big Data, al igual que los sistemas analíticos convencionales, es convertir el dato en información que facilita la toma de

decisiones, incluso en tiempo real. Sin embargo, más que una cuestión de tamaño es una oportunidad de negocio.

Las empresas ya están utilizando Big Data para entender el perfil, las necesidades y el sentir de sus clientes respecto a los productos y/o servicios vendidos. Esto adquiere especial relevancia ya que permite adecuar la forma en la que interactúa la empresa con sus clientes y en cómo les prestan servicio. (pág.1)

1.2. Principales tipos de comercio electrónico: B2C; B2E; B2B; C2C; G2C; C2B y M2B.

Dependiendo de la naturaleza de la relación comercial los principales tipos de comercio electrónico son: B2C[47], de negocio a consumidor; B2E[48], de negocio a empleado; B2B[49]: de negocio a negocio; C2C[50], de consumidor a consumidor; G2C[51], de gobierno a consumidor; C2B[52], de consumidor a negocio, M2B[53], de móvil a negocio. También existe el comercio electrónico social, en cuyo caso el ejemplo más relevante es Facebook, que se incluye en el presente trabajo de tesis.

Comercio electrónico de negocio a consumidor (B2C - *business to consumer*):

Este modelo de comercio se lleva a cabo entre el negocio o tienda virtual y un consumidor interesado en comprar un producto o adquirir un servicio. Al respecto Laudon & Traver (2013) afirman que:

El tipo de comercio electrónico que se analiza con más frecuencia es el comercio electrónico de negocio a consumidor (B2C), en el que los negocios en línea tratan de llegar a los consumidores individuales. Aun cuando el B2C es comparativamente pequeño (cerca de $ 342 mil millones durante 2012 en Estados Unidos), ha crecido de manera exponencial desde 1995, y es el tipo de comercio electrónico que más probablemente encontrará la mayoría de los consumidores. (pág. 22)

[47] B2C: Business To Consumer.
[48] B2E: Business To Employee.
[49] B2B: Business To Business
[50] C2C: Consumer To Consumer.
[51] C2G: Consumer To Government.
[52] C2B: Consumer To Business
[53] M2B: Movil To Business

Estos autores consideran que existen siete modelos de negocios B2C: portales, vendedores minoristas en línea, proveedores de contenidos, corredores de transacciones, creadores de mercados, proveedores de servicios, y proveedores comunitarios.

El modelo B2C presenta las ventajas que el cliente puede acceder a la tienda virtual desde cualquier lugar a través de un dispositivo electrónico tener actualizadas las ofertas y los precios de manera constante. Un ejemplo típico y muy popular es la empresa Amazon que vende productos a clientes minoristas.

Comercio electrónico de negocio a empleado (B2E - *business to employee*):

Este modelo se efectúa exclusivamente entre una empresa y sus empleados. Está constituido por las ofertas que la empresa puede proporcionar, en bienes y servicios, a sus empleados directamente desde su tienda online, de su portal de Internet o de la red Intranet de la empresa.

De esta forma, el empleado puede acceder a cursos de formación (*e-learning*), pedidos de documentos, seguimiento de trámites, comunicación interna con el resto de los empleados, consulta de archivos, pedidos de material de oficina y/o producción, y ofertas de ventas de productos.

Este tipo de comercio electrónico incentiva la pertenencia de los empleados con la empresa, posibilita a éstos últimos gestionar automáticamente su labor y ofrece oportunidades únicas de compra de productos que pueden ser consultadas en cualquier momento y lugar y no son de libre acceso al público externo.

Comercio electrónico de negocio a negocio (B2B - *business to business*):

Este tipo de comercio electrónico se limita a negocios en línea que venden a otros negocios, la transacción comercial únicamente se realiza entre empresas que operan en Internet, lo que quiere decir que no intervienen consumidores. Es el comercio electrónico que tiene mayor potencial de crecimiento. Al respecto Laudon & Traver (2013) afirman que:

> El comercio electrónico de negocio a negocio (B2B), en el que los negocios se enfocan en vender a otros negocios, es la mayor forma de comercio electrónico, con aproximadamente $ 4,1 billones de transacciones en Estados Unidos durante 2012. Hubo un estimado de $ 11,5 billones en intercambios de negocio a negocio de todo tipo, en línea y fuera de línea, lo cual sugiere que el comercio electrónico B2B tiene potencial de crecimiento considerable. (pág. 22)

En este modelo participan los denominados mayoristas y minoristas o autónomos. En general se trata de direcciones web destinadas al intercambio de productos y servicios entre empresas que pretenden reducir los costos de la operación. Dichas direcciones son sitios que en su mayoría tienen acceso restringido por lo cual para operar se requiere disponer de un usuario y la *password* correspondiente a efectos de realizar las transacciones.

El empleo del comercio electrónico entre empresas permite no solo bajar los costos operativos y administrativos, sino además brindar seguridad y eficacia en las comunicaciones. Por otro lado, se logra un mayor monitoreo de las transacciones realizadas, agilidad en el proceso de compra y evita el traslado de los compradores a las instalaciones del vendedor.

> Algunos de los ejemplos más representativos de los negocios B2B, incluyen por ejemplo, la venta de software CRM[54], a las empresas para que puedan realizar un seguimiento de sus clientes, gestionar los ciclos de ventas, etc. La venta de equipos de oficina para empresas que desean actualizar su mobiliario existente es otro de los negocios B2B, incluso la venta de hardware de seguridad y sistemas de control de acceso a universidades o entidades. (Urbano, 2017)

Comercio electrónico de consumidor a consumidor (C2C - *consumer to consumer*):

El modelo C2C se refiere al comercio electrónico entre consumidores individuales. El caso más frecuente se presenta cuando una persona ya no utiliza algún producto y busca ofrecerlo en venta, entonces puede emplear el comercio electrónico C2C como medio para realizar esta transacción con otro consumidor. Para ello se emplean sitios web que proveen una plataforma de intercambio desde donde los consumidores realizan sus transacciones económicas, si la operación se concreta el sitio recibe una comisión por la venta realizada. Existen varios ejemplos de estos sitios como Mercadolibre, Ebay, etc.

[54] CRM: Customer Relationship Management,

Este modelo ofrece para los consumidores las ventajas de la reutilización de productos, las compras a menores precios y la posibilidad de ofertas únicas en el medio.

Comercio electrónico gobierno a consumidor (G2C - *goverment to consumer*):

El comercio gobierno a consumidor G2C se efectúa cuando los gobiernos municipal, provincial o nacional permiten que los ciudadanos realicen sus trámites en línea a través de un portal, por ejemplo, la Agencia Federal de Ingresos Públicos (AFIP), Agencia de Recaudación de la provincia de Buenos Aires (ARBA), etc. Este tipo de comercio no solo involucra el pago de una tasa, impuesto o gravamen sino también se utiliza para consultas de trámites en general y/o acceso a información específica de interés del ciudadano.

Presenta ventajas notorias para los usuarios como son: el ahorro de tiempo, trámites más rápidos y seguros, costos más bajos y registros confiables de la operación.

Comercio electrónico consumidor a negocio (C2B - *consumer to business*):

El modelo C2B se basa en transacciones de negocio originadas por el usuario final, siendo éste quien fija las condiciones de venta a las empresas. Existen páginas en las cuales los usuarios ofrecen bienes inmuebles en alquiler y las compañías de viajes toman dichas ofertas, otras páginas web se dedican a dicho negocio como pagar noches de hotel, billetes de avión, etc. Un ejemplo de C2B es la página web Priceline.com.

> El comercio electrónico C2B se relaciona con el concepto de *name your* Price patentado por Priceline, en EE.UU. Jay Walker, fundador de dicha empresa, pensó que podría ser interesante realizar subastas inversas de billetes de avión o noches de hotel; servicios perecederos que si no son consumidos un día concreto, lógicamente no se pueden almacenar y pierden su valor (Modelo Consumer To Business, 2015).

Comercio electrónico de móvil a negocio (M2B – *movile to business*):

El modelo M2B se basa en el empleo de entornos de Internet móvil como son los teléfonos inteligentes. En este esquema de negocio se utiliza el teléfono y otros dispositivos móviles para conectar al usuario con el sitio web. La proliferación de dichos dispositivos móviles ha expandido las ventas por M2B y sin duda será el futuro de muchas empresas comerciales.

Las tecnologías emergentes como SMS[55], WAP[56], GPRS[57], UMTS[58] y JAVA[59], han impulsado la proliferación de transacciones mediante este modelo de comercio electrónico.

1.3.Componentes del sistema de comercio electrónico

En el comercio electrónico existen tres componentes básicos: el comprador que adquiere el bien o el servicio deseado, el vendedor que es el comerciante o agente de venta y la entidad de servicios financieros que autoriza el pago y ejecuta los movimientos de dinero correspondiente. En el presente trabajo no se considera el sistema basado en la moneda electrónica por tratarse de un medio de pago no trazable.

Al respecto Valles (2002) afirma: "La moneda electrónica deberá ser: universal, es decir, deberá poderse utilizar en cualquier lugar y a través de cualquier medio electrónico; segura, de difícil falsificación y duplicación; anónima, deberá poder utilizarse sin que su propietario sea identificado." (pág. 40)

En la figura 2 se detalla el funcionamiento de una transacción online de comercio electrónico con la utilización de la tarjeta de crédito. Para esta operación intervienen cinco partes, el usuario que hace la compra, el vendedor, la cámara de compensación, el banco del comerciante y el banco emisor de la tarjeta de crédito.

Si profundizamos en el detalle del proceso podemos afirmar que los componentes del comercio electrónico son: el navegador web, el host del cliente, la aplicación informática que sustenta la operación en el sitio web, los protocolos de comunicaciones que brindan conectividad a través de la red Internet, como así también, los que otorgan seguridad al flujo de datos y el sitio web del vendedor. También pueden formar parte de la transacción entidades intermedias (bancos y cámara de compensación).

En el comercio electrónico trazable no solo se conoce el origen y destino de la transacción sino que también queda registrada la operación en cada componente del sistema, lo cual facilita las actividades de auditoria en caso de controversias entre los agentes intervinientes.

[55] SMS: Short Message Service
[56] WAP: Wireless Application Protocol
[57] GPRS: General Packet Radio Service
[58] UMTS: Universal Mobile Telecommunications System
[59] JAVA: Lenguaje de programación.

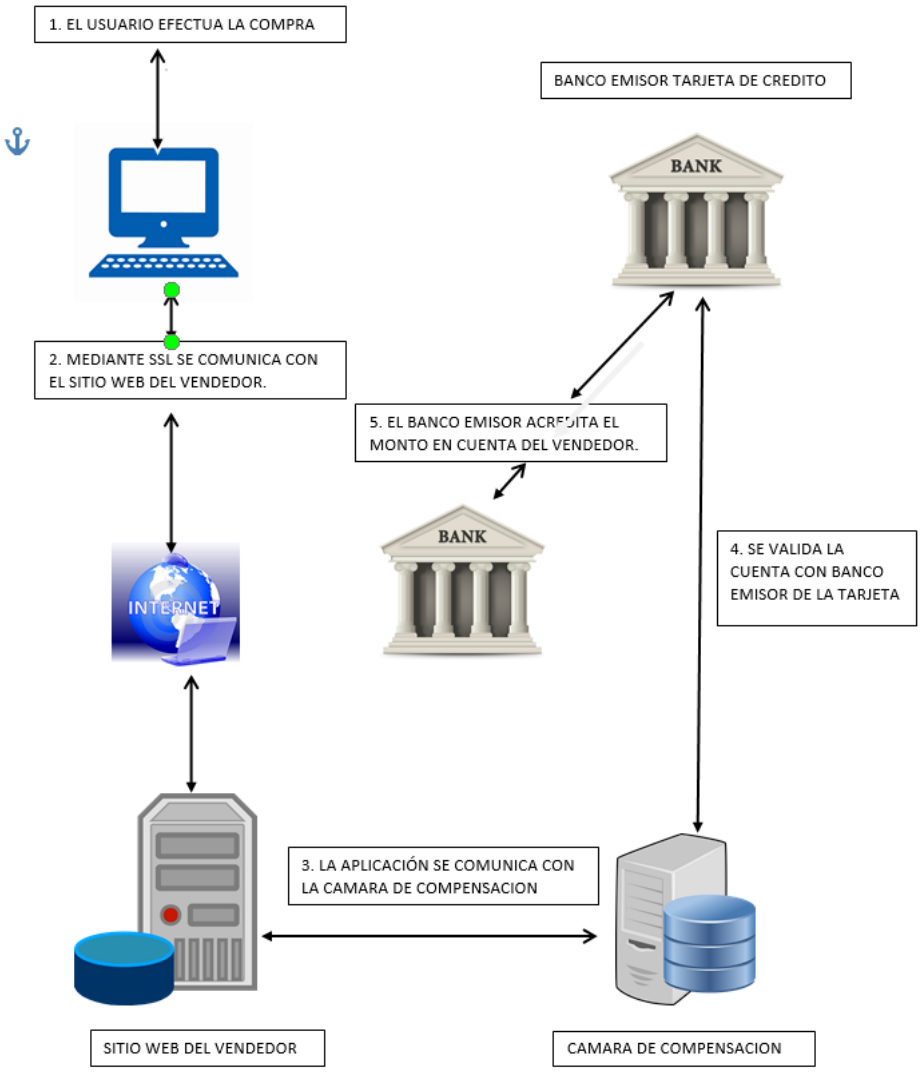


Figura 2: Operación online de comercio electrónico
Fuente: Traver L. (2013)

Como se indicó anteriormente, el término comercio electrónico se refiere a cualquier transacción financiera que involucre la transmisión de información en forma electrónica.

La información que se transmite en la operación transita en paquetes de bytes denominados testigos electrónicos o *electronics tokens*, el soporte físico de éstos se denomina comúnmente tarjeta de crédito.

No obstante, debemos diferenciar el proceso de comercio electrónico del de pagos electrónicos, al respecto Valles (2002) afirma:

> Un caso particular de comercio electrónico es el pago electrónico. Un protocolo de pago electrónico consiste en una serie de transacciones al final de las cuales se ha realizado un pago mediante el uso de un testigo que ha sido acuñado por una entidad autorizada. Para mayor simplicidad consideremos que dicha entidad autorizada no puede coincidir con el comprador ni el vendedor. (pág. 41)

En la figura 3 se detalla el esquema de pago electrónico, donde los usuarios A y B comparten el mismo Banco. El usuario A retira el dinero del banco, en forma electrónica, y luego transfiere el importe al usuario B, quien a su vez lo deposita en el banco.

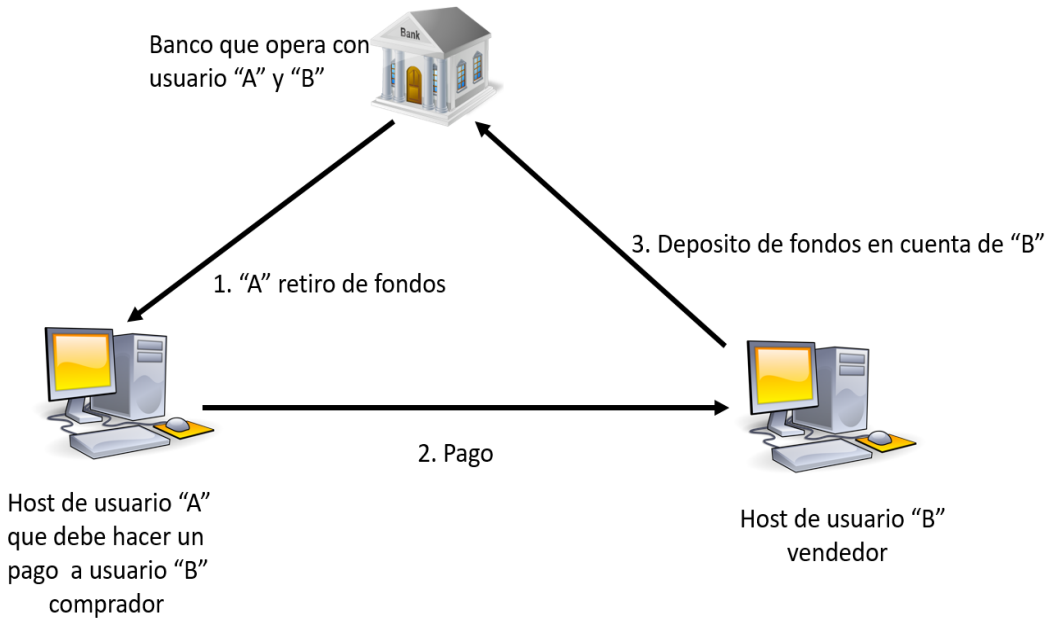


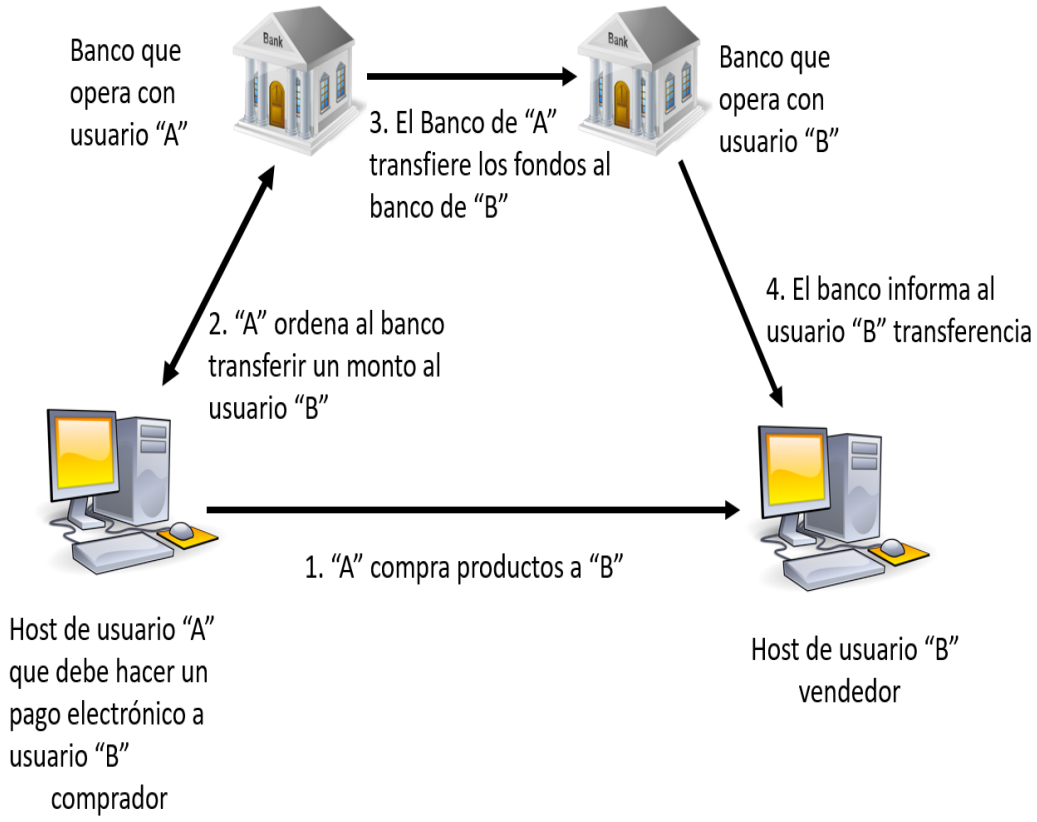
Figura 3: Esquema básico de pago electrónico
Fuente: Pegueroles Valles J. (2002)

Por otro lado, en la figura 4 se detalla el esquema de pago electrónico a través de una transferencia bancaria, se puede observar que deben existir cuatro componentes: comprador, vendedor, banco del comprador y banco del vendedor. Se reduce a tres componentes, suponiendo que vendedor y comprador tienen sus cuentas bancarias en el mismo banco.

En esta operación no hay intervención de las tarjetas de créditos ni de las entidades reguladoras de las mismas. El primer paso de la operación es la navegación del usuario en la página web del vendedor para realizar la compra del producto y/o servicio requerido.

Una vez decidida la compra, el usuario orden la transferencia del monto de la compra al banco en el cual tiene su cuenta de ahorros y/o cuenta corriente, esto lo puede realizar por *home banking*. El sistema es seguro si se emplean por ejemplos mecanismos como el de la tarjeta coordenadas o más recientemente el basado en una clave de sesión enviada *on line*, método denominado *token*, para tal fin, se emplea una aplicación accionada a través de un teléfono celular inteligentes o *Smart phone*.

Una vez efectuada la transferencia el banco del usuario B, el vendedor, avisará al usuario B sobre el depósito recibido.



Nota: no hay intervención de tarjetas de crédito ni entidades reguladoras.

Figura 4: Esquema de pago electrónico mediante transferencia bancaria.
Fuente: Pegueroles Valles J. (2002)

1.4. Medios de pago empleados en las transacciones de comercio electrónico

Los principales medios de pago empleados en las transacciones comerciales son: contra reembolso, cargos en cuenta bancaria, tarjetas de crédito, intermediarios electrónicos, tarjetas inteligentes, micro pagos o monederos virtuales, terminal de punto de venta virtual y plataforma de pagos móviles.

En primer término, el pago contra reembolso es el único que implica la utilización de dinero en efectivo para efectivizar la entrega del bien o el servicio contratado. Respecto a los cargos en cuenta bancaria, se emplean generalmente para suscripciones o cargos periódicos, los cuales se debitan de la cuenta bancaria del que recibe el bien o el servicio -generalmente caja de ahorros o cuenta corriente-.

En el esquema de pago de las tarjetas de crédito intervienen los siguientes actores: el comprador, el vendedor, el banco emisor de la tarjeta de crédito, el banco que en nombre del vendedor recibe la transacción y la red de medios de pago como pueden ser VISA, MASTERCARD, AMERICAN EXPRESS, CABAL, DINERS CLUB, DISCOVER, etc.

Un informe de Ignis Argentina describe un análisis sobre la evolución de la sociedad argentina en lo que respecta a la incorporación al sistema bancario, y particularmente al uso de tarjetas de crédito. Se observó que a nivel mundial, las economías más fuertes son las que poseen la mayor penetración de tarjetas de crédito. Con respecto a América se advierte que los países con mayor presencia de tarjetas son Estados Unidos, Brasil y Canadá con valores por encima al 60%. Argentina, en cambio, se encuentra en la quinta posición por debajo de Chile en términos de posesión de tarjetas de crédito, con un 35% de inserción (finanzas por iprofesional, 2013) .

Con respecto a la tarjeta de crédito, ésta es de material plástico y su tamaño se ha generalizado según la norma puesta en vigencia a partir de 1989 por la Organización Internacional de estandarización / Comisión Electrotécnica Internacional (ISO/IEC)[60] en 85,60 mm de ancho por 53,98 mm de alto. Se caracteriza por disponer de una banda magnética y un número de dieciséis dígitos en relieve según la norma ISO/IEC 7812; en las más modernas se agrega un microchip. Cabe aclarar que el número total de dígitos de una tarjeta es variable, pudiendo oscilar entre 13 y 18. Por ejemplo, American Express tiene 15 dígitos, Dinners Club tiene entre 14 y 15 dígitos y otras tienen 16 dígitos.

En la figura 5 se indican los países en América con mayor presencia de tarjetas de crédito; encabeza el grupo EEUU, Brasil y Canadá con porcentajes superiores al 60%, seguido por Chile con 42% y Argentina con el 35%. México es el país con menor porcentaje que llega al 11%.

[60] ISO/IEC: International Organization for Standardization (ISO), International Electrotechnical Commission (IEC). Organización Internacional de Normalización / Comisión Electrotécnica Internacional

Figura 5: Distribución de las tarjetas de crédito en Países de América
Fuente: Iprofesional.com (2013)

Cada número que aparece en las tarjetas de crédito tiene un significado: tipo de tarjeta, entidad emisora, país donde se emite o dígito de control son algunos de ellos. Las matemáticas y las finanzas están íntimamente relacionadas dado que cualquier relación financiera que tengamos se basa en medios de transmisión de datos a través de las redes y la codificación de los datos financieros requiere el soporte numérico para organizar y estructurar correctamente la información, En este sentido, las tarjetas de crédito o débito tienen una serie de números que no son aleatorios y presentan una sistematización (Banco Bilbao Vizcaya Argentina, 2015).

Las tarjetas de crédito que tienen 16 dígitos están estructuradas según el siguiente esquema: el primer número indica el tipo de tarjeta por rango del emisor, por ejemplo; 1 para tarjetas emitidas por aerolíneas, 4 y 5 para las emitidas por bancos y financieras, 7 para tarjetas emitidas por empresas petroleras, etc.

Al primer digito mencionado se agregan seis más de forma que estos primeros siete dígitos de todas las tarjetas corresponden con el tipo de tarjeta, el tipo de emisor y la zona geográfica en la que se ha emitido la misma. Los rangos completos de emisores y países

son privados, sin embargo se conocen los principales rangos de comienzo de cada una de las tarjetas, por ejemplo; las tarjetas VISA comienzan con el digito 4 y si son del tipo VISA Electrón tienen rangos comprendidos entre 4026, 417500, 4508, 4844, 4913, 4917; Mastercard tiene asignados los rangos entre 51 y 55, etc.

Los restantes números de la tarjeta corresponden al código interno de la entidad para asociar la tarjeta al cliente; dicho criterio es propio de cada entidad emisora. Finalmente, la mayoría de las tarjetas, entre ellas VISA y MasterCard, destinan el último digito (posición 16) para control mediante la utilización del algoritmo Luhn[61]. Algunas tarjetas no tienen un dígito de control asociado, como es el caso de Dinners Club; otras utilizan otro algoritmo verificador en lugar del Luhn como es el caso de las tarjetas emitidas por China Mobipay.

La tarjeta de crédito se gestiona a través de un banco o entidad financiera y una vez emitida autoriza a la persona, a cuyo nombre se encuentra, a utilizarla como medio de pago en los comercios y/o negocios adheridos al sistema.

El pago con tarjeta de crédito se efectúa con dinero crediticio (denominado M1) que por ser un agregado monetario distinto del M0 (dinero generado por el Banco Central) es creado por los bancos o empresas que otorgan los créditos. Por esta razón el cobro por parte del vendedor del bien o el servicio depende de la solvencia de la entidad emisora de la tarjeta; posteriormente el usuario debe asumir la obligación de devolver el importe pagado además de los intereses, en caso de no realizar al vencimiento el pago total de lo consumido en el periodo, comisiones bancarias y otros gastos, según corresponda.

Dependiendo del límite de crédito, que el banco emisor estima se puede otorgar al usuario de la tarjeta en función de sus ingresos y situación financiera general, es posible acceder a cuatro tipos principales de tarjetas denominados: clásica, dorada, *platinum* y *signature* o *black*.

Cabe aclarar que los datos de la tarjeta del comprador viajan por Internet mediante el protocolo SSL a efectos de brindar confidencialidad e integridad, como así también la autenticación del vendedor. Asimismo, con la finalidad de evitar fraudes en la operación, se emplea el protocolo de Transacción Segura Electrónica (SET) que permite que el propietario de la tarjeta, el vendedor, la red de medios de pago y la autoridad certificadora

[61] LUHN: Algoritmo de validación creado por Hans Peter Luhn in 1954

estén conectados a través de Internet al disponer de una firma digital emitida por una autoridad de certificación SET.

El pago a través de intermediarios electrónicos, refiere a empresas que permiten efectuar compras sin difundir los datos que identifican a las tarjetas de crédito y sus propietarios. Algunas de las aplicaciones más conocidas son: PayPal[62] y Cyber Cash.

CyberCash, desarrollado en 1994 por CyberCash Corporation, constituye un mecanismo de pago muy similar a SET, que ofrece a los comerciantes una solución rápida y segura para procesar los pagos con tarjeta de crédito a través de Internet. Al igual que en SET, el usuario necesita utilizar un software de cartera que reside permanentemente en su máquina, también el comerciante necesita instalar un software en su servidor. De esta forma, el comerciante no necesita adquirir un sistema de back office[63] para el procesamiento de las operaciones de venta con tarjeta, puesto que es el servidor de CyberCash el que gestiona con el banco todas las complejas operaciones de pago. Desde el punto de vista del cliente, esta estrategia le concede mayor seguridad, al implicar que su número de tarjeta nunca llega a ser conocido por el comerciante, sino solamente por el servidor de CyberCash y, por supuesto, por los bancos participantes. Desde el punto de vista del comerciante también aumenta la seguridad, ya que el cobro de la mercancía se produce incluso antes de que sea vendida, como ocurre en las transacciones en puntos de venta en las tiendas (de la calle).

Por tanto, puede decirse que CyberCash actúa como intermediario entre el comerciante y el consumidor, asegurando que el primero reciba el pago, mientras el segundo recibe la mercancía. Por supuesto, su papel en el escenario de compra-venta ocasiona la carga de una pequeña comisión al comerciante, variable en función del volumen de ventas. (Comercio electronico, 2017).

Las tarjetas inteligentes empleadas como medio de pago son aquellas que poseen capacidad de almacenar información; básicamente ésta consiste en una identificación y una cantidad de dinero disponible que se carga a través de un cajero automático.

[62] PAYPAL: Empresa que posibilita hacer el envio de dinero a la cuenta del vendedor a través de la tarjeta de crédito, sin compartir información financiera con el vendedor.
[63] BACK OFFICE: Sistema que permiten gestionar las actividades dentro de una empresa sin la necesidad de tener contacto con los clientes, optimizando sus procesos de operación y negocios

De esta forma se pueden realizar micro pagos tanto en el comercio del mundo físico como en el comercio electrónico, para este último caso se requiere un dispositivo conectado al computador para la lectura de la tarjeta.

Los micro pagos o monederos virtuales se basan en el empleo de software residente en la PC del cliente para almacenar el valor monetario respaldado por una cuenta bancaria, una transferencia de fondos o una tarjeta de créditos. Existen varias plataformas para efectivizar este servicio, entre ellas podemos citar: KLELine, MILLICENT, NETBILL, etc.

La terminal de punto de venta virtual es el sistema ofrecido por la mayoría de los bancos, también conocido como cajeros virtuales o pasarela de pagos. Se inscribe dentro de los servicios de banca electrónica y ofrece mayor seguridad debido a que los datos de la tarjeta de crédito del comprador son transmitidos directamente al banco, en lugar de hacerlo al sitio web del vendedor.

La plataforma de pagos móviles PPM es un nuevo canal de pagos que ofrece la modalidad de Pago Electrónico Inmediato PEI y fue impulsado por el Banco Central de la República Argentina. Su empleo permite realizar pagos a través del celular, tableta o computadora móvil, con débito y crédito en línea, en cualquier lugar y sin costo. Las modalidades contempladas son: el POS Móvil y el Botón de Pago, orientadas a comercios, y la Billetera Electrónica, para transferencias entre personas.

Al respecto, Carlos Arabia (2017) dice:

> A partir de año pasado, desde el Banco Central de la República Argentina (BCRA) se implementaron medidas para incrementar y facilitar las operaciones electrónicas a fin de eliminar el uso de efectivo y que el usuario de servicios financieros pueda operar sin la necesidad de ir a una sucursal bancaria para reducir el costo de las transacciones. (Arabia, 2017)

El método POS Móvil requiere de la adquisición de un dispositivo, con un costo por única vez, que se conecta al teléfono móvil o tableta y posibilita validar las transacciones mediante la tarjeta de débito del comprador. De esta forma, se puede realizar el pago en el punto de venta, mediante la transferencia inmediata sin costo adicional.

Por su parte, el botón de pago, puede incorporarse en la página web del comercio, integrarse con distintas redes sociales o enviarse por correo electrónico, posibilita la compra y venta de bienes o servicios mediante transferencias inmediatas con débito en cuentas a la vista.

El método Billetera Electrónica permite enviar dinero entre usuarios, sin costo a través de la web y mediante una aplicación en el celular. Sólo se requiere cargar los datos en la aplicación correspondiente de la cuenta bancaria o de las tarjetas de débito.

Por otro lado, Alejo Espora Gerente del Banco Ciudad especializado en medios de pagos electrónicos, manifestó a Infobae que lo importante para utilizar la modalidad PEI mediante POS-Móvil y Botón de Pago, el comercio debe estar adherido a un producto/servicio dentro de la Plataforma de Pagos Móviles (PPM), como Todo Pago M Pos de Red Banelco, Red MOB de Red Link y luego, a partir de la adhesión, el proveedor del servicio o la entidad financiera debe proporcionarle sin ningún costo, una aplicación que pueda descargarse en sus equipos (Arabia, 2017).

1.5. Requerimientos de seguridad en las operaciones a través de la red Internet

Para la definición de los servicios de seguridad utilizaremos las recomendaciones X.800[64] y la RFC[65] 2828. La primera, generada por la Unión Internacional de Telecomunicaciones (UIT), define en que capa del Modelo de Interconexión de Sistemas Abiertos (OSI)[66] se puede aplicar cada servicio, los mecanismos para implementarlos y la administración de la seguridad para garantizar la transferencia de datos segura en los sistemas.

Por su parte, la recomendación RFC 2828 define el alcance de un servicio de procesamiento o de comunicación proporcionado por un sistema, para ofrecer un tipo de protección especial a los recursos del mismo. Los servicios de seguridad son los que llevan adelante las políticas de seguridad, y a su vez, dichos servicios son implementados por mecanismos y procedimientos de seguridad.

En los sistemas teleinformáticos la seguridad absoluta no existe sino que se presentan distintos grados de seguridad.

[64] Recomendación X.800: Describe los servicios de seguridad básicos a aplicar para proteger la comunicación entre sistemas.
[65] RFC: Request For Comments; publicaciones (recomendaciones) que ingenieros y expertos hacen llegar al IETF para mejorar el funcionamiento de la red Internet y protocolos asociados.
[66] OSI: Open Systems Inteconnection

Stallings (2004) agrega que "En X.800 estos servicios quedan divididos en cinco categorías y catorce servicios específicos" (pág. 9). Las categorías son: confidencialidad, integridad, autenticación o autentificación, no repudio y control de acceso.

La confidencialidad brinda protección contra escuchas no autorizadas y es especialmente importante en las transacciones con tarjetas de créditos, evitando la difusión de los datos a personas no autorizadas. Al respecto, Stallings, (2004) señala:

> El otro aspecto de la confidencialidad es la protección del flujo del tráfico frente al análisis del tráfico. Para ello el atacante no debería poder ver la fuente, el destino, la frecuencia, la longitud ni otras características del tráfico en una comunicación. (pág. 11)

La integridad brinda el servicio de protección respecto a la sustitución total o parcial del mensaje original emitido en la transacción; de esta forma el mensaje se recibe como fue enviado, sin duplicación, inserción, modificación, reordenamiento del mismo, ni repeticiones. Obviamente la destrucción de los datos también queda cubierta con este servicio.

La autenticación o autentificación es un servicio que se encarga de garantizar la autenticidad de la comunicación. La función de este servicio es asegurar al receptor que el mensaje pertenece a la fuente de la que dice proceder.

El no repudio brinda el servicio de protección frente a posteriores negaciones respecto del bien o servicio brindado por el vendedor y/o recibido por el comprador.
Con respecto a los controles de acceso, éstos se diferencian según su origen, el cual puede ser para individuos internos a la organización o externos a la misma.

Al respecto Traver (2014) afirma:

> Por lo general, la organización de seguridad administra los controles de acceso, los procedimientos de autenticación y las políticas de autorización. Los controles de acceso determinan que individuos externos e internos pueden obtener acceso legítimo a las redes de la organización. Los controles de acceso para los individuos externos incluyen

> firewalls[67] y servidores proxy[68], mientras que los controles de acceso para los individuos internos por lo general consisten en procedimientos de inicio de sesión (nombres de usuario, contraseñas y códigos de acceso). (pág. 306)

La disponibilidad de los datos y del sistema, servicios también contemplados en las normas X.800 y RFC 2828, garantizan que datos y operación estén disponibles en todo momento para las partes autorizadas.

Para llevar adelante los requerimientos mínimos de seguridad se emplean diferentes métodos de cifrado o encriptado de la información. Cabe aclarar, que la información en los sistemas se puede encontrar en alguno de los dos estados siguientes:

Información en claro o texto plano: es la que no ha sufrido ningún tipo de modificación que oculte su significado.

Información encriptada o cifrada: es la que ha sufrido un proceso por el cual su texto en claro se transformó en ininteligible para cualquiera que acceda a ella. La única manera de obtener nuevamente el texto claro es mediante el proceso de descifrando del mensaje.

1.6. Técnicas para la protección de los datos en Internet: la criptografía y la esteganografía

Para la protección de los datos se pueden emplear dos técnicas tan antiguas como la necesidad de los seres humanos de comunicarnos; tales son la criptografía y la esteganografía. Estos métodos tratan de evitar la interceptación de los mensajes o en caso de que suceda, que sean ininteligibles para personas no autorizadas. Se describirán a continuación sus principales características, protocolos y la factibilidad de su empleo en el comercio electrónico.

Respecto al riesgo de interceptación de los mensajes en las redes Halsall (2006) indica:

> Al extenderse los conocimientos sobre redes y protocolos, se ha incrementado el riesgo de que un mensaje sea interceptado y decodificado durante su viaje por la red. Por

[67] FIREWALLS: Dispositivo que a la entrada de una red controla el acceso, bloqueando las comunicaciones no permitidas y registrando todo el tráfico desde y hacia la red que protege.
[68] SERVIDORES PROXY: Equipo informático que intercepta y controla las conexiones de red efectuadas desde un cliente a un servidor especifico. Para que la conexión tenga lugar deben cumplirse las condiciones impuestas por el programa proxy.

ejemplo, los sistemas finales (estaciones o computadoras) asociados con la mayoría de las aplicaciones están ahora conectados a una LAN.

La aplicación puede involucrar a una única LAN o en un entorno distribuido, a Internet. Sin embargo, con la mayor parte de las LAN, las transmisiones en el medio compartido pueden ser fácilmente interceptadas por cualquier sistema si un intruso coloca el interfaz de la red en modo promiscuo y recoge todas las transmisiones del medio. (pág. 648)

1.6.1. La criptografía y los métodos de cifrado simétrico, asimétrico y *hashing*

Los principales protocolos que brindan seguridad en el comercio electrónico se basan en la criptología, que ha sido definida por diferentes autores:

> La Criptología, del griego Criptos –oculto- y logos - tratado, ciencia-, es el nombre genérico con el que se designan dos disciplinas opuestas y a la vez complementarias: Criptografía y el Criptoanálisis. La criptografía se ocupa del diseño de procedimientos para cifrar, es decir para enmascarar una determinada información de carácter confidencial. El criptoanálisis, por su parte se ocupa de romper esos procedimientos de cifrado. (Sabater, Martinez, Hernandez, Montoya, & Muñoz, 2001, pág. 1).

Con referencia al origen de la criptografía Gomez (2011) afirma:

> El interés por transmitir un mensaje de forma que su significado quede oculto a los ojos de todo lector que no sea el destinatario o destinatarios es, posiblemente, tan antiguo como la propia escritura. De hecho, se tiene constancia de una serie de jeroglíficos no estándar de más de 4.500 años de antigüedad. (pág. 9)

Cabe aclarar que en criptografía se emplean los términos codificación y cifrado, con acepciones diferentes. Si se trata de sustituir una palabra por otra estamos en presencia de un proceso de codificación, mientras que la sustitución de letras o caracteres del mensaje se denomina cifrado o encriptado del mensaje.

Los procesos inversos que permiten hallar el mensaje en claro, se denominan decodificación y desencriptado respectivamente.

La encriptación o codificación (Caballero, 2002) es un proceso que consiste en transformar una información expresada en un lenguaje determinado a otro con reglas sintácticas y semánticas distintas.

Respecto del proceso de encriptado Gomez (2011) dice: "A la regla general de encriptación se la denomina a menudo algoritmo de encriptación, mientras que el parámetro concreto empleado para cifrar o codificar el mensaje se denomina clave." (pág. 12).

También si nos referimos al encriptado de los mensajes Carlson, Crilly, & Rutledge (2007) nos dicen que "la encriptación es la transformación de un texto común en un texto cifrado; la desencriptación es el proceso inverso. El cifrado es la serie de transformaciones y las claves son los parámetros de transformación." (pág. 594).

La necesidad de intercambiar mensajes de forma segura, de manera que solo puedan ser leídos por las personas a quienes van dirigidos, dió origen a la esteganografía y a la criptografía. La primera trata de ocultar el mensaje, mientras que la segunda provee técnicas de codificación y decodificación para que el mensaje sea ininteligible, excepto para el destinatario legítimo .

Con la aparición de las redes de datos e Internet la necesidad de intercambiar información digital de manera segura fue mayor y es donde aparecen implementaciones de distintos métodos de cifrado.

Como se mencionó precedentemente los protocolos que ofrecen cierto nivel de seguridad en las transacciones económicas efectuadas a través de la web deben brindar los servicios de: confidencialidad, integridad, autenticación, no repudio y disponibilidad mediante procesos de encriptación. En el sistema de la figura 6 se puede apreciar que la entrada es un texto original en claro, que será objeto de cifrado o encriptado.

Éste en el lado transmisor consiste en la transformación del texto original en un texto cifrado o mensaje cifrado, según la nomenclatura de la Organización Internacional de Normalización (ISO)[69].

[69] ISO: International Estándar Organization.

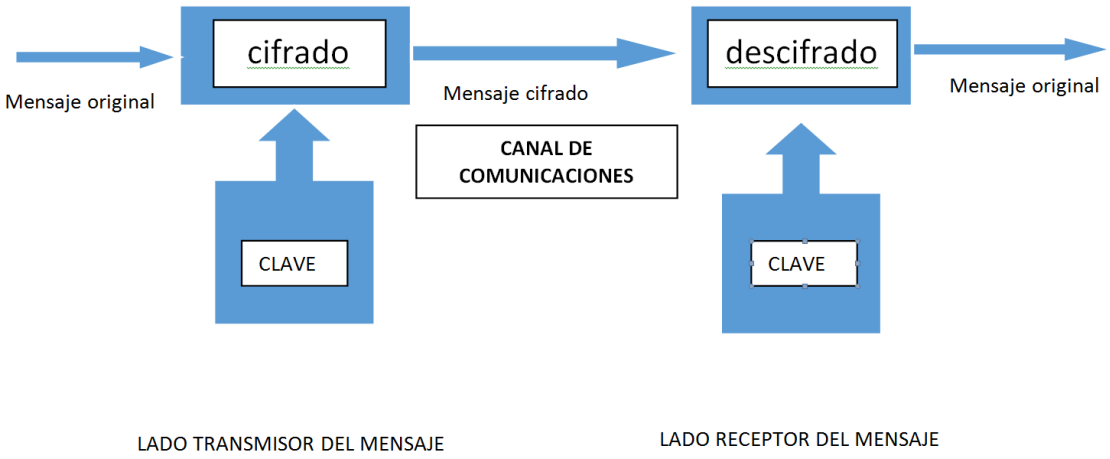


Figura 6: Sistema criptográfico para el cifrado de mensajes
Fuente: Elaboración propia

El proceso de descifrado en el lado receptor consiste en la transformación del texto cifrado en un texto en claro. Tanto en el proceso de cifrado como en el de descifrado se debe introducir una clave que puede ser la misma o diferente según el método de cifrado empleado.

Con respecto al sistema de criptográfico Gallardo (2004) afirma:

> La criptografía ha sido usada desde muy antiguo, aunque modernamente, con el concurso de los computadores, resulta de más fácil uso y mucho más eficaz que la que se conseguía con los sistemas tradicionales, (…) la gracia está en encontrar los algoritmos adecuados para el proceso de cifrado y descifrado, así como para el adecuado transporte y compartición de las claves por parte del usuario que emite el mensaje original y el usuario que recibe este en el extremo opuesto. (pág. 20)

Los métodos de cifrados empleados en los sistemas se clasifican en tres tipos: cifrado de clave simétrica, cifrado de clave asimétrica y cifrado de dispersión o *hashing*. En las operaciones de comercio electrónico se emplean de forma aislada o combinada, como se describirá a continuación.

Cada uno de estos métodos de cifrado emplea algoritmos diferentes para su implementación. Al respecto, Chapra & Canale (1999) nos dicen que: “Un algoritmo es la secuencia de pasos lógicos necesarios para llevar a cabo una tarea específica, como la resolución de un problema.” (pag, 31). Los utilizados en los sistemas criptograficos se

caracterizan porque los procesos siempre terminan después de un numero finito de pasos, son procesos deterministicos y el algorimos es conocido por el publico en general. Su fortaleza en términos de seguridad se encuentra en la longitud de la clave y no en el secreto de sus operaciones.

El método de cifrado de clave simétrica, o simplemente cifrado simétrico, utiliza una única clave tanto para cifrar como para descifrar el mensaje; son mecanismos muy rápidos pero tienen la dificultad de la distribución de las claves. En la figura 7 se detalla el proceso de cifrado simétrico. Para cifrar debe introducirse en el cifrador la clave y el texto en claro; a la salida se obtiene el texto cifrado. La operación de descifrado en el lado receptor, es la inversa; entra al cifrador el texto cifrado y la misma clave y se obtiene el texto en claro.

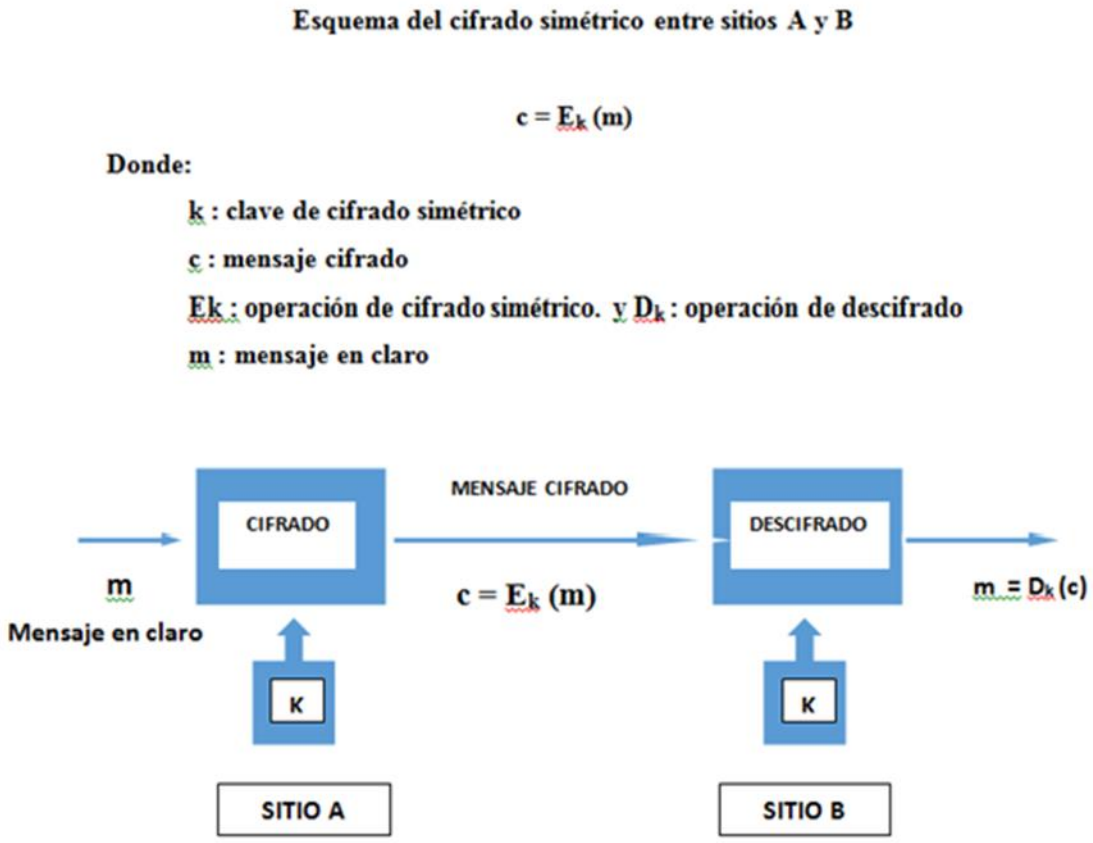


Figura 7: Elementos del cifrado simétrico
Fuente: Elaboración propia

Con referencia a la distribucion de las claves Stallings, W. (2004) afirma:

> El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. Si alguien puede descubrir la clave y

> conoce el algoritmo, toda comunicación que utilice esta clave puede ser leída (pág. 727).

El cifrado simétrico está constituido por cuatro elementos básicos: algoritmo de cifrado, texto plano o nativo, clave secreta y el texto cifrado.

El algoritmo de cifrado lleva a cabo varias operaciones de transformación basadas en técnicas de permutación y sustitución sobre el texto plano. El texto plano o nativo, es el mensaje que se quiere transmitir. En lo que respecta a la clave secreta, es el elemento indispensable para que, a partir del texto en claro, se pueda obtener el texto cifrado. En la recepción, para el descifrado, la clave permite revertir las transformaciones producidas durante el cifrado. La clave es la misma para cifrar y para descifrar y permite obtener el mensaje en claro en el extremo receptor El texto cifrado es el mensaje de salida del cifrador y el resultado depende del texto plano, de la clave empleada y del algoritmo de cifrado utilizado.

Con respecto al cifrado simétrico Willian Stallings (2004) advierte:

> Existen dos requisitos para la utilización segura del cifrado simétrico: se necesita un algoritmo de cifrado robusto. Como mínimo, es de desear que el algoritmo cumpla que aunque un oponente conozca el algoritmo y tenga acceso a uno o más textos cifrados, sea incapaz de descifrar el texto o averiguar la clave (…) El emisor y el receptor tienen que haber obtenido las copias de la clave secreta de una forma segura y deben mantenerla en secreto. (pág.727)

Los métodos básicos que se emplean en el cifrado simétrico son la sustitución y la transposición. El cifrado por sustitución consiste en reemplazar las letras o conjunto de letras por otras letras o conjunto de letras. El más antiguo y conocido es el cifrado Cesar, que reemplaza cada letra del mensaje original por la letra ubicada tres posiciones después en el abecedario.

De esta forma, la A es reemplazada por la D, la B por la E, la C por la F, etc. y las últimas letras la X, la Y y la Z son reemplazadas por la A, la B y la C respectivamente. Si bien, el cifrado Cesar rotaba el abecedario de tres en tres letras, el método funciona con cualquier otro número.

Otro método de cifrado por sustitución está basado en el empleo de una palabra clave, la cual es usada por el codificador para comenzar el abecedario cifrado. El final del abecedario cifrado es el resto del alfabeto en el orden correcto, pero sin repetir las letras ya usadas en la palabra clave. En la figura 8 se incluye un ejemplo de cifrado por sustitución en el cual se utilizó como clave la palabra "secreto". Las letras de la palabra "mesa" son reemplazadas por las letras que ocupan los mismos lugares en el alfabeto cifrado, en este caso el mensaje cifrado de "mesa" será "*wefs*".

La clave es la palabra; SECRETO

El abecedario cifrado (codificado) sería el siguiente:

Abecedario normal: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Abecedario cifrado: **S E C R E T O** P Q U V W Y Z A B D F G H I J K L M N

Cifrado de la palabra MESA = WEFS

Figura 8: Ejemplo de cifrado por sustitución monoalfabético
Fuente: Elaboración propia

En este caso se ha presentado un ejemplo de cifrado por sustitución monoalfabético, ya que solo emplea ~~usa~~ un alfabeto cifrado. También pueden realizarse cifrados por sustitución polialfabéticos, en los cuales se emplean varios alfabetos cifrados.

El cifrado por transposición emplea un método en el cual no se cambian las letras por otras, sino que se cambia el orden de éstas, de acuerdo con un esquema bien definido que en muchos casos es un diseño geométrico. En la figura 9 se detalla un caso cifrado por transposición, en él, que se efectúa el cifrado en forma de columna, colocando en la fila superior la clave y a continuación el mensaje. La clave sirve para asignar un número a cada columna. El número correspondiente a la letra de la clave estará determinado por su posición en el alfabeto.

En el ejemplo la palabra clave es TAN y el mensaje es LA ESPERA ES CORTA**.** Allí es posible observar que existen tantas columnas como letras tiene la clave; el texto en claro se escribe de corrido a través de las columnas y luego se arma el mensaje cifrado según el

conjunto de letras que quedan agrupadas en cada columna. La secuencia de los grupos de letras se ordena según la clave y la posición de las letras de la misma en el alfabeto.

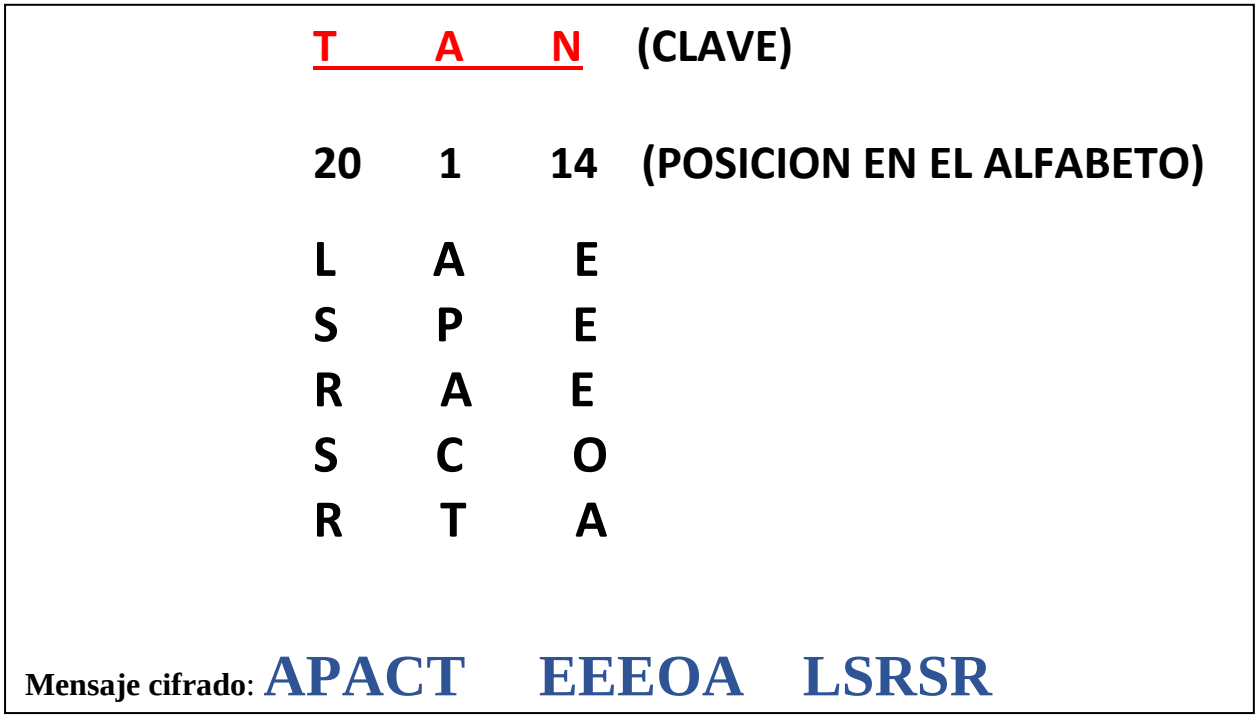


Figura 9: Ejemplo de cifrado por transposición.
Fuente: Elaboración propia

El mensaje cifrado por trasposición está conformado por el lugar que ocupan las letras de la clave en el abecedario. En el ejemplo de la figura 9 se comienza por la columna de la A, luego la de la N y por último la de la T; además podemos separar el mensaje cifrado en bloques de cinco letras.

En los sistemas de cifrado simétrico actuales se emplean cifradores de producto, éstos emplean una combinación de técnicas de difusión y confusión. La difusión se lleva adelante mediante la sustitución y transposición, es decir se dispersa la estructura estadística del mensaje sobre la totalidad del texto cifrado obtenido; de esta forma, se oculta la relación entre el texto en claro y el texto cifrado.

Por su parte, con la confusión se pretende ocultar la relación entre el texto cifrado y la clave secreta, dado que dificulta la tarea de los criptoanalistas que solo disponen del conocimiento del algoritmo de cifrado y del texto cifrado para tratar de obtener la clave secreta. El método de cifrado simétrico cumple con los siguientes seis principios de Kerckhoffs, A. (1883).

- El sistema debe ser en la práctica indescifrable, en caso de que no lo sea matemáticamente
- El sistema no debe ser secreto y no debe ser un problema que éste caiga en manos del enemigo.
- La clave debe ser fácilmente memorizable de manera que no haya que recurrir a notas escritas.
- El sistema debe poder aplicarse a la correspondencia telegráfica (digital).
- El sistema debe ser portable y no deberá requerir la intervención de varias personas.
- El sistema debe ser fácil de utilizar, no requerirá conocimientos especiales ni tendrá una larga serie de reglas.

En realidad, el único principio que se ha actualizado es el cuarto, dado que Kerckhoffs (1883) se refería a la correspondencia telegráfica que constituía la tecnología de esa época, y no a la digital. Los restantes principios tienen vigencia hasta el presente.

Entre los protocolos de cifrado simétrico más conocidos se encuentran el estándar de Encriptación de Datos, DES[70] ; Triple encriptación de datos, TRIPLE DES[71]; Estándar Criptográfico Avanzado, AES[72]; Código de RON Rivest dos RC2[73]; Código de RON Rivest cuatro, RC4[74]; Código de RON Rivest cinco RC5[75] ; Algoritmo de Encriptación de Datos Internacional, IDEA[76,] ; Rutina de Encriptamiento Rápida y Segura, SAFER[77] y BLOWFISH[78]. Cualquiera sea el protocolo de cifrado simétrico que consideremos, todos adolecen del inconveniente de requerir para la comunicación que ambos participantes conozcan la clave secreta, lo cual en principio genera problemas por la distribución segura de las claves.

Los algoritmos de encriptado de clave simétrica son conocidos; la fortaleza del cifrado no radica en el conocimiento o no del algoritmo sino exclusivamente en la longitud de la clave. El método de ataque más difundido es el denominado método de fuerza bruta, que consiste en probar todas las combinaciones posibles de claves sobre un fragmento del texto cifrado, hasta que se obtenga una traducción inteligible del texto original.

[70] DES: Data Encription Standard
[71] TRIPLE DES: Triple Data Encription Standard
[72] AES: Advanced Encription Standard
[73] RC2: Ron's Code 2.
[74] RC4: Ron's Code 4
[75] RC5: Ron's Code 5
[76] IDEA: International Data Encription Algorithm
[77] SAFER: Secure And Fast Encription Routine
[78] BLOWFISH: Algoritmo de cifrado por bloques simétrico

En la figura 10 se detalla el tiempo necesario para descifrar, según distintas longitudes de claves, y suponiendo que se procesa una clave por 1 microsegundo o como se indica en la cuarta columna que se procesan un millón de claves por microsegundo. Esto último es factible de obtener con procesamiento paralelo. Se puede observar que claves de 32 y 56 bits de longitud son claramente inseguras.

Tamaño de la Clave en bits	Numero de claves posibles	Tiempo de proceso 1 clave /µ seg	Tiempo de proceso 10^6 claves / µ seg
32	**$4{,}3 \times 10^9$**	**35,8 minutos**	**2,15 milisegundos**
56	**$7{,}2 \times 10^{16}$**	**1.142 años**	**10 horas**
128	**$3{,}4 \times 10^{38}$**	**$5{,}4 \times 10^{24}$**	**$5{,}4 \times 10^{18}$**
168	**$3{,}7 \times 10^{50}$**	**$5{,}9 \times 10^{36}$**	**$5{,}9 \times 10^{30}$**

Figura 10: Tiempo promedio para hallar la clave por medio del método de fuerza bruta
Fuente: Stallings W. (2004)

El protocolo DES, originado en el Instituto Nacional de Estándares y Tecnología ,NIST[79] del Departamento de Comercio de Estados Unidos, fue publicado por primera vez en el año 1977 y es el algoritmo de cifrado simétrico más conocido y empleado del mundo. Originariamente se lo describió como Algoritmo de Encriptación de Datos, DEA[80]; no obstante, se lo conoce más como algoritmo DES.

Este algoritmo emplea bloques de 64 bits de tamaño y la clave con la que originariamente comenzó a funcionar tuvo una longitud de 56 bits y no estaban incluidos los 8 bits de paridad. El nivel y potencia de las computadoras fue creciendo y, en consecuencia, la clave de 56 bits dejó de otorgar seguridad al método ya que a partir del procedimiento denominado de fuerza bruta, en poco tiempo se obtiene la clave del mensaje. Es por ello que desde 1998 el protocolo DES dejó de ser el algoritmo empleado por el gobierno de EEUU y fue reemplazado por el Triple DES.

El Triple DES consiste en encriptar tres veces sucesivas, con claves diferentes; a este procedimiento se lo denominado DES-EEE3. Otras variantes que se emplean, aun cuando ofrecen menor seguridad son la que consiste en encriptar-desencriptar-encriptar con tres claves diferentes, denominada DES-EDE3 y la opción denominada DES-EEE2 y DES-EDE2 que consiste en que la primera y tercera operación emplean la misma clave.

[79] NIST: National Institute of Standards and Technology
[80] DEA: Data Encription Algorithm

El AES, también conocido bajo el nombre de Rijndael, es un algoritmo de cifrado por bloque que fue desarrollado por Joan Daemen y Vincent Rijndael (2001) estudiantes belgas de la universidad Katholieke Universiteit Leuven. Este protocolo se caracteriza por los siguientes aspectos: ser de dominio público, soportar bloques no menores a 128 bits, las claves de cifrado pueden ser de 128, 192 y 256 bits y se puede implementar tanto por software como por hardware.

El RC2 diseñado por Ron Rivest (1984) es un algoritmo de cifrado por bloques de 64 bits, con clave de tamaño variable. Es mucho más rápido que el DES y también tiene la facilidad de incrementar la seguridad eligiendo claves de mayor longitud. Ron Rivest diseño también el algoritmo conocido como RC4, el cual opera por cifrado de flujo y también tiene la facilidad de utilizar claves de longitud variable. Se basa en el empleo de una permutación aleatoria y su ejecución por software es muy rápida. El algoritmo se emplea para encriptación de archivos y para encriptar la comunicación en protocolos como el SSL y TLS, que constituyen los protocolos empleados en comercio electrónico para brindar confidencialidad, integridad y autenticación en la comunicación entre el cliente y el sitio web del proveedor.

El algoritmo RC5, también diseñado por Ron Rivest, se caracteriza por ser parametrizable con tamaño de bloque y clave variables. También presenta un tamaño de clave variable hasta 2040 bits y número de vueltas hasta 255. Una característica importante de RC5 es el uso de rotaciones dependientes de los datos.

El algoritmo IDEA, se puede implementar fácilmente en hardware o software y posee una eficiencia comparable al método DES. Se caracteriza por ser un algoritmo de cifrado por bloques de 64 bits interactivo y emplear una clave de 128 bits. La encriptación se lleva a cabo mediante ocho rotaciones y ha sido inmune al criptoanálisis diferencial y lineal.

El SAFER es un algoritmo de cifrado que tiene un número variable de rotaciones (generalmente seis), orientado a bytes. Emplea un tamaño de bloque de 64 bits y claves de 64 y 128 bits. Existen dos variantes denominadas SAFER K-64 y SAFER K-128.

El algoritmo inicial, considerado originariamente inmune al criptoanálisis tanto lineal como diferencial, presentó una debilidad en el generador de claves ocasionando la modificación correspondiente que dio lugar a las versiones SAFER SK-64 y SAFER SK-128.

Por último, el algoritmo BLOWFISH desarrollado por Bruce Schneier en 1993 para equipos de 32 bits, opera con bloques de 64 bits donde cada rotación consiste en una sustitución que depende de la clave y de los datos, y una permutación que depende solo de la clave. La clave es variable con un máximo de 448 bits.

El método de cifrado de claves asimétricas o criptografía de clave pública.

El cifrado asimétrico, a diferencia del cifrado simétrico, utiliza dos claves para cada usuario. Al respecto Gallardo (2004) afirma que "Este método se distingue porque cada usuario o sistema final dispone de dos claves: una privada, que debe mantener secreta, y una publica, que debe ser conocida por todas las restantes entidades que van a comunicarse con ella." (pág. 22)

La clave privada se emplea para firmar los mensajes que se envían, de forma tal que el usuario que recibe el mensaje, para descifrarlo, debe introducir la clave pública del remitente. Por el contrario, si se recibe un mensaje que ha sido cifrado con la clave pública del destinatario, es este último el único que lo puede descifrar mediante su clave privada.

Con respecto a este tipo de cifrado (Stallings W. , 2004) agrega: " El cifrado de clave pública, propuesto públicamente por primera vez por Diffie y Hellman en 1976, es el primer avance realmente revolucionario en cuanto algoritmos de cifrado en, literalmente, miles de años (…) se basa en funciones matemáticas en lugar de operaciones simples sobre patrones de bits" (pag.742)

En la figura 11 se detalla el proceso de cifrado asimétrico. En el ejemplo, el usuario A desea enviar un mensaje cifrado al usuario B, de forma que solo este último pueda descífralo.

Para ello, ha cifrado el mensaje original (en claro) con la clave pública del usuario B. De esta forma, cualquiera que capture el mensaje en la red no podrá descífralo porque necesita la clave privada de B, que solo éste conoce.

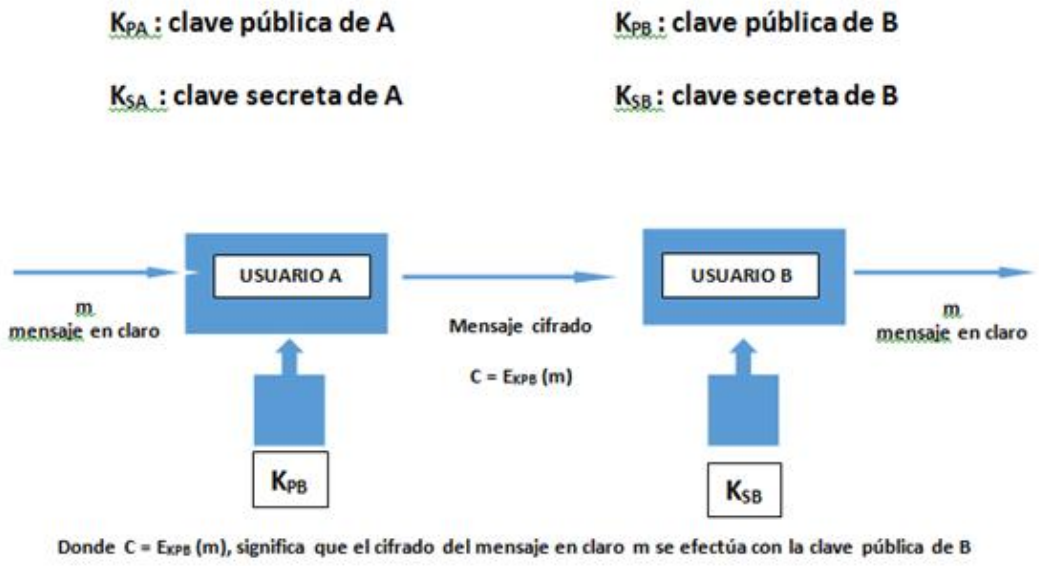


Figura 11: Ejemplo de cifrado asimétrico
Fuente: Elaboración propia

El mensaje viaja cifrado por toda la red hasta que llega al usuario B, que lo descifra con su clave privada. De esta forma se mantiene la confidencialidad del mensaje durante la transmisión y el usuario A puede confiar que solo B será capaz de recibir el mansaje.

Si en el ejemplo anterior también se requiriera asegurar la autenticidad del origen del mensaje emitido por el usuario A, éste debería cifrar el mensaje, ya cifrado con la clave pública de B con su clave privada; de esta forma el mensaje original sufrió un doble cifrado.

En recepción, el usuario B al descifrar el mensaje con la clave pública de A, tendría la certeza que el mensaje lo emitió el usuario A; el mensaje ha sido autenticado. Luego debe descifrarlo con su clave privada para acceder al mensaje en claro, como se explicó en el párrafo anterior.

El esquema de clave pública fue desarrollado por Ron Rivest, Adi Shamir y Len Adleman en 1977 y se lo conoce como algoritmo RSA en reconocimiento a sus autores.

El esquema de clave asimétrica soluciona el problema de distribución de claves que existe con los sistemas de clave simétrica, al respecto Stallings (2004) dice: “El problema más difícil para utilizar cifrado simétrico consiste en cómo distribuir las claves secretas de

forma segura. Este problema desaparece en el cifrado de clave pública por el simple hecho de que nunca se distribuye la clave privada." (pag.748)

Asimismo, Gallardo Carracedo (2004) afirma:

> A modo de conclusión parcial, cabe decir que las dos aportaciones más significativas y revolucionarias de la criptografía de clave pública al mundo de las comunicaciones son:
> El que solamente la clave pública tenga que darse a conocer permite una adecuada gestión de claves en entornos distribuidos donde se requiere la interconexión de sistemas abiertos (heterogéneos).
> Las facilidades que estos sistemas ofrecen para el diseño de mecanismos de autenticación, permitiendo emular sobre las redes, mediante el cifrado con la clave privada del emisor, los esquemas de firmas de documentos que se presentan en las comunicaciones convencionales mediante papel. (pág.139)

En el comercio electrónico se emplea el cifrado asimétrico para encriptar las claves de sesión que se utilizan en los procesos de cifrado simétrico. Se utiliza cifrado simétrico para los datos intercambiados en el proceso, dado que este método es más rápido que el asimétrico. A su vez, el cifrado asimétrico no presenta las dificultades inherentes al cifrado simétrico respecto a la distribución de las claves.

Se puede concluir que la criptografía de clave pública es un método único, básicamente porque las claves públicas pueden compartirse sin poner en riesgo el cifrado. El usuario puede compartir su clave pública a través de la página web del mismo o colocarla en un directorio público, como podría ser www.keyserver.net u otros. Puede darse el caso que alguien distribuya una clave pública falsa de otra persona, en ese caso Engst & Fleishman, (2003) nos dicen:

> Afortunadamente, aunque puede ser complicado verificar que una clave pública pertenece a una persona concreta, el peor resultado posible es que alguien distribuya una clave pública utilizando nuestro nombre, poniendo en cuestión los documentos firmados por nosotros. Pero cuando alguien nos envía un archivo o mensaje cifrado que utiliza esta clave pública falsa, no podemos descifrarlo con nuestra clave privada. Esto nos avisa de posibles problemas, pero nuestra seguridad sigue intacta. (pág. 238)

Un aspecto importante del sistema de claves asimétricas es asegurar la disponibilidad de la clave pública del destinatario. Para resolver este problema, existen servidores de claves que guardan un gran número de claves públicas, normalmente accesibles libremente a través de Internet. Al respecto Bustamante (1999) señala: "Estos servidores pueden ser administrados por Autoridades Certificadoras, quienes emiten los así llamados Certificados (datos de identidad y clave pública de la persona, firmados digitalmente por la AC), asegurando que no se carguen en estos servidores claves públicas que no pertenezcan realmente a la persona cuya identidad está contenida en la clave pública". (pág. 3)

El método de cifrado por dispersión o *hashing*.

El método de cifrado *hashing*, también conocido como función de dispersión H de un solo sentido, no solo se emplea para la autenticación de los mensajes sino también para la implementación de la firma digital. El objetivo principal de este método de cifrado es producir una huella dactilar, también denominada *digest*, código o resumen, a partir de un archivo, mensaje o cualquier tipo de bloque de datos.

La función de dispersión H puede ser aplicada, mediante software o hardware, a bloques de cualquier tamaño y producen una salida de longitud fija que no depende de la longitud del bloque original.

El método *hashing* es una herramienta criptográfica utilizada para generar un resumen compuesto por una cadena única de bits de una longitud específica. Su finalidad no es proteger la confidencialidad del mensaje, dado que el mensaje original en claro no se puede recuperar a partir del resumen. Este método se utiliza principalmente para comprobar la integridad del mensaje y conocer si ha sido modificado o se mantiene intacto, tal como salió de la fuente que lo emitió. El Hash es sin duda la mejor herramienta para la verificación de documentos.

La operación de *hashing*, como se mencionó precedentemente, no tiene inversa, o sea que es de un solo sentido. Es sencillo hallar un resumen o *digest* dado un mensaje, pero es imposible hallar el mensaje original a partir del resumen. Por otro lado, no es posible encontrar un mensaje alternativo que produzca el mismo resumen o *digest* que el generado para un mensaje dado.

Además de proporcionar autenticación, el *hashing* permite detectar la integridad de los datos en forma similar al campo denominado Secuencia de Verificación de Trama (FCS)[81] empleado en los códigos de comunicaciones para detectar la presencia de errores en las tramas. Si uno o más bits se encuentran alterados respecto del mensaje original, el campo FCS lo detecta. Para el caso del cifrado *hashing*, basta que un solo bit cambie para que el resumen o *digest* sea completamente diferente.

En el proceso *hashing*, se transmite desde la fuente u origen el mensaje y el *digest* calculado; ambos llegan al destino donde se vuelve a calcular el *digest* y se compara con el proveniente de la fuente. Si ambos son iguales no ha habido alteraciones en el mensaje transmitido; en caso de que difieran los *digest* se comprueba que se ha alterado el mensaje original. De este modo el proceso *hashing* permite verificar la integridad de los mensajes transferidos.

De los algoritmos de dispersión que existen en el mercado, se impuso el denominado Algoritmo de Dispersión Seguro, SHA[82], desarrollado en EEUU en 1993 por la NIST. En 1995 se publicó una versión mejorada, identificada como SHA1 y en el 2002 la versión SHA 2. El algoritmo genera un *digest* o código de salida de 160 bits.

Una aplicación específica del cifrado *hashing* es el Código de Autenticación de Mensaje, conocido como MAC[83] que combina el cifrado *hashing* con una clave secreta que deben conocer ambos extremos de la comunicación. Si el valor MAC enviado conjuntamente con el mensaje coincide con el calculado en el destinatario, se puede asegurar que el mensaje no fue alterado y que proviene del remitente indicado.

Mientras que el proceso *hashing* permite verificar solo la integridad de los mensajes transferidos, el MAC agrega la verificación de la autenticación del origen del mensaje.

Con respecto al código de autenticación de mensajes, Stallings (2004) aclara que:

> Una variante del código de autenticación de mensajes al que se le ha prestado mucha atención recientemente es la función de dispersión de un solo sentido, también conocida como: *one way hash function*. Como ocurre con el código de autenticación de mensajes, una función de dispersión acepta un mensaje M de longitud variable como entrada y produce un resumen del mensaje de longitud fija H (M) como salida. A diferencia del

[81] FCS: Frame Check Sequency. Campo de una trama que se utiliza para detectar errores.

[82] SHA: Segure Hash Algorithm

[83] MAC: Message Authentication Code

MAC, la función de dispersión no toma como entrada una clave secreta. Para autenticar un mensaje se envía junto a él el resumen del mensaje de forma que el resumen sea auténtico. (pág.738)

En la figura 12 se puede observar la autenticación de un mensaje mediante la función *hashing* y la utilización de un valor o clave secreta S, que se adiciona por concatenación al mensaje y que sólo conocen ambos extremos de la comunicación.

El lado A calcula la función *hashing* sobre la concatenación de la clave o valor secreto y el mensaje, generándose un resumen que se transmite conjuntamente con el mensaje en claro. En el extremo receptor B de la comunicación, se efectúa la función dispersión sobre el mensaje recibido y la clave secreta S, que es la misma empleada en el lado A, obteniendo como resultado un resumen que debe ser exactamente igual al recibido del extremo A.

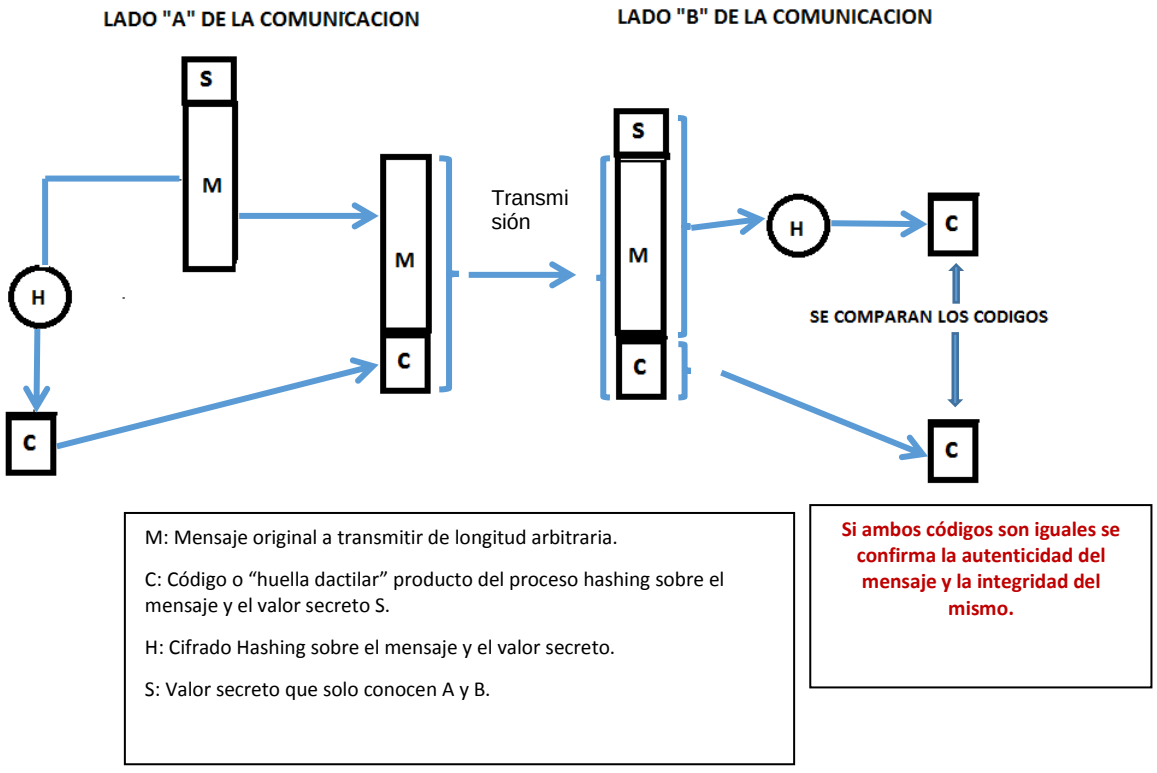


Figura 12: Autenticación de mensajes usando cifrado *hashing* y un valor secreto S
Fuente: Elaboración propia

Los protocolos que emplean *hashing* son el Algoritmo *Hashing* Seguro, SHA, que fuera diseñado por el Instituto Nacional de Estándares y Tecnología, NIST de EEUU y se encuentra en la versión SHA–3, dado que la seguridad de las versiones anteriores fueron superadas.

Otro algoritmo es el empleado para Mensajes Digest 5, MD5[84], desarrollado por Ronald Rivest del Instituto de Tecnología de Massachusetts MIT[85]. Éste se encuentra seriamente comprometido desde 2004 y en el 2008 se rompió la seguridad de SSL atacando el MD5.

Al respecto, Velazco en el sitio RedesZone informa que el SHA-3[86] es muy diferente al actual SHA-2, sin embargo, el NIST afirma que este nuevo algoritmo no pretende sustituir de momento al actual SHA-2, quien no ha demostrado por el momento ninguna vulnerabilidad, sino que simplemente pretende ser un salvoconducto por si ocurre algo con el estándar actual. Los investigadores de seguridad afirman que se tardan años en crear un nuevo estándar, y por ello han querido estar preparados para el futuro desarrollando y estandarizando este nuevo algoritmo que, sin duda, protegerá de la mejor forma posible la información de los usuarios. El desarrollo de SHA-3 comenzó hace 10 años por temor a que aparecieran en SHA-2 vulnerabilidades similares a las de SHA-1. Trece años desde el lanzamiento del SHA-2 el algoritmo sigue siendo seguro y fiable y, en el caso de que apareciera alguna vulnerabilidad en él, ya tenemos un sustituto aprobado para poder aguantar varios años más (Velasco, 2015).

Como se ha dicho el cifrado *hashing* es irreversible, no obstante, es vulnerable a algunos ataques que se enumerarán a continuación:

El ataque de fuerza bruta está limitado por los recursos informáticos de cálculo que se dispongan y consiste en calcular códigos hash para un conjunto posible de valores de entrada, e ir comparando el hash obtenido con el hash atacado.

Si se halla una igualdad, se ha encontrado la contraseña original. Cuando en lugar de generar combinaciones se emplea una lista de palabras predefinidas, el ataque se denomina ataque diccionario.

El ataque de códigos precalculados o Tablas Rainbow supera el obstáculo que presentan los de fuerza bruta, ocasionado por el tiempo que insumen y los recursos que se requieren. En este sentido, la alternativa es disponer de una tabla de códigos hash ya calculados, que permite buscar directamente el código hash en la tabla.

[84] MD5: Message Digest Algorithm 5
[85] MIT: Massachusetts Institute of Technology de EEUU
[86] SHA-3: Versión tres del protocolo SHA.

Otro ataque posible es el de generación de colisiones. Cuando se encuentran al menos dos valores distintos que producen el mismo código hash estamos en presencia de una colisión de hash.

Este tipo de ataque solo es posible en algoritmos hash débiles, como es el caso del protocolo MD5.

Hasta aquí se han descripto los tres métodos de cifrados empleados en criptografía. Para poder cumplir con los requerimientos mínimos de seguridad enunciados, se deberían utilizar en forma combinada los tres métodos de cifrado; simétrico, asimétrico y hashing. Sin embargo, existen situaciones en las cuales no son necesarios los tres métodos.

Al respecto, Forouzan (2006) sostiene:

> El cifrado y descifrado proporcionan secreto, o confidencialidad, pero no integridad. Sin embargo, en ocasiones puede no ser necesario el secreto, pero en su lugar es necesario tener integridad. Por ejemplo, alguien puede escribir un testamento para distribuir sus bienes después de su muerte. No es necesario que el testamento este cifrado. Después de su muerte, cualquiera puede examinarlo, sin embargo, es necesario preservar la integridad del testamento. (pág. 808)

Dado que las aplicaciones informáticas que interactúan en la web, entre ellas las inherentes al comercio electrónico, se basan para su funcionamiento en el Protocolo para el Control de Transmisiones / Protocolo Internet (TCP/IP) se ha desarrollado una nueva versión de éste denominada IPv6, que ha introducido mecanismos de seguridad a nivel IP.

Con respecto a insertar en la capa de red (IP) la seguridad, Feit (1998) afirma:

> Todo el mundo está de acuerdo en que se necesita la seguridad, pero ¿por qué en la capa IP? ¿Porque no utilizar la capa de aplicación? De hecho, es probable que muchas aplicaciones añadan sus propios mecanismos de seguridad.
>
> Pero en un entorno en que los fisgones pueden capturar trafico fácilmente, usarlo todo o parte para repetirlo posteriormente falsificando sus direcciones de IP cuando lo hacen, no se puede estar seguro de que cualquier datagrama sea válido. (pág. 542)

1.6.2. La criptografía y el comercio electrónico

En el comercio electrónico trazable no se tiene como objetivo de seguridad ocultar la operación comercial, sino protegerla de terceros para que éstos no accedan a los datos confidenciales intercambiados entre los participantes, ni los alteren.

En definitiva, la criptografía insertada en protocolos como el SSL/TLS posibilita que se obtenga en la operatoria de comercio electrónico: confidencialidad, integridad, autenticación y no repudio. Para el logro de este objetivo se emplean los tres métodos de encriptado descriptos anteriormente: cifrado simétrico, asimétrico y *hashing*, en forma aislada y/o combinada como se describirá en el próximo capítulo.

No obstante, la criptografía no es el único método para proteger la información cuando se intercambian mensajes. Existe otro método, más antiguo aún, denominado esteganografía.

1.6.3. La esteganografía, características técnicas

Si bien la criptografía es tan antigua como la necesidad de los seres humanos de comunicarnos, como se expresó previamente, no se trata del único método de transmitir información en secreto. Existe una técnica más antigua que la criptografía, que se denomina esteganografía, del griego *steganos*: cubierto u oculto, y *graphos*: escritura, que consiste en ocultar la existencia misma del mensaje en el soporte que lo transporta.

La esteganografía se practica desde hace miles de años. Podemos remontarnos a la Grecia del año 440 AC donde Herodoto de Halicarnaso relata en su libro *La historia de Herodotus*, cómo los griegos lograron durante la guerra entre Persia y Grecia transmitirse mensajes ocultos, a la vista de los soldados persas. Éstos eran escritos sobre tablas de madera que luego se recubrían con cera para hacer creer que eran tablas que aún no se habían utilizado y circular ante la vista de los persas.

Cornejo (2015) señala que:

> John Wilkins (1614-1672) desarrolló, además, obras relacionadas directamente con el mundo de la criptografía y esteganografía como Mercury, or The Secret and Swift Messenger en 1641. Es destacable el desarrollo de procedimientos para ocultar

> información utilizando dibujos geométricos, es decir usando puntos, líneas o triángulos de un dibujo para enmascarar información. Según Jacqueline L. Tobin y Raymond G. Dobard, autores de la obra *Hidden in Plain View: A Secret Story of Quilts and the Underground Railroad*, ideas de este tipo permitieron a esclavos afroamericanos establecer comunicaciones enmascaradas, aprovechando las tradiciones de su civilización, cultura y religión, desde finales del siglo XVIII hasta por lo menos la Guerra de la Independencia Estadounidense, siglo XIX. A lo largo de los años, los esclavos afroamericanos constituyeron una red encubierta apoyados por familias blancas comprometidas para asistir a los esclavos fugitivos. Se habilitaron casas seguras, estaciones y refugios para ocultarse, al igual que se estableció diferentes códigos secretos de comunicación para facilitar a los esclavos el viaje a la libertad. Uno de los códigos de comunicación oculto consistía en bordar en colchas, en terminología inglesa *quilt code*, una serie de patrones que proporcionaban determinada información. Los captores no veían nada raro en que las mujeres de los esclavos colgaran las colchas al aire libre para airearlas, especialmente en primavera y verano (Cornejo, 2015)

La esteganografía pretende ocultar una información dentro de otra; esta última haría la función de cubierta con la intención de que no se perciba ni siquiera la existencia de ella Frecuentemente una cubierta con fines esteganográficos recibe el nombre de estegomedio; dependiendo de la cubierta que se utilice tendremos la estego-imágenes si se usa una imagen, estego-vídeo si se emplea un video; estego-audio si se utiliza un audio; y estego-texto si para ocultar el mensaje se emplea un texto determinado.

Para acceder a la información oculta se debe conocer un secreto, una clave. Como se describió en la criptografía, no se oculta la existencia del mensaje sino que se hace ilegible para quien no esté autorizado y por lo tanto no disponga de la clave de acceso. No obstante, una característica que ambas técnicas comparten es que requieren que un emisor envíe un mensaje que sólo puede ser entendido por uno o varios receptores y que ambos extremos de la comunicación comparten un secreto específico, la clave.

Un mecanismo esteganográfico utilizado desde la antigüedad es el que se basa en el empleo de tintas invisibles que se aplican sobre la superficie a escribir y al secarse no dejan rastros de su presencia. Con posterioridad, el método para recuperar el mensaje depende de los componentes químicos que conformen la tinta invisible; algunos se activan con otros químicos, otras veces con calor o por medio de la luz solar, etc.

El primer registro de uso de esta técnica fue realizado por Plinio el Viejo, quien en el siglo I AC utilizaba una planta llamada *Tithymallus*, que contenía una savia invisible al secarse, pero que al exponerla al calor toma un color marrón.

En el siglo pasado esta técnica fue frecuentemente empleada en la primera y segunda Guerra Mundial; en esta última fue muy notorio el método de esteganografia alemán denominado micropunto que consistía en reducir fotográficamente una página de texto a un punto de menos de un milímetro de diámetro. Por ejemplo, un mensaje podía ir oculto en el punto de una i, para luego esconderlo en una carta aparentemente normal e inofensiva.

La esteganografía se orienta en la actualidad hacia la utilización de medios digitales como ser archivos de texto, audio, video e imágenes digitales. Este último es el medio de transporte preferido dadas las posibilidades que ofrece para ocultar la información en una cantidad muy grande de bytes necesarios para la transmisión de la imagen. Para que tenga éxito el proceso de ocultamiento del mensaje, es imprescindible que las modificaciones introducidas en ella mediante el mensaje oculto, también denominado "ruido visual", no sean perceptibles. Los tipos de archivos de imágenes sobre los que se aplican en general son el Mapa de Bits (BMP)[87]; el Formato de intercambio de gráficos (GIF)[88]; el Grupo de Expertos en Fotografía (JPEG)[89] y los Gráficos para Redes Portátiles (PNG)[90] .

Con respecto al método JPEG que es el más difundido, Li & Drew (2004) nos dice: El JPEG es el método más importante y estándar para la compresión de imágenes. Esta norma fue creado por un grupo, perteneciente a la Organización Internacional de Estandarización (ISO), que informalmente se lo conoce como Grupo de Expertos en Fotografía Unidos y continua actualmente identificado bajo esa denominación (pag, 75).

El método esteganográfico más utilizado en archivos de imágenes es el LSB, del inglés *Least Significant Bit*, que es también el más fácil de detectar mediante las técnicas de estegoanálisis[91]. La ventaja de transmitir la información a través de imágenes es que éstas circulan por Internet sin despertar sospechas; además la leve modificación de algunos de los pixeles en la imagen para introducir la información no es generalmente percibida por el

[87] BMP: BitMaP, Mapa de Bits.
[88] GIF: Graphic Interchange Format
[89] JPEG: Joint Photographic Experts Group
[90] PNG: Portable Network Graphics
[91] ESTEGOANALISIS: Disciplina que se encarga de la detección de mensajes ocultos mediante la esteganografia.

ojo humano. La imagen puede ser almacenada en diferentes formatos, siendo el más utilizado el GIF que utiliza 8 bits, si bien el formato BMP color de 24 bits es el que posibilita ocultar mayor volumen de bits de información.

No solo se puede ocultar información en las imágenes sino también es posible introducir un código que luego se podría ejecutar a través del navegador web. Esta técnica, que en realidad es una pseudoesteganografia, fue desarrollada por Saumil Shah en el 2013 y se basa en la inclusión de código JavaScript dentro de las imágenes, de forma tal que el navegador web puede interpretar a la imagen como tal, pero también se le podría solicitar la ejecución del código JavaScript que dicha imagen transporta.

Uno de los protocolos frecuentemente utilizado para este fin, es el Protocolo para Mensajes de Control en Internet ICMP[92], que cuenta con una utilidad muy difundida entre los usuarios de computadoras y administradores de redes, para el diagnóstico de la red denominada buscador de paquetes en Internet PING[93]. Esta herramienta posibilita comprobar el estado de la comunicación en la red IP entre un host con uno o varios equipos remotos. Para ello envía datagramas IP en los cuales se transportan mensajes ICMP denominados solicitud. El host o equipo interrogado responde con replicas y del análisis de las mismas se puede diagnosticar el estado, la velocidad y la calidad de la red que conecta ambos equipos. La información, órdenes o comandos se ubican en el campo de datos de los datagramas ICMP los cuales se transmiten fácilmente a través de los Firewalls de las redes que en general no filtran el tráfico ICMP.

Adicionalmente a la técnica ya mencionada que consiste en la modificación de los bits menos significativos de una imagen, también se insertan bits de información ocultos en los coeficientes de las imágenes, como es el caso de la técnica denominada Transformada del Coseno Discreto, DCT[94] o la Transformada Rápida de Fourier, FFT[95]. En el caso de la DCT aplicada a video, la técnica se basa en cambiar levemente cada imagen del video de forma que pase inadvertido al ojo humano el ingreso de los bits de información del mensaje oculto. El método DCT toma la imagen y la transforma en una secuencia de números que contiene aproximadamente la misma información que la imagen original, con una pequeña pérdida por la compresión que se genera. Mediante el método de sustitución

[92] ICMP: Internet Control Message protocol
[93] PING: Packet Internet Groper
[94] DCT: Discrete Cosine Transform
[95] FFT: Fast Fourier Transform

del bit menos significativo LSB de cada octeto se reemplaza este último de cada pixel de la imagen por otro bit del mensaje que se quiere ocultar en dicha imagen. En la figura 13 se puede observar cómo se oculta la letra A = 01000001 dentro de la imagen. Esta última está formada por pixeles, cada uno requiere de 3 bytes de información un byte para cada color rojo, verde y azul, denominados RGB[96]. Al utilizar el método de sustitución del LSB se podrá emplear el último bit de cada octeto de información de cada pixel. En consecuencia, se requieren 3 pixeles para transmitir los 8 bits de la letra A.

También se puede observar la aplicación de la sustitución del bit menos significativo de cada número binario, por cada bit del carácter A -mensaje secreto-; se ha sustituido entonces cada bits LSB -recuadro rojo- por cada bits del carácter A, formando nuevos valores para los colores RGB. Estos nuevos colores no cambian mucho con respecto al original y así no pueden ser distinguidos por el ojo humano, pasando inadvertidos. Se utilizaron 8 bits LSB en total, uno por cada bit del mensaje. Los que no se utilizan, se dejan como están.

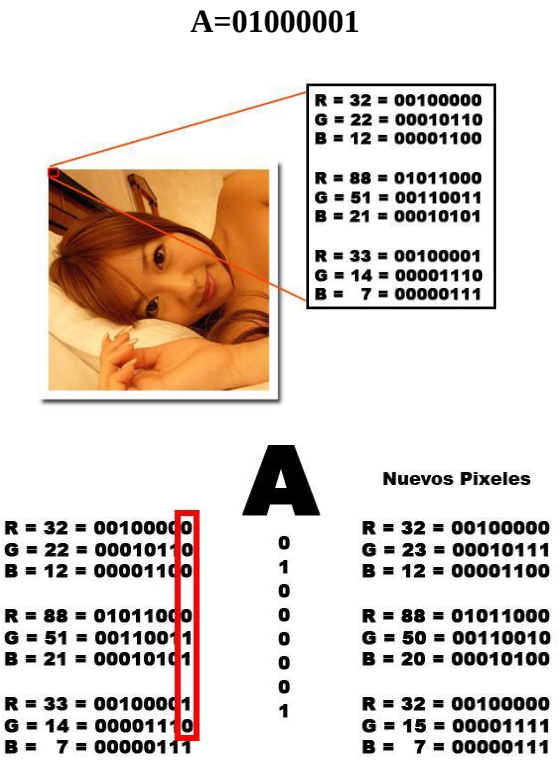


Figura 13: Ejemplo de esteganografía mediante el método de sustitución
Fuente: J.C. Mouse (2017)

[96] RGB: Red, Green, Blue

Otra técnica esteganográfica empleada en la actualidad, aunque en menor medida, es la esteganografía en archivos de audio que consiste en agregar funciones senoidales, denominadas armónicas, al archivo de audio, sin que éstas originen ruido perceptible sobre el audio original. Al efectuarse el filtrado en el extremo receptor se separa el audio original del mensaje oculto. Otro método es embeber información en sonidos débiles, que quedan cubiertos por sonidos más fuertes y en consecuencia pasan desapercibidos al oído humano.

También se emplea esteganografía en videos a efectos de grabar la autor del mismo, técnica que se conoce como *watermarking*, que significa marca de agua digital y consiste en la inserción de un mensaje que contiene información sobre el autor.
También es factible insertar archivos en disco rígidos en forma oculta para el usuario que no disponga del nombre del archivo y la clave de acceso y en consecuencia no revela si existe o no información oculta en un disco rígido a ojos de un atacante. Los autores de esta técnica son Ross Anderson, Roger Needham y Adi Shamir que en 1998 plantearon la teoría de un sistema de archivos que oculte información directamente en el disco, técnica que se denominó *The Steganographic File System*. Ésta fue implementada en herramientas como Sistema de archivos Steganograficos (StegFS)[97] y Sistemas de Archivos Steganograficos para Linux (Magikfs).

La técnica de ocultación denominada final de archivo, EoF[98], demuestra cómo es posible ocultar información cuando no se realizan las validaciones oportunas de la estructura de los archivos. Esta técnica es sencilla y consiste en añadir la información a ocultar al final del archivo. Normalmente el software que carga e interpreta un formato de archivo, lee los datos contenidos en la estructura definida, no reconociendo más allá del fin de archivo en dicha estructura. De esta forma se puede añadir información al final del fichero sin que afecte al uso normal del mismo. Cornejo (2015) dice que:

> Se puede ocultar información al final de imágenes digitales, audio, vídeo, ejecutables, ficheros de ofimática, etc. En Internet existen muchas herramientas que hacen uso de esta técnica, por ejemplo, la herramienta Camouflage. Además, hoy día, esta técnica es usada, por su sencillez y capacidad de ocultación, ampliamente para la distribución de material protegido por derechos de autor y pornografía adulta. Típicamente se utilizan herramientas que trocean la información (por ejemplo, camuflaweb) y luego la añaden en diferentes cubiertas (típicamente

[97] STEGFS: Steganographic File System
[98] EoF: End Of File.

imágenes) que se distribuyen por Internet, por ejemplo, a través de cuentas de correo electrónico accesibles mediante clientes de peer2mail u otras propuestas similares (Cornejo, 2015).

Podemos concluir con el tema de la estenografía con el concepto brindado por Gomes (2010):

> La esteganografia constituye, al fin, un recurso de indudable utilidad, aunque para el caso de un número masivo de comunicaciones es seguramente inviable. Además, empleada como recurso único, adolece de un importante defecto: en el caso que el mensaje sea interceptado, el significado del mismo resulta transparente. Es por eso que la esteganografía suele emplearse principalmente como un método complementario a la criptografía para así reforzar la seguridad de la transmisión. (pag.22)

1.6.4. La esteganografia y el comercio electrónico

Como se detalló precedentemente el objetivo fundamental de la técnica esteganográfica es ocultar la existencia del mensaje en el comercio electrónico. También se pretende que terceros no autorizados tengan acceso a los detalles y/o datos confidenciales de la operación; esto se consigue con el cifrado de los datos, pero de ninguna manera se trata de ocultar la existencia de la comunicación producto de la operación comercial; por el contrario, se requiere la trazabilidad de la operación entre el usuario comprador y el sitio de venta.

Por otro lado, los hackers podrían emplear técnicas esteganográficas para ocultar información y/o programas espías en el servidor del sitio web, por ejemplo, la descripta en el párrafo anterior: EoF (*End of File*). No obstante, si en el sitio se realizan las validaciones de archivos correspondientes las mismas pueden ser detectadas y eliminadas a tiempo.

Conclusiones del capítulo 1: Estructura del comercio electrónico

En el presente capítulo se han descripto los diferentes modelos de comercio electrónico y los posibles medios de pago. Para el trabajo de tesis se ha considerado solo el modelo B2C por ser el que presenta mayor difusión, y se ha seleccionado como medio de pago la tarjeta de crédito, también por ser el más extendido comercialmente. En el modelo elegido existe trazabilidad de la operación desde el usuario que inicia la transacción, hasta el vendedor que entrega el bien o servicio y recibe el pago.

En el esquema de pago con tarjeta de crédito se determinó que intervienen los siguientes actores: el comprador, el vendedor, el banco emisor de la tarjeta de crédito, el banco que en nombre del vendedor recibe la transacción y la red de medios de pago como pueden ser VISA, MASTERCARD, AMERICAN EXPRESS, CABAL, DINERS CLUB, DISCOVER, etc. La tarjeta se gestiona a través de un banco o entidad financiera y una vez emitida autoriza a la persona, a cuyo nombre se encuentra extendida, a utilizarla como medio de pago en los comercios y/o negocios adheridos al sistema.

Los modelos de comercio electrónico analizados fueron los siguientes: B2C, de negocio a consumidor; B2E, de negocio a empleado; B2B: de negocio a negocio; C2C, de consumidor a consumidor; G2C, de gobierno a consumidor; C2B, de consumidor a negocio, M2B, de móvil a negocio. Sin embargo, el modelo B2C, que se lleva a cabo entre el negocio o tienda virtual y los consumidores interesados en comprar productos o adquirir servicios, es el más utilizado por los negocios y tiendas en línea para llegar permanentemente a los consumidores individuales.

Asimismo, se detallaron los componentes del comercio electrónico y se determinó que en el proceso intervienen el navegador web en el host del cliente, los protocolos de comunicaciones y los protocolos de seguridad que brindan conectividad a través de la red Internet y seguridad en la comunicación respectivamente, como así también, el sitio web del vendedor con la aplicación informática que sustenta la operación. También pueden formar parte de la transacción entidades intermedias y bancos, según la estructura implementada. Se detalló también que la encuesta posibilitara determinar cuál de los componentes mencionados es el que presenta mayor nivel de vulnerabilidad para la seguridad del comercio electrónico, según la opinión de los futuros profesionales de TIC.

Para realizar las transacciones comerciales los principales medios de pago analizados fueron los siguientes: contra reembolso, cargos en cuenta bancaria, tarjetas de crédito, intermediarios electrónicos, tarjetas inteligentes, micro pagos o monederos virtuales y terminal de Punto de Venta Virtual.

Se ha excluido de la investigación de esta tesis al sistema de pago electrónico denominado moneda electrónica, debido a la dificultad de su implementación y a la falta de trazabilidad de sus operaciones.

A lo largo del capítulo se analizaron las principales vulnerabilidades en la seguridad de la web y en especial las inherentes al comercio electrónico trazable, lo cual posibilitará confeccionar parte de la encuesta.

Se determinó que las vulnerabilidades o debilidades~~,~~ de la seguridad del comercio electrónico son aquellos aspectos técnicos, operativos y de procedimiento que pueden ocasionar la captura intencional de información confidencial por parte de terceros para ejecutar acciones, en tiempo real o diferidas, que afecten económicamente al comprador y/o al vendedor.

Se analizaron los aspectos que hacen a la seguridad de una transacción comercial a través de la web y los principales riesgos que tienen los usuarios cuando operan entre los que podemos mencionar el robo de datos personales mediante *phishing* y *spyware*, la suplantación de identidad, el ataque al sistema de cómputos del usuario mediante virus informáticos, *botnets*, troyanos y gusanos, la divulgación de la identidad del usuario comprador. Estas acciones son ejecutadas por atacantes denominados *hackers* y/o *crackers*. También se indicó como un posible riesgo de la operación comercial, el fraude por parte de la empresa vendedora al no entregar los productos o servicios.

Por otro lado, se detallaron los requerimientos generales de seguridad que debe tener toda operación que se efectúa a través de Internet los cuales están basados en los conceptos de ~~la~~ confidencialidad o privacidad, que consiste en la protección contra escuchas no autorizadas y que es especialmente importante en las transacciones con tarjetas de créditos, evitando la difusión de datos a personas no autorizadas; la autenticación que abarca los conceptos de identificación; la integridad y el no repudio.

La identificación del usuario brinda protección frente a la suplantación de personalidad; la integridad se refiere a la protección de los datos originales a efectos de evitar su modificación total o parcial; y el no repudio concierne a la protección frente a posteriores negaciones respecto del bien o servicio brindado por el vendedor y/o recibido por el comprador. También se agrega un concepto muy importante para garantizar la operación en el comercio electrónico que es la disponibilidad del sistema y los datos, a efectos que la operación esté disponible en todo momento para las partes autorizadas.

Por otro lado, se detalló que para la protección de la información se dispone en general de técnicas como la criptografía y la esteganografía. Con respecto a la primera existen tres diferentes métodos de encriptado o cifrado, los cuales se pueden aplicar en forma aislada o combinada, los métodos son el cifrado simétrico, el cifrado asimétrico y el cifrado *hashing*.

El método de cifrado de clave simétrica o simplemente cifrado simétrico utiliza una única clave, tanto para cifrar como para descifrar los datos, son mecanismos muy rápidos, pero tienen la dificultad de la distribución de las claves. Entre los protocolos de cifrado simétrico más conocidos se encuentran el DES, TRIPLE DES, AES, RC2, RC4, RC5, IDEA, SAFER y BLOWFISH.

El método de cifrado asimétrico o también denominado de clave pública utiliza dos claves para cada usuario, una publica y otra privada. La clave pública del usuario o entidad está en Internet y es conocida por todos; la privada solo la conoce el usuario y la debe mantener en secreto. El sistema permite encriptar con cualquiera de las dos; por ejemplo, si se encripta con la clave privada de un usuario sólo se podrá desencriptar con la clave pública de dicho usuario y viceversa. Este método tiene la ventaja que no necesita un sistema de distribución de claves pero tiene la desventaja que es muy lento, especialmente para mensaje o archivos extensos. El esquema de clave pública fue desarrollado por Ron Rivest, Adi Shamir y Len Adleman en 1977 y se lo conoce como algoritmo RSA en reconocimiento a sus autores.

El tercer método denominado cifrado *hashing*, también conocido como función de dispersión H de un solo sentido, no solo se emplea para la autenticación de los mensajes sino también para la implementación de la firma digital. El objetivo principal de este método de cifrado es producir a partir de un archivo, mensaje o cualquier tipo de bloque de datos, una huella dactilar también denominada *digest* o resumen. Este método de

encriptado no tiene inversa, no se puede desencriptar, o sea que a partir del *digest* no se puede obtener el texto en claro del cual se partió. Los protocolos que emplean *hashing* son el SHA en su versión actual SHA3 y MD5.

Estos tres métodos se emplean combinados para obtener seguridad en la transmisión de datos. Con el cifrado simétrico se encriptan los mensajes, datos y/o documentos debido a que es un método rápido. No obstante, la clave de la sesión para el cifrado simétrico se transmite mediante encriptado asimétrico. Para acreditar la integridad de un documento se emplea el cifrado *hashing*. En el extremo transmisor se cifra con el método *hashing* y se obtiene el *digest* que se trasmite conjuntamente con el documento, en el extremo receptor, se cifra el documento mediante el mismo método *hashing* obteniendo un nuevo *digest*. Se comparan los dos *digest* si son iguales no hubo ataques a la integridad del documento. Por otro lado, para autenticar y/o firmar un documento se emplea el cifrado *hashing* y el cifrado asimétrico.

Para tratar de contrarrestar la vulnerabilidad de la seguridad en el comercio electrónico se emplean los métodos criptográficos descriptos. Asimismo, se analizó la técnica basada en la esteganografía que es otro método de ocultar la información, no obstante, se concluyó que ésta no es una técnica aplicable al proceso de comercio electrónico, dado que el objetivo de la misma es ocultar la transmisión de datos, siendo que, en el comercio electrónico se requiere la trazabilidad de la operación entre el usuario comprador y el sitio de venta.

<u>Capítulo 2</u> Vulnerabilidades en la seguridad del comercio electrónico trazable, protocolos de red y de seguridad utilizados

Introducción

En el capítulo anterior hemos analizado los principales componentes y tipos de comercio electrónico, incluida la red Internet, y los medios de pagos. También se analizaron los requerimientos generales de seguridad para las operaciones online en la web y las técnicas criptográficas y esteganograficas para la protección de los datos.

Para completar el marco que dará sustento teórico y técnico para la encuesta, que se presenta en el capítulo 3, evaluaremos en el presente capitulo las vulnerabilidades de la seguridad en la web que se manifiestan a través de los delitos cibernéticos. Al respecto, detallaremos algunos aspectos sobresalientes de esta verdadera guerra cibernética que se libra en la red Internet entre las principales potencias mundiales y detallaremos especialmente los fraudes con tarjetas de crédito, que constituye el medio de pago considerado en la tesis.

Se describirán las principales vulnerabilidades de la seguridad en la web, que afectan también al comercio electrónico. Dichas vulnerabilidades podemos definirlas como aquellos aspectos técnicos, operativos y procedimientos que pueden ocasionar la captura intencional de información confidencial por parte de terceros para ejecutar acciones, en tiempo real o diferido, que afectan económicamente al comprador y/o al vendedor. El delito cibernético tiene diferentes variantes, la mayoría de los ataques se llevan a cabo mediante el denominado código malicioso o malware, éste incluye amenazas de diferente tipo como virus informáticos[99], gusanos[100], troyanos[101], PUPs[102] y *botnets*[103].

Constituye un caso especial el fraude que se realiza con tarjetas de crédito, que es el medio más difundido al operar en comercio electrónico. Éste se ha incrementado y actualmente afecta al 0,6 % del monto total de las transacciones realizadas en comercio electrónico a nivel mundial.

[99] VIRUS INFORMATICO: Programa o malware que sin el conocimiento del usuario altera el comportamiento de la computadora o dispositivo informático.
[100] GUSANOS: Programas cuyo objetivo es ejecutar copias de si mismo y alojarlas en diferentes ubicaciones para hacer colapsar el sistema.
[101] TROYANOS: Software malicioso que al ejecutarlo permite el acceso remoto al equipo infectado.
[102] PUPS: Programas potencialmente no deseados, se instalan camuflados durante la instalación de otros programas. No constituyen un malware.
[103] BOTNETS: Red de robots informáticos o bots, que se ejecutan de manera automática y que posibilita a quien lo creo controlar todos los computadores infestados.

También se analizarán los dos protocolos que brindan confiabilidad y seguridad a las transacciones de comercio electrónico que se realizan a través de la red Internet: el TCP y el SSL/TLS.

Se describirán las principales características del protocolo TCP, el cual, dado que posee calidad de servicio brinda confiabilidad a la comunicación entre el usuario y el sitio web del vendedor. El protocolo TCP dispone de los mecanismos necesarios para garantizar la calidad de servicio, por lo cual, es orientado a la conexión y tiene además controles de: errores, flujo, secuenciamiento y de congestionamiento.

Por su parte, y a partir de sus características técnicas y operativas, el protocolo SSL/TLS ofrece seguridad a las transacciones a través de la web.

El estudio de la calidad de servicio de una red, en este caso la red Internet, como así también la seguridad informática en general, excede el alcance del presente trabajo de tesis. Por esta razón, solo se analizarán los protocolos que intervienen en la operatoria del comercio electrónico.

En el momento de la encuesta, los estudiantes deberán expedirse respecto a los servicios brindados por ambos protocolos y determinar si son suficientes para asegurar confiabilidad y seguridad a la comunicación entre el host del usuario y el sitio web del proveedor. Si así lo consideran, podrán desechar a este componente, la comunicación entre el host del usuario y el servidor del proveedor, como causa de la vulnerabilidad en la seguridad del comercio electrónico.

Para completar el análisis de los protocolos que brindan seguridad en la web es posible mencionar brevemente las características de los protocolos IPSEC, SSH, 3D *secure*, iKP y SET. Si bien podrían utilizarse en el comercio electrónico, no se incluirán en este trabajo ya que el SSL/TLS es el de mayor difusión.

Analizaremos también las principales amenazas y ataques que enfrenta el sitio web del vendedor. En primer término por tratarse de una aplicación informática más, que opera en la insegura red Internet. Además, porque es un sistema que gestiona recursos monetarios, bienes y servicios, lo que representa una atracción permanente para los delincuentes cibernéticos. Dichos factores, se incorporarán posteriormente a la encuesta para su

evaluación por parte de los estudiantes de las carreras de Licenciatura e ingeniería en Sistemas de Información, en lo que concierne a su importancia relativa respecto de la seguridad del sitio web.

Cabe aclarar, que no se incluirán en la encuesta los factores que afectan la seguridad del host del usuario en su conexión con la red Internet, debido a que las alternativas de conexión son numerosas y en general los riesgos son semejantes que en cualquier computador conectado a la red Internet. Sin embargo, sí se incluirán en la encuesta las amenazas y ataques que pudieran surgir a través del servidor web hacia el host del usuario por deficiencias en los mecanismos de seguridad del servidor.

Por último, somos conscientes de que aun cuando se describirán las principales amenazas conocidas hasta el presente y que afectan la seguridad informática, en este caso aplicadas al comercio electrónico, mientras escribimos estas líneas seguramente se están desarrollando nuevas y más sofisticadas amenazas para implementar en futuros ataques.

2.1. El delito cibernético y el costo de la información robada en Internet

Como camino rápido y económico para lograr dominación comercial, el espionaje cibernético es más efectivo que la investigación y el desarrollo de productos y servicios nuevos. Uno de los países que encabeza los ataques cibernéticos es China, al punto que, en 2010 la empresa Google considero cerrar sus operaciones en dicho país tras sufrir un ataque en su sistema de cómputos que permitió a los activistas chinos acceder a las computadoras de los informáticos que desarrollaban software para Google en EEUU (California). El ataque no fue muy sofisticado, se basó en un simple mensaje de *phishing* (suplantación de identidad) enviado a un desprevenido empleado de Google, en las oficinas de esa empresa en China, quien, al hacer clic en el vínculo, posibilito la descarga de un software que tomó el control de su computadora y a partir de ésta llego a los equipos mencionados.

Según el congresista de los EEUU Mike Rogers (Traver, 2014) “China ha obtenido más de 500.000 millones de dólares de empresas americanas mediante el espionaje cibernético” (pág. 258). Además, en el Congreso de ese país se difundió la información de que desde el comienzo del nuevo milenio, China ha penetrado en las redes de más de 760

corporaciones, proveedores de servicios de Internet, universidades y organismos gubernamentales.

Los ataques cibernéticos entre países han sido desarrollados por diversos autores. Sierra (Clarín, 2015) afirma que:

> Esta guerra cibernética no tiene un solo culpable, sino que EEUU también ha fomentado y estimulado a espías cibernéticos con la excusa de proceder a la defensa del país de milicias y grupos terroristas extranjeros. Un ejemplo es el gusano informático STUXNET diseñado en el 2010 por un grupo de investigadores rusos para afectar al sistema operativo Windows, se aplicó para atacar y reprogramar sistemas industriales que operaban con Windows, específicamente al sistema de control SCADA[104], el objetivo fue desactivar las computadoras que controlaban las maquinas centrifugadoras en el proceso de enriquecimiento de uranio en Irán. La empresa europea Kaspersky ha demostrado que más de la mitad de los equipos infectados en el mundo se encontraban en Irán y lo definió como "un prototipo funcional y aterrador de un arma cibernética que conducirá a la creación de una nueva carrera armamentista mundial. (Sierra, 2015)
>
> Otro incidente, pero esta vez con un *malware* denominado FLAME, atacó a los sistemas informáticos del Ministerio del Petróleo de Irán. En realidad, se lanzaron dos agentes de malware: FLAME (un agente de espionaje) y WIPER (un agente diseñado para la eliminación de datos). Los chinos no se quedaron inermes frente a éstos y otros ataques y crearon una unidad denominada Equipo de Respuesta a Emergencias Informáticas Nacionales; esta unidad rápidamente genero una herramienta que posibilitó detectar y destruir al gusano FLAME. Posteriormente EEUU introdujo el gusano DUQU diseñado para recopilar contraseñas, realizar capturas de pantallas, robo de documentos, etc. (Laudon & Traver, 2013, pág. 259)

Podemos deducir con bastante aproximación, que la red Internet y la web son cada vez más vulnerables a ataques no solo de gobiernos sino también, como producto de la globalización: de bandas organizadas de delincuentes que operan en forma global.

Por otro lado, las compañías de seguridad digital no tienen demasiado campo de acción dado que cualquier contramedida que se pretenda implementar, necesariamente implicaría intervenir las comunicaciones a efectos de realizar las inspecciones y procedimientos técnicos necesarios, y es en este punto se enfrentan a la decidida oposición de grupos defensores de la privacidad.

[104] SCADA: Supervisory Control And Data Acquisition

El problema principal radica en el diseño conceptual de la red Internet, concebida originariamente para un mercado de pocos nodos y usuarios. Recordemos que nació a partir de la red ARPANET[105], que tenía al comienzo solo cuatro nodos, no ciento de miles como tiene Internet en la actualidad. Para esta cantidad actual de nodos, carece entonces de mecanismos de seguridad intrínsecos como ocurre con otras redes. Comparando la red Internet con el caso de la red telefónica, que opera mediante el mecanismo de la conmutación física de circuitos, se advierte que para realizar un ataque en esta última, es necesario interferir el enlace telefónico ya sea urbano, interurbano o internacional. Por el contrario, en la red internet, que opera en el modo datagrama[106], no resulta necesario interferir físicamente los enlaces, por otro lado, ofrece a la actividad delictiva la ventaja del anonimato, que permite enmascarar a cualquier delincuente con una apariencia legitima, posibilitándole realizar pedidos fraudulentos a comerciantes en línea, inhabilitar sitios web, robar información confidencial, etc. De esta forma, Internet permite a los delincuentes robar a las personas a distancia y de manera casi anónima, en lugar de la tarea riesgosa de robar en persona un banco.

Al respecto Traver (2013) nos dice:

> Para la mayoría de los ciudadanos respetuosos de la ley, Internet ofrece la esperanza de un enorme y conveniente mercado global que proporciona acceso a bajo precio a personas, bienes, servicios y negocios en todo el mundo. Para los delincuentes, Internet ha creado formas completamente nuevas – y lucrativas- de robar a los más de 1000 millones de consumidores que hacen transacciones por Internet en el mundo. Desde productos y servicios hasta efectivo e información, todo está expuesto ahí en Internet para tomarlo si es posible. (pág.262)

2.1.1. Costo de la información robada en Internet

El robo de información en Internet es una actividad delictiva muy lucrativa, dado que los delincuentes pueden vender la información cuyo valor varía según el tipo de dato. En la figura 14 se puede observar el cibermercado negro de datos robados.

No obstante, en algunos casos, los delincuentes cibernéticos no buscan vender datos sino causar daño a sitios web específicos por orden de terceros, quienes contratan sus servicios.

[105] ARPANET: Advanced Research Projects Agency Network (Agencia de Proyectos de Investigación Avanzada).
[106] MODO DATAGRAMA: Modo de funcionamiento de la red Internet en la cual no hay circuitos virtuales preestablecidos y en cada router de la red se decide el camino a tomar por el datagrama hasta el siguiente router.

De esta forma, logran desestabilizar, desprestigiar o alterar el sitio web, con el consiguiente daño a la reputación del mismo, además de originar costos importantes por la reparación y el tiempo en el que éste permanece inactivo, y la consecuente pérdida de negocios y clientes.

Para contrarrestar estas acciones delictivas, los encargados de los sitios web y de la seguridad informática deben mantenerse al día sobre las técnicas emergentes en seguridad que involucra nuevas tecnologías, políticas y procedimientos organizacionales y también en la actualización de las leyes que regulan la actividad.

> Podemos concluir entonces que una buena seguridad en el comercio electrónico requiere de un conjunto de leyes, procedimientos, políticas y tecnologías que, en la medida de los posible, protejan a los individuos y las organizaciones contra el comportamiento inesperado en el mercado del comercio electrónico (Traver Laudon, 2013, pág.266).

ítem	Descripción de la información robada en Internet	Costo en dólares de EEUU
1	Tarjeta de crédito	$2 a $90
2	Una identidad completa(cuenta bancaria, tarjeta de crédito, fecha de nacimiento, seguro social, etc)	$3 a $20
3	Cuenta bancaria	$80 a $700
4	Cuentas en línea (PayPal, eBay, etc)	$10 a $1500
5	Cuentas de Correo electrónico	$5 a $12
6	Renta de *Botnets*	$15
7	Una sola computadora comprometida	$6 a $20
8	Número de seguro social	$5 a $7
9	Kits de herramientas de ataques	$120 al mes

Figura 14: Costo de la información robada en Internet
Fuente: Laudon & Traver (2014)

2.2. Principales vulnerabilidades de la seguridad en la web

"La seguridad no es una función que pueda ser verificada, como una reacción química o un proceso de manufactura. Por el contrario, solamente es efectivamente verificada cuando algo no sale bien." (Cano, 2013, pág. 26)

Las vulnerabilidades o debilidades de la seguridad del comercio electrónico son parte de las vulnerabilidades generales que existen en la red Internet. Podemos definirlas como

aquellos aspectos técnicos, operativos y procedimientos que pueden ocasionar la captura intencional de información confidencial por parte de terceros para ejecutar acciones, en tiempo real o diferidas, que afecten económicamente al comprador y/o al vendedor.

El delito cibernético tiene diferentes variantes. La mayoría de los ataques se llevan a cabo mediante el denominado código malicioso o malware, término que proviene de las palabras *MALicius* (malicioso) y *WARE* (software o programa).

Generalmente nos referimos al código malicioso como malware e incluye amenazas de diferente tipo como virus informáticos, gusanos, troyanos, crackers y hackers. Cuando se accede a un sitio y se baja un archivo, puede activarse el ataque denominado *drive by download*, que consiste en un malware incluido en el archivo que se baja del sitio web falso. También es común el código malicioso incrustado en archivos PDF[107] o en los mensajes de correo electrónico que llevan los tradicionales archivos adjuntos para infectar las computadoras. Los vínculos pueden llevar al usuario a sitios web falsos, que incluyen códigos JavaScript[108] malicioso.

Los virus son programas informáticos que se caracterizan por la capacidad para reproducirse y hacer copias de sí mismo con la finalidad de extenderse a otros archivos. También pueden llevar una carga útil destructiva, con la finalidad de reformatear discos, destruir archivos o causar la ejecución errónea de programas. En el caso más benigno, la carga solo incluye propaganda.

Si los virus se combinan con un gusano, entonces estarán diseñados para extenderse de una computadora a otra. Un caso muy popular fue el gusano SLAMMER, que estaba dirigido a explotar una vulnerabilidad conocida del sistema de base de datos Microsoft SQL Server. Luego de haber sido liberado en Internet, infecto a cajeros automáticos, cajas registradoras de supermercados e interrumpió la mayoría de las conexiones a Internet de Corea del Sur provocando una caída importante del Mercado Bursátil de ese país. Posteriormente, en 2008, el gusano CONFICKER logro infectar a más de 9 millones de computadoras en todo el mundo, según informo la empresa Symantec.

> Los orígenes de los virus de las computadoras podrían sorprenderte, sus objetivos no eran exactamente los mismos que hoy. En un comienzo, los virus tenían utilidades variadas y fueron diseñados en su mayoría por personas en la industria de la

[107] PDF: Portable Document Format.
[108] CODIGOS JAVA SCRIPT: Rutinas escritas en lenguaje de programación orientado a objetos.

> informática. Los estudiantes universitarios creaban virus para proyectos de investigación con el fin de ayudar a ampliar sus estudios y perfeccionar sus habilidades de codificación. Además de la investigación, los estudiantes también construían códigos para hacerles bromas a sus compañeros de clase. Los ingenieros de Xerox crearon un *worm*[109] informático destinado a la búsqueda de procesos de inactividad en una red informática (…) en otro lugar un par de programadores crearon un virus de sector de arranque para defender su programa contra la piratería. (Norton by Symantec, 2017)

Los troyanos son programas maliciosos que entran en la categoría de malware y cuya finalidad es, en la mayoría de los casos, generar una puerta trasera o *backdoor* para acceder al equipo infectado y obtener información. Toda esta acción se ejecuta sin ser advertido por el usuario legítimo del equipo.

El *hacker*, desde el punto de vista de la seguridad informática, es el atacante que accede de manera no autorizada a recursos informáticos como computadoras, servidores, etc., para obtener información o atacar la integridad de los datos. El cracker se diferencia del hacker en el hecho que toma el control remoto del recurso informático, también para fines delictivos.

El ataque mediante *botnet* (red de robots) se basa en el empleo de un conjunto de robots informáticos, que operan de manera automática para controlar en forma remota los computadores y servidores infectados.

> Las *botnets* (redes de robots) son conjuntos de computadoras capturadas que se utilizan para realizar actividades fraudulentas como el envío de *spam*[110], la participación en un ataque DDoS[111], robo de información de computadoras y almacenamiento del tráfico de las redes para su posterior análisis. No se sabe cuántos *botnets* operan en el mundo, pero se estima que son miles (Traver Laudon, 2013, pág.272)

También existen los Programas Potencialmente Indeseables (PUPs) que consisten en códigos maliciosos que se instalan por sí mismos en la computadora, por lo general sin el consentimiento del usuario. Las variantes más frecuentes de PUPs son los programas *adware* (que proviene de las palabras en inglés *Advertising* –publicidad- y *Ware* –programa-), el parasito del navegador, el *Spyware* (que proviene de las palabras en inglés *spy* –espía- y *ware* -programa-).

[109] WORM: Gusano.
[110] SPAM: Mensajes no solicitados, habitualmente de tipo publicitario y de envío masivo.
[111] DDoS: Distributed Denial of Service

La empresa McAfee diferencia los programas PUPs de los otros tipos de malware como son los virus, troyanos y gusanos. Éstos pueden, en cierta forma ser rechazados por el usuario, dado que para su instalación en el equipo atacado requieren de alguna acción del propio usuario. (Rouse, 2005)

El programa *aware* se utiliza en general para insertar publicidad emergente en la computadora infectada cuando se visitan ciertos sitios web. Se puede decir que en sí, no constituye una actividad delictiva. No obstante, puede resultar muy molesto para el usuario que no solicitó ni autorizó dicha publicidad.

El programa denominado parasito del navegador, tiene como finalidad cambiar la página de inicio del navegador cada vez que el usuario abre el mismo. Otra acción que puede realizar es enviar información a un host determinado, sobre las páginas web que el usuario ha visitado durante el periodo que uso el navegador.

Existen también los ataques de denegación de servicio distribuido o (DDoS) que para llevarse a cabo requieren la generación de muchas conexiones simultaneas sobre el mismo servidor, desde diferentes puntos de la red.

Aparte de los troyanos, el robo de identidad y de datos se puede realizar mediante dos técnicas muy conocidas: los programas *spyware*[112] y el *phishing*.

El software spyware es un programa malicioso parasito. A diferencia de los virus no trata de replicarse en otros archivos o dispositivos, sino que su finalidad es obtener datos y transmitirlos a un host externo, sin consentimiento del usuario afectado. Se lo puede utilizar para obtener copias del correo electrónico del usuario, archivos que se abrieron en el sistema, el registro de las pulsaciones de las techas cuando se opera el teclado y de esta manera obtener contraseñas y datos confidenciales. También es posible grabar las direcciones URL de sitios Web visitados e incluso crear un video con todas las actividades realizadas en el equipo.

> Los registradores de pulsaciones de teclas pueden ser parte del software o del hardware. En el caso del software, puede tratarse de un proceso oculto (o uno con un nombre que se parezca demasiado al nombre de un proceso del sistema real), que escribe la información recolectada en un archivo oculto. Los registradores de pulsaciones de teclas también pueden ser parte del hardware, en cuyo caso es un dispositivo (cable o llave) ubicado entre el conector del teclado del equipo y el teclado (CCM, 2017).

[112] SPYWARE: Programa espía que obtiene información de un computador y transmite ésta a una entidad externa sin el consentimiento del usuario.

El *phishing* es un ciberdelito que comienza en general con el envío de un correo electrónico que conduce al usuario a sitios web falsos, construidos a imagen y semejanza de los auténticos. De este modo el usuario, que no sospecha que el sitio es falso, se conecta brindando sus datos personales. El atacante obtiene los datos confidenciales, principalmente números de tarjetas de crédito o cuentas bancarias, con el objetivo principal de robar dinero o efectuar un fraude como realizar compras a nombre del usuario legítimo.

En el informe *Phishing Activity Trends Report* del último trimestre del 2016 perteneciente al Grupo de Trabajo Anti *Phishing* (APWG)[113], se indica que el número de ataques a través de *phishing* a nivel mundial fue de 1.220.523, lo que representa un incremento del 65% respecto del año 2015. Si se compara el cuarto trimestre del 2004 -con 1.609 casos promedio por mes- con el cuarto trimestre del 2016 -92.564 casos promedio por mes-, el incremento es del 5.753%, en 12 años (APWG News, 2017).

Con respeto a los ataques de *phishing* Traver (2014) señala:

> Miles de ataques más de *phishing* utilizan otras estafas; algunos fingen ser eBay[114], PayPal o Citibank que le escriben para verificar su cuenta (ataque conocido como *spear phishing*, literalmente pesca con arpón, consiste en seleccionar a un cliente conocido de un banco especifico u otro tipo de negocio). (pág. 275)

> También con respecto al *Phishing* en el sitio CCM Comunidad Informática, se informa que la suplantación de identidad es una técnica de ingeniería social[115], lo que significa que no aprovecha una vulnerabilidad en los ordenadores sino un fallo humano al engañar a los usuarios de Internet con un correo electrónico que aparentemente proviene de una empresa fiable, comúnmente de una página Web bancaria o corporativa. Estos hackers envían un correo electrónico usurpando la identidad de una empresa (un banco, una página Web de comercio electrónico, etc.) e invitan al usuario a conectarse a través de un vínculo de hipertexto y a llenar un formulario en una página Web falsa, copia exacta de la original, con el pretexto de actualizar el servicio, una intervención de soporte técnico, etc. (…) de esta forma, los hackers obtienen con éxito los nombres de registro y las contraseñas de los usuarios o incluso información personal o sobre sus cuentas (número de cliente, número de la cuenta bancaria, etcétera). Gracias a esta información, los hackers pueden transferir directamente el dinero a otra cuenta u

[113] APWG: Anti Phishing Working Group
[114] eBay: Sitio destinado a la subasta de productos a través de Internet.
[115] INGENIERIA SOCIAL: Permite obtener información confidencial a través de la manipulación de los usuarios.

> obtener la información necesaria más tarde al usar con destreza la información personal que han recopilado. (Suplantacion de identidad Phishing, 2017)

Debido a las escuchas no autorizadas llevadas a cabo por alguno de los métodos descriptos precedentemente, se puede generar el robo de la información relativa a la transacción comercial que debería ser confidencial, y de esta forma, divulgar y/o difundir en la web la identidad del comprador.

Otro ataque frecuente es el denominado *ramsonware*, que consiste en un código malicioso que se instala en el equipo del usuario y encripta los archivos mediante un cifrado simétrico. El atacante solicita luego el pago de un rescate, para proporcionar la clave que posibilite al usuario obtener el archivo en claro.

En esta descripción de las vulnerabilidades a la seguridad de la web, no podemos dejar de mencionar la posible estafa por parte de la empresa vendedora. Ésta podría actuar fraudulentamente y nunca enviar los productos o servicios adquiridos. No obstante, por tratarse de comercio electrónico trazable donde el vendedor está identificado, el comprador puede emprender reclamos y acciones legales. Sin embargo, el costo de dichas acciones puede superar el valor del bien o servicio no brindado, provocando que generalmente, el usuario desista de este recurso.

Por otro lado, el objetivo de la seguridad informática es disminuir los riesgos, entendiendo como riesgo informático la probabilidad de que se materialice una amenaza, al respecto Nombela (1997) afirma:

> Hacer un análisis de riesgos, supone estudiar las amenazas a las que un sistema está expuesto, el grado en el que lo está, así como sus posibles consecuencias. La forma más sencilla de hacer este estudio sería anotar en una columna todas las amenazas posibles y al lado, como un valor numérico, dentro de la escala, el grado en el que se considera que el sistema estaría expuesto. (pág. 2)

Hasta aquí nos hemos referido a los riesgos más frecuentes para las compras online y fundamentalmente surgidas por efecto de las transacciones llevadas a cabo por la web. Sin embargo, los riesgos inherentes al proceso de compra son anteriores a la aparición del comercio electrónico por internet. Siempre existieron riesgos reales al efectuar una

compra; no obstante, éstos son percibidos de diferente forma e intensidad según las personas. Antes de la irrupcion del comercio electronico, Jacoby & Kaplan (1972) en la *3rd Annual Conference of the Association for Consumer Research*, evaluaron el riesgo percibido por los usuarios por la compra de productos según los siguientes cinco aspectos considerados:

Riesgo financiero: Ocasionado por la pérdida de dinero debido a la adquisición de un producto que no satisface las expectativas del comprador. Dado que el costo del producto puede ser rápidamente comparado y evaluado este es el riesgo principal según Harris, Rethie & Kuan, (2005).

- Riesgo social: Temor del comprador respecto a la evaluación negativa que personas de su entorno pudieran hacer de la compra.
- Riesgo psicológico: Pérdida de autoestima por la adquisición de un producto erróneo o de precio elevado respecto del vigente en el mercado.
- Riesgo físico: Mientras se utiliza el producto pueden surgir daños a terceros o al comprador.
- Riesgo funcional*:* Debido a que el producto no funcione según lo estimado al comprar el mismo.

Un aspecto que no debemos descuidar al analizar el tema de la seguridad en la web es el concerniente a la inversión que efectúan las empresas y organizaciones respecto a la seguridad de la información y de los datos, siendo estos últimos la materia prima que los negocios de este siglo demandan con mayor avidez. Pero en consecuencia ¿hacia dónde apunta la inversión en seguridad? Según Kuper (2005), la inversión en seguridad se concentra en la red perimetral donde se encuentran los dispositivos (hardware y software) *antispam*, *antispyware*, antivirus, etc.; luego le sigue la red interna o segura, las aplicaciones informáticas y por último los datos.

2.2.1. Fraudes con las tarjetas de crédito

Como se indicó en la introducción general, el crecimiento del uso del comercio electrónico y en especial mediante el empleo de las tarjetas de crédito, ha experimentado un crecimiento exponencial en la última década.

Asimismo, el fraude con tarjetas de crédito se ha incrementado, alcanzando en la actualidad el 0,6 % del total de transacciones realizadas, que para el área de América Latina en 2016 fue de aproximadamente de 400 millones de dólares.

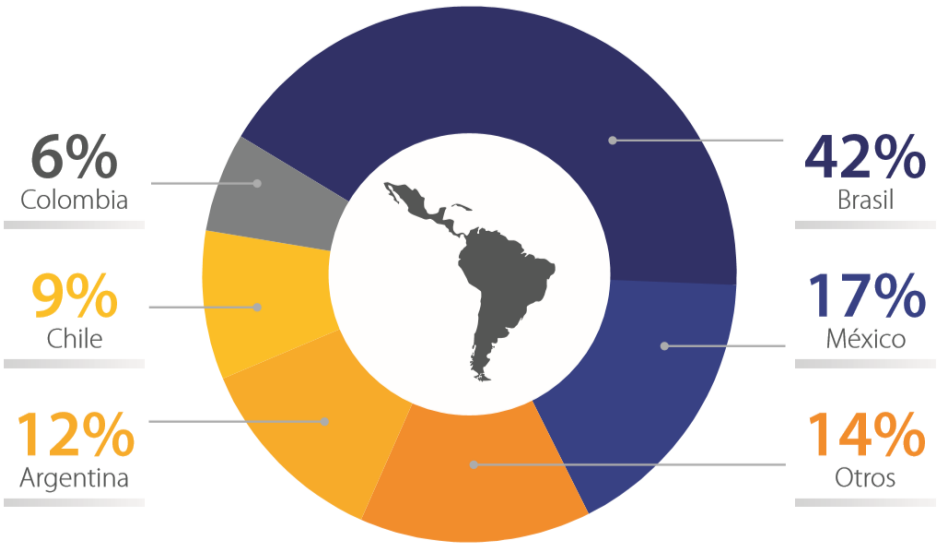


Figura 15: Crecimiento del comercio electrónico en América Latina
Fuente: Instituto Latinoamericano de Comercio Electrónico (2016)

Por otro lado, en muchos países se hace actualmente responsable a los comerciantes por las compras efectuadas con tarjetas de crédito falsas o robadas, lo que ha motivado que estos comenzaran a exigir el empleo de tarjetas con chips.

La tecnología del chip, conocida como EMV (por Europa, MasterCard y Visa), existe desde hace décadas en Europa, pero no fue hasta el 2016 que se hizo popular en EEUU. Un problema detectado en ellas es la demora de aproximadamente 8 a 10 segundos desde que se pasa la tarjeta por la ranura del terminal hasta que se recibe la respuesta desde el banco. Al insertarse la tarjeta en la ranura del terminal el chip genera un código, que se envía al banco por la red; el banco confirma el código y envía la verificación de regreso a la terminal.

Al respecto en la figura 15 se explicita el crecimiento del uso de la tarjeta de crédito por país para América Latina. Brasil ostenta el primer lugar con un 42% y le siguen México con el 17%, Argentina con el 12%, Chile 9% y Colombia 6%.

En esta carrera vertiginosa del comercio electrónico debemos analizar como enfrentan los comercios y la industria en general el ciberdelito, específicamente con respecto a las tarjetas de crédito. Se debe tener en cuenta que la prevención de fraude en *e-Commerce* tiene un costo y éste se debe balancear con el impacto total y real del fraude.

Para evaluar la administración que hacen los comercios sobre el fraude online, se deben considerar los siguientes indicadores:

- índice de revisión manual
- índice de contracargos
- índice de órdenes rechazadas
- índice de órdenes aceptadas post revisión manual

El contracargo es un procedimiento de gestión que permite solucionar cualquier disputa sobre cargos hechos a una tarjeta de crédito. Cuando un usuario de una tarjeta de crédito se comunica con el banco para notificar que no reconoce un cargo hecho a su tarjeta, en ese momento, el banco crea una solicitud de contracargo hacia el negocio que lo emitió y descuenta de su saldo dicho monto. El negocio tiene en general hasta cinco días hábiles para aportar las evidencias de que el cargo es auténtico. Si la entidad financiera acepta dichas evidencias, se restituye el monto al negocio y se carga al usuario el monto de la compra. Si por el contrario decide a favor de este último, queda firme el descuento efectuado por contracargo al negocio.

Algunas de las causas por las que una disputa puede terminar en contracargo son casos en que el cargo este duplicado, cuando el comprobante o *boucher* de compra no tiene la firma del usuario, en casos en que el vendedor no cumplió con el servicio contratado o con la calidad del producto vendido, si el usuario reclama que se usó sin autorización su tarjeta de crédito o cuando el vendedor no entrego al banco toda la documentación requerida.

Para América Latina los índices de fraudes online se indican en la figura 16. El índice de revisión manual lo realiza el 83% de los comercios, México es el país con el mayor índice registrado de revisión manual, éste es del 89%. Con respecto a las órdenes revisadas, el índice alcanza al 29% de los comercios en América Latina; Argentina presenta el mayor registro que llega al 35%. El índice de contracargos para América Latina alcanza el 1,4% de las transacciones efectuadas; Colombia y México tienen el mayor índice que es del 19%. En lo que respecta al índice de órdenes rechazadas para América Latina este es del

8%. El rechazo se produce por revisión manual o automática; México es el país con mayor índice de órdenes rechazadas con el 14,3%. Finalmente, el índice de órdenes aceptadas post revisión manual en América latina es del 63%, destacándose Argentina con el mayor índice que es del 66%.

	Índice de contracargos por ingresos	Órdenes rechazadas	Índice de revisión manual	Órdenes revisadas	Órdenes aceptadas post-revisión
	Promedios lineales				
Argentina	0.8%	8.2%	87%	35%	66%
Brasil	1.5%	4.6%	77%	22%	71%
Colombia	1.9%	10.1%	85%	26%	43%
México	1.9%	14.3%	89%	23%	56%
América Latina	1.4%	8%	83%	29%	63%
EUA y Canadá[1]	-	2.8%	83%	29%	82%
Europa[2]	0.8%	4.8%	75%	14%	62%

Figura 16: Indicadores globales de fraude online del 2016
Fuente: Instituto Latinoamericano de Comercio Electrónico (2016)

Con un índice de 8 % de órdenes rechazadas, los comercios de América Latina pueden estar desechando una cantidad importante de órdenes válidas y perdiendo oportunidades de negocio. Sin embargo, para distinguir las órdenes válidas de las fraudulentas, es necesario contar con herramientas precisas y confiables.

Para la detección de estos fraudes, existe dos métodos el manual tradicional y el de evaluación automatizado. Este último emplea tecnologías emergentes de avanzada, que permiten evaluar riesgos en tiempo real, empleando sistemas basados en reglas preestablecidas.

La empresa Visa y CyberSource ofrecen una plataforma para la detección automática de fraude (Souza, 2017)

> CyberSource ofrece una plataforma de prevención de fraude que opera en capas -desde el monitoreo de cuenta hasta la detección de fraude en transacciones, y desde la

> optimización de reglas hasta la autenticación del pagador- que ayuda a los comercios a minimizar las pérdidas por fraude, aumentar sus ingresos, y minimizar sus costos operativos. Basada en inteligencia de datos tomada de 68 mil millones de transacciones que Visa y CyberSource procesan cada año y en la fusión de algoritmos de aprendizaje automático. (pág. 14)

Según el Reporte de Fraude Online América Latina 2016 que elabora el Instituto Latinoamericano de Comercio Electrónico, las herramientas de detección de fraude más utilizadas durante el proceso de evaluación automatizada son: Número de verificación de tarjeta (CVN)[116], Servicios de validación de domicilio postal, Google® Maps™ Lookup, Verificación de número telefónico / Búsqueda inversa, Autenticación del pagador (3-D Secure®), Redes sociales, Historial crediticio.

"Los comercios de América Latina muestran un índice de contracargos de 1.4%. Al mismo tiempo, con un índice de 0.8% de rechazo de órdenes, puede que los comercios de América Latina estén sacrificando una cantidad importante de órdenes válidas, generando así un impacto negativo en sus clientes y en su balance final". (Souza, 2017, pág. 6)

2.3. El TCP y la calidad de servicio en las comunicaciones del comercio electrónico

Para materializar con éxito la transferencia de datos del comercio electrónico a través de la web, se debe garantizar que la red provea calidad de servicio (QoS)[117] en la comunicación y que además se preserve la seguridad informática durante toda la sesión correspondiente a dicha transmisión de datos.

La calidad de servicio se logra mediante los protocolos de comunicaciones como el TCP, respecto a la calidad de servicios Lechtaler & Fusario (2015) afirman:

> La calidad de servicio de un protocolo de comunicaciones está dada porque ejecuta todas o algunas de las siguientes funciones, (citaremos solo las más relevantes):
> Control de errores: se entiende por control de errores no solo la detección del error sino también la recuperación del paquete recibido con error, en general mediante la retransmisión del mismo.

[116] CVN: Número de seguridad de tres dígitos que aparece generalmente en la parte posterior de la tarjeta de crédito. También denominado código de seguridad de la tarjeta
[117] QoS: Quality of Service

> Control de flujo: capacidad de reserva de almacenamiento de los datos en el extremo receptor.
> Control de secuenciamiento: capacidad de mantener en el mismo orden la secuencia de paquetes de como salieron en el extremo transmisor.
> Control de congestionamiento: capacidad de evitar la pérdida de paquetes por falta de espacio de almacenamiento y/o procesamiento de los nodos. (pág. 804)

El protocolo TCP dispone de los mecanismos para garantizar la calidad de servicio; es un protocolo orientado a conexión[118] y además realiza controles de errores, flujo, secuenciamiento y también de congestionamiento.

Pero la calidad de servicio de una red no garantiza la seguridad en lo concerniente a la confidencialidad, integridad, disponibilidad, autenticación y no repudio. No obstante, ésta es fundamental para garantizar la confiabilidad de la comunicación, y en definitiva la disponibilidad del sistema y de los datos. Como se mencionó anteriormente, no se incluyen en este análisis los equipos terminales de los usuarios ni los sistemas de protección de datos (hardware y/o software) involucrados.

Una vez que está garantizada la confiabilidad de la red de comunicaciones, podemos centrarnos en el problema de la seguridad informática, dado que sería ineficaz un sistema de comunicaciones con alto nivel de seguridad, si sus comunicaciones no son confiables debido a demoras excesivas, perdidas de paquetes, congestión, falta de control de flujo, etc.

> En el campo de la seguridad lo que se busca es una mayor fiabilidad de los equipos, posibilidad de recuperación de datos, control de accesos mediante claves, cifrado de la información, aplicaciones de copias de seguridad, sistemas tolerantes a fallos, etc. (Nombela, 1997, pág. 18)

2.3.1. La arquitectura TCP/IP

Para desarrollar los negocios en forma globalizada, las empresas internacionales deben necesariamente innovar en forma permanente, prestando servicios digitales de última generación.

[118] PROTOCOLO ORIENTADO A CONEXIÓN: Es aquel que previo a la transmisión de los datos establece fehacientemente la conexión con el extremo receptor.

Al respecto, Rubalcaba (2010) opina que se trata de servicios altamente digitalizados, vinculados especialmente a la economía online, como el comercio por internet, los servicios informáticos, el desarrollo de aplicaciones y contenidos, etc.

El caso más notable de un negocio basado en el comercio electrónico de los últimos tiempos lo constituye el sitio Alibaba, la empresa de *e-Commerce* más grande del mundo. Según Forbes, durante el año 2016 se realizaron a través de la plataforma de la compañía transacciones por US$ 463.000 millones. Según el sitio Clarin Negocios (2 de mayo 2017), su dueño y fundador, el Sr. Jack Ma, es el segundo hombre más rico de China, quien reunió una fortuna valuada en unos 30,6 mil millones de dólares en base a su empresa. Alibaba genera el 70% de los paquetes postales que se envían en China; su negocio se basa en las tasas y comisiones por las transacciones que se efectúan en internet.

Para materializar esos servicios digitales fue imprescindible la aparición en la década de los años 80 del protocolo TCP/IP y de la red Internet. El tráfico en las redes de datos, y en especial Internet, se basa en el protocolo IP, el cual forma parte de la familia de protocolos mencionados.

Con respecto al origen de TCP/IP (Feit, 1998) agrega: "Los protocolos iniciales de ARPANET[119] eran lentos y solían sufrir frecuentes problemas. En 1974 Vinton G. Cerf y Robert E. Kahn propusieron, en un artículo, el diseño de un nuevo núcleo de protocolos. El diseño de Cerf y Kahn supuso la base para los siguientes desarrollos del Protocolo de Internet (IP) y del Protocolo de Control de Transmisión (TCP)". (pag. 2).

Como se detalla en la figura 17, la arquitectura del modelo TCP/IP está constituida por cuatro niveles: el nivel superior es la capa de aplicación, en el que se encuentran los protocolos de aplicación de acceso directo, como el Protocolo para Transferencia de Archivos (FTP)[120], el protocolo Red de Telecomunicaciones (TELNET)[121], etc.

Los protocolos de acceso indirectos, como el Protocolo Simple para Administración de Red (SNMP)[122], el Protocolo Simple para la Trasferencia de Correo (SMTP)[123], el Protocolo Sistema de Nombres de Dominio (DNS)[124], etc.

[119] ARPANET: En 1983 Arpanet conmutó oficialmente del protocolo NCP (Networ Control Program) al TCP/IP.
[120] FTP: File Transfer Protocol.
[121] TELNET: Telecommunication Network.
[122] SNMP: Simple Network Management Protocol
[123] SMTP: Simple Mail Transfer Protocol

Luego le sigue la capa de transporte, en la cual se hallan los protocolos TCP y el Protocolo de Datagrama de Usuario (UDP)[125].

La siguiente es la capa internet, conformada por los protocolos: IP (Internet Protocol), Protocolo para Resolución de Direcciones (ARP)[126], Protocolos de Enrutamiento (RP)[127] y Protocolo de Mensajes de Control de Internet (ICMP).

Por último, en el nivel inferior, está la capa denominada interfase de red donde se encuentran los protocolos que corresponden a las diferentes placas de red de los dispositivos.

Por ejemplo, podría ser una red Ethernet, en este caso el protocolo elaborado por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE)[128] para esta red se denomina IEEE 802.3[129], también podría ser una red ATM[130] (Modo de Transferencia Asíncrona) (ATM) o una red que *Frame Relay* (Retransmisión de Tramas), etc.

El modelo TCP/IP se ha impuesto, desde el comienzo de la aparición de la arquitectura de red denominada de procesamiento descentralizado, no propietaria y abierta; en contraposición al modelo vigente en las décadas de los años 60, 70 y parte de los 80, denominada de procesamiento centralizado, propietario y cerrado.

Con respecto al concepto de arquitectura de una red, Tomasi (2003) afirma que:

> El objetivo primario de la arquitectura de una red es proporcionar a sus usuarios los medios necesarios para establecer la red y efectuar el control de flujo de datos. Una arquitectura de red describe la forma en que se arregla o estructura una red de comunicaciones de datos y, en general, incluye el concepto de niveles o capas dentro de la arquitectura. (pág. 605)

[124] DNS: Domain Name System
[125] UDP:User Datagram Protocol
[126] ARP: Address Resolution Protocol
[127] RP: Routing Protocols
[128] IEEE: Institute of Electrical and Electronics Engineers
[129] IEEE 802.3: Norma correspondiente a las redes ETHERNET, elaborad por el instituto IEEE de los EEUU.
[130] ATM: Asynchronous Transfer Mode

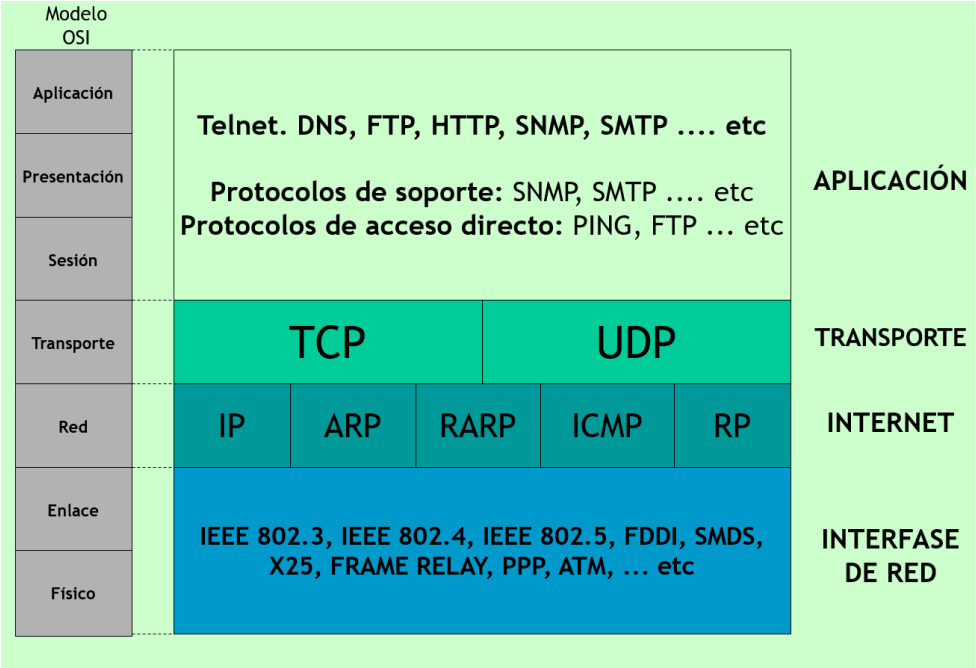


Figura 17: Arquitecturas comparadas de los modelos TCP/IP y OSI
Fuente: Elaboración propia

En la figura 17 se detalla la arquitectura TCP/IP[131] y se la compara con la estructura del modelo OSI (Interconexión de Sistemas Abiertos), de la Organización Internacional de Normas (ISO). Se puede observar que sólo coinciden dos niveles[132]: el de transporte y el de red. Este último, tiene esa denominación en el modelo OSI mientras que para el modelo TCP/IP se denomina nivel internet[133].

El modelo OSI no sólo ha sido un esquema para sistematizar las tareas de comunicación en las redes, sino que también ha facilitado las funciones y procedimientos inherentes a la seguridad. Al respecto Stallings (2004) dice:

> Para analizar de forma efectiva las necesidades de seguridad de una organización y evaluar y elegir distintos productos y políticas de seguridad, el responsable de la seguridad necesita una forma sistemática de definir los requisitos de seguridad y caracterizar los enfoques para satisfacer dichos requisitos. Esto es bastante difícil en un entorno centralizado de procesamiento de datos, y con el uso de redes de área local y de área ancha, los problemas se agravan. La recomendación X.800 de la ITU-T, Arquitectura de seguridad OSI, define este enfoque sistemático. La arquitecta de

[131] ARQUITECTURA TCP/IP: La arquitectura define los niveles que conforman el protocolo TCP/IP, en este caso son cuatro niveles.
[132] El modelo TCP/IP se desarrolló diez años antes que el modelo OSI, y en consecuencia no se adapta totalmente a este último.
[133] NIVEL INTERNET: En este caso no se refiere a la red Internet sino a la conectividad entre redes.

> seguridad OSI es útil a los administradores de red para organizar la tarea de proporcionar seguridad. (pág. 5)

En la capa de transporte del TCP/IP están presentes los protocolos UDP y TCP. El primero opera en el modo datagrama[134], no es orientado a conexión y no tiene calidad de servicio, por lo tanto no se utiliza en comercio electrónico.

Recordemos que un protocolo es orientado a conexión cuando antes de enviar los datos, establece la conexión con el protocolo homónimo ubicado en el otro host; luego envía los datos y cuando éstos se terminan, cierra la comunicación con la correspondiente desconexión. Como decíamos, el protocolo UDP no lo es por lo cual, envía los datos sin establecer previamente la conexión. Al respecto, Forouzan (2006) agrega:

> En un servicio sin conexión, los paquetes son enviados de una parte a la otra sin necesidad de establecer o liberar una conexión. Los paquetes no están numerados; pueden retrasar, perderse o llegar fuera de orden. No hay ningún tipo de confirmación. Vemos pronto que uno de los protocolos de nivel de transporte en el modelo de Internet, UDP, no es orientado a conexión. (pág. 657)

A diferencia del descripto, el protocolo TCP es orientado a la conexión y dispone de calidad de servicio brindando control de errores, control de flujo, control de congestión, administración de temporizadores que permiten controlar activamente las retrasmisiones, evita la fragmentación a nivel IP y establece conexiones, en base al número de puerto y dirección IP en cada extremo de la comunicación - a esta combinación se la denomina Socket-.

En consecuencia, el producto generado en la capa de transporte puede ser un datagrama UDP o un segmento TCP, dependiendo de si la aplicación está programada para operar con uno u otro. Si se debe brindar un servicio rápido, interactivo, de bajo volumen de datos y no interesa la calidad, se utiliza UDP. Si, por el contrario, se requiere un servicio confiable se debe emplear TCP. Independientemente si se trata de un datagrama UDP o un segmento TCP, deben ser transportados en el campo de datos del datagrama IP de la capa inferior, denominada internet.

[134] MODO DATAGRAMA: Modo de funcionamiento de una red que no se basa en circuitos físicos ni virtuales, se decide en cada nodo (router) el encaminamiento a seguir para cada datagrama.

Con respecto al servicio que brinda el protocolo IP este no es orientado a conexión y no tiene calidad de servicio; por esta razón para el caso del comercio electrónico la tarea de brindar confiabilidad a la comunicación recae exclusivamente en el protocolo TCP.

Al respecto, Black (1997) dice:

> IP es un ejemplo de servicio no orientado a conexión. Permite, sin establecimiento de llamada previo, el intercambio de datos entre dos computadores (sin embargo, los dos computadores generalmente comparten un protocolo común de transporte orientado a conexión). Como IP no es orientado a conexión, se pueden perder datagramas entre las dos estaciones de usuario. Por ejemplo, las pasarelas IP utilizan un tamaño máximo de cola, y si se sobrepasa, los buffers se desbordarán. En esta situación se descartarán datagramas en la red. Por esta razón es fundamental un protocolo de transporte de nivel superior (como TCP) que solucione esos problemas. (pág. 356)

2.3.2. El protocolo TCP en el comercio electrónico

En el comercio electrónico, se emplea el Protocolo Seguro para la Transferencia de Hipertexto (HTTPs)[135], ubicado en el nivel de aplicación del modelo TCP/IP de la figura 17, y destinado a la transferencia segura de datos de hipertexto.

Cuando se inicia una comunicación de comercio electrónico y un usuario requiere comunicarse con un sitio para realizar una compra, la aplicación HTTPs del primero genera un paquete de datos denominado Unidad de Datos de Protocolo (PDU)[136]. Se trata de una solicitud de servicio que se envía al nivel inmediato inferior (el de transporte); específicamente al protocolo TCP instalado en la computadora del usuario. Este protocolo por ser orientado a conexión, antes de transmitir directamente el requerimiento del HTTPs, tiene que establecer la comunicación con el otro TCP, que está instalado en el servidor del sitio del vendedor.

Para realizar esta última operación, TCP inicia un proceso que se denomina intercambio inicial de los tres segmentos.

Con respecto al paquete que genera el TCP, Halsall (1998) observa que:

[135] HTTPS: Hipertext Transfer Protocol Secure
[136] PDU: Unit Data Protocol

> Para obtener un servicio confiable, el TCP transmite todos los datos en unidades llamadas segmentos. Lo normal es que el TCP decida cuándo se ha de transmitir un segmento nuevo. En el lado del destino, el TCP receptor almacena temporalmente los datos recibidos en un segmento en un buffer de memoria asociado a la aplicación y los entrega cuando el buffer se llena. Así, un segmento puede consistir en varios mensajes de usuario si se están intercambiando unidades de mensajes cortas, o en una parte de un solo mensaje grande si se está transfiriendo, digamos, el contenido de un archivo grande. (pág. 678)

El proceso de intercambio inicial de los tres segmentos, o también llamado saludo de tres etapas, se detalla en la figura 18. Este intercambio previo de información para la configuración es imprescindible para implementar la sesión entre los dos TCP: el ubicado en el host del cliente y el instalado en el servidor del sitio web del vendedor.

En el primer segmento el TCP A le informa la TCP B los siguientes parámetros:

Numero de secuencia (SEC) que es un numero de 32 bits elegido al azar a partir del cual contará los bytes que envíe A hacia el lado B. La ventana (W) que es la capacidad de almacenamiento de A (en bytes) en ese instante. El bit o bandera de reconocimiento (ACK) activado. El tamaño máximo que puede tener el segmento que envíe B hacia A o MSS[137]. Luego de enviado este primer segmento desde A hacia B, en el segundo segmento, el TCP B es el que informa sus parámetros al TCP A. El tercer segmento cierra este intercambio de datos de configuración inicial, luego comienza el intercambio de datos de la aplicación entre el lado A y el lado B.

Recordemos que se denominan segmentos o unidad de transferencia, a los paquetes que genera el protocolo TCP en una conexión. Como se detalló previamente, estos segmentos se trasmiten en la red Internet encapsulados en el campo de datos de los datagramas IP.

Como el protocolo TCP es orientado a conexión, previo a la transmisión de los datos entre ambos TCP deben conectarse e intercambiar los parámetros necesarios para configurar la conexión. Al proceso inicial de intercambio de tres segmentos, le sigue la transferencia de datos entre ambos TCP (de acuerdo a los requerimientos de cada aplicación), y por último

[137] MSS: Maximum Segment Size

la conexión concluye, mediante el intercambio de los dos segmentos finales con el *flag*[138] de FIN activado, cuando ambos TCP no tienen más datos que transmitir. El intercambio de tres segmentos es imprescindible para parametrizar el protocolo y posibilitar que brinde servicios como los que indica Moya (2006):

> El protocolo TCP posee funciones tales como: fragmentación de mensajes, transmisión de segmentos, reordenamiento, establecimiento de prioridades; también define formatos de datos, asentimientos, procedimientos de establecimiento y finalización de conexiones. Todo ello con la finalidad de lograr un servicio orientado a la conexión y extremadamente fiable para la transmisión de datos. (pág. 265)

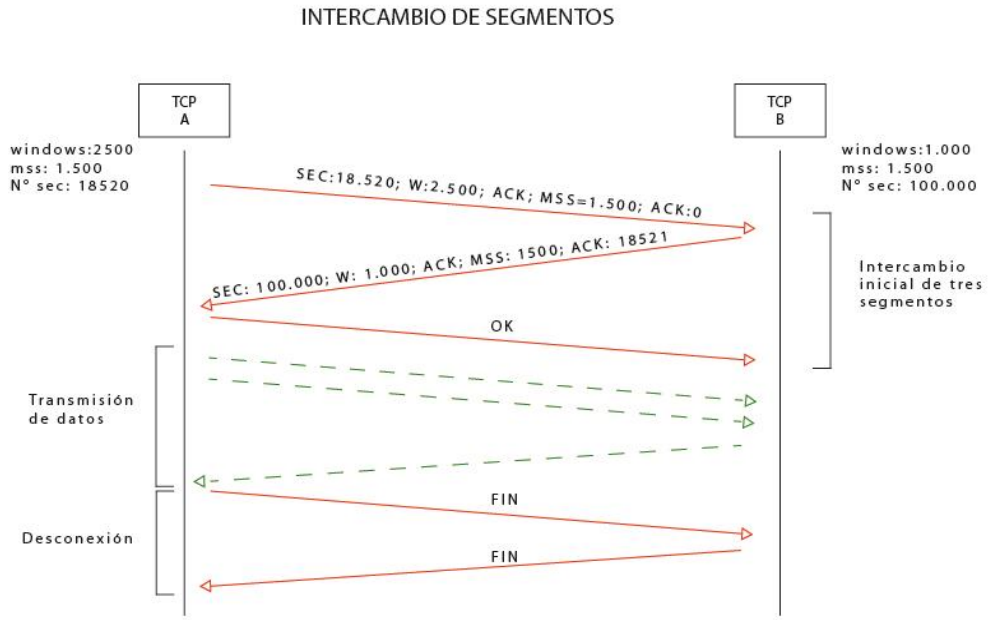


Figura 18: Intercambio de los tres segmentos, ejemplo de una conexión TCP entre el host A y el B
Fuente: Elaboración propia.

Durante el intercambio de los tres segmentos iniciales, los dos TCP actualizan el valor de los parámetros que son importantes para que la conexión sea confiable, y en consecuencia, tenga calidad de servicio. Entre los parámetros que intercambian los más relevantes son la ventana, que indica la capacidad de almacenamiento de datos que cada TCP posee y es imprescindible para el control de flujo; el número de secuencia, necesario para llevar el control de los bytes trasmitidos; y el tamaño máximo que puede tener el segmento en

[138] FLAG: Bandera, se trata de un bit que activado es "uno" desactivado "cero".

función de la red en la cual se encuentra el host, dato que evita la fragmentación a nivel datagrama IP.

Con respecto al proceso de intercambio de información entre los dos TCP, Comer (1996) agrega:

> El saludo de tres etapas es necesario y suficiente para la sincronización correcta entre los dos extremos de la conexión. Para entender porque, recuerde que el TCP se construye sobre un servicio de entrega no confiable de paquetes (el protocolo IP), así que los mensajes pueden perderse, retrasarse, duplicarse o entregarse en desorden. Por lo tanto, el protocolo debe utilizar un mecanismo de terminación de tiempo y retransmitir las solicitudes perdidas. (pág. 218)

Como se indicó en el párrafo anterior el protocolo IP no tiene calidad de servicio (servicio de entrega no confiable), por lo cual, la tarea de realizar una comunicación confiable recae exclusivamente en el TCP. Para esta tarea, el TCP debe llevar el control exacto de los bytes transmitidos y recibidos, de forma tal que cuando se produzca la pérdida o la recepción con errores solicite la retransmisión inmediata de dichos bytes.

> TCP es un protocolo dúplex, lo cual significa que el procedimiento de intercambio de datos bidireccional es regulado dentro del marco de una conexión simple. Cada parte actúa de manera simultánea como emisor y como receptor y cada una tiene un par de búferes: uno es para almacenar los segmentos recibidos, mientras que el otro se destina a los segmentos que esperan a ser enviados. Aparte de esto, existe un búfer para almacenar copia de los segmentos enviados, cuyos reconocimientos o acuses de recibo todavía no han llegado. (Olifer & Olifer, 2009, pág. 627)

El TCP utiliza un mecanismo de ventana deslizable para el control de errores y el control de flujo. Al respecto, Comer (1996) afirma:

> El mecanismo TCP de ventana deslizable opera a nivel de octeto, no a nivel de segmento ni de paquete. Los octetos del flujo de datos se numeran de manera secuencial, y el transmisor guarda tres apuntadores asociados con cada conexión. Los apuntadores definen una ventana deslizable. (pág. 203)

La ventana no solo es deslizable, sino que su tamaño varía según la capacidad de memoria intermedia del receptor; Comer (1996) afirma:

> La ventaja de utilizar una ventana de tamaño variable es que esta proporciona control de flujo, así como transferencia confiable. Si la memoria intermedia del receptor se llena, no puede aceptar más paquetes, así que envía un anuncio de ventana más pequeño. En caso extremo, el receptor anuncia un tamaño de ventana igual a cero para detener toda la transmisión. Después, cuando hay memoria intermedia disponible, el receptor anuncia un tamaño de ventana distinto de cero para activar de nuevo el flujo de datos. (pág.204)

Del análisis de la estructura del segmento TCP, indicada en la figura 19, surge que los principales campos componentes son:

- Puerto fuente: es el número que identifica al programa de aplicación en el extremo fuente de la conexión.
- Puerto destino: es el número que identifica al programa de aplicación en el extremo destino de la conexión.
- Número de secuencia: indica la posición de los datos del segmento en el flujo de datos del transmisor.
- Número de acuse de recibo: indica el número de octeto a partir del cual espera recibir datos.
- Longitud cabecera: Cantidad de bloques de 32 bits que contiene la cabecera del segmento TCP.
- Reservado: son seis bits no utilizados.
- Banderas: las banderas o *flags* son las siguientes:
  URG: (urgente), el campo de puntero urgente es válido.
  ACK: (*Acknowledgement)*, el campo de acuse de recibo es válido.
  PSH: (*Push*), la activación de este *flag* indica que se deben entregar los datos inmediatamente al nivel aplicación.
  RST: (*restart*), se reinicia la conexión.
  SYN: (*Sincrhonous*), sincronizar números de secuencia entre los dos TCP de la conexión.
  FIN: El TCP que activa este *flag* ha llegado al final de su flujo de octetos a transmitir.

- Ventana[139]: tamaño de la memoria intermedia del TCP que envía el segmento.
- Suma de verificación: este campo se emplea para la verificación de errores, y está basado en el mecanismo denominado suma de verificación, que consiste en la suma de todos los bits del segmento en grupos de 16 bits y con aplicación del complemento a_1 .
- Puntero de urgencia: cuando se activa la bandera o *flag* URG, éste indica la posición dentro del segmento en el que terminan los datos urgentes que deben transmitirse inmediatamente.
- Opciones: la opción frecuentemente empleada es Tamaño Máximo del Segmento (MSS) que indica, durante el intercambio de los tres segmentos iniciales, cuál debería ser el tamaño máximo del segmento para no generar fragmentación en el nivel IP.
- Datos: son los que envía la aplicación, en el caso del comercio electrónico serían los datos enviados por la aplicación HTTPs.

Aunque no está reflejado en ningún campo del segmento detallado en la figura 19, el TCP también emplea un medidor de tiempo de retransmisión para detectar segmentos perdidos.

Al respecto Tanenbaum (2003) dice:

> El TCP usa varios temporizadores (al menos virtualmente) para hacer su trabajo. El más importante de estos es el temporizador de retransmisión. Al enviarse un segmento, se inicia un temporizador de retransmisiones. Si la confirmación de recepción del segmento llega antes de expirar el temporizador, éste se detiene. Si, por otra parte, el temporizador termina antes de llegar la confirmación de recepción, se retransmite el segmento (y se inicia nuevamente el temporizador). (pág. 550)

En resumen, cuando el TCP envía un segmento arranca un temporizador y espera un ACK, enviado por parte del TCP instalado en el extremo receptor. Si el ACK no llega en un plazo establecido, retransmite el segmento. Si el plazo de retransmisión es demasiado corto, la red se verá invadida por numerosos segmentos innecesarios y cargará al receptor con segmentos duplicados. Por otro lado, si los plazos son demasiados largos se pierde la oportunidad de recuperar rápidamente el segmento perdido o eliminado en el receptor por la detección de errores.

[139] VENTANA: Ambos TCP envían sus respectivos valores del tamaño de memoria intermedia asignada para la aplicación en curso.

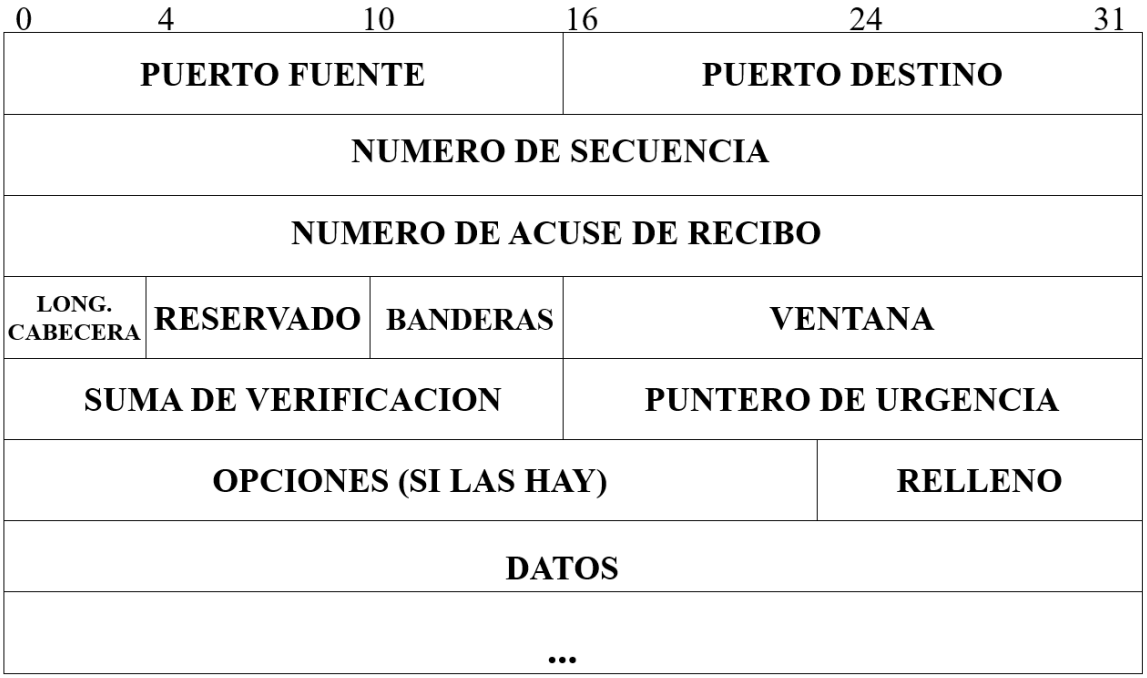


Figura 19: Campos que conforman el segmento TCP
Fuente: Elaboración propia

En resumen, podemos afirmar que la base para sustentar la confiabilidad de la comunicación entre el host del usuario y el sitio web del vendedor esta sostenida por el protocolo TCP, sin embargo, éste no brinda seguridad a dicha comunicación.

2.4. El protocolo SSL/TLS y su aporte a la seguridad de la comunicación entre el host del usuario y el sitio web del proveedor

El protocolo criptográfico SSL es el protocolo de seguridad más extendido en la Red (Chou, 2002); (Rescorla, 2000); (Viega, Messier, & Chandra, 2002). Fue desarrollado en la década de los 90 por la Empresa NETSCAPE para ser incluido en su navegador web. Proporciona autenticación, integridad y confidencialidad en las comunicaciones, a través de la red Internet, entre el navegador de los clientes y el servidor del sitio web del proveedor.

Las versiones 1 y 2 de este protocolo proporcionaban autenticación del servidor y usaban claves simétricas de 40 bits como máximo. Esta limitación en la longitud tuvo validez sólo en EEUU por intereses gubernamentales que imponían restricciones sobre la exportación de tecnología criptográfica. En realidad, el protocolo soportaba claves de longitudes

mayores (128 bits). Estas versiones presentaban algunas debilidades por lo que Netscape continuó trabajando y desarrolló la versión 3 que solucionaba los problemas de las anteriores versiones y agregaba la autenticación del cliente, utilizando los certificados digitales de cliente y del servidor. (Martínez López, Mata Mata , & Rodríguez Domínguez, 2009)

SSL se ejecuta en un nivel ubicado entre el de aplicación, donde se encuentran los protocolos HTTP, SMTP, etc. y el nivel de transporte, donde están los protocolos TCP y UDP. En el caso de utilizar HTTP con SSL, el protocolo se denomina HTTPs, donde la "s" al final significa que es seguro debido al empleo del SSL.

Al respecto Scolnik, H. (2014) dice:

> Normalmente enviamos los datos por la Web mediante un protocolo llamado HTTP (*Hypertext Transfer Protocol*; protocolo de transferencia de hipertexto), que no maneja encriptación y, por lo tanto, es vulnerable. En cambio, el SSL conduce al HTTPS (*Hypertext Transfer Protocol Secure*) que si encripta los datos y es la base del comercio electrónico. (pág. 135)

El protocolo SSL ha servido de base para el desarrollo del TLS. Se diferencian en muy pocos aspectos; el último presenta mejoras en la protección frente a ataques, la incorporación de nuevos algoritmos criptográficos y que es menos vulnerable por forzar el uso de versiones actualizadas del protocolo.

Al respecto Stallings (2004) afirma:

> Uno de los servicios de seguridad más ampliamente utilizados es el de capa de sockets[140] segura (SSL) y el posterior estándar de Internet conocido como capa de transporte segura (TLS), definido este último en el RFC 2246. SSL es un servicio de propósito general implementado como un conjunto de protocolos que hacen uso de TCP. (pág. 749)

[140] SOCKETS: En TCP/IP son pares de valores constituidos por la dirección IP de la computadora o host y el número de puerto que identifica al programa dentro de la computadora o host. (dirección

Podemos decir que el TLS es el sucesor del SSL y su última actualización se encuentra incorporada en el RFC 5246 correspondiente a la versión 1.2 del TLS. Se identifica a la última versión del protocolo como SSL/TLS.

El SSL/TLS es un protocolo de gran importancia para la seguridad en las comunicaciones a través de Internet, dado que cuando se navega en dicha red se pueden producir múltiples ataques a la información en lo concerniente a la confidencialidad e integridad de los datos.

Para poder detectar y prevenir los ataques conocidos como fabricación, los cuales, son producidos cuando alguien no autorizado, falsificando su identidad, inserta información en el sistema; se implementa el mecanismo de autenticación que tiene como objetivo identificar perfectamente el origen del mensaje.

Cuando no se implementa en la comunicación el protocolo el SSL/TLS puede presentarse un tipo de ataque denominado hombre en el medio (*man in the middle*) que consiste en alterar la información en tránsito, como así también, suplantar la identidad de los extremos de la comunicación.

En el caso del comercio electrónico, por ejemplo, se podría suplantar la identidad del banco con el cual nos comunicamos a través del *home banking* y terceros no autorizados tendrían acceso a nuestras *passwords* de operación con dicha entidad.

Estos ataques en su gran mayoría se basan en robar las cookies[141]de sesión del usuario que se generan cuando éste se autentica al acceder a las páginas Web de los vendedores.

Las cookies son archivos de texto pequeños que se guardan en el directorio del navegador o en carpetas de datos del mismo. Son indispensables en las webs que tienen bases de datos muy grandes, requieren inicio de sesión y tienen temas personalizables.

Existen dos tipos de cookies, las de sesión y las permanentes. Al visitar una página web se crea una cookie de sesión que, como su nombre lo indica, tiene una duración asociada a la vigencia de la sesión; abandonado el sitio ésta se elimina.

[141] COOKIES: Archivos de texto pequeños que facilitan el proceso de navegación en las páginas webs.

Por el contrario, las cookies permanentes continúan en las carpetas del navegador, aunque se abandone la página web, y se activarán cuando se acceda nuevamente a dicha página. En este último caso, la duración de la cookie en la carpeta dependerá del tiempo que se haya establecido para la misma o si se la elimina manualmente.

Las cookies se crean cuando a través del navegador se visita un sitio web que las utiliza, y su objetivo es realizar un seguimiento de los movimientos que los usuarios efectúan en él. También permiten a los usuarios conocer en qué punto o página dejaron la navegación, recordar el inició de sesión y tema seleccionado, conocer las preferencias y otras funciones personalizadas.

El archivo cookie es generado por el sitio web seleccionado en el navegador, no contiene ningún código ejecutable y es el propio navegador el que utiliza la información contenida en la cookie para realizar una navegación más rápida y sencilla, realizar el inicio de sesión en forma automática, recordar las preferencias seleccionadas en vistas anteriores al sitio, etc. Las cookies también se pueden utilizar para registrar el historial de navegación del usuario.

Los contenidos de las cookies varían de un sitio a otro, y como se dijo, son creadas por el servidor web. Una vez creadas no contienen información personal, ni escanean la computadora en busca de información adicional. En la mayoría de los casos la información personal está encriptada y solo la puede desencriptar el servidor que creo la cookie.

Las cookies hacen posible las compras online en comercio electrónico facilitando al usuario no tener que volver a llenar su carrito de compras cuando, dentro de un mismo sitio, tiene que pasar de una página a otra. Mediante la cookie se determina rápidamente su identidad posibilitando recordar los artículos que va incorporando a su carro de compras.

También posibilitan mantener ciertas configuraciones o ajustes realizados en visitas previas, como la selección del idioma, recordar contraseñas de inicio de sesión, evitar la repetición de anuncios en ventanas emergentes, etc. Las cookies limitan el número de veces en que se muestra un anuncio, como es el caso de las ventanas emergentes[142], garantizando que ésta se muestre una vez por visita.

[142] VENTANAS EMERGENTES: También conocidas en inglés como POP-UP

Otra aplicación muy común de las cookies es posibilitar a los anunciantes conocer la cantidad de usuarios que han accedido a una página web. De esta forma pueden determinar la efectividad de una campaña publicitaria.

Para conocer y comprender cómo los usuarios navegan y procesan el contenido almacenado en una página, se emplean las cookies en combinación con otra herramienta denominada baliza o faro web[143] . Se trata de un archivo con una imagen en Formato de Intercambio Grafico (GIF) que les permite a las empresas monitorear el tráfico, hacer el seguimiento de los servicios y la navegación. Un ejemplo típico se presenta en empresas que poseen varias páginas web y quieren conocer como los usuarios viajan de una a otra.

Otra función importante de las cookies se pone de manifiesto en las páginas web que ofrecen contenidos gratuitos y en consecuencia dependen de la publicidad para seguir operando. En estos casos, en general se recurre a terceras empresas que realizan la publicidad y el marketing, para obtener y administrar los anuncios publicitarios. En ese contexto, la web de estas empresas crea una cookie en la carpeta del navegador de los usuarios, para unir y configurar las distintas fuentes de información de forma tal que todos los elementos se presenten coordinados en la misma página web.

Las cookies se pueden eliminar fácilmente de la carpeta de cookies[144] del navegador. Muchos de ellos aceptan de forma universal ciertos perfiles de privacidad entre los cuales el usuario puede elegir; otros soportan un protocolo denominado Plataforma de Preferencias de Privacidad (P3P) que tiene como función principal analizar la política de privacidad de los sitios webs -que obviamente también deben soportar P3P- y que permite al usuario que accede al sitio, controlar el manejo de los datos privados a través del navegador, atendiendo a la política de manejo de los datos que efectúa el servidor del sitio web.

De esta forma, una vez completada la configuración del servidor web, el sitio informa automáticamente a los visitantes de la página que es compatible con el protocolo P3P. El navegador del usuario comprueba la política de seguridad del sitio web e informa al usuario acerca de las prácticas de manejo de la información del mismo. Si alguna práctica no concuerda con las preferencias establecidas previamente por el usuario durante la

[143] FARO WEB: también conocido como web bug.
[144] CARPETA DE COKIES: Generalmente son archivos ocultos.

configuración de su navegador, el protocolo P3P le preguntará si desea continuar o no; en caso de no estar de acuerdo, aborta la operación de conexión con el servidor del sitio web.

Retornando a la descripción del ataque hombre en el medio, podemos concluir que el atacante debe tener acceso al tráfico intercambiado en la red entre el usuario y el sitio web, como podría ser el caso de estar en la misma red WiFi[145]. De esta forma, dispondría de la cookie de sesión que autentica al usuario. Una vez en posesión de ella, el atacante podrá tener acceso a las páginas para las cuales el usuario legítimo estaba habilitado.

Para contrarrestar este tipo de ataque, conocido como ataque mediante el secuestro de la sesión HTTP (HTTP sesión *hijacking attacks*), muchas empresas comerciales habilitaron el empleo del protocolo SSL/TLS para acceder a sus servicios de forma más segura.

2.4.1. Funcionamiento del protocolo SSL/TLS

Actualmente para implementar una comunicación con SSL/TLS se deben efectuar dos fases previas a la transferencia de datos cifrados, que son ejecutadas por los siguientes protocolos: protocolo de negociación bilateral de SSL/TLS (SSL/TLS *Handshake Protocol*) y protocolo de registro de SSL/TLS (SSL/TLS *Record Protocol*). El primero posibilita intercambiar los parámetros de seguridad que se van a utilizar en la comunicación segura, y el segundo especifica la forma de encapsular los datos trasmitidos y recibidos, incluso los de los parámetros indicados.

El intercambio de parámetros realizado por el *Handshake Protocol* involucra tres actividades que son el establecimiento de los algoritmos criptográficos a utilizar; la realización del intercambio de claves y la autenticación y el encriptado de los datos intercambiados entre el cliente y el proveedor.

El establecimiento de los algoritmos criptográficos a utilizar consiste en la negociación entre cliente y servidor para determinar los algoritmos criptográficos que se emplearán para cifrar la información, y para intercambiar las claves y firmas. Estos algoritmos pueden ser: 3DES, IDEA, AES, RSA, Diffie Hellmann, DSA, SHA2, etc.

[145] WIFI: Proviene de la marca comercial Wi-Fi (Wireless Fidelity)

En la realización del intercambio de claves y la autenticación, ésta se efectúa en base a certificados digitales, utilizando una validación mediante Infraestructura de Clave Pública (PKI)[146]. El certificado de clave pública es, en consecuencia, el mecanismo por el cual se garantiza la autenticidad de la clave pública de un determinado usuario.

Con referencia a los certificados digitales, los mismos están definidos por el estándar internacional ITU-T X.509[147] y no solo permiten garantizar legalmente la identidad de las personas, sino que también posibilitan la firma electrónica de documentos y el cifrado de las comunicaciones.

Como indica en su página web la Universidad Politécnica de Valencia:

> Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja. El titular del certificado debe mantener bajo su poder la clave privada, ya que, si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída. La clave pública forma parte de lo que se denomina Certificado Digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular. La Autoridad de Certificación se encarga de emitir los certificados para los titulares tras comprobar su identidad. (Universidad Politecnica de Valencia, 2017)

Al respecto, Stallings (2004) afirma:

> En esencia, un certificado consta de una clave pública más un identificador de usuario del propietario de la clave, todo ello firmado por una tercera parte de confianza. Normalmente la tercera parte es una autoridad de certificación (CA, *Certificate Authority)* en la que confía la comunidad de usuarios, como una agencia del gobierno o una institución financiera. Un usuario puede presentar su clave pública a la autoridad de un modo seguro y obtener un certificado. El usuario puede entonces publicar el

[146] PKI: Public Key Infraestructure.
[147] ITU-T X.509: Es un estándar de la Unión Internacional de Telecomunicaciones UIT-T para infraestructuras de claves públicas (cifrado asimétrico).

> certificado. Cualquiera que necesite la clave pública de ese usuario puede obtener el certificado y verificar que es válido mediante la firma adjunta en que se confía. (pag.748)

Finalmente, en lo que se refiere al encriptado de los datos intercambiados entre el cliente y el proveedor se emplea un método de cifrado simétrico. Al efecto, se genera una clave de sesión para la comunicación en función de los parámetros previamente negociados.

La elección del cifrado simétrico, según se detalló en el capítulo 1, responde a que éste es mucho más rápido que el asimétrico y requiere menos recursos de hardware lo cual es muy apropiado para el host del cliente, que dispone en general de menos recursos que el servidor.

La criptografía asimétrica solo se emplea para el intercambio de claves y para la firma de los mensajes. Cabe aclarar que, si alguna fase de la negociación falla, la conexión no se establece.

Con respecto al empleo de los métodos de cifrado simétrico y asimétrico Gómez (2011) dice:

> El protocolo TLS combina clave pública y simétrica en un proceso bastante complejo que se ofrece aquí de forma resumida. En primer lugar, el navegador de Internet del comprador comprueba que el vendedor online dispone de un certificado de clave pública válido. Si es el caso, emplea esta clave pública para encriptar una segunda clave, esta vez simétrica, que remite al vendedor. Éste emplea su clave privada para desencriptar el mensaje y hacerse con la clave simétrica, que será la empleada para cifrar todo el proceso de intercambio de información. En consecuencia, para hacerse con el número de tarjeta de crédito en una transacción online cualquiera, un espía deberá penetrar no uno, sino dos criptosistemas. (pág.112)

En la implementación de una conexión SSL/TLS con autenticación del servidor, se ejecutan los siguientes pasos:

1. El cliente envía una petición al servidor para realizar una sesión segura.

2. El servidor responde enviando un certificado X.509[148] que contiene la clave pública del servidor[149].
3. El cliente autentica el certificado con la lista de autoridades certificantes (CA) conocidas, si la CA es desconocida, el navegador del cliente puede ofrecer al usuario la posibilidad de aceptar el certificado bajo su propia responsabilidad.
4. El cliente genera una clave simétrica aleatoria de sesión y la cifra con la clave pública del servidor.
5. El servidor recibe la clave de sesión y la descifra con su clave privada. Ahora, tanto el cliente como el servidor emplearán la clave simétrica para cifrar la comunicación en ambos sentidos.
6. Una vez finalizada la sesión, si posteriormente se establece una nueva sesión entre el cliente y el mismo servidor, se generará una nueva clave.

El proceso empleado por el protocolo SSL para transmitir los datos encriptados a partir de los datos de la aplicación HTTPs consiste primero, en fragmentar los datos provenientes de HTTPs y luego, de acuerdo al protocolo de compresión consensuado, se comprime cada fragmento para posteriormente añadir la cabecera MAC (Código para la Autenticación del Mensajes) que posibilita la autenticación de cada fragmento.

Con referencia al método MAC para autenticar, Sabater, Martinez, Hernandez, Montoya, & Muñoz (2001) agregan:

> La autenticación o autentificación de mensajes se realiza mediante una sencilla manipulación criptográfica: Se envía un mensaje en claro y se le acompaña con su versión cifrada condensada, denominada MAC (*Message Authentification Code*). En recepción se vuelve a cifrar el mensaje con la misma clave, y se calcula de nuevo el MAC comprobando que coincide con el recibido junto con el mensaje. (pág.116)

El fragmento con su cabecera MAC se cifra mediante un protocolo de encriptado simétrico acordado previamente y con la clave de sesión también consensuada. Al bloque cifrado se le agrega la cabecera del protocolo de registro SSL (SSL/TLS *Register Protocol*).

[148] CERTIFICADO X.509: Especifica los formatos estándar para un certificados de claves públicas y un algoritmo de validación.
[149] El intercambio de clave de sesion se realiza mediante el cifrado asimétrico y el encriptado del mensaje o datos mediante el cifrado simétrico.

Por último, cada fragmento así procesado se transmite mediante un segmento TCP y éste a su vez se encapsula en un datagrama IP.

El éxito de este protocolo se debe principalmente al respaldo brindado por empresas como VISA, MASTERCARD, AMERICAN EXPRESS, etc. Estas empresas han priorizado la securización del tráfico web inherente al comercio electrónico mediante el protocolo SSL, los certificados digitales y la infraestructura de clave pública.

No obstante, el SSL también se puede emplear mediante el software libre Open VPN para la generación de redes virtuales privadas (VPN)[150] dado que además de cifrar la comunicación, posibilita la autenticación de los usuarios conectados.

2.4.2. Falencias en la seguridad del protocolo SSL/TLS

Si bien el protocolo SSL/TLS tiene un nivel de seguridad aceptable, dicho nivel depende de dos factores importantes: el primero es la versión del protocolo que se encuentra en servicio y el segundo factor es la forma en la cual éste se ha implementado.

En el caso de tener en servicio una versión antigua no actualizada del protocolo, y si el atacante tomara conocimiento de ello, podría utilizar las deficiencias en la seguridad de la versión vieja que siguen vigentes en la instalación, dado que no se actualizó el protocolo.

> Para poder implementar Webs con un buen nivel de seguridad hay que saber cómo pueden atacarlas. También hay que tener en cuenta que, aunque la Web sea totalmente segura, con el tiempo, pueden surgir ataques nuevos que puedan penetrar las defensas creadas. Lo mejor que podemos hacer para evitar estos ataques es tener siempre el código actualizado y disponer de medidas que permitan recuperarnos del ataque lo más rápido posible. (Saquete, 2013)

Por el contrario, el ataque basado en la inyección de código, que fuerza al protocolo a realizar renegociaciones de los parámetros de configuración u otras acciones que puedan vulnerar la seguridad del canal a establecer, son sencillamente neutralizadas si se dispone de la última versión del protocolo y de las extensiones recomendadas del mismo.

[150] VPN: Virtual Private Network.

La inyección de código se basa en tratar de insertar código malicioso HTML, Javascript, Lenguaje de Consulta Estructurada (SQL)[151], (PHP)[152], (CSS)[153], etc.

Si el computador del usuario está controlado por un troyano o posee una deficiente configuración del SSL, es muy probable que se reciban ataques tendientes a engañarlo. Lo más probable es hacerle creer que se encuentra en una comunicación cifrada segura, cuando en realidad no lo está, simulando el candado que se observa en una página web segura. Otras alternativas también empleadas son: forzar el uso de protocolos o algoritmos criptográficos con debilidades comprobadas, inducir a la aceptación de certificados digitales que no son válidos para el servidor al cual se desea conectar, etc.

Si bien estos ataques pueden presentarse, es posible implementar ciertos procedimientos para neutralizarlos, entre los que podemos citar los siguientes:

1. Escribir directamente la URL[154] con el prefijo HTTPs en la barra de direcciones del navegador
2. Si el navegador web indica que el certificado digital de la entidad a la que se desea acceder no es válido, no aceptarlo y no efectuar la conexión
3. Verificar la firma del certificado digital del servidor web. Se debe tener registrada previamente dicha firma
4. Instalar herramientas que fuercen naturalmente a la conexión HTTPS, por ejemplo, la extensión del navegador FIREFOX HTTPS Every Where
5. Consultar en forma frecuente la documentación de la organización OWASP[155] dedicada a determinar y combatir las causas que hacen que las aplicaciones web sean inseguras
6. Activar en el navegador el protocolo de Comprobación del Estado de un Certificado en Línea (OCSP)[156] que posibilita determinar el estado de vigencia de un certificado digital X.509 mediante procedimientos que no se basan solo en el empleo de las listas de revocación de certificados

[151] SQL: Structured Query Language. Lenguaje estructurado para acceso al sistema de gestión de base de datos relacional.
[152] PHP: Hypertext Preprocessor. Lenguaje de código abierto.
[153] CSS: Cascading Style Sheets. Lenguaje utilizado para describir la presentación de documentos HTML.
[154] URL: Uniform Resource Locator, localizador uniforme de recursos.
[155] OWASP: The Open Web Application Security Proyect
[156] OCSP: On line Certificate Status Protocol

7. Aplicar las normas Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS)[157]

En su documento "Requisitos y Procedimientos de Evaluación de Seguridad" (2013), el PCI *Security Standards Coucil* sostiene que las normas de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas. Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirientes, entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales) (Requisitos y procedimientos de evaluación de seguridad, 2013).

2.5. Otros protocolos que brindan seguridad en la web para pagos electrónicos: IPSEC, SSH (Secure Shell), 3 D Secure, iKP y SET

Los pagos electrónicos se efectúan a través de protocolos que consisten en una serie de transacciones. Una vez concluidas, se realiza un pago por parte de un tercero, que ha sido debidamente autenticado por una autoridad o entidad autorizada, que no es ni el comprador ni el vendedor.

Para que las transacciones económicas sean confiables se deben cumplir los conceptos básicos de la seguridad informática, ya mencionados anteriormente: la confidencialidad de los datos de la transacción y de los intervinientes en la misma, la identificación de los participantes o protección frente a la suplantación de identidad, la integridad de los datos de la operación, y el no repudio o protección frente a posteriores negaciones del servicio prestado o recibido.

Mencionaremos a continuación otros protocolos que podrían emplearse para la implementación confiable y segura del comercio electrónico. No obstante, recordemos que la principal combinación se efectúa con los protocolos TCP y SSL/TLS, ya descriptos.

[157] PCI DSS: Payment Card Industry Data Security Standard

El protocolo IPsec (*Internet Protocol Security*):

Este protocolo es de uso optativo en IPv4 (IP versión 4) y obligatorio en la versión 6. Proporciona autenticación, intercambio de claves y encriptación de los datagramas que constituyen el tráfico en Internet. Como ya se señaló, el protocolo IP no tiene ninguna medida de seguridad, por lo cual, este protocolo le agrega seguridad a la comunicación de datagramas IP.

En la figura 20 se detalla la topología de una red VPN[158] (red privada virtual) en la que el servidor web del vendedor está en la red perimetral[159], protegida de Internet (red insegura) por un firewall.

De esta forma, todos los usuarios que quieran acceder al servidor tienen que pasar a través del firewall. Sin embargo, existe una alternativa de acceso directo a la red interna del sitio (red perimetral) sin pasar por el firewall; dicha alternativa se implementa mediante la construcción de un enlace VPN que genera un túnel seguro a través de la red Internet entre un cliente VPN y el servidor VPN ubicado en la red perimetral.

> Una VPN es esencialmente una especie de túnel entre dos hosts en Internet entre los que se envían información segura de uno a otro mediante la encriptación de los datos. El túnel se crea utilizando un protocolo de tunelizado como el protocolo túnel de nivel dos (*Layer 2 Tunneling Protocol* - L2TP) o el protocolo de túnel punto a punto (*Point to Point Tunneling Protocol* - PPTP), los cuales se emplean para encapsular las tramas Protocolo Punto a Punto (PPP)[160] que transportan los datagramas IP.
>
> Usando estos protocolos configurados en los firewalls de la red de una empresa los clientes remotos pueden comunicarse en forma transparente y segura con un servidor de la compañía, como si estuvieran conectados en la propia red de la empresa. (Tulloch, 2003, pág. 357)

[158] TOPOLOGIAS DE LA RED VPN: Existen dos topologías basicas: modo túnel y modo transporte.
[159] RED PERIMETRAL: Conocida también como red DMZ.
[160] PPP: Point To Point Protocol

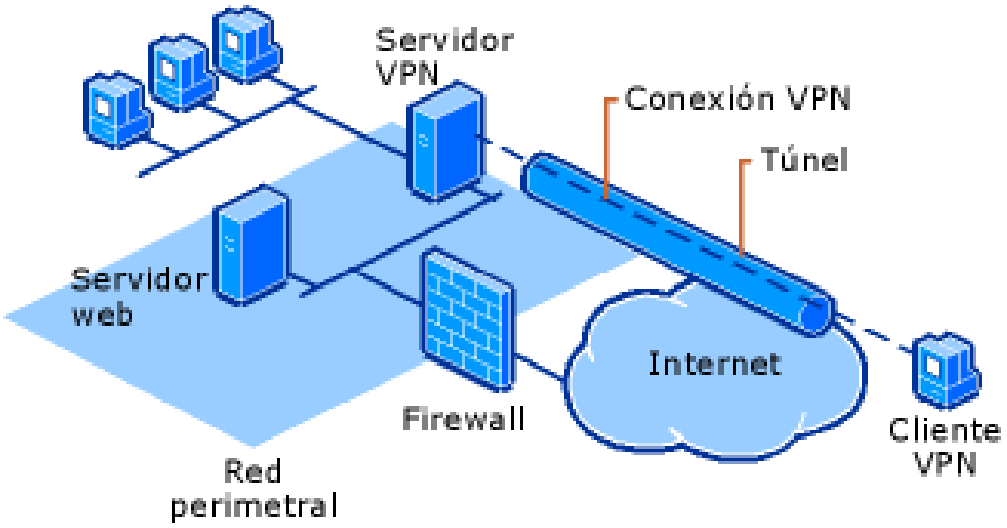


Figura 20: Implementación de una VPN, a través de Internet, entre un usuario y la red perimetral del sitio web
Fuente: Technet.microsoft.com

Este protocolo se emplea básicamente para la construcción de redes privadas virtuales o VPN a través de Internet, lo que posibilita economizar en la construcción de redes corporativas.

En el caso de una empresa con varias sucursales o clientes, éstos podrían implementar una red privada virtual y evitar de esta manera la contratación de líneas dedicadas o la contratación de costosas redes de transporte públicas tipo Internet Protocolo / Multi Protocolo por Conmutación de Etiquetas (IP/MPLS)[161] o Frame Relay[162].

Con respecto a las redes VPN, Black (1999) agrega:

> La VPN se llama así porque un usuario individual comparte canales de comunicación con otros usuarios. Se colocan conmutadores en estos canales para que un usuario final pueda acceder a múltiples sitios terminales. Idealmente, los usuarios no se dan cuenta que están compartiendo una red con otros, de ahí el término red privada virtual: el usuario cree que tiene una red privada, aunque no es así. (pág. 11)

Esta arquitectura, implementada con accesos VPN, no es práctica cuando el número de usuarios es elevado o muy variable, por esta razón no se utiliza en comercio electrónico

[161] IP/MPLS: Internet Protocol/Multiple Protocols Lavel Swiching
[162] Frame Relay: Protocolo para redes WAN que opera por retransmisión de tramas.

(C2B). La dificultad radica en la implementación de túneles VPN, dado que sería necesario uno con cada usuario que quiera comunicarse con el sitio web. Si bien no es práctico para los usuarios sí se puede emplear para el acceso del personal técnico informático de soporte del sitio web del vendedor, dicho personal podría acceder a través de Internet sin pasar por el firewall.

La primera versión del IPsec data de 1995 y actualmente se encuentra en servicio la tercera generación de diciembre de 2005, a través de los documentos RFCs números 4301 y 4309.

En este protocolo se destaca el concepto de la Asociación Segura (AS) que consiste en la reunión de algoritmos y parámetros que se emplean para encriptar y autenticar una comunicación. Si la transmisión es bidireccional se utilizan dos AS que ofrecen los siguientes servicios de seguridad:

- Confidencialidad: evita que un atacante pueda leer los datos de la comunicación.
- Integridad del mensaje: que evita que terceros modifiquen el paquete y éste pueda ser aceptado en el extremo receptor.
- Control de acceso: mediante las políticas de establecimiento de las conexiones IPsec
- Anti repetición: protege contra la repetición de la sesión segura.
- Autenticación del originador del mensaje: que evita la falsificación del mensaje.

IPsec opera en el nivel tres o nivel de red del modelo OSI, por lo cual puede brindar protección y seguridad a los protocolos de niveles superiores como el UDP y el TCP que se encuentran en la capa de transporte. Está constituido por los siguientes tres protocolos:

Authentication Header (AH): que provee integridad, autenticación y no repudio a la comunicación.

Encapsulating Security Payload (ESP): que proporciona confidencialidad, pero opcionalmente puede brindar autenticación e integridad.

Internet key exchange (IKE): posibilita el intercambio secreto de claves de sesión. Los algoritmos criptográficos que utiliza IPsec son: SHA-1, triple DES y AES.

Respecto a los modos de operar, IPsec puede hacerlo en el modo transporte o en el modo túnel. Sobre este aspecto Pacheco (2014) describe que:

> Modo Transporte: donde se protege el dato del paquete IP (se cifran solo los datos, no la cabecera). Sirve para comunicación punto a punto entre equipos, proveyendo confidencialidad, y requiere implementar el protocolo en ambos extremos. Modo Túnel: se protegen los paquetes IP completos, sirve para comunicación punto a punto entre *gateways*, proveyendo confidencialidad en el túnel sin necesidad de que los equipos entiendan el protocolo. A los paquetes de le agrega una nueva cabecera (la del túnel) y se cifra todo el paquete incluyendo la cabecera original. (pág. 202)

El protocolo SSH (*Secure Shell*):

El protocolo SSH que puede traducirse como intérprete de órdenes seguro, utiliza un modelo de operación cliente – servidor y permite copiar archivos y acceder a equipos de red remotos y comandarlos en forma casi similar al modo en que lo realiza el protocolo TELNET. La diferencia fundamental radica en que en SSH la comunicación entre los dispositivos es cifrada, lo cual otorga seguridad a la operación.

Utiliza criptografía de clave pública para autentificar al computador y al usuario; en el nivel de transporte emplea el protocolo TCP, puerto[163] 22, para que la comunicación sea confiable. SSH soporta autentificación basada en el método de clave pública y utiliza los algoritmos RSA (Rivest, Shamir y Adleman) y DSA (*Digital Signature Algorithm*), propiedad del gobierno de los Estados Unidos, esta última es la que mayormente se emplea en la actualidad.

En SSH el cliente que comienza la sesión envía en una trama un conjunto de valores para ejecutar el algoritmo de cifrado correspondiente en el servidor, y también el listado de protocolos de cifrado que soporta el cliente. El servidor calcula su clave de sesión y le responderá en una segunda trama, con otro conjunto de valores y con los algoritmos de cifrado que éste acepta. Con esta segunda trama, el cliente calcula la clave de sesión que será la misma que obtuvo el servidor. A partir de ese instante, todas las tramas que intercambien serán cifradas con esa clave de sesión. Finalizada la sesión, si ambos equipos

[163] PUERTO o PORT: Dirección única en el equipo o computador, codificada en 16 bits, asignada para cada aplicación.

tienen que establecer una nueva comunicación, se calculará una nueva clave de sesión con el mismo procedimiento.

Por lo tanto, únicamente viajan dos tramas en texto plano, pero en ellas no se envía ningún dato privado. Si estas tramas fueran interceptadas por un hacker no servirían para descifrar la comunicación.

SSH protege contra los siguientes ataques:

- IP *Spoofing*, que consiste en que una computadora se hace pasar por otra en la que se confía
- Interceptación de *password* y datos a través de la red
- Modificación de la IP de origen de los paquetes para que parezca que proviene de una IP válida.
- DNS *Spoofing*, modificación de los registros del servicio de nombres de dominio o DNS
- Modificación de datos en equipos intermedios de encaminamiento en la red

Al quedar establecida una comunicación SSH queda formando un túnel entre ambos equipos, por lo cual sólo entra al mismo aquel que tenga permiso. Si se produce la captura del tráfico SSH no habrá forma de descifrarlo y en consecuencia no se podrá modificar, ni desviarlo de su destino.

Protocolo 3 D *Secure*:

Si consideramos el tema del pago online, la mayoría de las transacciones se efectúan mediante la tarjeta de crédito. No obstante, el vendedor no tiene ante sí más que los datos, que podrían pertenecer a una tarjeta clonada o robada. Del otro lado, el comprador envía los datos confidenciales de su tarjeta de crédito al sitio web, sin conocer cómo van a ser tratados dichos datos.

Por lo expuesto, para que la operación se realice de la forma más segura posible para ambos es conveniente emplear una empresa intermediaria especializada en pagos por

Internet con la tecnología e infraestructura necesaria para garantizar la seguridad en el pago, tanto al comprador como al vendedor.

De este modo se evita los fraudes de tipo Tarjeta no Presente (CNP)[164], es decir los pagos fraudulentos con tarjeta de crédito sin la presencia física de la misma, circunstancia que ocurre cuando el número de la tarjeta es robado.

En caso de que no se quiera utilizar una empresa intermediaria, se podría emplear el protocolo 3D *Secure*, que permite garantizar la autenticación del propietario de la tarjeta, y por lo tanto impedir los fraudes.

Este protocolo fue creado por la empresa VISA y tiene la finalidad de mejorar la seguridad de los pagos a través de Internet, tanto para el usuario como para el vendedor. También protege la información de pago durante su transmisión. Visa utiliza el logo *Verified by* Visa, para indicar que el pago ha sido soportado por este protocolo.

Por su parte, MasterCard utiliza el logo MasterCard *Secure Code* para indicar que la transacción de pago esta soportada por el protocolo 3D *Secure* y que garantiza la seguridad de la misma.

El objetivo de su empleo es disminuir las estafas a los comercios en línea y dar seguridad a los clientes en sus pagos.

El procedimiento implementado por el protocolo 3 D *Secure* es el siguiente:

1. El titular de la tarjeta de crédito introduce su número de tarjeta y valida la compra
2. Aparece en la pantalla los datos de la compra
3. El banco al que está asociada la tarjeta de crédito solicita la contraseña
4. El banco verifica si la tarjeta tiene suficiente límite autorizado para realizar la compra
5. Una vez autenticado el pago, se produce la autorización de la compra y el banco procede a realizar la transacción

[164] CNP: Card No Present

Este protocolo presenta dos ventajas respecto SSL dado que autentifica los bancos y verifica que el comprador está autorizado a utilizar la tarjeta de crédito que le proporciona al vendedor.

Protocolos iKP (*Internet Keyed Payment Protocols*):

Los protocolos iKP (1KP, 2KIP y 3KP) tienen como finalidad garantizar los pagos online en las transacciones comerciales. Es una familia de protocolos desarrollada por el IBM *Research Group*. Todos ellos operan con criptografía de clave pública, pero se diferencian en el número de participantes que se autentifican en el procedimiento de pago; el número de participantes es el indicado en el índice *i*.

En el 1KP sólo el Broker[165] tiene clave pública y certificado; en el 2KP el Broker y el comerciante tienen autenticación y en el 3KP todos los participantes tienen certificado y clave.

En el caso de 1KP es el bróker que concentra todos los intercambios entre el comprador y el vendedor y ambos cifran sus mensajes empleando la clave pública del bróker. Para el protocolo 2KP, dado que el bróker y el comerciante poseen cada uno de ellos un par de claves públicas y privada además del certificado que los autentica, se garantiza el no repudio por parte del comerciante. Por último, en el caso de 3KP se ofrece no repudio tanto del comerciante como del comprador.

Protocolo SET (*Secure Electronic Transaction*):

Inicialmente la compra por Internet se realizaba sin ningún proceso de cifrado de los datos de la transacción; simplemente el comprador insertaba los datos de su tarjeta de crédito. Esto trajo aparejados problemas graves cuando los datos comenzaron a caer en manos de personas no autorizadas. Este proceso fue reemplazado rápidamente por el uso del SSL que comenzó a requerir un certificado de seguridad para el sitio del vendedor y el cifrado de toda la transacción.

Pero entonces, el que estaba desprotegido era el vendedor pues no había manera de garantizar que el comprador fuera el titular de la tarjeta de crédito empleada para el pago.

[165] BROKER: Intermediario entre un comprador y un vendedor para hacer una transacción.

Para evitar este último inconveniente, se implementó el protocolo SET que protege la integridad de la información de pago, la confidencialidad de la información y la autenticación del comerciante y del dueño de la tarjeta de crédito.

Con respecto al protocolo SET, Stallings W (2004), señala:

> SET no es un sistema de pago en sí mismo, sino que más bien es un conjunto de protocolos de seguridad y formatos que permite a los usuarios emplear las infraestructuras existentes de pago por tarjeta de crédito, de forma segura, en una red abierta como Internet. (pág. 246)

El Protocolo SET o Transacción Electrónica Segura, fue desarrollado en 1995 por las empresas Visa y Mastercard, con la colaboración de otras empresas como American Express, Microsoft, IBM, etc. quienes convinieron en aunar esfuerzos para elaborar un único protocolo para el pago electrónico con tarjetas denominado SET (Drew , 1999), (Agnew, 2003) y (Merkow & Breithaupt, 1998).

En este protocolo, orientado a transacciones y que responde al esquema petición - respuesta, el comerciante, el titular de la tarjeta de crédito, el banco y la autoridad certificante deben estar conectados a Internet. Las tres entidades implicadas directamente en la operación -el comprador, el vendedor y el banco- deben disponer del certificado de la autoridad certificante.

Con el SET es posible proteger el número de tarjeta de crédito del titular y asegurar que solo pueden usarla las personas autorizadas. Desde un comienzo se buscó un protocolo normalizado para todos los productos, con el fin de evitar la proliferación de múltiples soluciones patentadas que demorarían el despliegue y complicarían el proceso para bancos y comerciantes.

Este protocolo permite la identificación y autenticación del comerciante y el cliente mediante certificados digitales, pero lo que es más importante es que la transacción cierra entre el comprador y el banco, con lo cual el comerciante no se entera de los datos de la tarjeta del cliente. En las transacciones mediante el protocolo SET, los datos del cliente se envían al servidor del vendedor, pero éste sólo recibe la orden. Los números de la tarjeta se

remiten directamente al banco del vendedor, quien tiene acceso a los detalles de la cuenta bancaria del comprador y puede contactarse con el banco para verificarlos en tiempo real.

SET emplea criptografía de clave pública (cifrado asimétrico) para cifrar la clave de sesión (clave de encriptación). Esta última, se utiliza para cifrar mediante encriptado simétrico los datos - recordemos que éste es mucho más rápido que el asimétrico-. Por otro lado, dada la lentitud del cifrado asimétrico, se utiliza para la firma digital una función *Hash* sobre un conjunto de datos, obteniendo como resultado el cifrado correspondiente, denominado resumen o *digest*.

La combinación de los métodos de cifrado arriba indicados permite que SET ofrezca: confidencialidad en los intercambios comerciales; autenticación del comprador como legitimo usuario dela tarjeta de crédito; autenticación del comercio como legitimo poseedor de una cuenta con un banco vendedor; integridad de los datos intercambiados entre el comprador, el comerciante y el banco de este último, sin la participación de intermediarios; y por último, identificación y autenticación de todos los participantes.

Los pasos del protocolo SET son los siguientes:

1. El cliente comienza la compra con la selección de los productos/servicios que le interesa adquirir
2. El cliente envía la orden al vendedor
3. El banco verifica la validez del requerimiento
4. La empresa emisora de la tarjeta autoriza la transacción
5. El banco del vendedor autoriza la operación
6. La transacción se completa con la intervención del servidor del vendedor, donde queda registrada la operación
7. El generador de la tarjeta de crédito envía un aviso de crédito al cliente

Para gestionar la evolución de la especificación SET, Visa y MasterCard constituyeron la compañía *Secure Electronic Transaction* LLC (SETCo), quien coordina los esfuerzos tendientes a la adopción del protocolo SET como un estándar global para el procesamiento de pagos mediante las tarjetas de crédito (Tulloch, 2003). Por último, cabe señalar que este protocolo presenta como ventaja respecto del SSL que permite autentificar a los bancos.

2.6. Principales factores que inciden en la seguridad del sitio web del proveedor, relacionados con el usuario, la red, la operación del sitio y el mantenimiento del mismo

En este apartado se describen los factores que forman parte de la gestión de seguridad que acompaña todo sistema informático que opera en la web.

Al respecto Barba Marti (2001) nos dice:

> La gestión de seguridad está relacionada con la generación, distribución y almacenamiento de claves de cifrado, información de passwords (contraseñas) o bien información de control de acceso y autorización que debe mantenerse y distribuirse. Es decir, proporciona facilidades para incorporar mecanismos de seguridad contra ataques a las comunicaciones, como protección contra interrupción del servicio, capturas no autorizadas de información, modificación de información o suplantación de identidad. (pág. 95)

Desde el punto de vista de la seguridad informática, los sistemas están expuestos a dos factores de peligro que son por un lado, las amenazas externas e internas y por otro, las vulnerabilidades del hardware y software.

Las vulnerabilidades se pueden definir como aquellas debilidades de los sistemas informáticos, pero de un modo más preciso, podemos decir que son aquellos elementos del sistema que pueden ser aprovechados por atacantes para violar la seguridad, con el objeto de causar daño en el sistema y/o en los datos.

En el sitio Red y Seguridad de la Universidad Nacional de México, se expresa que una vulnerabilidad informática es un elemento de un sistema informático que puede ser aprovechado por un atacante para violar la seguridad, así mismo pueden causar daños por sí mismos sin tratarse de un ataque intencionado. A las vulnerabilidades se las consideran un elemento interno del sistema, por lo que es tarea de los administradores y usuarios el detectarlos, valorarlos y reducirlos. Las vulnerabilidades son el resultado de errores de programación (*bugs*), fallos en el diseño del sistema, incluso las limitaciones tecnológicas pueden ser aprovechadas por los atacantes. (vulnerabilidades, 2017)

El sistema de comercio electrónico trazable, como se indicó en el capítulo uno, tiene como principales componentes: el host del cliente, su navegador web, la red Internet y los protocolos de comunicación que brindan conectividad y seguridad a través de la red y el sitio del vendedor con su aplicación web correspondiente y las entidades intermedias.

Esos componentes del sistema de comercio electrónico tienen factores de orden técnico y operativo que condicionan los requerimientos mínimos de seguridad. Al respecto, en la figura 21 se detallan los factores de seguridad que toda operación online de comercio electrónico debe tener. Estos son: la autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto al seguimiento de la transacción y/o la identidad de alguna de las partes, el reconocimiento (no repudio) que garantiza que la transacción es consentida por cada una de los participantes y la disponibilidad de los datos en el sitio web.

Las dimensiones de la seguridad en el comercio electrónico deben ser analizadas desde los puntos de vista correspondientes al cliente y también al comerciante.
También es necesario evaluar las amenazas sobre los sistemas informáticos inherentes al comercio electrónico, caracterizado por su permanente evolución.

Con respecto a la vulnerabilidad en la seguridad de los sitios web y/o cualquier dispositivo conectado a Internet, Tanenbaum (2003) afirma:

> La capacidad de conectar una computadora, en cualquier lugar, con cualquier computadora, de cualquier lugar, es una ventaja a medias. Para los usuarios domésticos, navegar en Internet significa mucha diversión. Para los gerentes de seguridad empresarial, es una pesadilla. Muchas empresas tienen en línea grandes cantidades de información confidencial, secretos de comercio, planes de desarrollo de productos, estrategias de marketing, análisis financieros, etcétera. Si esta información cae en manos de un competidor podría tener graves consecuencias. Además del peligro de la fuga de información, también existe el peligro de la infiltración de información. En particular, virus, gusanos y otras pestes digitales pueden abrir brechas de seguridad, destruir datos valiosos y hacer que los administradores pierdan mucho tiempo tratando de arreglar el daño que hayan hecho. (pág.776)

Dimensiones	Perspectiva del cliente	Perspectiva del comerciante
Integridad	¿Se ha alterado la información que yo transmití o recibí?	¿Se han alterado sin autorización los datos en el sitio? ¿Son válidos los datos que están recibiendo los clientes?
No reconocimiento	¿Una parte que realizo una acción conmigo puede negar después haberla realizado?	¿Puede un cliente negar que pidió productos?
Autenticidad	¿Con quién estoy tratando? ¿Cómo puedo estar seguro de que la persona o entidad es quien afirma ser?	¿Cuál es la verdadera identidad del cliente?
Confidencialidad	¿Puede alguien que no sea el destinatario específico leer mis mensajes?	¿Los mensajes o datos confidenciales son accesibles para otras personas aparte de las que están autorizadas?
Privacidad	¿Puedo controlar el uso de la información acerca de mí que se transmite a un comerciante de comercio electrónico?	¿Qué uso, si acaso pasa, puede hacerse de los datos personales recopilados como parte de una transacción de comercio electrónico? ¿La información personal de los clientes se está utilizando de una manera no autorizada?
Disponibilidad	¿Puedo tener acceso al sitio?	¿El sitio es operativo?

Figura 2: Perspectivas del cliente y del comerciante sobre distintas dimensiones de la seguridad en el comercio electrónico
Fuente: Traver L. (2013)

Es por ello que un elemento importante en el sistema de comercio electrónico es la seguridad del sitio web del vendedor o comerciante. Cuando la seguridad se ve vulnerada se producen los denominados incidentes de seguridad, con graves consecuencias para los usuarios que acceden a él.

> Según la norma ISO 27035, un Incidente de Seguridad de la Información es indicado por un único o una serie de eventos de seguridad de la información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información (Centro de respuestas a incidentes de seguridad informatica de Uruguay, 2013)

En lo concerniente a la operatoria, cualquier usuario que necesite realizar una transacción de comercio electrónico debe primero ingresar al sitio web (empresa o negocio) con el que quiere operar, y sentirse seguro para realizar la operación comercial.

Se describió previamente que la transferencia de los datos a través de Internet, entre el host del usuario y el servidor web de la empresa, se realiza con protocolos que brindan confiabilidad (TCP), cifrado y autenticación mediante el protocolo (SSL/TLS). Decíamos que este último, se lleva a cabo en base a los métodos de encriptado del tipo simétrico, asimétrico y *hashing*.

El empleo combinado de los protocolos SSL/TLS y TCP aseguran en la comunicación: confiabilidad, confidencialidad, integridad, autenticación y no repudio.

Es por ello que analizaremos a continuación los factores que determinan las vulnerabilidades en la seguridad del sitio web del vendedor, que se incorporarán a la encuesta, para que sean evaluados por los estudiantes de las carreras de Licenciatura e Ingeniería en Sistemas de Información. A partir de ella, se podrá conocer la opinión técnica de dichos estudiantes (futuros profesionales de TIC) y la valoración que efectúan sobre la importancia de cada factor.

Cabe aclarar que se describirán las principales amenazas conocidas a la seguridad informática, en este caso aplicadas al comercio electrónico. No obstante, somos conscientes de que mientras escribimos estas líneas, seguramente se están desarrollando nuevas y más sofisticadas amenazas para implementar en futuros ataques.

Respecto a las amenazas que se ciernen sobre las aplicaciones informáticas que corren en la web, Mifsud (2012) nos dice que:

> Entendemos la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático. Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo.
>
> Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama 'impacto'. Integrando estos conceptos podemos decir que un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él. Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas. (pág. 4)

Por su parte, Guasch (2013) describe y ejemplifica el caso de ventas durante el Black Friday en los Estados Unidos, lo que constituye una situación de alta vulnerabilidad:

> Cuando todo el mundo en Estados Unidos aprovechaba el fin de semana del pasado Black Friday para hacer compras con increíbles rebajas, y comprar mediante sus tarjetas de crédito (...) otros obtenían los datos de dichas tarjetas de crédito, comprometido así uno de los comercios americanos más importantes, con más de 2000 tiendas físicas, Target. Hasta ahora, tras varias comunicaciones publicadas por la propia empresa, se conoce que la información robada por estos ladrones digitales correspondería con los siguientes datos: nombre completo del cliente, número de tarjeta de crédito o débito, fecha de caducidad y código de seguridad CVV (pág. 34).

En la figura 22 se detalla la ubicación del *Card Verification Value* (CVV) o código valor de verificación/validación, al respecto, Romero L, (2016) expresa que es un número de tres o cuatro dígitos que está situado en la parte trasera de las tarjetas de crédito y débito, al final del cuadro situado para la firma del titular de la tarjeta. Mientras las tarjetas VISA, Mastercard o Euro6000/CECA tienes 3 dígitos en el CVV, las American Express tienen 4 dígitos.

Figura 22: Código de seguridad CVV
Fuente: Rankia.com

Las vulnerabilidades en la seguridad del sitio web del vendedor consideradas en la presente tesis son las siguientes:

- Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras, y sin usar la facilidad CAPTCHA
- Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web, y deficiente protección de los mismos en la base de datos.
- No se realiza el registro de las acciones de los usuarios en bitácoras o "*logs*" del servidor.
- No se efectúa el control de los datos introducidos por los usuarios en el sitio web.
- No se obtienen los certificados digitales a través de una Autoridad de Certificación (CA).
- No se ha instalado un firewall para el control del tráfico de paquetes entrantes y salientes del sitio, mediante el empleo de filtros y programas proxy.
- El ataque *phishing* a la estación del usuario implementado a través de sitios web falsos o simulados.
- Ataques de denegación de servicio a los servidores de sitios web.
- No se controlan los datos introducidos por los usuarios en el sitio web, mediante le protocolo P3P.
- No se realiza la actualización permanente del software utilizado en el sitio web.
- Deficiente seguridad física del sitio web y del servidor.
- No se realizan pruebas de vulnerabilidad del sitio web (pruebas de penetración).
- No se aplican estándares de la industria relativos a la operación y mantenimiento de sitios web.
- Ataques internos originados por el personal técnico del sitio web

Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras y sin usar la facilidad CAPTCHA

Cuando un usuario desea acceder a un sitio web para realizar una operación de compra lo primero que debe verificar es si la URL del sitio comienza con https://; el color de la barra de estado del navegador debería ser verde o a lo sumo blanco y el usuario debería poder acceder al certificado digital, como se desarrollará más adelante en este capítulo. De esta forma, se comprueba que el sitio cuenta con el respaldo de una autoridad certificante, que ha validado a la empresa propietaria del mismo, legalmente constituida y se asegura además que la comunicación entre su navegador y el sitio web estará permanentemente encriptada.

Para que la conexión del usuario se efectúe exclusivamente por personas y no por una aplicación, se debería usar la facilidad CAPTCHA.

> Un CAPTCHA (test de *Turing* público y automático para distinguir a los ordenadores de los humanos, del inglés "*Completely Automated Public Turing test to tell Computers and Humans Apart*") es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta. Un CAPTCHA te ayuda a protegerte del *spam* y del descifrado de contraseñas pidiéndote que completes una simple prueba que demuestre que eres humano y no un ordenador que intenta acceder a una cuenta protegida con contraseña. La prueba de un CAPTCHA consta de dos partes simples: una secuencia de letras o de números generada aleatoriamente que aparece como una imagen distorsionada y un cuadro de texto. Para superar la prueba y probar que eres un ser humano, simplemente tienes que escribir los caracteres que veas en la imagen del cuadro de texto. (Administrador de G Suite, 2017)

El acceso del usuario al sitio debe estar restringido a unas pocas opciones hasta el momento que se conecta. Una vez registrado, el usuario debería poder acceder en forma plena a todas las opciones del sitio.

Por otro lado, el acceso a algunas opciones debe estar restringido hasta tanto el usuario efectué el acceso mediante el uso de contraseña segura y también (en lo posible) de un CAPTCHA, como se indicó precedentemente.

Traver Laudon, (2013) sostiene:

> Por lo general, la organización de seguridad administra los controles de acceso, los procedimientos de autenticación y las políticas de autorización. Los controles de acceso determinan que individuos externos e internos pueden obtener acceso legítimo a las redes de la organización.
>
> Los controles de acceso para los individuos externos incluyen firewalls y servidores proxy, mientras que los controles de acceso para los individuos internos por lo general consisten en procedimientos de inicio de sesión (nombre de usuario, contraseñas y códigos de acceso). (pág.306)

Las contraseñas seguras son difíciles de descifrar y su fortaleza radica en la longitud de las mismas y en su composición. Con respecto a la longitud, ésta debe tener como mínimo 8 caracteres y la composición debe contener caracteres, alfabéticos (mayúsculas y minúsculas), caracteres numéricos y de puntuación.

Una contraseña de ocho caracteres que contenga números, letras mayúsculas y minúsculas, y caracteres de puntuación, tiene más de 30.000 combinaciones posibles comparadas con una que sólo contenga letras en minúscula.

En la web existen generadores gratuitos de contraseñas, como por ejemplo el Norton *Identity Safe*, para crear contraseñas seguras y difíciles de descifrar o adivinar. En ellos se pueden seleccionar los criterios a emplear en la generación de las contraseñas.

Podemos concluir que los métodos de autenticación se dividen en tres grandes categorías en función de la información y tecnologías que utilizan para verificar la identidad (Wang, 2006): información que el usuario sabe (contraseña); elementos que el usuario posee (hardware), como puede ser una tarjeta inteligente o *Smart card*; y características físicas del usuario (autenticación biométrica).

El reconocimiento de patrones, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos.

Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web, y deficiente protección de los mismos en la base de datos

En las transacciones de comercio electrónico todos los datos de los usuarios son almacenados en bases de datos, que deben disponer de mecanismos de seguridad para que no accedan a ellos personas no autorizadas para leerlos o modificarlos.

"Una base de datos es una estructura en memoria secundaria construida pensando en los problemas de acceso múltiple y simultaneo a la información almacenada." (Villalobos Jorge A, 2008, pág. 409)

Las bases de datos tienen la información ordenada en forma lógica y guardan un ordenamiento cuyo cumplimiento permite acceder a ella en forma coherente a través del sistema de gestión de la base (SGBD). Al respecto Gomez A.L. (1993) dice:

> Un SGBD (Sistema de Gestión de Base de Datos) es un conjunto de programas que va a permitir insertar, modificar, borrar y buscar eficazmente datos específicos entre un volumen masivo de información compartida por todos los usuarios de la base; pero también es una herramienta que va a permitir ordenar, buscar, reordenar y convertir datos. (pág. 171)

El orden jerárquico de una base de datos está compuesto por tablas, campos y registros. Las tablas se utilizan para guardar datos, los campos son cada una de las columnas que forman las tablas y los registros son cada una de las filas en que se divide la tabla.

Las bases de datos se caracterizan por las siguientes propiedades: acceso recurrente por parte de múltiples usuarios, redundancia mínima, integridad de los datos, copias de respaldo con recuperación de datos, seguridad de acceso, independencia física y lógica de los datos y controles de auditoria.

Dado que en la base de datos se almacenan datos críticos que hacen a la confidencialidad de la transacción, es un punto del sistema de comercio electrónico muy codiciado por lo hackers, que tratan de acceder a la lectura o modificación de los datos y en algunos casos borrarlos. Pero estas amenazas fraudulentas no son las únicas; también se pueden producir

incidentes accidentales producto de una operación incorrecta en la gestión de la base de datos por parte del personal que la administra o por errores de hardware y/o software.

Para proteger la información de la base pueden guardarse los datos encriptados mediante tres procedimientos: con cifrado reversible, cifrado irreversible aplicando una función hash con guarda del *hash* obtenido, y por último se podría aplicar una función *hash* + *salt* y guardar el *hash* obtenido.

El método de cifrar la información mediante un cifrado reversible presenta el inconveniente del almacenamiento seguro de la clave. Si ésta es descubierta, toda la información de la base queda a disposición del atacante. Además, para el administrador de la base de datos es muy sencillo obtener las *password* de los usuarios y con ella acceder a la información confidencial de estos, porque puede acceder a las tablas y, por supuesto, a la clave de encriptación.

El cifrado irreversible utiliza una función hash como MD5 o SHA-1, que se describió en el capítulo 2. Recordemos que el cifrado *hashing* encripta un texto de forma irreversible, esto significa que éste no se puede desencriptar. En este caso, en la tabla de la base de datos se guarda la contraseña del usuario y el hash correspondiente; de esta forma, cuando el usuario ingresa con su *password*, se calcula el hash y se lo compara con el que se encuentra almacenado; si coinciden puede acceder a la base.

Este último método tiene el inconveniente de que podrían presentarse registros duplicados, por ejemplo, si dos o más usuarios emplean la misma contraseña. Para evitar esta debilidad, se emplea el método denominado cifrado -*hash* + *salt*-, donde el término *salt* es un texto o un conjunto de caracteres que varía de usuario en usuario - por ejemplo, podría ser el ID (identificación) de cada uno de ellos. En este caso, se cifra la *password* más el ID del usuario; como no puede haber dos ID iguales, aun cuando las *passwords* fueran las mismas, el *hash* será diferente. Este es el método más seguro si también se emplea un cifrado *hashing* como el SHA-512.

La estructura de la base de datos tiene un elemento fundamental para acelerar la búsqueda de la información, que es el índice de la base de datos; éste permite buscar un elemento que está indexado sólo con examinar su presencia en el índice. Una vez hallado se tendrá acceso al registro donde se encuentra el dato.

No obstante, la importancia de la indexación en las bases de datos para acelerar las búsquedas, en casos en que los datos se encuentran indexados por ser sensibles - como ocurre en las bases de datos afectadas a transacciones comerciales- se emplean otras variantes. Una de ellas es la creación de un valor identificatorio nuevo, que no constituya un dato sensible del usuario. También se puede crear una nueva columna para almacenar el hash de los datos del texto y a continuación el índice de esa columna. Otra alternativa es utilizar un Código de Autenticación de Mensajes (MAC) del texto, como fue descripto en el capítulo 2, para crear una columna nueva de indexación. En este último caso, se requiere de una clave secreta para calcular el MAC.

Para la validación, detección de errores y verificación de la consistencia e integridad de los registros de la base de datos se emplea el digito verificador, que posibilita comprobar la corrección de cada dato. Este consiste en uno o más caracteres añadidos al dato original y calculado mediante determinado algoritmo, como por ejemplo el módulo 11[166].

Con respecto a la seguridad de la información almacenada en las bases de datos, la organización IOUG[167] liberó un estudio realizado con 430 de sus miembros acerca de la seguridad en los datos, donde se revelan cinco puntos claves que muestran porqué falla la seguridad en las bases. Allí se señala que:

1. Las organizaciones no saben aún donde residen sus datos sensibles
2. El monitoreo de la seguridad sigue siendo aún irregular y no sistemático
3. Los usuarios privilegiados se siguen ejecutando sin un adecuado control y seguimiento
4. Los parches en las bases de datos se despliegan y aplican lentamente
5. Existe un evidente retraso en la aplicación de técnicas de cifrado sobre las bases de datos. (ITInsecurity , 2010)

Si se registran en el sitio web del proveedor alguna de las deficiencias en la seguridad informática descriptas, que se manifiestan en las bases de datos, se está exponiendo la información de los usuarios y de la empresa proveedora a posibles fallas o vulnerabilidades que podrán ser explotadas por atacantes internos o externos.

[166] MODULO 11: Este método posibilita detectar errores en un solo dígito y se basa en aplicar un factor de chequeo ponderado a cada dígito original.
[167] IOUG: Independent Oracle Users Group's

No se realiza el registro de las acciones de los usuarios en bitácoras o *logs* del servidor

Cuando el usuario ingresa al sitio web, toda la actividad que realice debe quedar registrada en *logs* o bitácoras, que son tablas ubicadas en la base de datos que están indexadas según el código que identifica al usuario. Los *logs* posibilitan, en caso de que se produzca algún incidente de seguridad o de operación, que el episodio quede registrado para su análisis y/o recuperación posterior.

Otra ventaja de utilizar *logs* o bitácoras es que permiten un control sobre todas las acciones que efectúan los usuarios, detectando los inconvenientes e incidentes ante actividades anormales propias o fallas del sistema.

Finalmente, estos registros posibilitan al administrador del sitio localizar errores, detectar ataques maliciosos y hasta conocer qué hacen los usuarios en el sistema, la fecha y hora en la que acceden, etc.

No se efectúa el control de los datos introducidos por los usuarios en el sitio web

Para proteger un sitio web de sentencias maliciosas, como SQL *Injection*, que pueden modificar la operatoria de la aplicación y originar la ejecución de códigos malicioso, es necesario poner atención en el momento en el que los usuarios ingresan sus datos al sitio. Una medida de prevención recomendada es la incorporación de códigos de control en los formularios de los datos solicitados. En caso de que éstos contengan errores o sentencias maliciosas, aparecerán mensajes de alerta abortando la transacción preventivamente.

Por otro lado, debemos considerar que, si algún atacante logra introducir un SQL *Injection*, que no fue considerado dentro de los controles de cadenas de caracteres, la integridad de los datos almacenados en la base de datos estará seriamente comprometida.

No se obtienen los certificados digitales a través de una Autoridad de Certificación (CA)[168]

Los certificados digitales son emitidos por un tercero denominado Autoridad de Certificación (CA). La CA puede ser un organismo o empresa privada que realiza

[168] CA: Certification Authority.

importantes inversiones en tecnología, prácticas e infraestructura, que le posibilita administrar un volumen elevado de tráfico de información, a efectos de combinar la criptografía con los protocolos de seguridad y que éstos operen eficientemente con las aplicaciones web del usuario, y con las complejas y seguras bases de datos, que son su principal capital.

Las CA también deben contar con enlaces de comunicaciones redundantes, copias de seguridad automatizadas (sistemas de almacenamiento de datos sofisticados) y mecanismos de recuperación en general, que aseguren una disponibilidad elevada del sistema en cualquier momento.

En el negocio de las CA existen las denominadas declaraciones de prácticas, que son documentos que establecen la infraestructura legal, técnica y operativa para ejercer como autoridad de certificación en Internet. En estos documentos se detallan los requisitos de validación que se deben emplear para la aplicación, el proceso de solicitud del certificado, el proceso de emisión, la aceptación, la suspensión, la derogación y el vencimiento de los certificados. Se incluyen también las formas de empleo de los mismos y las obligaciones de la autoridad de certificación y de las autoridades emisoras.

Las CA pueden brindar en general certificados clase 1, 2, 3 y 4.

Certificado digital clase 1: es el más sencillo y el de menor nivel de seguridad dado que provee un nombre y una dirección de correo electrónico. Se utiliza para navegar en Internet con un nivel de confianza aceptable.

Certificado digital clase 2: tiene mayor nivel de seguridad que el anterior, dado que proporciona la identidad verificada por un tercero, la dirección y otras informaciones personales. Estos certificados son aptos para las compras o suscripciones online.

Certificado digital clase 3: presenta mayor nivel de seguridad que el predecesor al requerir que la identidad sea verificada ante escribano público y el solicitante del certificado debe enviar por correo la copia certificada que la solicitud sea procesada. Este certificado ofrece el mayor nivel de confianza que una persona puede requerir para su identificación electrónica.

Se utiliza especialmente en aplicaciones bancarias, comercio electrónico entre empresas o servicios en línea.

Certificado digital clase 4: además de los requerimientos inherentes al de clase 3 tiene la particularidad que se verifica y asegura la relación del individuo con una determinada organización o empresa a la cual dice pertenecer. Se emplea en el exclusivo mundo de los negocios.

En el empleo de herramientas y aplicaciones en la web para detectar si un sitio es o no fraudulento, también se deben tener en cuenta otros factores que permiten identificarlo y en definitiva, saber si la conexión es segura o no lo es.

En principio, como se mencionó anteriormente, se debe comenzar la URL con https://, que significa que se opera con el protocolo SSL y en consecuencia, cuenta con el respaldo de una Autoridad Certificante. En estos casos, si el sitio web trata de utilizar un certificado SSL falso, el navegador muestra un mensaje de alerta.

En forma gráfica, si el sitio es seguro debe aparecer un candado cerrado al principio o al pie de página, si el candado está abierto no es un sitio seguro. En muchos casos se emplea la imagen de una llave al pie de la página; si ésta aparece es un sitio seguro.

También es muy importante que el usuario mediante el botón del mouse seleccione el icono del candado o en la imagen de la llave, como se indica en la figura 23, a los efectos de visualizar la información inherente al certificado digital, dado que ésta podría estar impuesta en forma fraudulenta.

Existen otros indicadores que advierten sobre la presencia o no de una conexión segura como son los colores de la barra de estado de seguridad de los sitios. Cuando se accede a una página de un sitio web que emplea conexión segura, el color indica la validez de su certificado y el nivel de validación por parte de la organización de certificación. Estos colores pueden ser verde, blanco, amarillo y rojo.

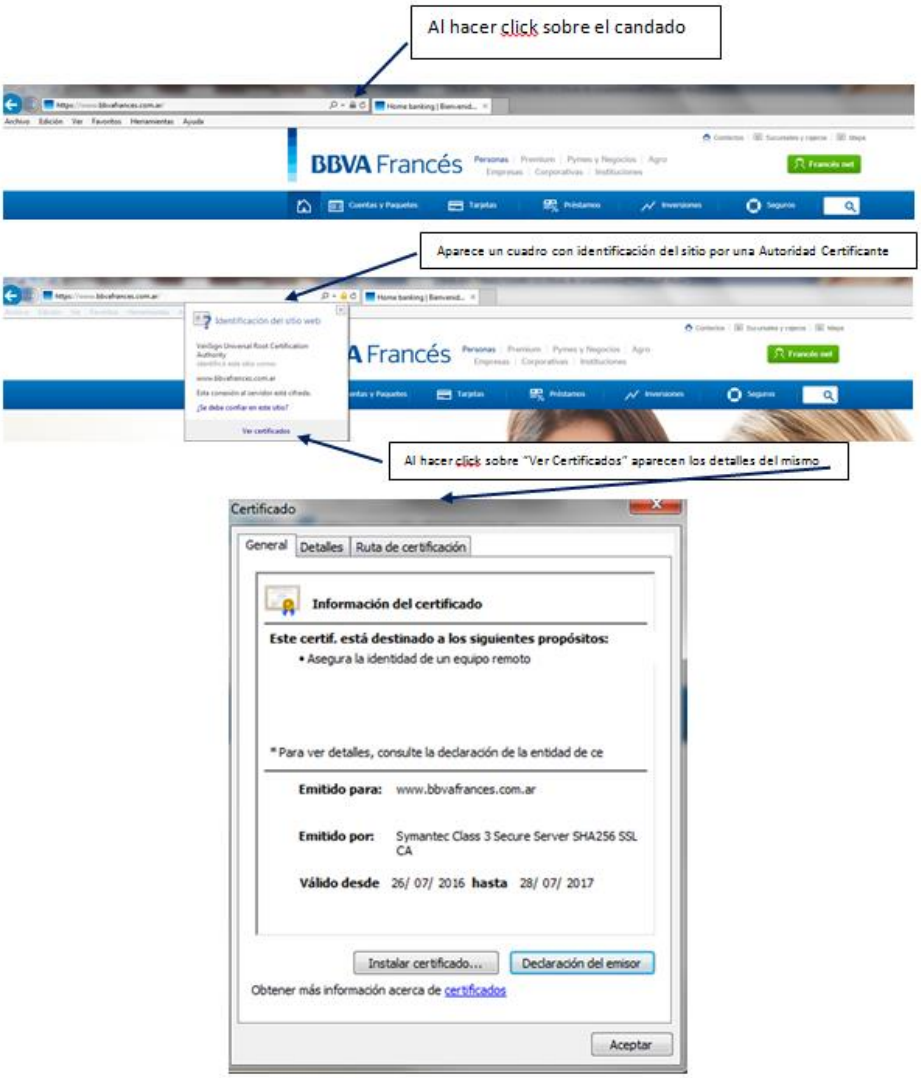


Figura 23: Verificación de un sitio web mediante su certificado correspondiente
Fuente: Pagina web Banco BBVA Francés

Color de la barra verde: es el máximo nivel de validación y de confianza. No solo especifica que la comunicación está cifrada, sino que la entidad emisora del certificado confirma que el dueño o administrador del sitio web es una empresa legalmente constituida. El certificado en este caso, tiene una validación ampliada.

Color de la barra blanco: indica que la comunicación entre el navegador y el servidor del sitio web está cifrada. El certificado tiene una validación normal.

Color de la barra amarillo: indica que no se ha podido verificar la autenticidad del certificado emitido por el sitio web o tampoco se ha podido verificar la autenticidad de la entidad emisora del certificado. El sitio web es presumiblemente inseguro.

Color de la barra rojo: el certificado ha caducado y en consecuencia no es válido o presenta un error que impide su uso. El sitio web es inseguro; no conectarse.

En los casos de barra verde y blanco descriptos, la autoridad emisora del certificado garantiza la conexión segura entre navegador y servidor, pero no las prácticas comerciales del sitio web ni de la empresa que lo administra y gestiona.

Cabe destacar que, aunque la conexión entre el equipo del usuario y el sitio web se encuentre cifrada mediante el protocolo SSL/TLS, esto no le garantiza al usuario que el sitio web sea totalmente confiable; éste podría hacer un uso irresponsable de los datos por negligencia, impericia o por disponer de una infraestructura de seguridad ineficaz.

Como se ha detallado en este capítulo, el comercio electrónico se basa principalmente en la confianza no solo de los consumidores o compradores sino también de los vendedores y entidades intermedias. Un factor de importancia para construir dicha confianza es el certificado digital, que se fundamenta en la firma digital.

Tradicionalmente la firma de puño y letra ha permitido atribuir a una persona su conformidad en un documento, pero ¿cómo verificar la autenticidad de un documento electrónico?

Esa función la cumple la firma digital que debe cumplir con dos objetivos básicos. El primero es que permita verificar fehacientemente que la firma pertenece al firmante y la segunda que sea imposible su alteración por terceros.

Para implementar la firma digital se utilizan dos métodos de cifrado: el cifrado asimétrico con el par de claves pública y privada del sujeto firmante, y el cifrado irreversible o *hashing* - ambos métodos detallados anteriormente -. Para firmar un documento se aplica primero un cifrado hash con lo cual se obtiene un resumen o valor hash, como resultado del proceso *hashing*. Posteriormente se encripta este resumen o valor hash con la clave privada del sujeto firmante, mediante un algoritmo especifico. Dado que la clave pública del firmante, generada conjuntamente con la privada, está disponible en Internet y es accesible a cualquier persona, se puede en todo momento verificar la autenticación de la firma del documento.

Para validar el documento, el receptor debe generar un valor hash del documento recibido y desencriptar la firma digital mediante la clave pública del firmante. Si los dos hashes son idénticos, el documento no ha sufrido modificación y la firma es auténtica. Cabe aclarar que tanto el emisor como el receptor del documento emplean el mismo algoritmo *hashing* para el encriptado del documento.

Un inconveniente a la seguridad es el almacenamiento de las claves que se emplean para la firma digital. Si se las guarda en el disco duro de la computadora, están expuestas al robo mediante programas especializados en capturarlas. Si se emplea un medio removible se evita la situación anterior, pero para utilizar la clave privada se debe desencriptar mediante la computadora y copiar la misma en memoria, con lo cual sigue siendo vulnerable a programas hostiles.

El método que presenta mayor seguridad es el que se basa en la utilización de un dispositivo inteligente que cuente con microprocesador para crear y almacenar la clave privada. De esta forma, la clave no puede ser capturada por programas hostiles instalados en el computador; obviamente, siempre existe la posibilidad de la pérdida o robo del dispositivo.

Un certificado digital relaciona la clave pública de una persona, empresa u organismo con su correspondiente entidad propietaria a través de una autoridad en la que confía.
Gallardo Carracedo J. (2004) dice:

> Un certificado concreto es simplemente una estructura de datos organizada en una serie de campos que, a su vez, están descompuestos en diversas partes, todo ello conforme a una sintaxis bien definida. En último extremo, esa estructura estará representada por un conjunto de bits (o si se prefiere de octetos), que será lo que viaje por la línea de comunicación y lo que se almacene en la memoria de un computador o de una tarjeta inteligente. (pág.230)

Los certificados digitales, imprescindibles en el comercio electrónico, son documentos firmados digitalmente por una entidad o persona denominada Autoridad Certificante (CA) y tienen como finalidad constatar la identidad de la misma y vincularla con su clave encriptada. Estos certificados también posibilitan cifrar las comunicaciones en Internet, protegiendo su confidencialidad e integridad. Cuando un usuario recibe el certificado

digital del sitio web al cual se conectó le permite verificar en primer lugar la autenticidad del sitio y de la comunicación.

Según el tipo de certificado, está constituido por un archivo que contiene en general información personal de su dueño: nombre, dirección, correo electrónico, número de tarjeta de crédito, clave pública del remitente. Mediante esta última clave, se podrá verificar la firma digital dado que el mensaje fue encriptado en su origen mediante la clave privada del emisor o remitente. También se incluye el nombre de la autoridad certificante que emitió el certificado, fecha de emisión del mismo, fecha de caducidad o período de validez y la firma del mismo realizada por la autoridad certificante.

En el comercio electrónico, cuando el navegador del usuario se conecta al servidor del sitio web del vendedor recibe el certificado digital que le posibilita autenticarlo. En el certificado, recibe también la clave pública que le permitirá encriptar la clave de sesión.

También es posible realizar la identificación del certificado digital del servidor con la autoridad de certificación que lo emitió. La clave de sesión se utiliza para cifrar toda la comunicación entre el usuario y el sitio web empleando un método de cifrado simétrico, que como se explicó anteriormente es mucho más rápido que el asimétrico. La validez de los certificados digitales es generalmente de un año y cuando expiran, la entidad o el usuario deben obtener uno nuevo. Generalmente la breve duración de los certificados se justifica en disminuir la probabilidad de que la clave privada sea violada y de esta forma, aumentar la confianza de los usuarios en el sistema de claves públicas. No obstante, debemos destacar que existe un negocio muy rentable en la exigencia de renovación de los certificados.

El formato de certificados X.509 es un estándar del ITU-T (*International Telecommunication Union-Telecommunication Standarization Sector*) y del ISO/IEC (*International Standards Organization / International Electrotechnical Commission*) que se publicó por primera vez en 1988.). Es muy utilizado para verificar la identidad de una persona y está basado en clave pública. En la figura 24 se detallan los campos principales del certificado.

Versión. El campo de versión contiene el número de versión del certificado codificado. Los valores aceptables son 1, 2 y 3.

Número de serie del certificado. Este campo es un entero asignado por la autoridad certificadora. Cada certificado emitido por una CA debe tener un número de serie único.

Identificador del algoritmo de firmado. Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).

Nombre del emisor. Este campo identifica la CA que ha firmado y emitido el certificado.

Periodo de validez. Este campo indica el periodo de tiempo durante el cual el certificado es válido y la CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.

Nombre del sujeto. Este campo identifica la identidad cuya clave pública está certificada en el campo siguiente. El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.

Información de clave pública del sujeto. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

Identificador único del emisor. Este es un campo opcional que permite reutilizar nombres de emisor.

Identificador único del sujeto. Este es un campo opcional que permite reutilizar nombres de sujeto.

Figura 24: Campos principales del certificado X.509 v3
Fuente: Universidad Politécnica de Valencia (2017)

Datos estándar que contienen los certificados digitales:

- Nombre del titular del certificado
- Tipo y número de documento de identidad del titular
- Clave pública del titular
- Algoritmo de cifrado asimétrico utilizado
- Número de serie del certificado
- Periodo de vigencia del certificado

- Nombre de la Autoridad de Certificación (CA) que emitió el certificado
- Firma Digital de la Autoridad de Certificación (CA) que emitió el certificado
- Direcciones de Internet:
    - Del manual de Procedimientos, Políticas de Certificación y Términos y Condiciones para la obtención de Certificados
    - De la lista de certificados revocados
    - De las condiciones de emisión del certificado y utilización del mismo

Con respecto a las propiedades de los certificados de clave pública, Acebey & Terrazas (2006) nos dicen que las características más importantes de los certificados digitales son:

> • Autentificación. Para el receptor de un documento, la autentificación implica asegurar que los datos recibidos han sido enviados por quien declara ser poseedor de la identidad contenida en la firma digital.
> • Confidencialidad. La confidencialidad implica asegurar que la información enviada no podrá ser interceptada por terceros.
> • Integridad. La integridad de los documentos implica tanto para el remitente como para el destinatario asegurar que la información enviada no será modificada por terceros.
> • Privacidad. La privacidad de los mensajes implica que los datos sólo podrán ser leídos por el destinatario por contener elementos cifrados.
> • No repudio. El no repudio implica para el receptor de un mensaje asegurar que el emisor no negará haber enviado la información recibida. (pág. 591)

No se ha instalado un firewall para el control del tráfico de paquetes entrantes y salientes del sitio, mediante el empleo de filtros y programas proxy

Los firewalls son dispositivos que restringen el acceso a redes protegidas desde Internet u otras redes. Al respecto Tanenbaum A. (2003), dice:

> Los *firewalls* (servidores de seguridad) son simplemente una adaptación moderna de la vieja estrategia medieval de seguridad: excavar un foso defensivo profundo alrededor de su castillo. Este diseño obligaba a que todos los que entraran o salieran del castillo pasaran a través de un puente levadizo, en donde los encargados de la E/S los podían inspeccionar. En las redes es posible el mismo truco: una compañía puede tener muchas

> LANs conectadas de forma arbitrarias, pero se obliga a que todo el tráfico desde o hacia la compañía pase a través de un puente levadizo electrónico (*firewall*) (pág.776).

Los firewalls protegen los sitios web de los ataques típicos que se ciernen sobre las transacciones de comercio electrónico. Los más frecuentes son los siguientes:

Man in the middle (hombre en el medio): como se explicó con anterioridad en este capítulo, consiste en capturar el tráfico intercambiado entre dos usuarios confiables. Para tener éxito, el atacante debe tener acceso al tráfico intercambiado en la red entre ambos, por ejemplo, si se encuentra en la misma red Wi-Fi del usuario. De esta forma puede disponer de la cookie de sesión que autentica al usuario ante sitio web y una vez en posesión de ella acceder a las páginas donde el usuario legítimo estaba habilitado.

Man in the browser (Hombre en el navegador): consiste en la instalación en el navegador web del usuario de software malware (software malicioso constituido por: troyanos, *key loggers, spywares,* etc.) cuya finalidad es tomar el control del computador en diversas formas.

Para proteger a los sitios web y específicamente a las redes en las cuales estos están instalados, los firewalls cuentan con las siguientes funciones básicas:

- Filtrado de Paquetes
- Programas Proxy
- Traducción de direcciones de red
- Implementación de redes privadas virtuales
- Registro del tráfico que circula desde y hacia la red protegida

> Los sistemas que efectúan filtrado de paquetes encaminan los paquetes entre host internos y externos, pero lo hacen selectivamente. Ellos permiten o bloquean ciertos tipos de paquetes de acuerdo a la política de seguridad del sitio (…) El tipo de ruteo que se emplean en el filtrado de paquetes del firewall se lo conoce como *screening router*[169] (Zwicky E. Cooper S., Chapman B, 2000, pág.105).

[169] SCREENING ROUTER: Son equipos enrutadores utilizados como firewall para el filtrado de paquetes generalmente en el acceso a redes internas protegidas.

El filtrado de paquetes se caracteriza porque éstos son aceptados o rechazados en función del contenido de su cabecera, teniendo en cuenta las reglas preestablecidas. La información que se analiza proviene de las cabeceras del datagrama IP, del segmento TCP y de los datagramas UDP e ICMP. También se tiene en cuenta la interfase del firewall por la cual entra y/o sale el paquete. Los campos que se consideran son:

- Del paquete IP: direcciones IP fuente y destino y tipo de protocolo que transporta (puede ser TCP, UDP o ICMP)
- Del protocolo TCP: puerto origen y puerto destino, estado del *flag* ACK
- Del protocolo UDP: puerto origen y puerto destino
- Del protocolo ICMP: tipo de mensaje y tamaño
- Del firewall: interfase por la cual arriba y/o sale el paquete

La empresa Cisco se ha destacado por ser una de las primeras que sistematizo la configuración de los filtros IP a través de listas de acceso[170], al respecto Leinwand & Pinsky, (2001) agregan:

> Desde la primera vez que se conectaron varios sistemas para formar una red, ha existido una necesidad de restringir el acceso a determinados sistemas o partes de la red por motivos de seguridad, privacidad y otros (…) la capacidad de restringir el acceso cobra mayor importancia cuando la red de una empresa se conecta con otras redes externas, como otras empresas asociadas o Internet. (pag, 149)

Los programas proxy están diseñados para efectuar tareas específicas relativas a la inspección de los paquetes que no pueden ser realizadas por el proceso de filtrado de los firewalls. Estos programas responden a las políticas de seguridad del sitio y para llevar adelante su acción deben inspeccionar no sólo la cabecera del paquete sino también su campo de carga. Cuando se navega a través de un proxy, no se está accediendo directamente al servidor, sino que en realidad se efectúa una solicitud sobre el proxy y éste es quien se conecta con el servidor al cual se quiere acceder - siempre y cuando el paquete cumpla con las condiciones establecidas en el proxy-.

La técnica denominada Traducción de Direcciones de Red (NAT)[171] permite cambiar la dirección IP de origen en un datagrama e instalar en su lugar otra dirección, con la

[170] LISTAS DE ACCESO: Conjunto de reglas que leídas secuencialmente por el router controlan el acceso de los paquetes.

finalidad de ocultar la verdadera de origen del datagrama. La operación NAT del firewall cambia la dirección IP origen por una dirección común en el datagrama IP, también el puerto en el segmento TCP o en el datagrama UDP.

La aplicación NAT lleva el registro exacto de los cambios efectuados, de tal manera que los paquetes del tráfico entrante, relacionados con los que previamente salieron del firewall, tienen que estar dirigidos a la IP común insertada por el firewall en el paquete de salida y referenciarse al puerto en uso. La operación NAT también puede utilizarse para compartir una sola dirección IP de destino. De esta forma, pueden acceder varios dispositivos que quieren comunicarse simultáneamente a un mismo servidor y/o aplicación.

Otra facilidad de los firewalls es la implementación de redes privadas virtuales (VPN), cuyas características se detallaron precedentemente.

Por último, los firewalls tienen una facilidad muy importante para la auditoria de los eventos de seguridad que se basa en el registro del tráfico que circula desde y hacia la red protegida y que lo hace a través del firewall. El análisis de los *logs* o registros posibilita reconstruir los eventos que causaron incidentes de seguridad, como así también, los relativos a fallas de funcionamiento no fraudulentas.

En el comercio electrónico es fundamental que la red del sitio web del vendedor este protegida en su conexión a Internet mediante un firewall, que restrinja el tráfico entrante y saliente del sitio y lo limite a lo necesario para mantener la disponibilidad del servicio.

El ataque *phishing* a la estación del usuario implementado a través de sitios web falsos o simulados

Uno de los principales problemas de seguridad para los usuarios que acceden a sitios web en Internet son los sitios inseguros o falsos, a través de los cuales se puede sufrir un ataque por parte de códigos maliciosos instalados en ellos. Este consiste en el robo de información sensible del usuario, quien cree que está conectado al sitio web verdadero y brinda, en consecuencia, su información confidencial.

[171] NAT: Network Address Translation

Existen numerosos incidentes de seguridad basados en accesos a páginas clonadas, al respecto Tirante J.C. (2006) dice:

> Durante el 2003, en el feriado de marzo, durante los Carnavales, los clientes de los Bancos ITAU, Bradesco e Do Brasil, recibieron un e-mail donde les ofrecieron participar en concursos con importantes premios, viajes, coches, etc., solo había que responder una pregunta, eso sí, para ingresar al cuestionario tenía que dejar el nombre de usuario y clave que usaba en la entidad bancaria. Para darle mayor veracidad al trámite las páginas web de los bancos fueron clonadas. (pág.90)

La descarga de estos códigos maliciosos o *malware* ocurre en la mayoría de los casos mediante la utilización de la ingeniería social, que se aprovecha de la curiosidad, codicia y credulidad humanas para hacer que los usuarios realicen acciones que generen la descarga de *malware*.

Kevin Mitnicck, fue uno de los delincuentes informáticos más notorio en EEUU hasta que fue detenido en 1999. Sin usar tecnología sofisticada y mediante técnicas de engaño sencillas lograba obtener contraseñas, números de seguro social, de cuentas bancarias y tarjetas de crédito, etc.

El *Phishing* (pesca) es una técnica que se basa en el envío de mensajes y/o mails masivos a efectos de que el usuario se conecte a la versión falsa de un sitio verdadero y al hacerlo revele información confidencial. Los ataques de *phishing* son una de las formas de delito más extendida y de mayor crecimiento en el comercio electrónico.

Existe una variante denominada *spear phishing* (pesca con arpón), que consiste en seleccionar un cliente de un negocio, empresa o entidad bancaria, fingir ser alguna de esas entidades y enviarle un correo para verificar su cuenta con la entidad.

Al hacer clic en el link que recibe, el usuario es direccionado hacia un sitio web controlado por el atacante, donde se le pedirá que introduzca datos confidenciales sobre sus cuentas. Parece muy trivial el engaño, pero estos *phishers* o pescadores envían miles de estos mensajes diariamente y un porcentaje de usuarios caen en la trampa.

Traver Laudon, (2013) afirma:

> Los ataques de *phishing* no incluyen código malicioso, sino que se basan en una impostura y un fraude directos denominados técnicas de Ingeniería social. El ataque de *phishing* más popular es la carta de estafas enviada por correo electrónico.
>
> La estafa empieza con un correo electrónico, a saber: un rico ex ministro petrolero de Nigeria busca una cuenta bancaria donde poder ocultar millones de dólares por un corto periodo, y le pide a usted su número de cuenta bancaria para depositar el dinero. A cambio, usted recibirá un millón de dólares. Este tipo de estafa por correo electrónico se conoce popularmente como la carta nigeriana. (pág.275)

Cuando la técnica se dirige al robo de información privada de personajes importantes o simplemente de gran transcendencia social (empresarios, cantantes, artistas, famosos, etc.) se denomina *whailing*, término que expresa un juego de palabras entre *whale* (ballena) y *phishing* (pescar).

Si bien la falsificación de sitios web no ataca archivos o al servidor de la red, ocasiona una amenaza importante a la integridad del sitio verdadero. Si la intensión es dañar la imagen de la empresa, los hackers pueden, por ejemplo, alterar los pedidos -modificando cantidades y/o direcciones de envió- lo cual origina la decepción en los clientes del sitio verdadero.
En el Reporte Global sobre Fraude, desarrollado por la firma Kroll (2001) se indican estrategias que se emplean, utilizando la red Internet y tecnologías emergentes, para afectar la imagen de las empresas y ocasionar daños a las mismas. (Kroll, 2011)

Existen navegadores como el Mozilla Firefox que ya incorporan una protección frente a sitios web peligrosos y cuando detectan que se quiere acceder uno de ellos, bloquean la navegación. Los propios usuarios son los que mantienen actualizada la base de datos del navegador respecto de los sitios web inseguros.

También para evitar el acceso a sitios web fraudulentos se pueden emplear aplicaciones y herramientas que informan sobre la seguridad o no del sitio web al cual se quiere acceder.

Algunas de las más populares son: Norton Safe Web, McAfee Site Advisor y ScanURLnet. En la figura 25 se puede observar la página de acceso a esta última herramienta.

Figura 25: Verificación de la URL de un sitio Web
Fuente: Scanurl (2017)

Con respecto a las tácticas de falsificación Traver L (2013) agrega:

> Los hackers que tratan de ocultar su verdadera identidad a menudo emplean tácticas de falsificación (*spoofing*)[172], presentándose con direcciones de correo electrónico falsas o haciéndose pasar por otra persona. La falsificación de un sitio web también se conoce como *pharming*, consiste en redirigir un vínculo a un sitio web que no es el deseado, pero se enmascara como si lo fuera. Los vínculos diseñados para conducir a un sitio se pueden restablecer para enviar a los usuarios a un sitio que no tenga ninguna relación con el deseado, pero que si beneficia al hacker. (pag.281)

En el 2012 se formó la organización DMARC Org. constituida por importantes bancos, empresas de compras en línea como Amazon, PayPal, y otras, y las empresas proveedoras de servicios de correo electrónico como: Google, Microsoft, Yahoo, etc. y cuya finalidad es disminuir el número de correos electrónicos con *phishing* en Internet.

[172] SPOOFING: Técnicas mediante la cual un atacante se hace pasar por una entidad distinta falsificando los datos de la comunicación.

Ataques de denegación de servicio a los servidores de sitios web

Los ataques de denegación de servicios[173] y denegación de servicios distribuidos, (DoS)[174] y (DDoS) respectivamente, consisten en la conexión simultánea e intencional de miles de computadoras para saturar el servidor del sitio, generando que los usuarios legítimos no puedan conectarse a él. Son amenazas a la disponibilidad de los sitios web y, llegado el caso, pueden inhabilitarlos de manera definitiva.

> Estos ataques son costosos para sitios de comercio electrónico con mucho tráfico, pues mientras el sitio está cerrado los clientes no pueden realizar compras, y cuanto más tiempo dura cerrado un sitio más daño sufre su reputación. Aunque tales ataques no destruyen información ni acceden a las áreas restringidas del servidor, pueden destruir el negocio en línea de una empresa." (Traver L,, 2013, pág. 281)

Los ataques DDoS utilizan cientos o miles de computadoras distribuidas para atacar el servidor y la red destino.

No se controlan los datos introducidos por los usuarios en el sitio web, mediante le protocolo P3P

Para brindar a los usuarios que acceden y navegan en sitios web un control mayor del manejo que éste realiza de su información personal, se ha diseñado e implementado el protocolo Plataforma de Preferencias de Privacidad (P3P). Este protocolo permite además que los sitios Web declaren el uso que hacen de la información que recopilan de quienes los visitan.

El protocolo P3P fue desarrollado por el consorcio W3C[175] y puesto en servicio en el año 2002. Para su aplicación, tanto el sitio web como el navegador del usuario deben tenerlo habilitado y configurado.

[173] ATAQUE DENEGACION DE SERVICIOS: Tiene como objetivo lograr que un sitio o una aplicación sea inaccesible para los usuarios.
[174] DoS: Denial of Service
[175] W3C: World Wide Web Consortium

Según indica en el sitio CIPRES - UPM la Plataforma para Preferencias de Privacidad (P3P) es un conjunto de estándares y protocolos que permiten a los usuarios especificar sus requisitos en cuanto al uso de datos personales. Igualmente, P3P permite a un servidor Web especificar su política de protección de tales datos. Así, P3P puede avisar al usuario cuando visita un servidor Web cuyos criterios de protección de datos privados no satisface los requisitos especificados previamente. (Estudio de situacion del comercio electronico en España, 1999)

Como se explicó anteriormente en este capítulo, las cookies son pequeños archivos que los sitios web instalan en el navegador de las computadoras de sus usuarios, con la finalidad de crear un perfil que permita, entre otras actividades, seleccionar los anuncios publicitarios compatibles con sus intereses y relacionados con el tipo de páginas que visita en la web.

> Existen navegadores como Safari que directamente bloquean las cookies de terceros, es decir, las que no tienen que ver directamente con la página que se visita, sino las que proceden de los anunciantes. Internet Explorer de Microsoft usa otro principio frente a las cookies de terceros y sólo bloquea las que no cumplen el llamado formato P3P de preferencias de privacidad. Dicho formato permite al usuario decidir si permite o no que se usen cookies para personalizar la web que visita o para fines publicitarios (TECNO, 2012)

No se realiza la actualización permanente del software utilizado en el sitio web

Un aspecto relevante para la seguridad del sitio web es la actualización permanente del software del sitio.

> Históricamente, el software informático era una forma estática de tecnología. Se compraba un programa, se cargaba en el equipo y se utilizaba "tal cual" hasta que aparecía la siguiente versión. Sin embargo, ese modelo ya no es aplicable. El mundo digital actual está en constante cambio y, con el fin de que los últimos avances estén disponibles de inmediato, el software es ahora mucho más dinámico. Muchos programas pueden descargar actualizaciones por Internet e incorporar eficazmente la nueva tecnología en el software original. Claro está que no todas las actualizaciones son de vital importancia. Si se trata del software de un procesador de texto o un videojuego, no es fundamental actualizar el programa entre una versión y otra. No obstante, si se

> trata de software de seguridad, pasar por alto las actualizaciones puede tener consecuencias (Centro de Seguridad de Norton, 2017).

Los servidores son los sistemas más frecuentemente atacados de Internet y muchos usuarios y administradores son reacios a las actualizaciones, bien porque les genera trabajo adicional, porque consideran que no es necesario, o sencillamente desconocen qué les puede aportar una nueva versión.

Entre las ventajas de actualizar el software, la más importante es la mejora y actualización de la seguridad, por ejemplo, a partir de ataques maliciosos nuevos, para los cuales las versiones anteriores no disponían de solución alguna.

Hemos analizado que si bien el protocolo SSL/TLS tiene un nivel de seguridad aceptable, en realidad, su eficacia depende de dos factores importantes: uno es la versión del protocolo que se encuentra en servicio y el otro el procedimiento empleado en la implementación del mismo. Al respecto, se aclaró que en el caso de tener en servicio una versión antigua no actualizada del protocolo, y el atacante tomar conocimiento de ello, se podrían utilizar las falencias en la seguridad que siguen vigentes.

Pero la actualización del software posibilita también, en algunos casos, agregar nuevas funcionalidades y optimizar el funcionamiento del hardware. Cabe aclarar que tener actualizados el sistema operativo, software y aplicaciones no es suficiente; también es importante actualizar permanentemente el antivirus.

> A medida que las amenazas evolucionan, también lo hacen las tecnologías anti amenazas. Los expertos en seguridad como Symantec trabajan continuamente para anticiparse y responder ante nuevas formas de ataques. Una vez que se conoce un método de ataque novedoso, no pasa mucho tiempo hasta que Symantec encuentra una forma de identificar la amenaza, impedir su propagación y remediar sus efectos. No obstante, desarrollar tecnologías nuevas y estrategias de respuesta es sólo parte de la solución. Las últimas tecnologías y la información deben recorrer un camino que va desde el laboratorio de desarrollo hasta el equipo de escritorio de los usuarios. Es ahí donde las actualizaciones del programa e Internet entran en juego (Centro de Seguridad de Norton, 2017).

El protocolo SSL/TLS se emplea en los sistemas abiertos, por ejemplo, el OpenSSL es un desarrollo Open Source que los implementa en numerosos programas que utilizan el protocolo HTTPS.
Al respecto, podemos leer en el sitio HISPASEC[176]:

> El proyecto OpenSSL ha anunciado la publicación de una nueva versión de OpenSSL destinada a corregir una vulnerabilidad, calificada de gravedad alta, que podría permitir la realización de ataques de denegación de servicio.
>
> La vulnerabilidad, con CVE-2017-3733, reside en que si durante una renegociación se encuentra la extensión *Encrypt-Then-Mac* pero esta no estaba en la negociación original (o viceversa) se puede provocar una denegación de servicio (dependiendo de la suite de cifrado). Se ven afectados tanto clientes como servidores (Ropero, 2017)

Para solucionar esta vulnerabilidad del OpenSSL, se ha publicado la versión 1.1.

Deficiente seguridad física del sitio web y del servidor

La seguridad física del servidor y de los equipos de red asociados al sitio web del proveedor, son un aspecto muy importante que frecuentemente se descuida, dado que se requieren de una inversión importante para su implementación, como sería el caso de la construcción de una sala de red.

En primer lugar, la sala de red desde la cual opera todo el equipamiento del sitio web del vendedor, debería cumplir con los estándares de seguridad física certificados bajo las normas (UNE - EN 1047- 2)[177], (ABNT NBR 15.247)[178] y normas conexas.

Al disponer de ella se previene los efectos nocivos ocasionados por incidentes como el robo de equipos, incendios, tormentas, inundaciones, acciones de sabotaje interno y externo, cortes de energía eléctrica, condiciones climáticas extremas, etc.

[176] HISPASEC: Sitio web que brinda el servicio diario de información técnica en español sobre seguridad informática, creado por un grupo de especialistas con el propósito de divulgar y concienciar a los usuarios de la importancia de este sector en el campo de las nuevas tecnologías de la información.
[177] UNE-E 1047-2: Unidades de almacenamiento de seguridad. Clasificación y métodos de ensayo de resistencia al fuego.
[178] ABNT NBR 15.247: Esta norma específica los requisitos para salas cofre (salas de red).

No se realizan pruebas de vulnerabilidad del sitio web (pruebas de penetración)

Las aplicaciones de los sitios web que forman parte del sistema de comercio electrónico son objeto frecuente de ataques maliciosos que tratan de acceder a la información allí contenida. Por otro lado, los programadores, analistas y desarrolladores pueden dejar, sin saberlo o ex profeso, algún hueco de seguridad o alguna puerta trasera de acceso, que constituyen en definitiva el eslabón de debilidad del sistema.

Sin embargo, en los sistemas informáticos es una práctica común durante la implantación tratar de buscar el eslabón más débil antes que se presente a sí mismo y provoque la falla o incidente de seguridad no deseado.

Al respecto Senn (1992) agrega que "siempre hay que buscar el eslabón más débil en un sistema durante la implantación. Todo sistema tendrá uno – un talón de Aquiles, por así decirlo- A menudo, no será el sistema de información en sí ni la gente, los eslabones más débiles aparecen donde menos se les espera." (pág. 835)

Por ello, es conveniente estar al tanto de los riesgos que afectan a la aplicación web del sitio, para lo cual se deben efectuar pruebas de vulnerabilidades, que pueden realizarse mediante aplicaciones como: *Security* AppScan de IBM, Web *Application Security Scanner*, Grabber scanner u otras herramientas informáticas existentes en al mercado.

> IBM *Security* AppScan ayuda a las organizaciones a disminuir la probabilidad de ataques a aplicaciones web, así como costosas sustracciones de datos mediante la automatización de las pruebas de vulnerabilidad de la seguridad de las aplicaciones. Por otro lado, mejora la gestión de los programas de seguridad de las aplicaciones y refuerza la conformidad con la normativa. Gracias a la opción de exploración de su web y aplicaciones móviles antes del despliegue, AppScan permite identificar las vulnerabilidades de seguridad, generar informes y establecer recomendaciones (IBM, 2017)
>
> *Web Application Security Scanner* es un programa de software que realiza las pruebas de manera automática en una aplicación web e identifica las vulnerabilidades de seguridad. Grabber es un escáner de aplicaciones web agradable que puede detectar

muchas vulnerabilidades de seguridad en aplicaciones web. Realiza exploraciones y nos muestra en donde está el error (Gomez V. , 2015).

Para las pruebas de vulnerabilidad se deberían considerar los ataques más críticos a las aplicaciones de los sitios web de comercio electrónico como ser: ataques de inyección, exposición de datos sensibles, ataque *Cross Site Scripting* (XSS), ataque *Cross Site Request Forguery* (CSRF), ataque por redirecciones y reenvíos no válidos y perdida de autenticación.

El ataque de inyección consiste en el envío de código malicioso al sitio web por parte de usuarios o provenientes de otro sistema. Se contrarresta con la validación permanente de las entradas al sistema (inclusive de otras aplicaciones) y la separación de los datos confidenciales de los usuarios, de los comandos y consultas.

La exposición de datos sensibles se produce por no proteger los datos sensibles como los relativos a las tarjetas de crédito, direcciones y otros datos personales. Se contrarresta este ataque, básicamente cifrando la información sensible no sólo en el proceso de la transmisión, sino también en el almacenamiento de la misma en el sitio web. Además, es conveniente desactivar el almacenamiento en memoria cache y el mecanismo de autocompletar en los formularios para captura de datos.

El ataque *Cross Site Scripting* (XSS) consiste en la inserción, por parte de atacantes maliciosos, de cadenas de texto no validas en la aplicación web. La instalación de este código malicioso puede ocasionar la destrucción del sitio web o la captura de datos de las sesiones de usuarios. Se contrarresta mediante pruebas de análisis de código, uso de herramientas de escaneo y la validación permanente de los datos de entrada. Por ejemplo, lo primero que se debería hacer es limitar los caracteres que un usuario puede introducir en los campos de texto. Si se tiene un campo para introducir el nombre del usuario, no se debe dejar abierto para que se puedan introducir un número indefinido de caracteres, sino que se lo debería limitar por ejemplo a 10 o 20 caracteres.

Los desarrolladores web dejan pasar frecuentemente la vulnerabilidad XSS, por falta de planificación o por desconocimiento. En general se origina por la falta de mecanismos en el filtrado de los campos de entrada de la web, permitiendo el envío de datos e incluso la ejecución de scripts completos.

El ataque *Cross Site Request Forgery* (CSRF) consiste en obligar a un usuario que está autorizado a entrar en la aplicación, a ejecutar acciones no deseadas en ella. Mediante ingeniería social el atacante actúa a través de un chat o un enlace enviado por correo electrónico. Si el usuario objetivo es la cuenta del administrador, todo el sitio web estará en serio peligro. Para contrarrestar se requiere realizar pruebas de penetración y revisar el código fuente.

> Con respecto a las pruebas de penetración leemos en internet: "Prueba de penetración. Es la mejor opción para evidenciar debilidades y vulnerabilidades de una manera segura. También llamado a veces "hacking ético" es una evaluación activa de las medidas de seguridad de la información. En los entornos de red complejos actuales, la exposición potencial al riesgo es cada vez mayor y securizar los sistemas se convierten en un auténtico reto. A través del Test de Penetración es posible detectar el nivel de Seguridad Interna y Externa de los Sistemas de Información de la empresa, determinando el grado de acceso que tendría un atacante con intenciones maliciosas. Además, el servicio chequea las vulnerabilidades que pueden ser vistas y explotadas por individuos no autorizados, *crackers*, agentes de información, ladrones, antiguos empleados, competidores etc. (EcuRed, 2017).

El ataque por redirecciones y reenvíos no válidos consiste en el reenvío por parte de la aplicación web a otros sitios web sin una validación adecuada; generalmente el atacante dirige a las víctimas a sitios con malware o *phishing*. Se contrarresta realizando el mapeo del sitio para detectar redirecciones maliciosas, evitar el uso de *redirects o forwards* y no añadir los parámetros de usuario en el destino.

La pérdida de autenticación permite a un atacante suplantar la información de un determinado usuario, con la posibilidad de obtener una cuenta de administración para sabotear los registros de la aplicación y controles de autorización. Se contrarresta con una autenticación exigente, protección de los datos de sesión y evitar vulnerabilidades de tipo XSS (*Cross Site Scripting* - inserción de cadenas de texto no validas en la aplicación web).

No se aplican estándares de la industria relativos a la operación y mantenimiento de sitios web

La actividad de implementación, operación y mantenimiento de sitios web vinculados al comercio electrónico esta estandarizada a través de normas, las más difundidas son las denominadas Estandar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS)[179] ;las entidades que operan en comercio electrónico deben cumplir como mínimo con ellos, a efectos de proteger los datos de los usuarios titulares de las tarjetas, no dañar la reputación comercial de la empresa y minimizar los riesgos financieros. El objetivo de las normas PCI DSS es garantizar que los datos privados y sensibles de los titulares de tarjeta estén siempre resguardados.

> En 2004, Visa y MasterCard crearon un conjunto de procesos y requisitos de la industria –el Estándar de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI DSS, *Payment Card Industry Data Security Standard*, en sus siglas en inglés) apoyados por todos los sistemas internacionales de pago con tarjetas (….) en septiembre de 2006, entidades financieras, proveedores de servicios, fabricantes y comercios a través del Consejo de Seguridad de los Estándares de la Industria de las Tarjetas de Pago (PCI *Security Standards Council*), se hizo cargo de las normas PCI DSS y su actualización y desarrollo (VISA INTERNATIONAL, 2017)

Forman parte del PCI las principales empresas emisoras de tarjetas de crédito: Visa Inc., Mastercard Worldwide, American Express, JCB International y *Discover Financial Services* y tiene como misión fundamental evitar el fraude relacionado con las tarjetas de crédito o débito.

> Las Normas de seguridad de datos de la industria de tarjetas de pago (PCI DSS) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad uniformes a nivel mundial. Las PCI DSS proporcionan una referencia de requisitos técnicos y operativos desarrollados para proteger los datos de los titulares de tarjetas.
>
> Las PCI DSS se aplican a todas las entidades que participan en el procesamiento de tarjetas de pago, entre las que se incluyen comerciantes, procesadores, adquirientes,

[179] PCI DSS: Las empresas que procesan menos de 80,000 transacciones por año pueden realizar una autoevaluación utilizando un cuestionario provisto por el Consorcio del PCI. Las demás deben ser auditadas externamente.

entidades emisoras y proveedores de servicios, como también todas las demás entidades que almacenan, procesan o transmiten CHD (datos del titular de la tarjeta) o SAD (datos de autenticación confidenciales). (PCI Security Standards Council , 2013)

Cualquier empresa u organización que opere con tarjetas de débito y crédito debe cumplir de forma directa o bien a través de un control de compensación, con los 12 requisitos de la norma PCI DSS que siguen, extraídos de su sitio web (PCI Security Standards Council , 2013)

- Instalar y mantener una configuración de firewall para proteger los datos de los titulares de tarjetas.
- No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
- Proteger los datos almacenados de los titulares de tarjetas.
- Cifrar la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.
- Usar y actualizar con regularidad el software antivirus.
- Desarrollar y mantener sistemas y aplicaciones seguras.
- Limitar el acceso a los datos de los titulares, únicamente a lo que los negocios necesiten saber.
- Asignar una identificación única a cada persona con acceso a una computadora.
- Restringir el acceso físico a los datos de los titulares de tarjetas.
- Rastrear y monitorear todo acceso a los recursos de la red y a los datos de titulares de tarjetas.
- Probar con regularidad los sistemas y procesos de seguridad.
- Mantener una política que aborde la seguridad de la información.(pág. 5)

Ataques internos originados por el personal técnico del sitio web

Las vulnerabilidades del sistema en general se originan en muchos de los factores externos mencionados en este capítulo. No obstante, existe un factor interno que es una de las mayores amenazas en el sistema financiero y que está originado en el comportamiento y abuso de confianza del personal del sitio.

Los empleados administrativos, técnicos de mantenimiento, programadores, analistas, etc. tienen acceso a información clasificada y conocen las fortalezas y debilidades del sistema de seguridad del sitio.

Por este motivo pueden en muchos casos entrar libremente a los sistemas y bases de datos del sitio sin dejar rastros modificando los logs de seguridad de la aplicación. Cabe aclarar, que esto es posible en sistemas donde la política de seguridad es débil y los controles se efectúan de manera deficiente.

Son numerosos los ejemplos de destrucción de sitios, robo de datos de usuarios (tarjetas de crédito) y sustracción de datos personales, realizados por personal de confianza del sitio.

En algunos casos provocados por actitudes delictivas de agentes desleales y en otras, también muy numerosa, por negligencia e impericia del personal que por descuido expone datos confidenciales de usuarios que pueden ser explotados por hackers y/o terceros no autorizados.

Al respecto, en el informe *The value of corporate data* confeccionado por Forrester Research para Microsoft, y liberado en marzo del 2010, se indica que el 57% de las fugas de información de las empresas están asociados con accidentes de los empleados de dichas empresas, ocasionados por perdidas de computadoras personales, discos externos, *pendrives* y teléfonos inteligentes con información confidencial y/o sensibles de las empresas. (Forrester Research, 2010)

Toso los incidentes de seguridad mencionados nos hablan de pronósticos acerca del fraude en sus diferentes manifestaciones. Al respecto (Cano, 2013) sostiene que predecir las tendencias y comportamientos del fraude en un mundo gobernado por las comunicaciones y la información instantánea es una apuesta abierta y sin límites para encontrar en la inseguridad de la información nuevas razones para continuar aprendiendo (pag.146).

Debemos diferenciar entre hacer un pronóstico o una predicción, al respecto R.Ackoff, en su libro *Differences that make a difference,* establece que un pronóstico es una declaración de un futuro esperado basada en una proyección del pasado y del presente, mientras que, una predicción es una declaración de un futuro esperado que no está basado en hechos y datos. (Ackoff, 2001)

Conclusiones del capítulo 2: Las Vulnerabilidades en la seguridad del comercio electrónico, protocolos de red y de seguridad utilizados

En este capítulo se analizaron las condiciones que deben cumplirse en el proceso de comunicación, entre el host del usuario y el sitio web del vendedor, para materializar con éxito la transferencia de datos en las operaciones de comercio electrónico. Al respecto, se detallaron dos aspectos esenciales como son: la confiabilidad de la comunicación, que tiene como elemento fundamental la calidad de servicio y la seguridad informática durante toda la sesión correspondiente a la transmisión de datos. Para ello, se analizaron los protocolos de comunicaciones y de seguridad que brindan esas facilidades.

Se determinó que el protocolo de comunicaciones de nivel de transporte TCP, brinda confiabilidad a la comunicación entre el navegador en el host del usuario y la aplicación web en el servidor del vendedor. Por otro lado, se analizaron varios protocolos de seguridad y se concluyó que el SSL/TLS, debidamente actualizado e implementado, es el empleado mayoritariamente en el comercio electrónico por ofrecer seguridad a la comunicación. La consideración e inclusión de estos dos protocolos posibilitará completar la encuesta en lo concerniente a la consideración de la seguridad en la comunicación a través de Internet, entre el host del usuario y el servidor web del proveedor.

El protocolo TCP, perteneciente al nivel de transporte en la familia TCP/IP, está orientado a la conexión y dispone de calidad de servicio, brindando las siguientes facilidades para la comunicación: control de errores, control de flujo, control de congestión y administración de temporizadores para regular activamente las retrasmisiones. Por otro lado, también posibilita evitar la fragmentación a nivel IP, y establece conexiones en cada extremo de la comunicación, en base al número de puerto y dirección IP.

El TCP genera un paquete denominado segmento TCP que es transportado en la web a través de los datagramas IP. Si bien el protocolo IP no tiene calidad de servicio, esta función la provee el TCP, con lo cual queda garantizada la realización de una comunicación confiable.

La seguridad en la transmisión se implementa con el protocolo SSL/TLS, que utiliza en el nivel de transporte al protocolo TCP. El protocolo SSL, desarrollado en la década de los 90 por la Empresa NETSCAPE para ser incluido en su navegador web, proporciona

autenticación, integridad y confidencialidad en las comunicaciones a través de la red Internet, entre el navegador del cliente y el servidor del sitio web del proveedor, para lo cual emplea métodos criptográficos.

La implementación de protocolos que brindan seguridad, como es el caso del SSL/TLS, protegen las comunicaciones a través de la web del peligroso ataque denominado hombre en el medio (*man in the middle*) que consiste en alterar la información en tránsito, como así también, suplantar la identidad de alguno de los extremos de la comunicación. Mediante este ataque, se puede por ejemplo suplantar la identidad del banco con el cual un usuario se comunica (mediante *home banking*). De esta forma, terceros no autorizados tendrían acceso a las *passwords* de operación que utiliza el usuario para comunicarse. Estos ataques en su mayoría se basan en robar las cookies de sesión del usuario, las cuales se generan cuando este último se autentica al acceder a páginas Web.

Las cookies son archivos de texto pequeños que se guardan en el directorio del navegador o en carpetas de datos del mismo. Se crean cuando el navegador visita un sitio web que las utiliza para hacer un seguimiento de los movimientos por el sitio, ayudan a indicar dónde se dejó la navegación, recordar el inició de sesión y la selección de temas abordados, preferencias y otras funciones de personalización.

Si bien el protocolo SSL/TLS tiene un nivel de seguridad aceptable, éste depende de dos factores importantes: uno es la versión del protocolo que se encuentra en servicio y el otro factor es la implementación del protocolo. En el caso de tener en servicio una versión antigua no actualizada del SSL y el atacante tomar conocimiento de este hecho, podría utilizar las falencias conocidas en la seguridad de la vieja versión del protocolo - que siguen aún vigentes en la instalación dado que no se actualizó el mismo- para atacar el sitio web del proveedor.

Por otro lado, si un computador está controlado por un troyano o posee una configuración deficiente del SSL, es muy probable que se reciban ataques tendientes a engañar al usuario. Lo más probable es hacerle creer que se encuentra en una comunicación cifrada, cuando en realidad no lo está, por ejemplo, simulando el candado que se observa en una página web segura. Otras alternativas también empleadas son: forzar el uso de protocolos o algoritmos criptográficos con debilidades comprobadas e inducir a la aceptación de certificados digitales que no son válidos para el servidor al cual se desea conectar.

Además de requerir tener actualizado e implementado en forma adecuada el protocolo SSL/TLS, y con la finalidad de neutralizar eficazmente los ataques mencionados, es necesario efectuar procedimientos adicionales, como por ejemplo: escribir directamente la URL con el prefijo HTTPs en la barra de direcciones del navegador; no realizar la conexión si el certificado no es validado; verificar la firma del certificado digital del servidor web; instalar herramientas que fuercen naturalmente a la conexión HTTPs; activar en el navegador el protocolo OCSP (Online *Certificate Status Protocol* - Protocolo de comprobación del estado de un Certificado en línea) que posibilita determinar el estado de vigencia de un certificado digital X.509 mediante procedimientos que no se basan solo en el empleo de las listas de revocación de certificados; por último es necesario consultar y aplicar en forma sostenida las normas y procedimientos que regulan y/o promueven la seguridad en las aplicaciones web.

Al respecto, es conveniente seguir las recomendaciones contenidas en la documentación de la organización OWASP (Open Web *Application Security Project*), que es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que las aplicaciones web sean inseguras. Otro estándar de relevancia son las normas PCI DSS.

Existen otros protocolos como los IPsec, SSH, 3D Secure, iKP y SET que también brindan seguridad informática en la web. No obstante, en el comercio electrónico trazable el protocolo SSL/TLS se halla presente en todas las implementaciones.

Si bien estos protocolos presentan en algunos casos seguridad adicional, no sólo para el comprador sino también para los bancos y el vendedor, no han registrado gran difusión en la industria y básicamente, como se indicó anteriormente, el que se emplea en forma más difundida es el SSL/TLS.

Se consideró también en este capítulo el tema del pago online, donde la mayoría de las transacciones se efectúan mediante la tarjeta de crédito. No obstante, el vendedor no tiene ante sí dicha tarjeta sino solo los datos que bien podrían ser de una tarjeta que fue clonada o robada; por su parte, el comprador envía los datos confidenciales de su tarjeta de crédito al sitio web, sin conocer cómo éstos van a ser tratados. Para que la operación se realice de la forma más segura posible, se recomienda emplear una empresa intermediaria especializada en pagos por Internet o emplear el protocolo 3 DSecure, llamado "*Verified by*

Visa" y "*MasterCard Secure Code*", que permite garantizar la autenticación del propietario de la tarjeta y por lo tanto, evita los fraudes generados con números de tarjetas robadas.

Se concluyó el marco teórico relativo al comercio electrónico trazable operado mediante tarjetas de crédito, con el análisis de los factores técnicos y procedimientos más importantes que intervienen en la operatoria del sitio web. Éstos, pueden generar vulnerabilidades en la seguridad del sistema e influyen en la confianza no solo de los consumidores, sino también de los proveedores y entidades intermedias. La identificación de estos factores posibilitará completar la encuesta a desarrollar en el capítulo 3.

Se han analizado los aspectos relativos a las actividades delictivas cibernéticas en Internet, el costo de la información robada en dicha red y en especial los ataques al sitio web en el comercio electrónico y en particular con las tarjetas de crédito.

Se detallaron las variantes más frecuentes del delito cibernético que se verifican en la web, no solo para las aplicaciones de comercio electrónico, sino en general, para todas las aplicaciones. La mayoría de estos ataques se llevan a cabo mediante el denominado código malicioso o malware.

Por otro lado, se detallaron las amenazas que pueden afectar específicamente al sitio web. Allí las vulnerabilidades en la seguridad son las debilidades o falencias del sistema informático y/o del hardware que lo soporta, que pueden ser aprovechadas por atacantes para violar la seguridad con el objeto de causar daño en el sistema y/o en los datos.

Uno de los factores básicos para sustentar la confianza del usuario es el tema del certificado digital de los sitios web. Su función es relacionar la clave pública de una persona, empresa u organismo con su correspondiente entidad propietaria a través de un tercero, denominado Autoridad de Certificación (CA) en el cual se confía. Los certificados digitales se fundamentan en la firma digital.

Por otro lado, se evaluaron diferentes opciones para almacenar la firma digital siendo la más apropiada la que se basa en la utilización de un dispositivo inteligente, que cuente con microprocesador para crear y almacenar la clave privada.

En el caso del comercio electrónico, cuando el navegador del usuario se conecta mediante el protocolo SSL/TLS al servidor del sitio web del vendedor, recibe de éste el certificado digital que posibilita autenticar a ambos. También recibe en el certificado la clave pública del sitio web, lo cual permitirá al navegador del usuario encriptar la clave simétrica aleatoria de sesión que propone y enviársela al sitio para comenzar a operar. Por otro lado, la identificación del certificado digital del servidor se puede comprobar con la autoridad de certificación que lo emitió. La clave de sesión se utiliza para cifrar toda la comunicación entre el usuario y el sitio web, empleando un método de cifrado simétrico.

En lo relativo a las Autoridades de Certificación (CA) se indicó que pueden brindar en general certificados clase 1, 2, 3 y 4. El certificado digital clase 1 es el más sencillo y el de menor nivel de seguridad dado que provee un nombre y una dirección de correo electrónico. El certificado digital clase 2 tiene mayor nivel de seguridad que el anterior, dado que proporciona la identidad verificada por un tercero, la dirección y otras informaciones personales. Estos certificados son aptos para las compras o suscripciones online.

El certificado digital clase 3, requiere que la identidad sea verificada ante escribano público. Estos certificados suministran el mayor nivel de confianza que una persona puede requerir para su identificación electrónica y se utiliza especialmente en aplicaciones bancarias, comercio electrónico o servicios en línea. Por último, el certificado digital clase 4, además de los requerimientos inherentes al de clase 3, tiene la particularidad que se verifica y asegura la relación del individuo con una determinada organización o empresa a la cual dice pertenecer. Se emplea en el exclusivo mundo de los negocios.

También se analizaron los diferentes tipos de ataques a las transacciones mediante códigos maliciosos implementados desde los sitios web inseguros, basados principalmente en los ataques de "*Phishing*", "*Whailing*", "*Man en the middle*" y "*Man in the brouser*" y se detallaron las herramientas y aplicaciones que podrían contrarrestar los mismos, como por ejemplo las aplicaciones: Norton Safe Web, McAfee Site Advisor y ScanURLnet o el caso de navegadores como el Mozilla Firefox, que ya incorpora una protección frente a sitios web peligrosos y cuando detecta que se quiere acceder a uno de ellos bloquea la navegación.

Con referencia a la identificación del nivel de seguridad de las conexiones con sitios web, ésta se efectúa mediante el análisis de la URL del sitio. En principio se detalló que la misma debía comenzar con https://, lo cual significa que se opera con el protocolo SSL y en consecuencia, cuenta con el respaldo de una Autoridad Certificante. Si el sitio web trata de utilizar un certificado SSL falso, el navegador muestra un mensaje de alerta. También se indicó la información que brindan los certificados y el significado de los colores de la barra de estado de seguridad de los sitios en relación al nivel de seguridad de los mismos.

Se consideró también la protección de los datos en las bases de datos del sitio web que disponen de diferentes métodos de seguridad a efectos de impedir que personas no autorizadas accedan a los mismos para tomar conocimiento de éstos, para modificarlos o eliminarlos.

Los tres métodos analizados son el encriptado reversible, el encriptado irreversible (con funciones MD5 o SHA-1) y el denominado cifrado -*hash + Salt*-, donde el termino Salt es un texto o un conjunto de caracteres que varía de usuario en usuario; por ejemplo, podría ser el ID (identificación) de los mismos. En este caso se cifra la *password* más el ID del usuario. Como no puede haber dos ID iguales, aunque las *passwords* sean las mismas, el *hash* será diferente. Este es el método más seguro, en especial si se utiliza un cifrado *hashing* como el SHA-512.

Por otro lado, también se vio que la estructura de la base de datos tiene un elemento fundamental para acelerar la búsqueda de la información: el índice de la base de datos. Para buscar un elemento que está indexado solo hay que examinar si está en el índice y una vez hallado, se tendrá acceso al registro donde se encuentra el dato. Además, mediante el empleo del digito verificador se puede verificar la consistencia e integridad de los datos en los registros de la base.

En lo que concierne a la protección respecto de los ataques desde la red Internet, se analizaron las ventajas de proteger el sitio web mediante la instalación de un *firewall* en la red de acceso, que restrinja el tráfico al estrictamente autorizado y necesario, desde y hacia la red del sitio.

Las funciones básicas de los firewalls son el filtrado de paquetes para controlar el tráfico de los mismos (según reglas prefijadas en el *firewall*), la utilización de programas Proxy

para un control más exhaustivo del tráfico, la traducción de direcciones de red para ocultar la dirección IP verdadera y que la misma no quede expuesta en Internet, la implementación de redes privadas virtuales para generar túneles seguros en internet, y el registro del tráfico que circula desde y hacia el sitio web como medida para el análisis posterior de lo ocurrido en un incidente de seguridad.

Con respecto al control que pueden efectuar los usuarios respecto al uso que hacen los sitios web de sus datos, se ha diseñado e implementado el protocolo Plataforma de Preferencias de Privacidad (P3P) que además permite a los sitios Web declarar el uso que hacen de la información que recopilan de los usuarios que lo visitan, según la política de seguridad del sitio. Tanto el navegador del host del usuario como la aplicación web del sitio deben soportar el protocolo P3P para que el control tenga efecto.

Por otro lado, se detalló que un requerimiento básico de seguridad es la necesidad de la actualización permanente del software utilizado en el sitio: sistemas operativos, parches, antivirus, aplicaciones, herramientas informáticas, etc. En Internet los servidores son los sistemas más atacados y muchos usuarios y administradores son reacios a las actualizaciones, bien porque les genera trabajo adicional, o porque consideran que no es necesario o sencillamente desconocen qué les puede aportar una nueva versión. La ventaja de actualizar el software es que mejora de la seguridad, dado que se obtienen soluciones actualizadas para problemas de inseguridad por ejemplo, los basados en ataques maliciosos nuevos, para los cuales las versiones anteriores no disponían de solución alguna.

El protocolo SSL, utilizado en comercio electrónico, tiene un nivel de seguridad aceptable. No obstante, ese nivel depende de dos factores importantes: uno es la versión del protocolo que se encuentra en servicio y el otro factor es el procedimiento empleado en la implementación del protocolo. Al respecto, se aclaró que en el caso de tener en servicio una versión antigua no actualizada del protocolo y si el atacante tomar conocimiento de este hecho, se podrían utilizar las falencias en la seguridad que la versión vieja del protocolo posee, las cuales siguen vigentes en la instalación.

La actualización del software también posibilita en algunos casos agregar nuevas funcionalidades, como también, optimizar el hardware en su funcionamiento. Cabe aclarar que tener actualizados el sistema operativo, software y aplicaciones no es suficiente; también es importante actualizar permanentemente el antivirus.

Por otro lado, considerando que los sitios web, que forman parte del sistema de comercio electrónico son frecuentemente objeto de ataques maliciosos que tratan de acceder a la información allí contenida y/o dañar el sitio, es conveniente estar al tanto de los riesgos que afectan a la aplicación web. Para ello, se deberían efectuar pruebas de vulnerabilidad del sitio, también conocidas como pruebas de penetración, las cuales pueden realizarse mediante herramientas informáticas como: Security AppScan de IBM, Web *Application Security Scanner*, Grabber Scanner u otras existentes en al mercado.

Con respecto a los ataques más frecuentes a las aplicaciones en producción en los sitios web de comercio electrónico se citaron: ataques de inyección, ataque por exposición de datos sensibles, ataque Cross Site Scripting (XSS), ataque Cross Site Request Forguery (CSRF), ataque por redirecciones y reenvíos no válidos, pérdida de autenticación y ataques de negación de servicio DoS o DDoS.

Los ataques detallados se producen debido a las vulnerabilidades en la seguridad del sitio web del proveedor, las cuales, a su vez se originan en los siguientes factores:

- Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras y sin usar la facilidad CAPTCHA.

Las contraseñas o *passwods* seguras son difíciles de descifrar y su fortaleza radica en la longitud de la misma y en su composición. Con respecto a la longitud ésta debe tener como mínimo 8 caracteres y la composición debe contener caracteres, alfabéticos (mayúsculas y minúsculas), caracteres numéricos y de puntuación. Una contraseña de ocho caracteres que contenga números, letras mayúsculas y minúsculas y caracteres de puntuación tiene más de 30.000 combinaciones posibles comparada con una que sólo contenga letras en minúscula. En la web existen generadores gratuitos, como por ejemplo el Norton *Identity Safe*, para crear contraseñas seguras difíciles de descifrar o adivinar. En ellos se pueden seleccionar los criterios a emplear en la generación de las contraseñas.

Por otro lado, la facilidad CAPTCHA es un test de Turing público y automático para distinguir a los ordenadores de los humanos; es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta. Un CAPTCHA ayuda a proteger al usuario del spam y del descifrado de contraseñas, al requerir del usuario que complete una simple

prueba que demuestre que se está en presencia de un humano y no un ordenador que intenta acceder a una cuenta protegida con contraseña.

- Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web y deficiente protección de los mismos en la base de datos

En las transacciones de comercio electrónico todos los datos de los usuarios son almacenados en bases de datos, que deben disponer de diferentes mecanismos de seguridad a efectos que a los datos no accedan personas no autorizadas y/o modificados.

Dado que en la base de datos se almacenan contenidos críticos, que hacen a la confidencialidad de la transacción, es un punto del sistema de comercio electrónico muy codiciado por los hackers y constituyen una verdadera amenaza contra la seguridad, porque tratan de acceder a su lectura, a modificarlos y en otros casos a borrarlos. Pero estas amenazas fraudulentas no son las únicas, también se pueden producir riesgos accidentales, producto de una operación incorrecta de la base de datos por parte del personal que la administra o por errores de hardware y/o software.

Para proteger la información de la base de datos se pueden guardar ~~los datos~~ encriptados mediante tres procedimientos: con cifrado reversible, cifrado irreversible aplicando una función hash con guarda del hash obtenido, y por último se podría aplicar una función *hash + salt* y guardar el *hash* obtenido.

Para la validación, detección de errores y verificación de la consistencia e integridad de los registros de la base de datos se emplea el digito verificador, que posibilita verificar la corrección de cada dato. Consiste en uno o más caracteres añadidos al dato original y calculado mediante determinado algoritmo, como por ejemplo el método 11[180]

- No se realiza el registro de las acciones de los usuarios en bitácoras o "*logs*" del servidor

Al ingresar un usuario al sitio web, toda la actividad que realice debería quedar registrada en "*logs*" o bitácoras que son tablas ubicadas en la base de datos, las cuales están

[180] MODULO 11: Es un método de detección de errores en un solo dígito e intercambios simples o dobles, aplica un factor de verificación ponderado a cada uno de los dígitos originales.

indexadas según el código que identifica al usuario y que posibilitan, en caso de que se produzca algún incidente de seguridad o de operación, que el mismo quede registrado para su análisis y/o recuperación posterior.

Estos registros posibilitan al administrador del sitio la localización de errores, detectar ataques maliciosos y hasta conocer que hacen los usuarios en el sistema, la fecha y hora en la que acceden, etc.

- No se efectúa el control de los datos introducidos por los usuarios en el sitio web

Normalmente los usuarios deben ingresar datos al sitio web, como podrían ser los relativos a la tarjeta de crédito u otros. En este aspecto se debe proteger al sitio web de sentencias maliciosas (SQL *Injection*), que modifican la operatoria de la aplicación y originan la ejecución de códigos maliciosos. Una medida de prevención recomendada es la incorporación de códigos de control en los formularios que los usuarios deben utilizar para llenar los datos que se les solicita; en caso que éstos contengan errores o sentencias maliciosas deberían aparecer los mensajes de alerta abortando la transacción preventivamente.

- No se obtienen los certificados digitales a través de una Autoridad de Certificación (CA)

Los certificados digitales son emitidos por un tercero denominado Autoridad de Certificación (CA) que puede ser un organismo o empresa privada. Las CA deben contar con enlaces de comunicaciones redundantes, copias de seguridad automatizadas (sistemas de almacenamiento de datos sofisticados) y mecanismos de recuperación en general, que aseguren una disponibilidad elevada del sistema en cualquier momento.

Las CA pueden brindar, en general, certificados clase 1, 2, 3 y 4. El Certificado digital clase 2, proporciona la identidad verificada por un tercero, la dirección y otras informaciones personales, por esta razón, estos certificados son aptos para las compras o suscripciones online, típicas del comercio electrónico.

El certificado digital identifica a un sitio web y en definitiva, si la conexión es segura o no lo es. En principio, debe comenzar la URL con https:// lo cual significa que se opera con el

protocolo SSL y en consecuencia cuenta con el respaldo de una Autoridad Certificante. Si el sitio web trata de utilizar un certificado SSL falso el navegador muestra un mensaje de alerta.

- No se ha instalado un firewall para el control del tráfico de paquetes entrantes y salientes del sitio, mediante el empleo de filtros y programas proxy

Los firewalls son una protección para los sitios web, de los ataques típicos que se ciernen sobre las transacciones de comercio electrónico. Para proteger los sitios y específicamente, a las redes en las cuales están instalados, los firewalls cuentan con las siguientes funciones básicas: filtrado de paquetes, programas proxy, traducción de direcciones de red, implementación de redes privadas virtuales, registro del tráfico que circula desde y hacia la red protegida.

En el comercio electrónico es fundamental que la red del sitio web del vendedor este protegida mediante un *firewall*, que restrinja el tráfico entrante y saliente del mismo y lo limite estrictamente al necesario para mantener la disponibilidad del servicio.

- El ataque *phishing* a la estación del usuario implementado a través de sitios web falsos o simulados

Uno de los principales problemas de seguridad para los usuarios que acceden a sitios web en Internet son los sitios inseguros o falsos, a través de los cuales se puede sufrir un ataque por parte de códigos maliciosos instalados en ellos. El ataque consiste en el robo de información sensible del usuario, quien el cual cree que está conectado al sitio web verdadero y brinda, en consecuencia, su información confidencial.

La descarga de estos códigos maliciosos o *malware*[181] ocurre en la mayoría de los casos mediante la utilización de la ingeniería social, que explora la curiosidad, codicia y credulidad humanas para hacer que los usuarios realicen acciones que generen la descarga de malware.

El *phishing* es una técnica que se basa en el envío de mensajes y/o mails masivos a efectos que el usuario se conecte a una versión falsa de un sitio y al hacerlo revele información

[181] MALWARE: Software malicioso, cuyo término fue ideado por Yisrael Radai en 1990.

confidencial. Los ataques de *phishing* son una de las formas de delito más extendida y de mayor crecimiento en el comercio electrónico.

- Ataques de denegación de servicio a los servidores de sitios web

Los ataques de denegación de servicios y denegación de servicios distribuidos, denominados DoS y DDoS respectivamente, consisten en la conexión simultánea e intencional de miles de computadoras para saturar al servidor del sitio, generando que los usuarios legítimos no puedan conectarse. Son amenazas a la disponibilidad de los sitios web y llegado el caso, pueden inhabilitarlos de manera definitiva.

- No se controlan los datos introducidos por los usuarios en el sitio web, mediante le protocolo P3P

Para brindar a los usuarios que acceden y navegan en sitios web un mayor control sobre el manejo que éste hace sobre su información personal, se ha diseñado e implementado el protocolo Plataforma de Preferencias de Privacidad (P3P) que también permite a los sitios Web declarar el uso de la información que recopilan de quienes lo visitan.

El protocolo P3P[182] permite a los usuarios especificar sus requisitos en cuanto al uso de datos personales. Por otro lado, posibilita que un servidor Web especifique su política de protección de tales datos. En igual sentido, P3P puede avisar al usuario cuando los requisitos especificados por el servidor WEB no cumplen los criterios de protección de sus datos.

- No se realiza la actualización permanente del software utilizado en el sitio web

Un aspecto relevante para la seguridad del sitio web es la actualización permanente del software del sitio. Los servidores son los sistemas más frecuentemente atacados de Internet, y muchos usuarios y administradores son reacios a las actualizaciones, bien porque les genera trabajo adicional, porque consideran que no es necesario, o sencillamente, desconocen qué les puede aportar una nueva versión

[182] PROTOCOLO P3P: Está constituido por un conjunto de estándares.

La ventaja de actualizar el software es la mejora de la seguridad, dado que se obtienen soluciones actualizadas para ataques maliciosos nuevos que las versiones anteriores no disponían.

Pero la actualización del software también posibilita en algunos casos, agregar nuevas funcionalidades, como así también, optimizar el hardware en su funcionamiento. Cabe aclarar que tener actualizados el sistema operativo, software y aplicaciones no es suficiente; también es importante actualizar permanentemente el antivirus y en el caso del comercio electrónico se debe actualizar permanentemente el protocolo SSL/TLS.

- Deficiente seguridad física del sitio web y del servidor

La seguridad física del servidor y de los equipos de red asociados al sitio web del proveedor, son un aspecto muy importante que frecuentemente se descuida, dado que se requiere de una inversión importante para su implementación, por ejemplo para la construcción de una sala de red.

Si el sitio web dispone de una sala de red certificada, se previene de los efectos nocivos ocasionados por incidentes como: robo de equipos, incendios, tormentas, inundaciones, acciones de sabotaje interno y externo, cortes de energía eléctrica, condiciones climáticas extremas.

- No se realizan pruebas de vulnerabilidad del sitio web (pruebas de penetración)

Estas pruebas deben realizarse periódicamente para evaluar el nivel de defensa del sitio a los ataques más críticos que se efectúan a las aplicaciones de los sitios web de comercio electrónico como ser: ataques de inyección, exposición de datos sensibles, ataque *Cross Site Scripting* (XSS), ataque *Cross Site Request Forguery* (CSRF), ataque por redirecciones y reenvíos no válidos y perdida de autenticación.

Para estar al tanto de los riesgos que afectan a la aplicación web del sitio se deben efectuar pruebas de vulnerabilidades, realizables mediante aplicaciones como: Security AppScan de IBM, Web *Application Security Scanner*, *Grabber scanner* u otras herramientas informáticas existentes en al mercado.

Para las pruebas de vulnerabilidad se debería considerar, entre otros, los ataques más críticos a las aplicaciones de los sitios web de comercio electrónico como ser: ataques de inyección, exposición de datos sensibles, ataque *Cross Site Scripting* (XSS), ataque *Cross Site Request Forguery* (CSRF), ataque por redirecciones y reenvíos no válidos y perdida de autenticación.

- No se aplican estándares de la industria relativos a la operación y mantenimiento de sitios web

La actividad de implementación, operación y mantenimiento de sitios web vinculados al comercio electrónico está estandarizada a través de normas. Las más difundidas son las denominadas Estandar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) y las entidades que operan en comercio electrónico deben cumplir como mínimo con ellos a efectos de proteger los datos de los usuarios titulares de las tarjetas, como así también, preservar la reputación comercial de la empresa y minimizar los riesgos financieros. El objetivo de las normas PCI DSS es garantizar que los datos privados y sensibles de los titulares de tarjeta estén siempre resguardados.

- Ataques internos originados por el personal técnico del sitio web

Las vulnerabilidades del sistema en general se originan en muchos de los factores externos mencionados en este capítulo. No obstante, existe un factor interno que es una de las mayores amenazas, por ejemplo en el sistema financiero, y que es el originado en el comportamiento y abuso de confianza del personal del sitio.

Dado que los empleados administrativos, técnicos de mantenimiento, programadores, analistas, etc. tienen acceso a información clasificada y conocen las fortalezas y debilidades del sistema de seguridad del sitio, pueden en muchos casos, entrar libremente a ellos y a las bases de datos del sitio, sin dejar rastros, modificando los logs de seguridad de la aplicación. Cabe aclarar, que esto es posible en sistemas donde la política de seguridad es débil y los controles se efectúan de manera deficiente.

Capítulo 3. La encuesta a futuros profesionales de TIC

Introducción

En los capítulos precedentes hemos analizado la estructura del comercio electrónico y los aspectos más relevantes de la seguridad del mismo, entre ellos, los protocolos empleados en los sistemas de comunicaciones y los protocolos que brindan seguridad informática, los métodos de cifrado y autenticación empleados y las vulnerabilidades más frecuentes presentes en los sitios web de los vendedores.

Los aspectos técnicos analizados permitieron describir el marco teórico general relativo a las vulnerabilidades de la seguridad del comercio electrónico trazable. En este capítulo se encara la tarea de conocer y evaluar la ponderación técnica de los futuros profesionales de TIC al respecto, a través de una encuesta.

Para hacerlo se analizarán las respuestas de estudiantes universitarios, de los dos últimos años de la carrera de la Licenciatura en Sistemas de Información de la Universidad de Buenos Aires, Facultad de Ciencias Económicas (UBA FCE) y de Ingeniería en Sistemas de Información de la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires (UTN FRBA).

En particular se evaluarán las predicciones que dichos estudiantes consideraron relevantes respecto de los componentes que presentan mayor nivel de vulnerabilidad en la seguridad del comercio electrónico, como también, el orden de importancia que le atribuyen a los factores determinantes que afectan la seguridad del sistema, en particular, los correspondientes al de mayor nivel de vulnerabilidad.

En primer término se realizó una encuesta piloto en un curso correspondiente a la materia Tecnología de Comunicaciones, de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires. Esto permitió ajustar formato y contenido hasta lograr el modelo de la encuesta final, que en la etapa correspondiente al trabajo de campo se aplicó a 110 estudiantes de las universidades mencionadas.

La investigación realizada, empírica y cuantitativa, posibilitará estudiar la relación entre las variables cuantificadas inherentes a la seguridad en el comercio electrónico. Para ello, se empleará el método de la estadística descriptiva a efectos de realizar el relevamiento de los datos cualitativos y su correspondiente análisis posterior.

La opinión técnica de los estudiantes (futuros profesionales de TIC) es relevante dado que serán los profesionales que posiblemente decidirán sobre las adecuaciones e innovaciones de los procedimientos y aplicaciones involucradas en el proceso de comercio electrónico.

Estos futuros profesionales muy probablemente se ocuparán tareas tales como el desarrollo y mantenimiento de aplicaciones informáticas, la administración de redes, la administración de bases de datos, la dirección de las áreas de sistemas tanto en organismos estatales como empresas, consultorías sobre comercio electrónico, el diseño de políticas de seguridad informática, control de calidad, etc. y en consecuencia, influirán decididamente desde esas áreas respecto a la evolución futura del sistema de comercio eléctrico.

Dada la amplia gama de posibilidades de esta modalidad de comercio, el estudio de la tesis consideró solo las operaciones trazables realizadas mediante tarjetas de crédito, excluyendo las transacciones efectuadas por pago electrónico.

Tampoco se incluyó en el análisis las vulnerabilidades relativas al computador y el navegador, que forman parte de la estación del usuario, dado que las variables son numerosas y ameritan un estudio específico aparte y que por otro lado,-sólo afectan a éste último y no a todo el sistema de comercio electrónico.

En el presente capítulo se analizarán en primer término las hipótesis de la tesis y su vinculación con las preguntas contenidas en la encuesta. Luego se evaluarán las respuestas a la encuesta piloto y las modificaciones que requirió, dando lugar a la consolidación de la encuesta definitiva.

Posteriormente se evaluarán las respuestas de los estudiantes a las ocho preguntas de la encuesta definitiva y su relación con el objetivo general y los objetivos específicos planteados en la tesis.

Por último, se detallarán los factores determinantes seleccionados por los estudiantes como los de mayor importancia e incidencia en la vulnerabilidad de la seguridad del sitio web del proveedor.

3.1. La encuesta y las hipótesis de la tesis

La encuesta posibilitará corroborar o desechar las hipótesis general y específicas del trabajo de tesis. En este sentido, la hipótesis general de esta investigación espera que los futuros profesionales de TIC determinen que el componente de mayor nivel de vulnerabilidad para la seguridad del comercio electrónico trazable se centraliza en el sitio web del proveedor, y ponderen el orden de importancia de los principales factores que afectan dicha seguridad.

Las hipótesis específicas que guiarán el trabajo y se articularán con la hipótesis general planteada, son cinco.

Como primera hipótesis específica se considera que el sistema de comercio electrónico trazable tiene como principales componentes: el host del cliente y su navegador web; las redes LAN e Internet, los protocolos de comunicaciones y de seguridad que brindan una conectividad confiable y segura; el sitio web del vendedor y entidades intermedias.

También se considera que los requerimientos mínimos de seguridad de toda operación online de comercio electrónico deben ser: autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto de los datos intercambiados, el no repudio que garantiza que la transacción es consentida por cada uno de los participantes y la disponibilidad de los datos y del sistema.

Se estima que, si se verifica que la transferencia de datos entre el host del usuario y el sitio web se efectúa a través de redes LAN e Internet mediante protocolos de comunicaciones con calidad de servicio como el Protocolo para el Control de las Transmisiones (TCP), que brinda confiabilidad[183]; y también con protocolos que brindan seguridad como el protocolo Nivel de Puertos Seguros/Nivel de Transporte Seguro (SSL/TLS), que autentica y encripta la comunicación; la vulnerabilidad principal en la seguridad del comercio electrónico no se produce en el transporte de datos entre el usuario y el sitio web del vendedor.

Se estima que el sitio web del vendedor es el componente del sistema de comercio electrónico que presenta mayor vulnerabilidad para la seguridad del sistema.

[183] CONFIABILIDAD: La confiabilidad en la comunicación forma parte de la calidad de servicio de esta última.

Se considera que la vulnerabilidad en la seguridad del sitio web del vendedor se debe a los siguientes factores, en orden de alta importancia decreciente: el sitio no está respaldado por una autoridad certificante; el acceso directo al sitio se efectúa sin el empleo de una contraseña seguras ni se efectúa la prueba de Turing[184] para diferenciar ordenadores de humanos (CAPTCHA); no se emplean los servicios de un *firewall* para limitar e inspeccionar el tráfico[185] entrante y saliente del sitio; existencia de sitios web falsos que utilizan el método de *phishing* que posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito; falta de actualización permanente del software utilizado en el sitio web; no se registran en el sitio las acciones de los usuarios en bases de datos o bitácoras[186] adecuadas; falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario; falta de validación de los datos antes de almacenarlos en el servidor de la empresa; seguridad física del servidor insuficiente; deslealtad del personal que opera la plataforma de e-Commerce del sitio; falta de realización de pruebas de vulnerabilidad del software[187] y de cumplimiento de las normas y estándares de la industria; y por último, el sitio web del vendedor no emplea el protocolo Plataforma de Preferencias de Privacidad (P3P) para el control, por parte de los usuarios, del uso que el sitio efectúa sobre sus datos personales.

3.2. Realización de la encuesta piloto

Para relevar la viabilidad de la encuesta propuesta, el 18 de octubre del 2016 se realizó una encuesta piloto[188] que se detalla en la figura 26.

Como se indicará antes, ésta se efectuó en un curso correspondiente a la materia Tecnología de Comunicaciones, de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

La estructura de la encuesta propuesta entonces, estaba conformada por las preguntas 1 a 8 cuyas respuestas admitían tres alternativas de respuesta: SI, NO y NO RESPONDE.

[184] PRUEBA DE TURING: Mide la capacidad de una máquina de exhibir un comportamiento inteligente similar al de un humano.
[185] TRAFICO ENTRANTE Y SALIENTE: Compuesto por datagramas IP.
[186] BASES DE DATOS O BITACORAS: Son archivos o bases de datos en los cuales se graba secuencialmente todos las acciones y eventos que se requieran registrar para su posterior análisis.
[187] PRUEBAS DE VULNERABILIDAD DEL SOFTWARE: Un método que se emplea con frecuencia son las pruebas FUZZING, mediante el cual se proveen datos al azar, inválidos y no esperados, de esa forma es posible comprobar la seguridad de la entrada en lo que respecta a la validación de datos.
[188] ENCUESTA PILOTO: Encuesta preliminar que se utiliza para ajusta el contenido de la encuesta definitiva.

Por su parte, las preguntas 9,10 y 11 se referían específicamente a la importancia dada a cada uno de los factores contribuyentes de las vulnerabilidades que afectan la seguridad del sitio web.

Se seleccionaron cinco factores para cada una de las vulnerabilidades del sitio, agrupados según estuvieran relacionados con: el usuario que se conecta al sitio; la implementación del sitio y la vinculación de éste con la red y los usuarios; y por último con el mantenimiento y operación del sitio web.

Para cada factor se contemplaba como respuesta alguna de siguientes alternativas: IMPORTANCIA ALTA, IMPORTANCIA MEDIA, IMPORTANCIA BAJA y NO RESPONDE.

Por último, en la pregunta 12 se requirió la opinión del alumno respecto al contenido y formato de la encuesta.

3.2.1. Análisis de las respuestas a la encuesta piloto

En la figura 27 se detallan los resultados de la encuesta piloto efectuada sobre un total de 20 estudiantes. Con referencia a su opinión, respecto al contenido y formato de la encuesta se puede observar (como lo indicado en la figura 28, que el 65% de los estudiantes estuvieron de acuerdo con la encuesta, efectuaron observaciones el 15% y no respondieron el 10%. Con respecto a los comentarios escritos por los estudiantes, los mismos fueron los siguientes:

Comentario N° 1: Es algo técnico pero la mayoría se puede contestar.
Comentario N° 2: Es un tema poco abordado, pero de gran importancia, el formato es sencillo.
Comentario N° 3: La encuesta es objetiva y un buen procedimiento para entrar en el debate del comercio electrónico.
Comentario N° 4: Adecuada.
Comentario N° 5: Rápida y clara. Fácil de responder y realizar un test de manera eficiente.
Comentario N° 6: Es apropiada para estudiantes o profesionales de sistemas.
Comentario N° 7: Es correcta y abarca muy bien los temas de seguridad informática.

Comentario N° 8: El formato de la encuesta es cómodo y fácil de responder y con respecto al contenido tal vez haya mucho que los usuarios comunes desconocen.

Comentario N° 9: Es adecuada para los estudiantes de sistemas de información, aunque un poco extensa, se podrían eliminar algunas preguntas obvias como la segunda.

Comentario N° 10: La encuesta es correcta, tal vez se debería incluir en las vulnerabilidades del sitio web el tema del *phishing*.

Comentario N° 11: Muy completa y clara.

Comentario N° 12: Muy buena.

Comentario N° 13: Interesante.

Comentario N° 14: La encuesta es fácil de responder, no obstante, se podrían eliminar preguntas como la segunda y tercera que no aportan mayor información.

Comentario N° 15: El formato y contenido es correcto.

Comentario N° 16: Muy completa la descripción de las vulnerabilidades del sitio web. La encuesta tiene un formato adecuado.

3.2.2. Modificaciones efectuadas en la encuesta definitiva en función de los resultados de la encuesta piloto

Para la adecuación y/o modificación de la encuesta propuesta se consideró prioritariamente la pregunta N° 12 y los comentarios a los que dio lugar, que fueron detallados precedentemente.

Del análisis de los mismos se deduce que fueron favorables al formato y contenido de la encuesta los comentarios N°: 1, 2, 3, 4, 5, 6, 7, 8, 11, 12, 13 y 15, mientras que los que efectuaron observaciones críticas fueron los comentarios N°: 9, 10 y 14. Por otro lado, la alternativa “NO RESPONDE” fue elegida por sólo el 10% de los encuestados.

VULNERABILIDADES DEL COMERCIO ELECTRONICO A TRAVES DE LA WEB

1. ***Se ha capacitado, mediante cursos y/o materias de grado, en seguridad informática y/o criptografía*?**

SI NO No responde

2. ***¿Le preocupa la seguridad informática cuando realiza una operación en la web de comercio electrónico?***

SI NO No responde

3. ***Los agentes básicos del sistema de comercio electrónico son: el comprador, el vendedor (comerciante o agente de venta) y la entidad de servicios financieros que autoriza el pago y ejecuta los movimientos de dinero correspondientes y los bancos.***
¿Coincide con esta composición de los agentes básicos del comercio electrónico?

SI NO No responde

4. ***En el comercio electrónico, desde el punto de vista del hardware y software, los principales componentes son: el host del cliente, su navegador web; la red Internet, los protocolos de comunicaciones y el sitio web del vendedor (servidor y aplicaciones).***
¿Coincide con esta composición relativa a los componentes principales (hardware y software) del comercio electrónico?

SI NO No responde

5. ***En las operaciones "online" de comercio electrónico, a efectos de garantizar la seguridad, se deberían considerar los siguientes aspectos relativos a la seguridad informática: la autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto a los datos del usuario, el no repudio, que asegura el consentimiento de la operación por cada uno de los participantes, y la disponibilidad de los datos.***
¿Esta de acuerdo con la necesidad de que se deben considerar en el comercio electrónico los aspectos de la seguridad informática arriba mencionados?

SI NO No responde

6. ***¿Considera que los protocolos TCP y SSL / TLS, empleados en las operaciones de comercio electrónico, garantizan una comunicación confiable y segura entre el equipo del usuario (navegador web) y el sitio Web del vendedor?***

SI NO No responde

7. ***¿Considera que la vulnerabilidad principal de la seguridad del comercio electrónico reside principalmente en el sitio web del vendedor?***

SI NO No responde

8. ***¿Es el phishing, implementado por sitios Web simulados o falsos, el mecanismo principal para engañar a los usuarios de comercio electrónico a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito?***

SI NO No responde

HOJA 1 de 2

NOTA: Considerar solo el comercio electrónico para operaciones trazables realizadas mediante tarjetas de crédito, no se incluye en el análisis las vulnerabilidades de la estación del usuario (computador y navegador web).

9. ***Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC) a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el usuario que se comunica con dicho sitio.***

Vulnerabilidades del sitio WEB relacionadas con el usuario	A	M	B	NC
Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.				
No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.				
Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.				
Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario				
No se emplea la facilidad "captcha" para el acceso de los usuarios al sitio web				

10. ***Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con la implementación y vinculación del sitio con la red y los usuarios.***

Vulnerabilidades del sitio WEB relacionadas con la implementación y vinculación del sitio con la red y los usuarios	A	M	B	NC
El sitio web no tiene la certificación vigente avalada por una autoridad certificante.				
En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.				
Falta de integración adecuada con empresas intermediarias dedicadas a soluciones de pago por Internet.				
No se emplean proxies en la conexión entre la red Internet y el entorno de la aplicación del sitio.				
El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.				

11. ***Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el mantenimiento y operación del sitio.***

Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web	A	M	B	NC
Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.				
Seguridad física del servidor deficiente.				
Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo.				
Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS.				
Deslealtad del personal que opera la plataforma de e-commerce del sitio.				

12. ***¿Cuál es su opinión respecto al contenido y formato de la encuesta?***
……..

HOJA 2 DE 2

Figura 26: Encuesta Piloto

TOTAL DE ENCUESTAS PILOTO: 20

Pregunta	Rta SI	Rta NO	Rta NC	% SI	% NO	% NC
1	5	15	0	25	75	0
2	18	2	0	90	10	0
3	15	3	2	75	15	10
4	13	5	2	65	25	10
5	19	1	0	95	5	0
6	15	2	3	75	10	15
7	16	3	1	80	15	5
8	14	2	4	70	10	20

Vulnerabilidades del sitio WEB relacionadas con el usuario	A	M	B	NC
Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.	15	4	1	0
No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.	9	7	3	1
Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.	8	9	3	0
Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario	3	11	4	2
No se emplea la facilidad "captcha" para el acceso de los usuarios al sitio web	3	8	8	1

Vulnerabilidades del sitio WEB relacionadas con la implementación y vinculación del sitio con la red y los usuarios	A	M	B	NC
El sitio web no tiene la certificación vigente avalada por una autoridad certificante.	15	5	0	0
En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.	15	4	1	0
Falta de integración adecuada con empresas intermediarias dedicadas a soluciones de pago por Internet.	7	10	3	0
No se emplean proxies en la conexión entre la red Internet y el entorno de la aplicación del sitio.	7	9	3	1
El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.	5	7	4	4

Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web	A	M	B	NC
Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.	15	4	1	0
Seguridad física del servidor deficiente.	12	6	2	0
Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo.	15	4	1	0
Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS.	6	5	3	6
Deslealtad del personal que opera la plataforma de e-commerce del sitio.	13	7	0	0

Respondieron la pregunta N° 12, relativa al contenido y formato de la encuesta: 16. (80%).

Figura 27: Resultados de la encuesta piloto
Fuente: Elaboración Propia

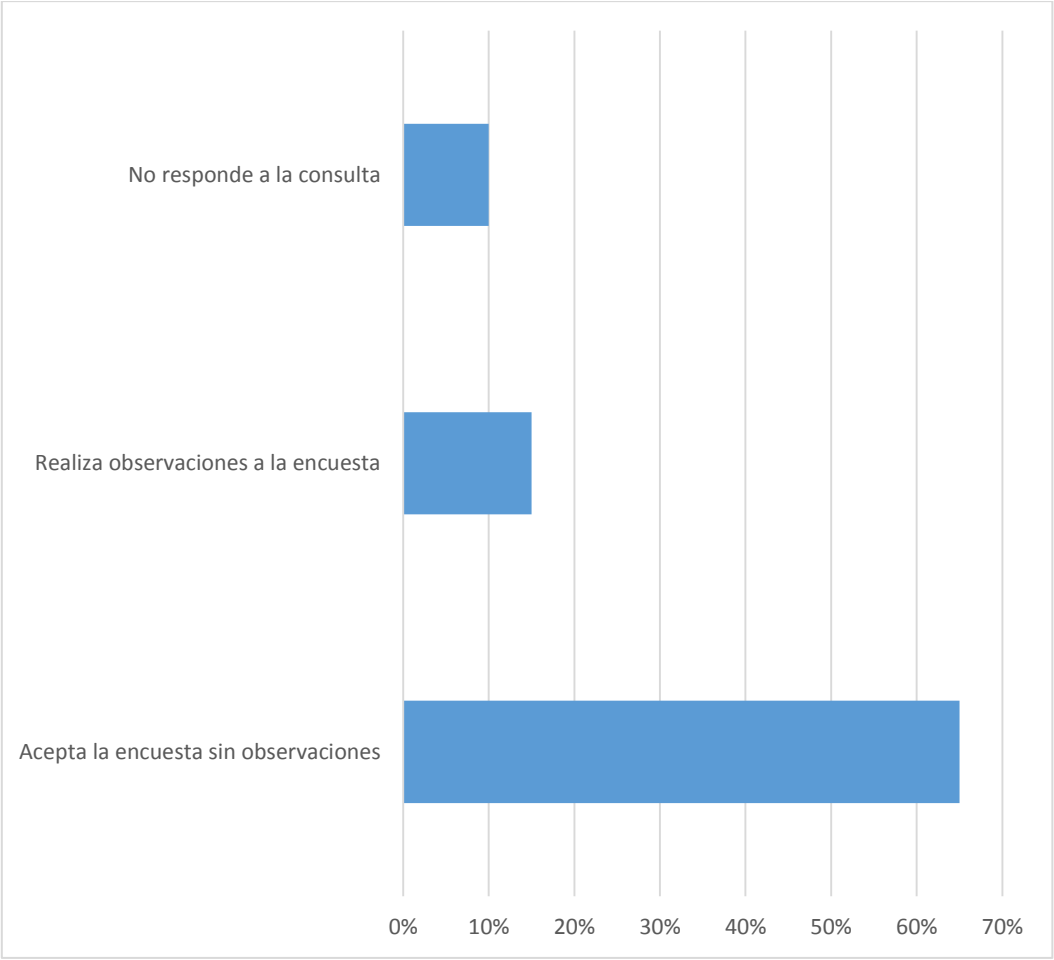


Figura 28: Respuestas a la pregunta N° 12 relativa al contenido y formato de la encuesta propuesta
Fuente: Elaboración Propia

Modificaciones a las preguntas 1 a 8 de la encuesta piloto

En la figura 29 se registran las respuestas a las preguntas 1 a 8. Del análisis de éstas surge que las preguntas 1, 2 y 5 fueron respondidas por el 100% de los estudiantes, las 3 y 4 tuvieron un 90% de estudiantes que respondieron, mientras que la 7 un 95%. La mayor proporción de no respuestas por parte de los estudiantes fueron la pregunta 6 referida a los protocolos TCP y SSL/TLS, con el 15%, y la pregunta 8, que indaga acerca del *phishihg* y su incumbencia en la captura de datos confidenciales con el 20%.

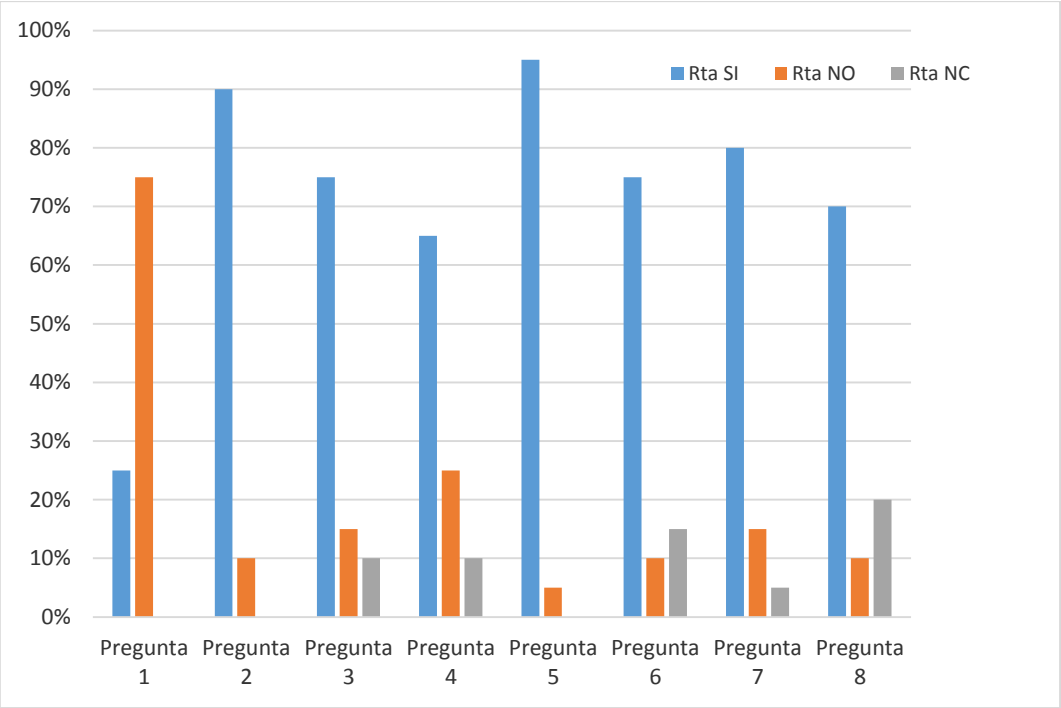


Figura 29: Respuestas a las preguntas 1 a 8 de la encuesta piloto
Fuente: Elaboración Propia

En el análisis efectuado, se relacionaron las respuestas de las preguntas 1 a 8 con los comentarios recibidos en la pregunta 12. En particular, se consideraron las observaciones que proponían eliminar preguntas obvias, como así también, aquellas planteadas en función del objetivo de la encuesta. De la evaluación se obtuvieron las siguientes conclusiones:

- La pregunta N° 2, relativa a la preocupación del alumno respecto a la seguridad informática cuando realiza operaciones de comercio electrónico, fue respondida por el 100% de los estudiantes y de ellos el 90% le preocupa el tema, mientras que sólo el 10% no.

  Por lo expuesto, se consideró que las respuestas a esta pregunta no aportaban información adicional o novedades respecto a las vulnerabilidades del comercio electrónico, dado que era esperable resultados similares en la encuesta definitiva, por lo cual, se eliminó esta pregunta.

- La pregunta N° 3 que consulta sobre los agentes básicos, también se eliminó debido que fueron conocidos por el 100% de los estudiantes y constituyó un concepto

elemental que no aportó elementos nuevos sobre las vulnerabilidades del comercio electrónico.

- La pregunta N°8 relativa al *phishing* tuvo un porcentaje medio/alto de desconocimiento por parte de los estudiantes, por lo cual, a efectos de facilitar su comprensión se incluyó entre los factores que afectan específicamente la vulnerabilidad del sitio web relacionadas con la implementación y/o vinculación del sitio con la red y los usuarios.

De esta forma se eliminaron en la encuesta definitiva las preguntas 2 y 3 y se modificó la 8.

Modificaciones a las preguntas 9 a 11 relativas a las vulnerabilidades del sitio web

Con respecto a las preguntas N° 9, 10 y 11, relativas a determinar la incidencia de cada uno de los factores que afectan la vulnerabilidad del sitio web y que tenían como opción de respuesta: alta, media, baja y no contesta, se obtuvieron los resultados abajo indicados.

Pregunta N°9:

"Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC) a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el usuario que se comunica con dicho sitio".

En la figura 30 se grafican los resultados, observándose que para los cinco factores considerados, el nivel de desconocimiento llega al 10% en uno de ellos (Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario), es menor para otros dos (no se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes y no se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web) y nulo para el resto (falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web y acceso directo de los usuarios sin el empleo de contraseñas seguras)

Por otro lado, no se recibió a través de la pregunta N° 12 ningún comentario crítico respecto de la complejidad en la comprensión de los cinco factores detallados para esta pregunta.

Por lo expuesto, no se realizaron modificaciones a esta pregunta conservando la indagación sobre los cinco factores considerados.

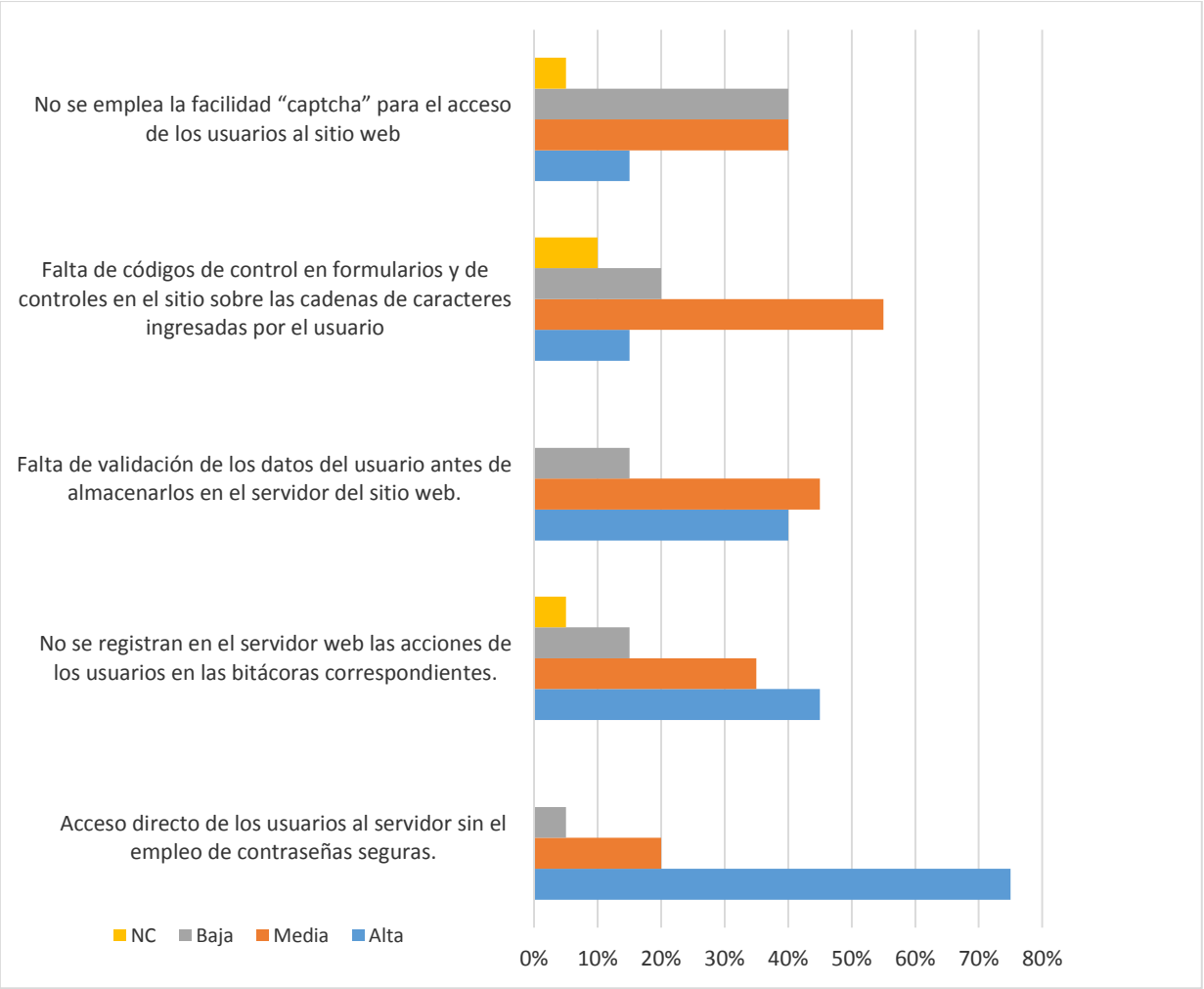


Figura 30: Vulnerabilidades del sitio WEB relacionadas con el usuario que se comunica con el sitio
Fuente: Elaboración Propia

Pregunta N°10:

“Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con la implementación y vinculación del sitio web con la red y los usuarios”.

En la figura 31 se grafican los resultados y se observa que de los cinco factores considerados para esta pregunta, tres (falta de integración adecuada con empresas intermediarias dedicadas a soluciones de pago por Internet; en el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio y el sitio web no emplea P3P) tuvieron un nivel de conocimiento total por parte de los estudiantes (NC = 0%).

Para el factor (no se emplean *proxis* entre la conexión a Internet y el sitio web) no respondió el 5% y para el factor relacionado con el protocolo P3P (*Platform for Privacy Preferences* - Plataforma de Preferencias de Privacidad) se obtuvo un nivel de desconocimiento del 20%, presumiblemente por tratarse de un protocolo específico aplicado a la política de seguridad informática de los sitios web.

Por otro lado, no se registraron en la pregunta N° 12 ningún comentario respecto a la complejidad en la comprensión de los cinco factores incluidos en la pregunta 10.

Por lo expuesto, no se realizaron modificaciones respecto a ellos, y solo se aclaró en las referencias de la encuesta definitiva el significado del acrónimo: P3P.

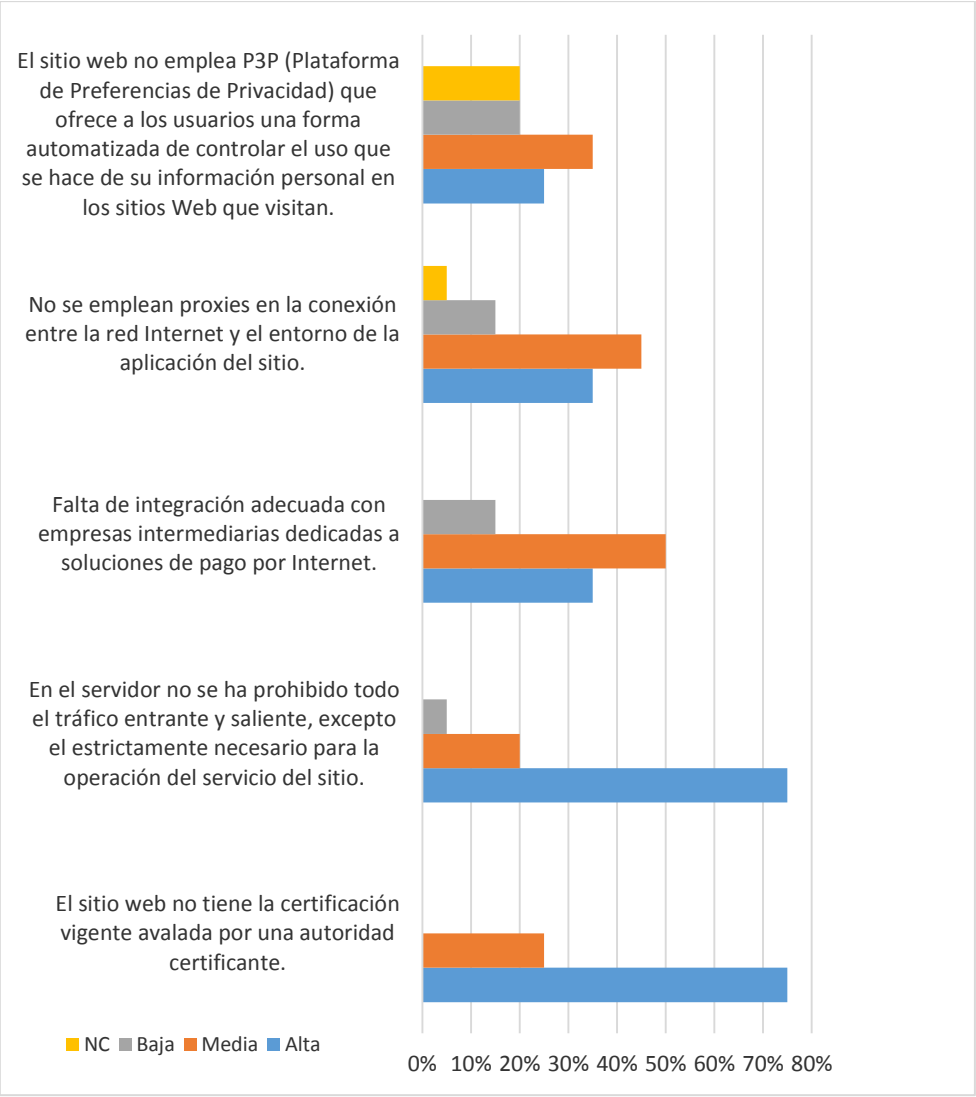


Figura 31: Vulnerabilidades del sitio WEB relacionadas con la implementación y vinculación del sitio con la red y los usuarios
Fuente: Elaboración Propia

Pregunta N°11:

"Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el mantenimiento y operación del sitio".

En la figura 32 se grafican los resultados y se observa que de los cinco factores considerados, cuatro (seguridad física del servidor deficiente; falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo; falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc. y deslealtad del personal que opera la plataforma de *e-commerce* del sitio) tuvieron un nivel de conocimiento total por

parte de los estudiantes (NC = 0%), sobre el restante factor (Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS) no respondió el 30%.

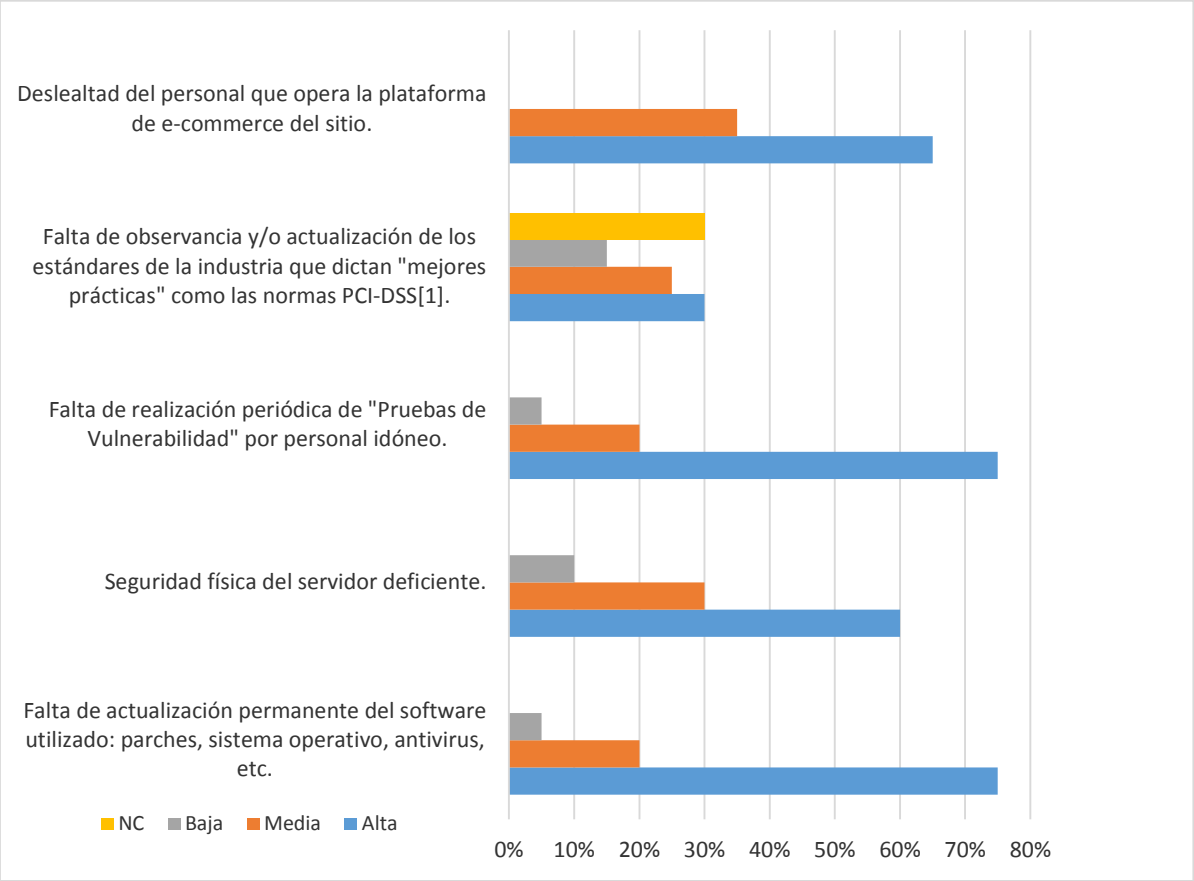


Figura 32: Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web
Fuente: Elaboración Propia.

Como en el caso anterior, la falta de respuesta se debió presumiblemente al desconocimiento por parte de los encuestados sobre los estándares de la industria que dictan mejores prácticas, como las normas PCI-DSS (*Payment Card Industry Data Security Standard* - Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago). Por otro lado, no se recibieron comentarios críticos como respuesta a la pregunta 12, respecto de la complejidad en la comprensión de los cinco factores mencionados en ~~de~~ la pregunta 11 lo que motivó a que no se realizaron modificaciones respecto a los cinco factores considerados en ella y solo se aclaró en referencias, el significado del acrónimo: PCI-DSS.

3.3. La encuesta definitiva

Al eliminar tres preguntas de la encuesta piloto, las preguntas 9, 10, y 11 (relativas al sitio web) pasaron a ser las 6,7 y 8 respectivamente en la encuesta, figura 33. El trabajo de campo se llevó a cabo durante la primera semana del mes de noviembre del 2016 en las carreras de Ingeniería en Sistemas de Información de la UTN, Facultad Regional Buenos Aires, y en la carrera de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires. El total de estudiantes encuestados fue 110 e incluyó a estudiantes de los dos últimos años de ambas carreras.

3.4. Resultados obtenidos en la encuesta para las preguntas 1 a 5

Se analizarán a continuación las respuestas de los estudiantes a los temas incluidos en las preguntas 1 a 5 de la encuesta. Se presentará cada tema, seguido del análisis de los resultados obtenidos en cada uno de ellos.

Pregunta 1: Nivel de capacitación en seguridad informática y/o criptografía por parte de los estudiantes

¿Se ha capacitado, mediante seminarios, cursos y/o materias de grado, en seguridad informática y/o criptografía?

Las respuestas a esta pregunta - presentadas en la figura 34- permiten dividir la muestra en dos submuestas según hayan realizado o no capacitación en el tema. La submuestra 1 está constituida por 49 estudiantes que tuvieron capacitación en seguridad informática y/o criptografía y las submuestra 2, por 61 estudiantes que no tuvieron capacitación en los temas mencionados.

La asignatura Seguridad Informática es una materia electiva en la carrera de Ingeniería en Sistemas de Información, por lo cual, los estudiantes que no optaron por esta materia no reciben la capacitación en esta temática.

Por otro lado, hasta el presente no se dispone en el plan de estudios de la Licenciatura ni tampoco en el de Ingeniería en Sistema de Información de la asignatura Criptografía. Si se puede obtener esta capacitación en cursos externos a las carreras mencionadas.

VULNERABILIDADES EN LA SEGURIDAD DEL COMERCIO ELECTRONICO A TRAVES DE LA WEB

1. **¿Se ha capacitado, mediante seminarios, cursos y/o materias de grado, en seguridad informática y/o criptografía?**

SI **NO** **No responde**

2. En el comercio electrónico, desde el punto de vista del hardware y software, los principales componentes son: el host del cliente, su navegador web; la red Internet, los protocolos de comunicaciones/seguridad y el sitio web del vendedor (servidor y aplicaciones informáticas).

¿Está de acuerdo que la descripción mencionada contiene los componentes principales (hardware y software) del comercio electrónico?

SI **NO** **No responde**

3. En las operaciones "online" de comercio electrónico, a efectos de garantizar la seguridad, se deberían considerar los siguientes aspectos relativos a la seguridad informática: la autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto a los datos del usuario, el no repudio, que asegura el consentimiento de la operación por cada uno de los participantes, y la disponibilidad de los datos.

¿**Esta de acuerdo considerar, en el comercio electrónico, los aspectos de la seguridad informática arriba mencionados como garantía de la seguridad?**

SI **NO** **No responde**

4.**¿Considera que los protocolos TCP y SSL / TLS, empleados en las operaciones de comercio electrónico, garantizan una comunicación confiable y segura entre el equipo del usuario (navegador web) y el sitio Web del vendedor?**

SI **NO** **No responde**

5.**¿Considera que la vulnerabilidad principal de la seguridad del comercio electrónico reside principalmente en el sitio web del vendedor?**

SI **NO** **No responde**

SSL / TLS: Secure Sockets Layer / Transport Layer Security- capa de puertos seguros / seguridad de la capa de transporte

NOTA: Considerar solo el comercio electrónico para operaciones trazables realizadas mediante tarjetas de crédito, no se incluye en el análisis las vulnerabilidades de la estación del usuario (computador y navegador web).

6. ***Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO RESPONDE (NR) a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el usuario que se comunica con dicho sitio.***

Vulnerabilidades del sitio WEB relacionadas con el usuario	A	M	B	NR
Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.				
No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.				
Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.				
Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario				
No se emplea la facilidad "captcha" para el acceso de los usuarios al sitio web				

7. Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con la implementación y/o vinculación del sitio con la red y los usuarios.

Vulnerabilidades del sitio WEB relacionadas con la implementación y/o vinculación del sitio con la red y los usuarios	A	M	B	NR
El sitio web no tiene la certificación vigente avalada por una autoridad certificante.				
En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.				
En sitios Web simulados o falsos el método de phishing posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito.				
No se emplean proxies en la conexión entre la red Internet y el entorno de la aplicación del sitio.				
El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.				

8. Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el mantenimiento y operación del sitio.

Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web	A	M	B	NR
Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.				
Seguridad física del servidor deficiente.				
Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo.				
Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS[2].				
Deslealtad del personal que opera la plataforma de e-commerce del sitio.				

Phishing: Método para intentar adquirir información confidencial de forma fraudulenta.
[2] PCI DSS: Payment Card Industry Data Security Standard - Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago. **Hoja 2 de 2**

Figura 33: Encuesta definitiva
Fuente: Elaboración Propia

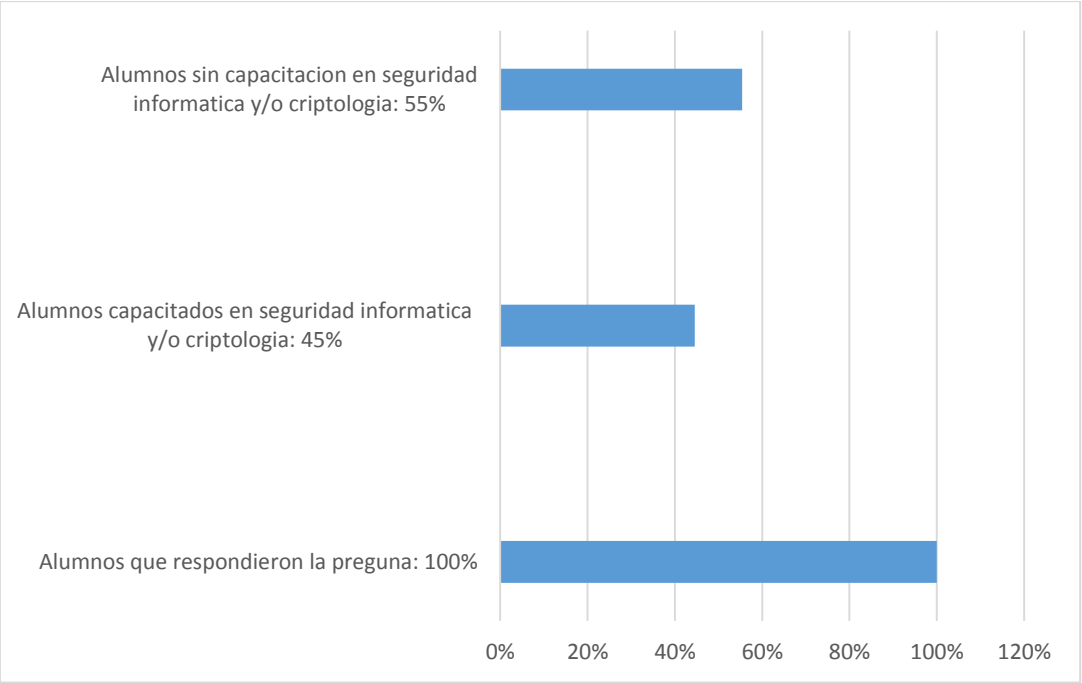


Figura 34: Capacitación de los estudiantes en seguridad informática y/o criptografía
Fuente: Elaboración Propia.

En función de las respuestas a esta pregunta, se efectuaron los análisis de cada una de las submuestras, cuyos resultados numéricos se detallan en las figuras 35 y 36. Se estima que los estudiantes de la submuestra 2, a pesar de no disponer de capacitación especial en seguridad informática y/o criptografía, poseen los conocimientos básicos necesarios adquiridos mediante las materias de grado de la carrera, para responder la mayoría de las preguntas de la encuesta.

En el caso de los estudiantes de la Facultad de Ciencias Económicas que cursan la carrera de Licenciatura en Sistemas de Información, adquieren conocimientos básicos en seguridad teleinformática en asignaturas como Tecnología de las Comunicaciones y Redes Informáticas.

Por su parte, los estudiantes de la carrera de Ingeniería en Sistemas de Información, de la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires, también se capacitan en temas inherentes a la seguridad en la transmisión de datos y aplicaciones informáticas en asignaturas como Comunicaciones, Redes de Información, Diseño de Sistemas y electivas específicas como Seguridad Informática y Seguridad en Redes.

TOTAL: 49 alumnos

Pregunta	Rta SI	Rta NO	Rta NC	% SI	% NO	% NC
2	44	5	0	89,795	10,204	0
3	44	4	1	89,795	8,163	2,041
4	31	10	8	63,265	20,408	16,326
5	43	4	2	87,755	8,163	4,081

Vulnerabilidades del sitio WEB relacionadas con el usuario	A	M	B	NC
Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.	38	9	2	0
No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.	16	24	9	0
Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.	26	18	5	0
Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario	24	17	7	1
No se emplea la facilidad "captcha" para el acceso de los usuarios al sitio web	9	22	18	0

Vulnerabilidades del sitio WEB relacionadas con la implementación y vinculación del sitio con la red y los usuarios	A	M	B	NC
El sitio web no tiene la certificación vigente avalada por una autoridad certificante.	33	14	2	0
En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.	32	13	1	3
En sitios Web simulados o falsos el método phishing posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o debito.	36	8	2	3
No se emplean proxies en la conexión entre la red Internet y el entorno de la aplicación del sitio.	12	24	11	2
El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.	8	24	9	8

Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web	A	M	B	NC
Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.	30	17	2	0
Seguridad física del servidor deficiente.	31	16	2	0
Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo.	33	15	1	0
Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS.	10	24	7	8
Deslealtad del personal que opera la plataforma de e-commerce del sitio.	33	12	3	1

Figura 35: Resultados de la encuesta correspondiente a la submuestra 1
Fuente: Elaboración Propia

TOTAL: 61 alumnos

Pregunta	Rta SI	Rta NO	Rta NC	% SI	% NO	% NC
2	41	14	6	67,213	22,951	9,836
3	54	5	2	88,524	8,196	3,278
4	33	13	15	54,098	21,311	24,590
5	38	16	7	62,295	26,229	11,475

Vulnerabilidades del sitio WEB relacionadas con el usuario	A	M	B	NC
Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.	50	7	4	0
No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.	26	27	8	0
Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.	38	17	6	0
Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario	22	26	9	4
No se emplea la facilidad "captcha" para el acceso de los usuarios al sitio web	11	27	15	8

Vulnerabilidades del sitio WEB relacionadas con la implementación y vinculación del sitio con la red y los usuarios	A	M	B	NC
El sitio web no tiene la certificación vigente avalada por una autoridad certificante.	46	10	4	1
En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.	40	16	0	5
En sitios Web simulados o falsos el método phishing posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito.	40	16	1	4
No se emplean proxies en la conexión entre la red Internet y el entorno de la aplicación del sitio.	4	33	9	15
El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.	12	22	8	19

Vulnerabilidades del sitio WEB relacionadas con el mantenimiento y operación del sitio web	A	M	B	NC
Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.	44	15	1	1
Seguridad física del servidor deficiente.	42	15	3	1
Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo.	31	23	3	4
Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS.	19	18	7	17
Deslealtad del personal que opera la plataforma de e-commerce del sitio.	41	12	6	2

Figura 36: Resultados de la encuesta correspondiente a la submuestra 2
Fuente: Elaboración Propia

Analizaremos a continuación el resultado de las respuestas a las preguntas 2, 3, 4 y 5 para ambas submuestras:

Pregunta N° 2: Principales componentes del sistema de comercio electrónico

En el comercio electrónico, desde el punto de vista del hardware y software, los principales componentes son el host del cliente, su navegador web, la red Internet, los protocolos de comunicaciones/seguridad y el sitio web del vendedor (servidor y aplicaciones informáticas).

¿Está de acuerdo que la descripción mencionada contiene los componentes principales (hardware y software) del comercio electrónico?

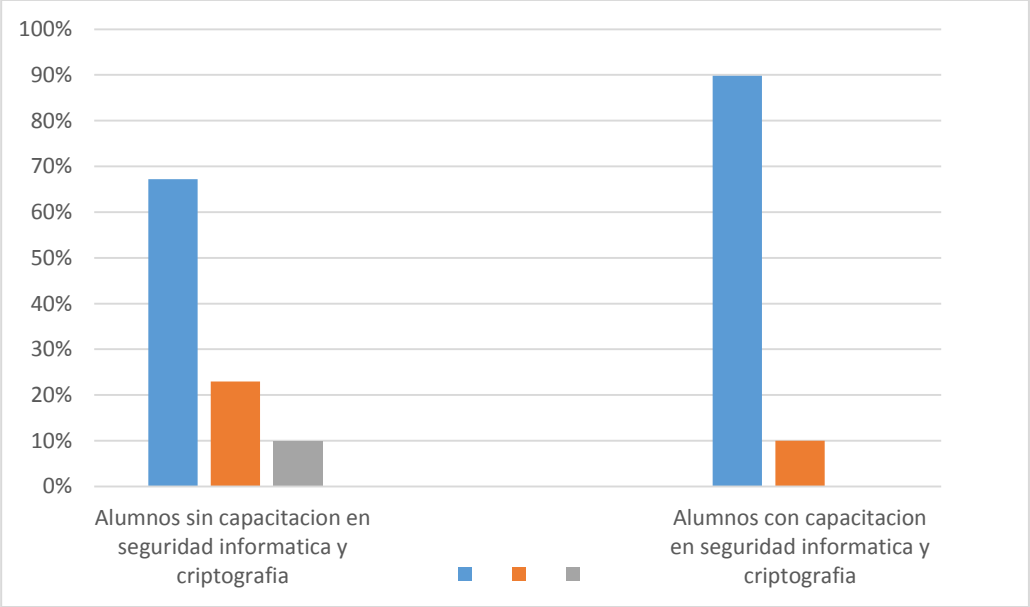


Figura 37: Nivel de acuerdo con la descripción de los principales componentes del comercio electrónico, según la capacitación de los estudiantes
Fuente: Elaboración Propia

En la figura 37 se puede observar que para la submuestra 2, estudiantes sin capacitación especial, el 67 % coincide con los componentes básicos del comercio electrónico propuestos: el host del cliente, su navegador web; la red Internet, los protocolos de comunicaciones/seguridad y el sitio web del vendedor (servidor y aplicaciones informáticas).

Para el conjunto de estudiantes capacitados en seguridad informática y/o criptografía, submuestra 1, el porcentaje es aún mayor llegando al 90 %, comparado con el 67 % de los que no recibieron capacitación. Por otro lado, el 10 % de estudiantes de la submuestra 2, no contestaron la pregunta; mientras que el 100 % de los estudiantes que recibieron capacitación (submuestra 1) la respondieron.

En la figura 38 se grafican las respuestas de los 110 estudiantes encuestados, se puede observar que el 77% opina que efectivamente el comercio electrónico, desde el punto de vista del hardware y software, tiene como principales componentes: el host del cliente, su navegador web, la red Internet, los protocolos de comunicación y seguridad y el sitio web del vendedor.

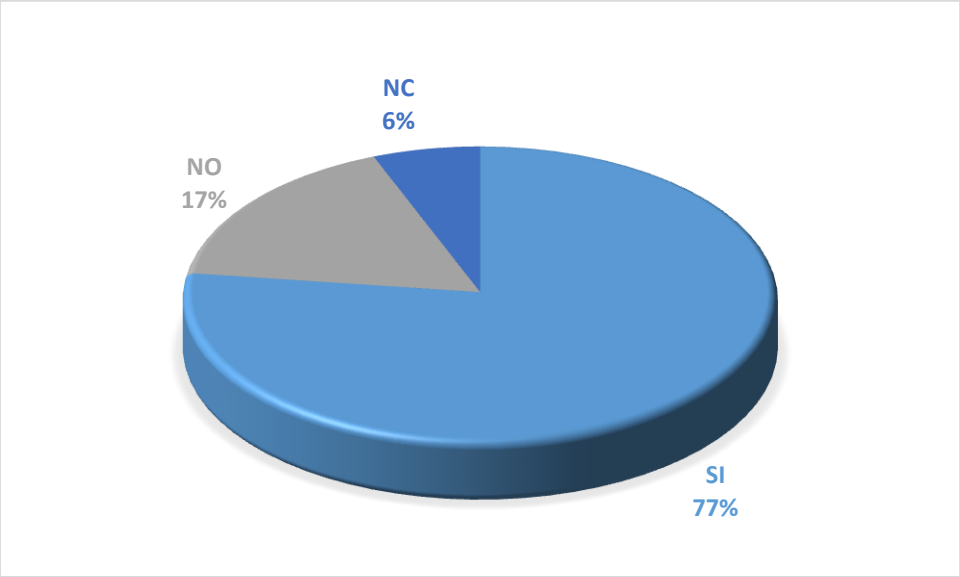


Figura 38: Niveles de acuerdo respecto a los principales componentes del comercio electrónico
Fuente: Elaboración Propia.

Pregunta N°3: Principales aspectos inherentes a la seguridad informática en operaciones online

En las operaciones online de comercio electrónico, a efectos de garantizar la seguridad, se deberían considerar los siguientes aspectos relativos a la seguridad informática: la autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto a los datos del usuario, el no repudio que asegura el consentimiento de la operación por cada uno de los participantes, y la disponibilidad de los datos.

¿Está de acuerdo considerar, en el comercio electrónico, los aspectos de la seguridad informática arriba mencionados como garantía de la seguridad?

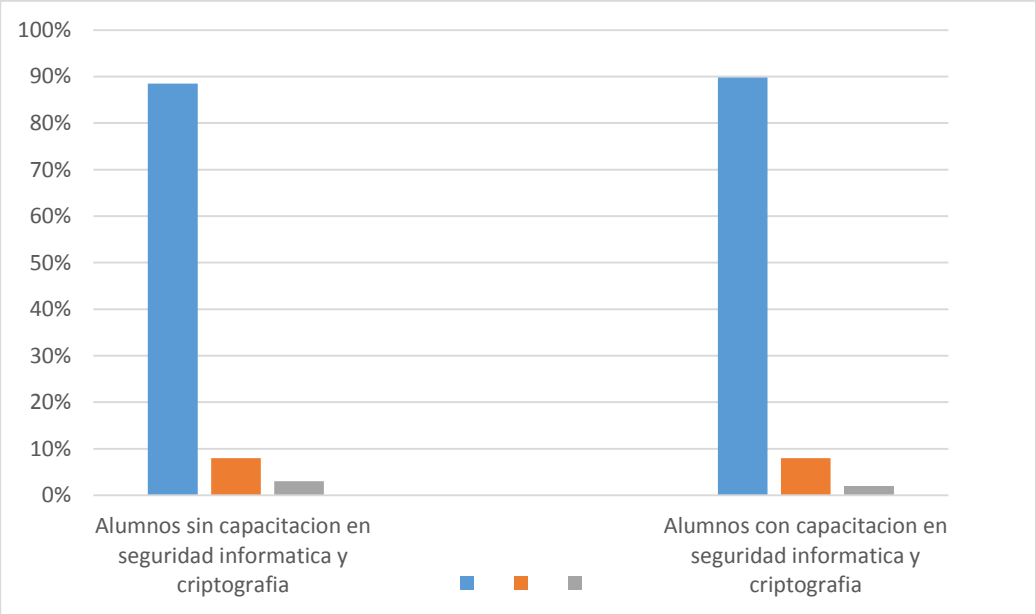


Figura 39: Nivel de acuerdo respecto a los aspectos de seguridad informática en operaciones online, según la capacitación de los estudiantes
Fuente: Elaboración Propia

En la figura 39 se puede observar que la diferencia entre los estudiantes que recibieron capacitación y los que no la tuvieron es mínima (menor al 1 %), esto se debe a que la pregunta se refiere a conceptos básicos de seguridad informática como son la autenticación, la confidencialidad, la integridad, el no repudio y la disponibilidad de los datos.

Estos conceptos se tratan en asignaturas como Redes de Información en la UTN, y Tecnología de Comunicaciones y Redes Informáticas en la FCE de la UBA.

Esta afirmación se corrobora cuando analizamos el gráfico de la figura 40, que presenta a la totalidad de los estudiantes encuestados. El 89% de los mismos concuerda con los conceptos básicos de la seguridad informática aplicados al comercio electrónico online.

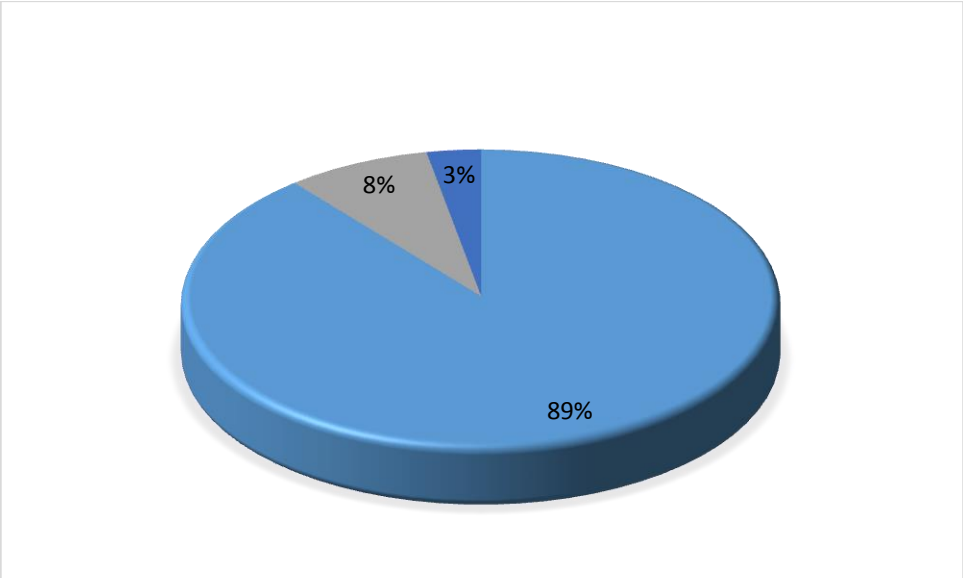


Figura 40: Nivel de acuerdo respecto a los aspectos de seguridad informática en operaciones online
Fuente: Elaboración Propia

Pregunta N° 4: Nivel de confiabilidad y seguridad brindado por los protocolos TCP y SSL/TLS en la comunicación.

¿Considera que los protocolos TCP y SSL / TLS, empleados en las operaciones de comercio electrónico, garantizan una comunicación confiable y segura entre el equipo del usuario (navegador web) y el sitio Web del vendedor?

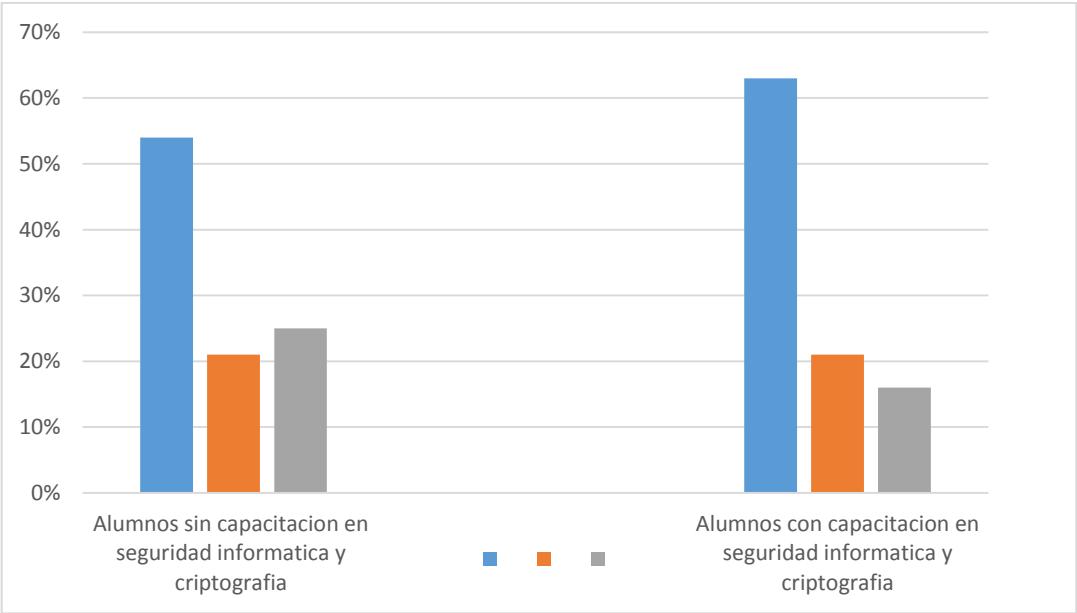


Figura 41: Valoración de la contribución de los protocolos TCP y SSL/TLS en la confiabilidad y seguridad de la operación, según la capacitación de los estudiantes
Fuente: Elaboración Propia

La figura 41 detalla las respuestas correspondientes a ambas submuestras. Se observa un mayor nivel de desconocimiento -el 25 %- en el grupo de estudiantes no capacitados, mientras que concuerdan que los protocolos TCP y SSL/TLS garantizan una comunicación confiable y segura un 54 %.

Por otro lado, el grupo de estudiantes capacitados tiene menor porcentaje de desconociendo del tema -sólo el 16 %- y está de acuerdo con lo afirmado en la pregunta respecto a los protocolos TCP y SSL/TLS, el 63 % de los estudiantes.

En la figura 42 se ha graficado la respuesta para el total de los estudiantes (110), de los cuales el 58 % está de acuerdo en afirmar que los protocolos TCP y SSL/TLS brindan confiabilidad en la comunicación y seguridad en la misma, entre el sitio web del vendedor y el host del cliente, pasando a través de las redes, específicamente; la insegura Internet.

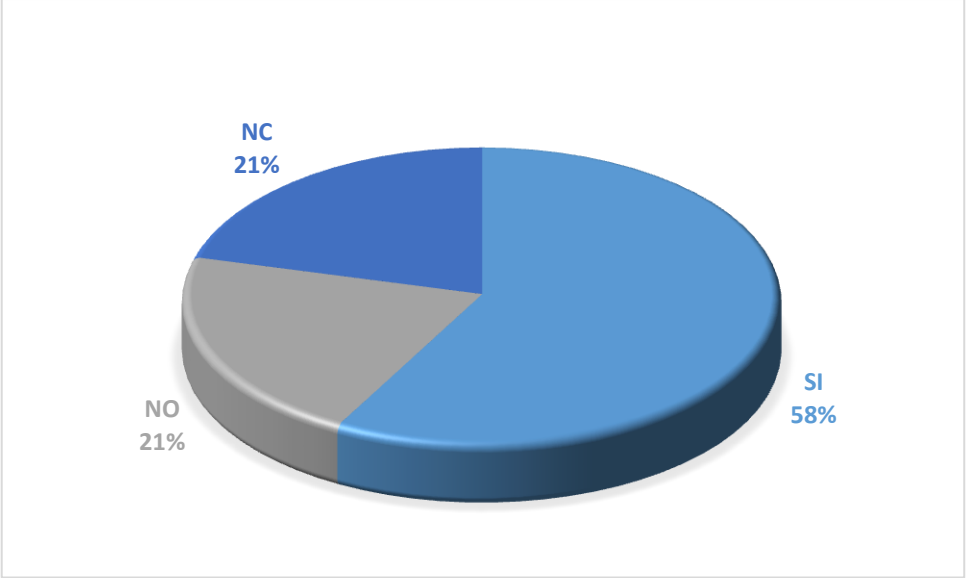


Figura 42: Valoración de la contribución de los protocolos TCP y SSL/TLS en la confiabilidad y seguridad de la operación.
Fuente: Elaboración Propia

El alto nivel de desconocimiento de los estudiantes, en comparación con las otras preguntas de la encuesta, se origina en el hecho de que en esta pregunta se interroga específicamente sobre protocolos como el TCP y el SSL/TLS y su implicancia en la comunicación de datos. Se destaca que el 21 % de los estudiantes parece desconocer los objetivos y funcionamiento de los mismos en la operación del comercio electrónico.

Pregunta N° 5: Componente de mayor nivel de vulnerabilidad para la seguridad en el proceso de comercio electrónico.

¿Considera que la vulnerabilidad principal de la seguridad del comercio electrónico reside principalmente en el sitio web del vendedor?

Esta pregunta se encuentra directamente relacionada con la hipótesis de la tesis la cual sostiene que se espera que los futuros profesionales de TICs determinen que las principales vulnerabilidades de la seguridad del comercio electrónico trazable se centralizan en la seguridad del sitio web donde se realiza la transacción.

En la figura 43 se grafican las respuestas de los estudiantes con y sin capacitación. En la submuestra 2, estudiantes sin capacitación especial en seguridad informática y criptografía, el 62 % de los estudiantes está de acuerdo en situar en el sitio web las principales vulnerabilidades de la seguridad del comercio electrónico, mientras que para los estudiantes con capacitación - submuestra 1- ese porcentaje se eleva al 88 %.

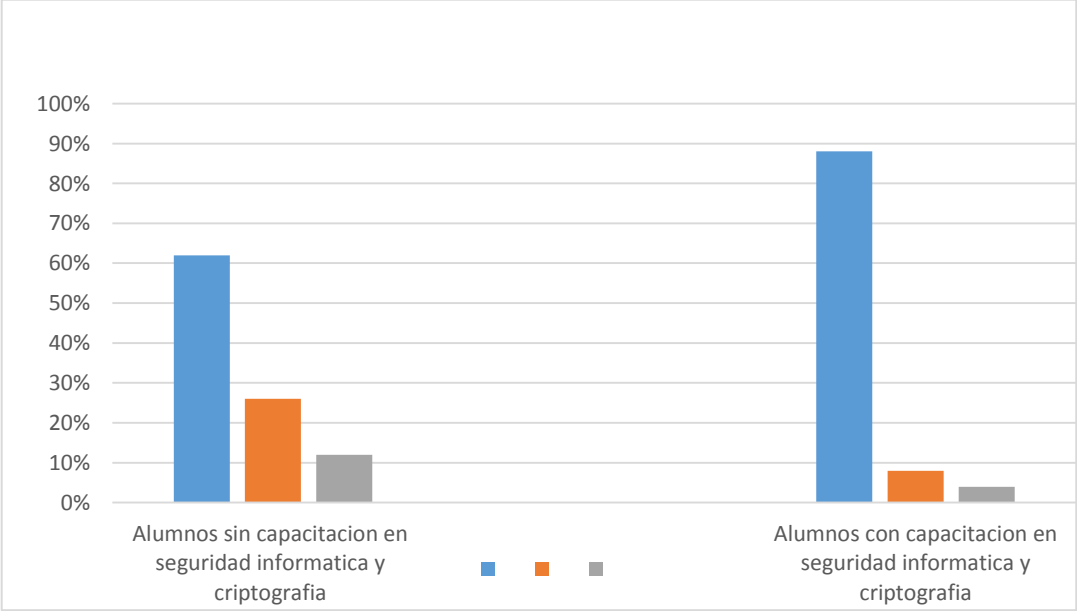


Figura 43: Nivel de acuerdo respecto a que la principal vulnerabilidad del sistema de comercio electrónico reside en el sitio web del vendedor, según la capacitación de los estudiantes
Fuente: Elaboración Propia

En la figura 44 se ha tomado el total de los 110 estudiantes encuestados. De ellos, el 74 % concuerda con la hipótesis en lo concerniente a ubicar el centro de la vulnerabilidad de la seguridad del comercio electrónico en el sitio web del proveedor y/o vendedor. Cabe destacar que existe un bajo porcentaje de estudiantes (8 %) que no respondieron a esta pregunta.

Las respuestas permiten corroborar una de las hipótesis planteadas, que sostiene que el sitio web del proveedor es, en definitiva, el componente de mayor importancia respecto a la vulnerabilidad a la seguridad del comercio electrónico.

Cabe recordar, que no se incluye en este análisis la estación del usuario, ya que el computador del cliente y su navegador pueden variar en su nivel de seguridad de acuerdo a la configuración implementada – desde un valor mínimo hasta un máximo-, que no afectará las sesiones de otros usuarios del sistema que están conectados con el sitio web del vendedor.

Por otro lado, como se indicó en el capítulo anterior, la transmisión de datos a través de Internet mediante los protocolos TCP y SSL/TLS debidamente configurados y actualizados, no debería constituir una fuente de inseguridad para el sistema de comercio electrónico.

Si se vulnera la seguridad del sitio web del vendedor, esta circunstancia afectará la seguridad de todas las sesiones que se mantengan con dicho sitio, independientemente que la transmisión de datos se encuentre encriptada con los clientes o no.

Por esta razón, las preguntas 6, 7 y 8 se enfocan en evaluar la importancia de los factores que influyen en la vulnerabilidad de la seguridad del sitio web.

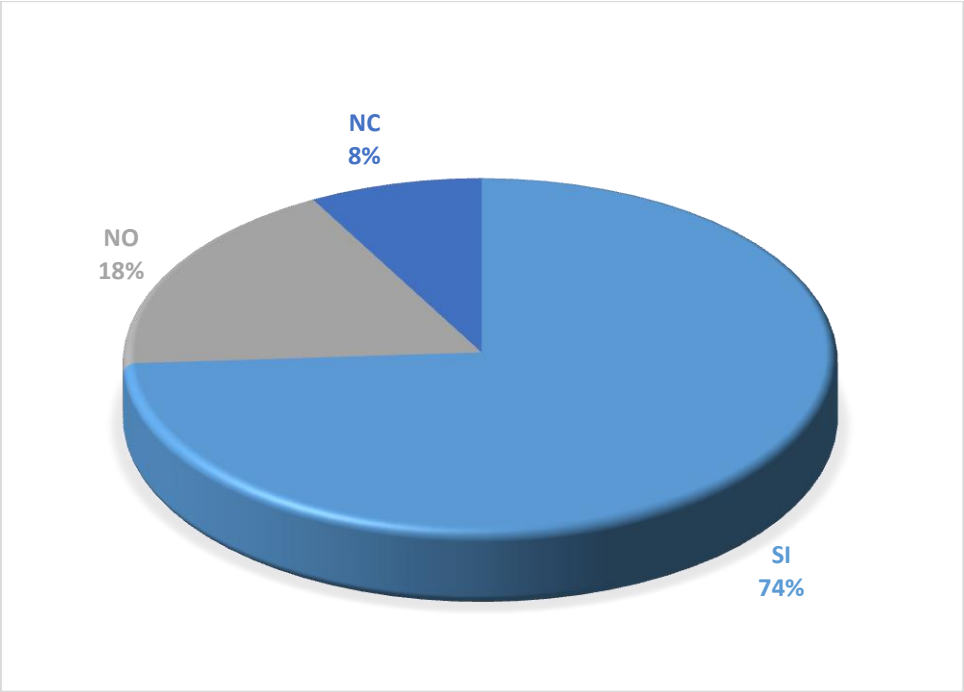


Figura 44: Nivel de acuerdo respecto a que la principal vulnerabilidad del sistema de comercio electrónico reside en el sitio web del vendedor
Fuente: Elaboración Propia

La pregunta N° 6 se refiere a los factores relacionados con el usuario que accede al sitio, la N° 7 se relaciona con los factores vinculados a la implementación y/o vinculación del sitio con la red y los usuarios, y la N° 8 está relacionada con los factores relativos al mantenimiento y operación del sitio web.
A continuación, analizaremos cada una de las respuestas a las preguntas mencionadas.

3.5. Resultados obtenidos en la encuesta para las preguntas 6 a 8 relativas a los factores que generan vulnerabilidad en la seguridad del sitio web

Pregunta N° 6: Factores que generan vulnerabilidad en la seguridad del sitio web, relacionados con el usuario

Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO RESPONDE (NR) a cada uno de los siguientes factores que afectan la vulnerabilidad de la seguridad del sitio web del vendedor y que están relacionados con el usuario que se comunica con dicho sitio.
Factor 1: Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	38	0,78	78
MEDIA	9	0,18	18
BAJA	2	0,04	4
NO CONTESTA	0	0	0
TOTALES	N = 49	1,0	100

Tabla N° 1: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía (submuestra 1). En efecto, como se observa en la figura 45, el 78% de ellos le asignó este nivel.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	50	0,82	82
MEDIA	7	0,12	12
BAJA	4	0,06	6
NO CONTESTA	0	0	0
TOTALES	N = 61	1,0	100

Tabla N° 2: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía (submuestra 2); como se puede observar en la figura 45 que muestra que así lo señala el 78 % de ellos.

Este factor no puede ser desconocido para los estudiantes de sistemas, por tratarse de un elemento básico de la seguridad, independientemente de la capacitación específica sobre seguridad informática que posea el estudiante encuestado.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	88	0,80	80
MEDIA	16	0,15	15
BAJA	6	0,05	5
NO CONTESTA	0	0	0
TOTALES	N = 110	1,0	100

Tabla N° 3: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras" es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía.

Se puede observar en la figura 45 que el 80 % del total de los estudiantes encuestados asigno alta importancia a este factor.

Por otro lado, ningún alumno dejo de contestar sobre el mismo (NC = 0); esto se debe a que se trata de un aspecto básico elemental de control de acceso a los sistemas sobre el cual los encuestados tienen conocimiento específico, adquirido durante el desarrollo de las aplicaciones informáticas y los módulos de seguridad asociados a las mismas. Por esta razón, pueden expedirse sobre el tema aun cuando no se hayan capacitado en seguridad informática y/o criptografía.

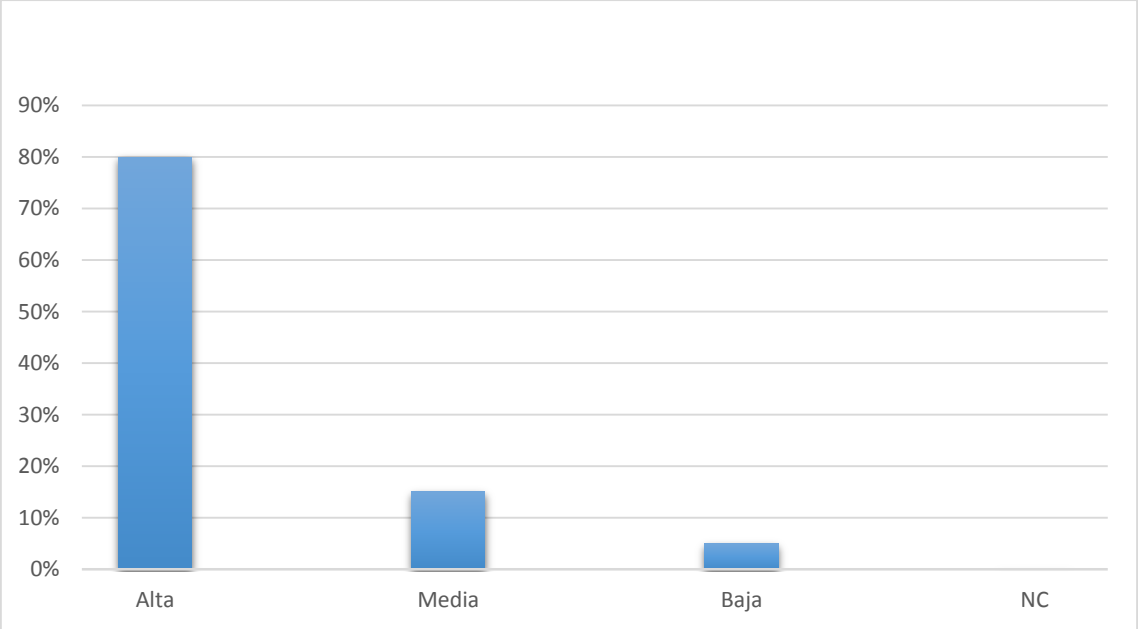


Figura 45: Valoración del factor: "acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras"
Fuente: Elaboración Propia

Factor 2: No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	16	0,33	33
MEDIA	24	0,49	49
BAJA	9	0,18	18
NO CONTESTA	0	0	0
TOTALES	N = 49	1,0	100

Tabla 4: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "no se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes" es de importancia MEDIA, para los estudiantes capacitados en seguridad informática y/o criptografía (submuestra 1), como se puede observar en la figura 46, que indica al 49 % de ellos.

En una primera apreciación parecería que la utilización de bitácoras o logs de seguridad son altamente importantes para la seguridad informática, y de hecho lo son. Aquí se interrogó a los estudiantes respecto de los factores que generan vulnerabilidad en la seguridad del sitio y la existencia de bitácoras no previene los ataques, sino que permite analizarlos luego de ocurridos.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	26	0,43	43
MEDIA	27	0,44	44
BAJA	8	0,13	13
NO CONTESTA	0	0,0	0
TOTALES	N = 61	1,0	100

Tabla 5: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "no se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes" es de importancia MEDIA, para los estudiantes sin capacitación en seguridad informática y/o criptografía (submuestra 2), dato que se observa en la figura 46 que muestra que esa ha sido la valoración del 44% de ellos.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	42	0,38	38
MEDIA	51	0,47	47
BAJA	17	0,15	15
NO CONTESTA	0	0	0
TOTALES	N = 110	1,0	100

Tabla 6: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes” es de importancia MEDIA, para la totalidad de los estudiantes encuestados de las dos submuestras, con y sin capacitación en seguridad informática y/o criptografía.

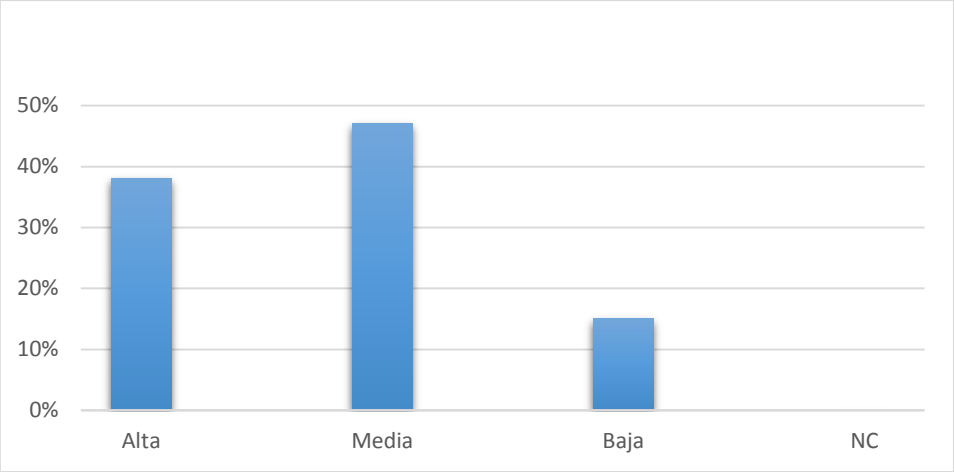


Figura 46: Valoración del factor “no se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes”
Fuente: Elaboración Propia

Se puede observar en la figura 46 que sólo el 38 % considera que este factor es de alta importancia mientras que el 62 % (47% + 15%) consideran que tiene una importancia media/baja (media (47%) y baja (15%)), en la vulnerabilidad del sitio web del vendedor relacionado con el usuario que se comunica con dicho sitio.

Factor 3: Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	26	0,53	53
MEDIA	18	0,37	37
BAJA	5	0,10	10
NO CONTESTA	0	0	0
TOTALES	N = 49	1,0	100

Tabla 7: Distribución de frecuencias absolutas y relativas para los datos cualitativos.

La moda del factor “falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web” es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía. Al respecto, se puede observar en la figura 47, que el 53 % de ellos, le asignó ese valor.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	38	0,62	62
MEDIA	17	0,28	28
BAJA	6	0,10	10
NO CONTESTA	0	0	0
TOTALES	N = 61	1,0	100

Tabla 8: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web” es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, representado por el 62% en la figura 47.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	64	0,58	58
MEDIA	35	0,32	32
BAJA	11	0,10	10
NO CONTESTA	0	0	0
TOTALES	N = 110	1,0	100

Tabla 9: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web” es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras, con y sin capacitación en seguridad informática y/o criptografía.

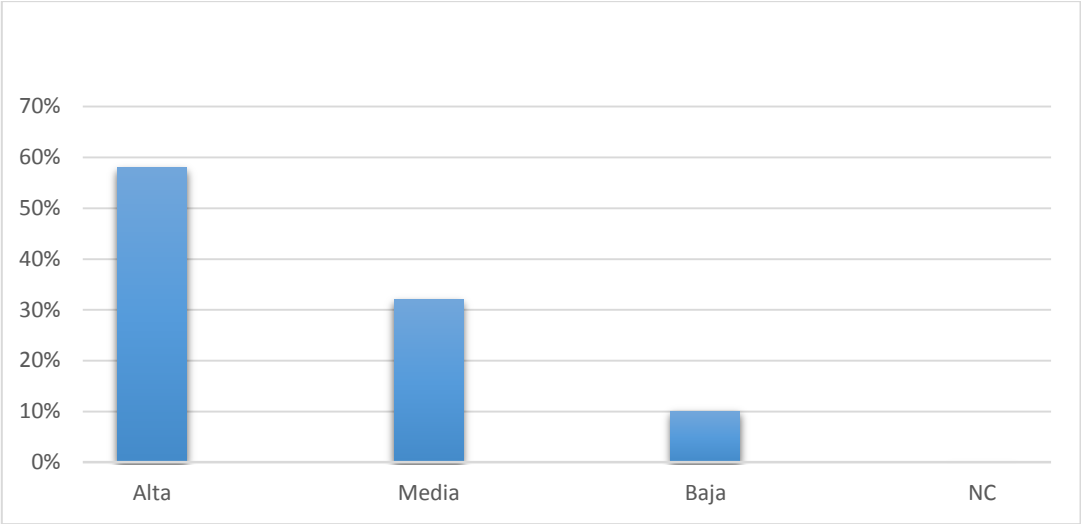


Figura 47: Valoración del factor: "falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web"
Fuente: Elaboración Propia

Se puede observar en la figura 47 que el 58 % del total de los estudiantes encuestados asignó alta importancia al factor "falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web", como vulnerabilidad del sitio web del vendedor y relacionado con el usuario que se comunica con dicho sitio.

Factor 4: Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	24	0,49	49
MEDIA	17	0,35	35
BAJA	7	0,14	14
NO CONTESTA	1	0,02	2
TOTALES	N = 49	1,0	100

Tabla 10: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía. Como se puede observar en la figura, 48 % evalúan de ese modo.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	22	0,36	36
MEDIA	26	0,43	43
BAJA	9	0,15	15
NO CONTESTA	4	0,06	6
TOTALES	N = 61	1,0	100

Tabla 11: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario" es de importancia MEDIA, para los estudiantes sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 48, que el 43 % de ellos asignan tal valor.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	46	0,42	42
MEDIA	43	0,39	39
BAJA	16	0,15	15
NO CONTESTA	5	0,04	4
TOTALES	N = 110	1,0	100

Tabla 12: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario" es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía.

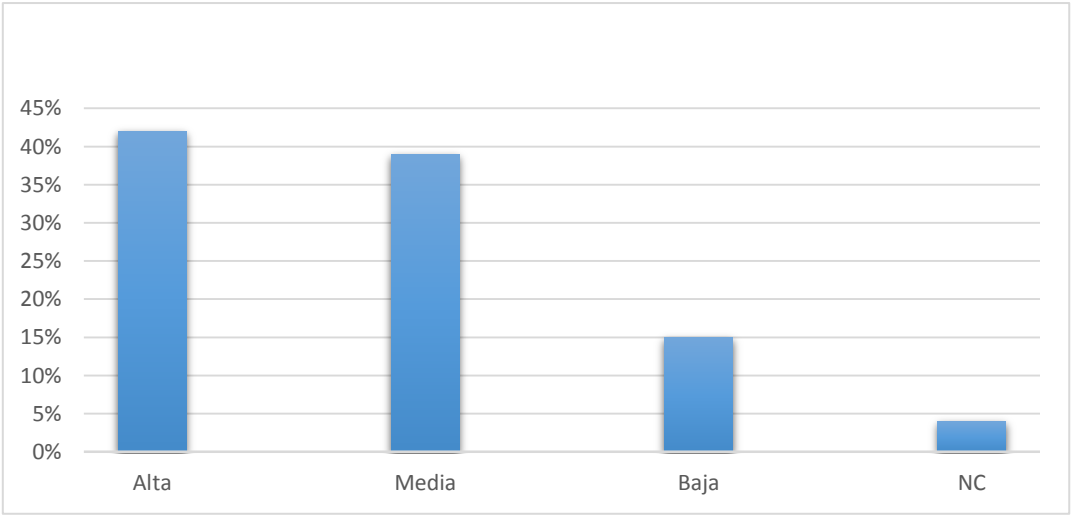


Figura 48: Valoración del factor "falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario"
Fuente: Elaboración Propia

Se puede observar en la figura 48 que el 42 % del total de los estudiantes encuestados asigno alta importancia al factor: "falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario", como vulnerabilidad del sitio web del vendedor y relacionado con el usuario que se comunica con dicho sitio.

Factor 5: No se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	9	0,18	18
MEDIA	22	0,45	45
BAJA	18	0,37	37
NO CONTESTA	0	0,0	0
TOTALES	N = 49	1,0	100

Tabla 13: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "no se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web" es de importancia MEDIA, para los estudiantes capacitados en seguridad informática y/o criptografía, como se puede observar en la figura 49, con una representación del 45 %.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	11	0,18	18
MEDIA	27	0,44	44
BAJA	15	0,25	25
NO CONTESTA	8	0,13	13
TOTALES	N = 61	1,0	100

Tabla 14: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "No se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web" es de importancia MEDIA, para los estudiantes sin capacitación en seguridad informática y/o criptografía. Esto se puede observar en la figura 49, con el 44 % de representación.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	20	0,18	18
MEDIA	49	0,45	45
BAJA	33	0,30	30
NO CONTESTA	8	0,07	7
TOTALES	N = 110	1,0	100

Tabla 15: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "No se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web" es de importancia MEDIA, para la totalidad de los estudiantes encuestados de las dos submuestras, con y sin capacitación en seguridad informática y/o criptografía. Esto se puede observar en la figura 49, representado con el 45 %.

Recordemos que: "Un CAPTCHA (test de *Turing* público y automático para distinguir a los ordenadores de los humanos, del inglés "*Completely Automated Public Turing test to tell Computers and Humans Apart*") es un tipo de medida de seguridad conocido como autenticación pregunta-respuesta. La facilidad CAPTCHA es una ayuda importante para brindar protección respecto de los mensajes *spam*[189] y del descifrado de contraseñas, al solicitar que el usuario complete una simple prueba que demuestre que es humano y no un ordenador que intenta acceder a una cuenta protegida con contraseña.

La respuesta de los estudiantes, considerando de importancia MEDIA este factor, es llamativa dado que una contraseña segura y el uso de CAPTCHA son básicos para el acceso al sitio con un nivel de seguridad adecuado.

El empleo de contraseñas seguras es una de las principales medidas de seguridad que se recomienda implementar cuando se analiza el acceso seguro a una red. Por otro lado, el uso de CAPTCHA evita el acceso automático, gestionado por robots a la red o sitio web; de esta forma se puede asegurar que quien pretende ingresar es un humano y no una aplicación informática.

[189] SPAM: Mensajes no solicitados, generalmente de origen publicitario.

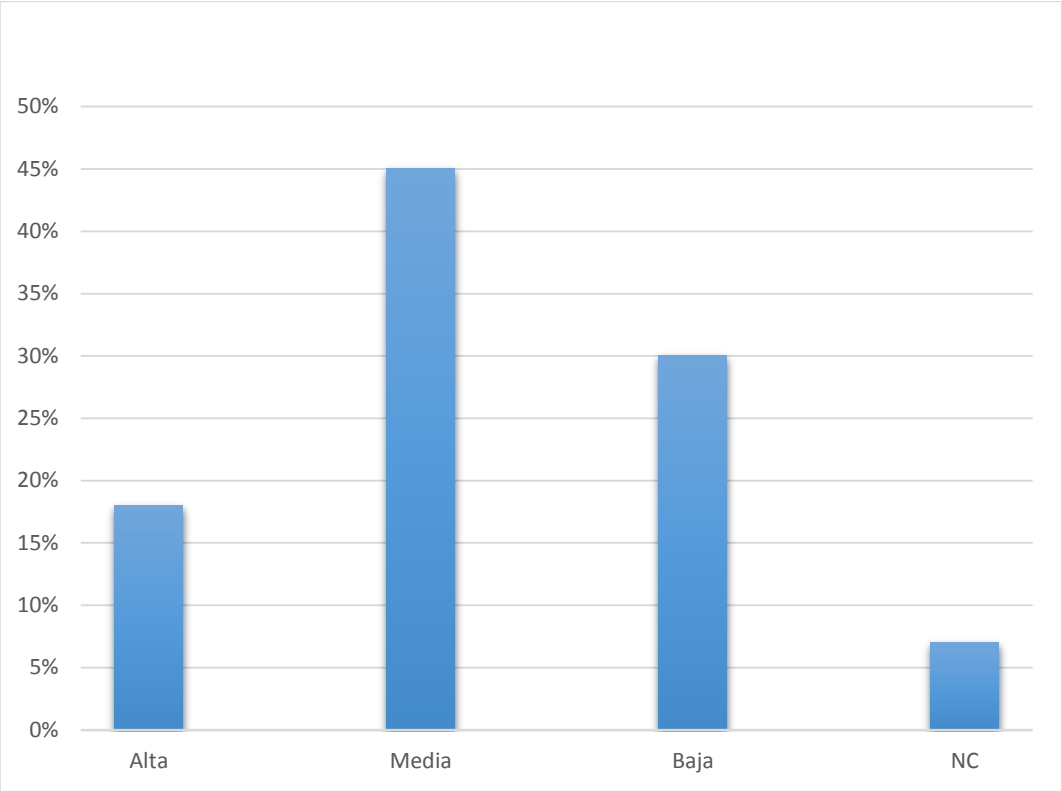


Figura 49: Valoración del factor "no se emplea la facilidad "CAPTCHA" para el acceso de los usuarios al sitio web
Fuente: Elaboración Propia

Clasificación de los factores que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionadas con el usuario

Como se puede apreciar en la figura 50, el resultado de la encuesta determinó que para la totalidad de los estudiantes los factores que tienen alta incidencia en la vulnerabilidad del sitio Web en relación con las acciones del usuario cuando interactúa con el sitio, ordenados por nivel de importancia, se presentan como sigue:

Factores determinantes:

1. Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras
2. Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web
3. Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario

Para los dos primeros factores los estudiantes con y sin capacitación en seguridad informática consideran que la incidencia es ALTA.

Para el tercer factor, los estudiantes con capacitación en seguridad informática consideran

que es ALTA mientras que para los estudiantes que no recibieron capacitación evalúan que la importancia es MEDIA. No obstante, tomando ambos grupos la evaluación para este último factor corresponde a ALTA incidencia.

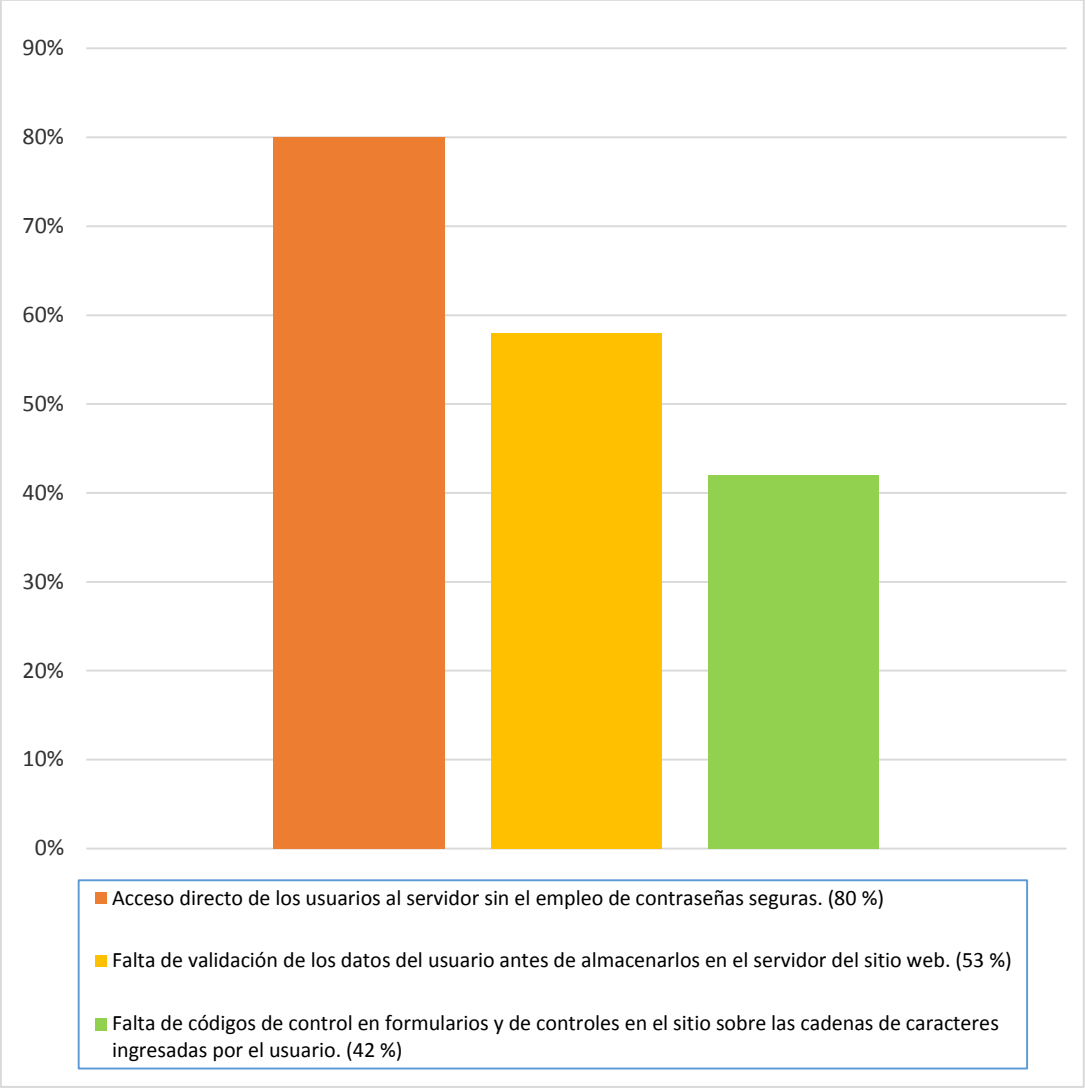


Figura 50: Clasificación de los factores determinantes que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionadas con el usuario
Fuente: Elaboración Propia

Pregunta N° 7: Factores que generan vulnerabilidad en la seguridad del sitio web, relacionados con la implementación y/o vinculación del sitio con la red y los usuarios.

Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con la implementación y/o vinculación del sitio con la red y los usuarios.

Factor 1: El sitio web no tiene la certificación digital vigente avalada por una autoridad certificante

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	33	0,67	67
MEDIA	14	0,29	29
BAJA	2	0,04	4
NO CONTESTA	0	0	0
TOTALES	N = 49	1,0	100

Tabla 16: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no tiene la certificación digital vigente avalada por una autoridad certificante" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía. Se puede observar en la figura 51 que el 67 % de ellos, le asignó ese valor al factor.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	46	0,75	75
MEDIA	10	0,16	16
BAJA	4	0,07	7
NO CONTESTA	1	0,02	2
TOTALES	N = 61	1,0	100

Tabla 17: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no tiene la certificación digital vigente avalada por una autoridad certificante" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, dato que se puede observar en la figura 51, representado por el 75% de las respuestas.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	79	0,72	72
MEDIA	24	0,22	22
BAJA	6	0,05	5
NO CONTESTA	1	0,01	1
TOTALES	N = 110	1,0	100

Tabla 18: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no tiene la certificación digital vigente avalada por una autoridad certificante" es de importancia ALTA, para la totalidad de los estudiantes

encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 51 que el 72 % del total de los estudiantes encuestados asignó alta importancia al factor que afecta la vulnerabilidad del sitio web del vendedor y que está relacionad con la implementación y/o vinculación del sitio con la red y los usuarios.

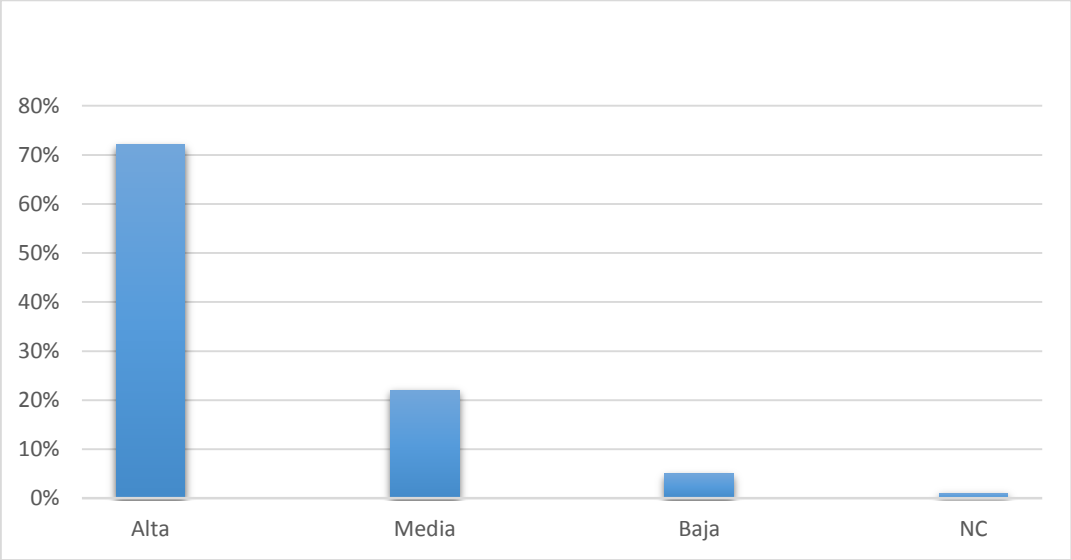


Figura 51: Valoración del factor "el sitio web no tiene la certificación digital vigente avalada por una autoridad certificante"
Fuente: Elaboración Propia

Factor 2: En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	32	0,65	65
MEDIA	13	0,27	27
BAJA	1	0,02	2
NO CONTESTA	3	0,06	6
TOTALES	N = 49	1,0	100

Tabla 19: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o

criptografía. Se puede observar en la figura 52 que el 65 % de los estudiantes, le asignó dicho nivel.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	40	0,66	66
MEDIA	16	0,26	26
BAJA	0	0,0	0
NO CONTESTA	5	0,08	8
TOTALES	N = 61	1,0	100

Tabla 20: Distribución de frecuencias absolutas y relativas para los datos cualitativos: importancia del factor

La moda del factor "En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, como se observa en la figura 52, representado por el 66% de ellos.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	72	0,66	66
MEDIA	29	0,26	26
BAJA	1	0,01	1
NO CONTESTA	8	0,07	7
TOTALES	N = 110	1,0	100

Tabla 21: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "en el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio" es de importancia ALTA, para la totalidad de los estudiantes.

Se puede observar en la figura 52 que el 66 % considera este factor de alta importancia, mientras que el 26 % considera que tiene una importancia media en relación a la vulnerabilidad del sitio web del vendedor cuando se lo relaciona con la implementación y/o vinculación del sitio con la red y los usuarios.

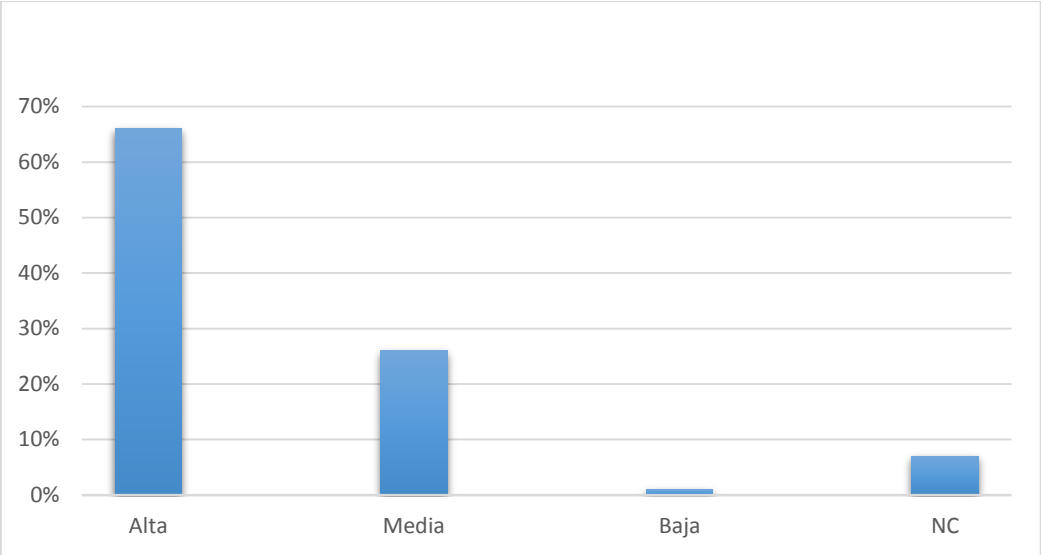


Figura 52: Valoración del factor "en el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio"
Fuente: Elaboración Propia

Factor 3: En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	36	0,74	74
MEDIA	8	0,16	16
BAJA	2	0,04	4
NO CONTESTA	3	0,06	6
TOTALES	N = 49	1,0	100

Tabla 22: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "en sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía. Se puede observar en la figura 53 que el 74 % de ellos lo evaluó en este sentido.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	40	0,66	66
MEDIA	16	0,26	26
BAJA	1	0,02	2
NO CONTESTA	4	0,06	6
TOTALES	N = 61	1,0	100

Tabla 23: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "en sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 53 que el 66 % de ellos lo expresan de este modo.

Existe similitud en los resultados de ambas submuestras por tratarse de un factor relevante para la seguridad informática. Recordemos que el *phishing* es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta, como contraseñas o información sobre tarjetas de crédito, cuentas bancarias, etc.

El estafador, conocido como *phisher*, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas (Rivero, 2017).

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	76	0,69	69
MEDIA	24	0,22	22
BAJA	3	0,03	3
NO CONTESTA	7	0,06	6
TOTALES	N = 110	1,0	100

Tabla 24: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito**"** es de importancia ALTA, para la totalidad de los estudiantes.

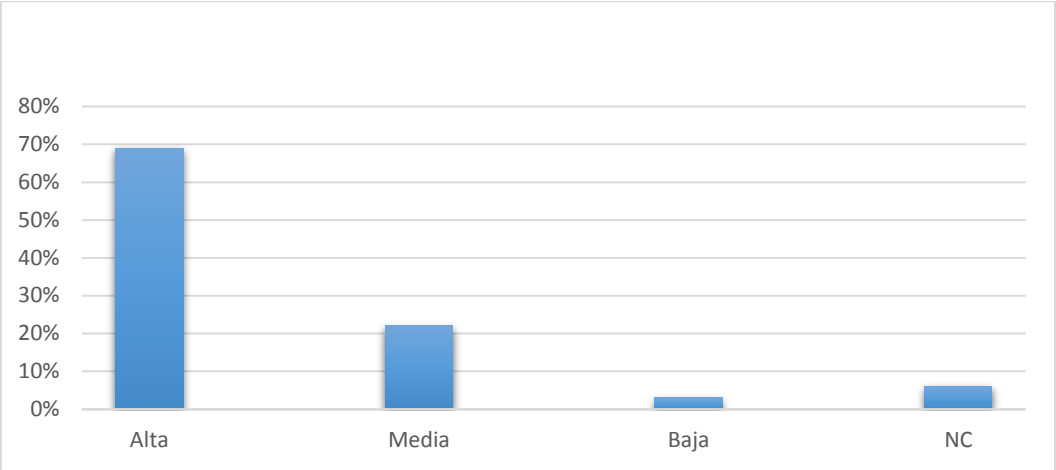


Figura 53: Valoración del factor "en sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito"
Fuente: Elaboración Propia

Factor 4: No se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	12	0,25	25
MEDIA	24	0,49	49
BAJA	11	0,22	22
NO CONTESTA	2	0,04	4
TOTALES	N = 49	1,0	100

Tabla 25: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "no se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio" es de importancia MEDIA, para los estudiantes capacitados en seguridad informática y/o criptografía. Se puede observar en la figura 54 que el 49 % de ellos respondió en este sentido.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	4	0,06	6
MEDIA	33	0,54	54
BAJA	9	0,15	15
NO CONTESTA	15	0,25	25
TOTALES	N = 61	1,0	100

Tabla 26: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “no se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio” es de importancia MEDIA, para los estudiantes sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 54 que el 54 % de ellos lo evalúa de esta manera.

Se observa también, que existe un porcentaje del 25 % de los estudiantes no capacitados en seguridad informática, que no contesta; probablemente debido a que no conocen como funcionan los *proxies* en los firewalls de acceso a la red Internet.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	16	0,15	15
MEDIA	57	0,52	52
BAJA	20	0,18	18
NO CONTESTA	17	0,15	15
TOTALES	N = 110	1,0	100

Tabla 27: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “no se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio” es de importancia MEDIA, para la totalidad de los estudiantes encuestados de las dos submuestras, con y sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 54 que el 52 % del total de los estudiantes asignan esa valoración.

No obstante, también es importante destacar que hubo un 15 % que desconoce del tema y otro 18 % que otorga un nivel de importancia bajo a este factor. Solo el 15 % del total de estudiantes encuestados considera que la importancia es alta.

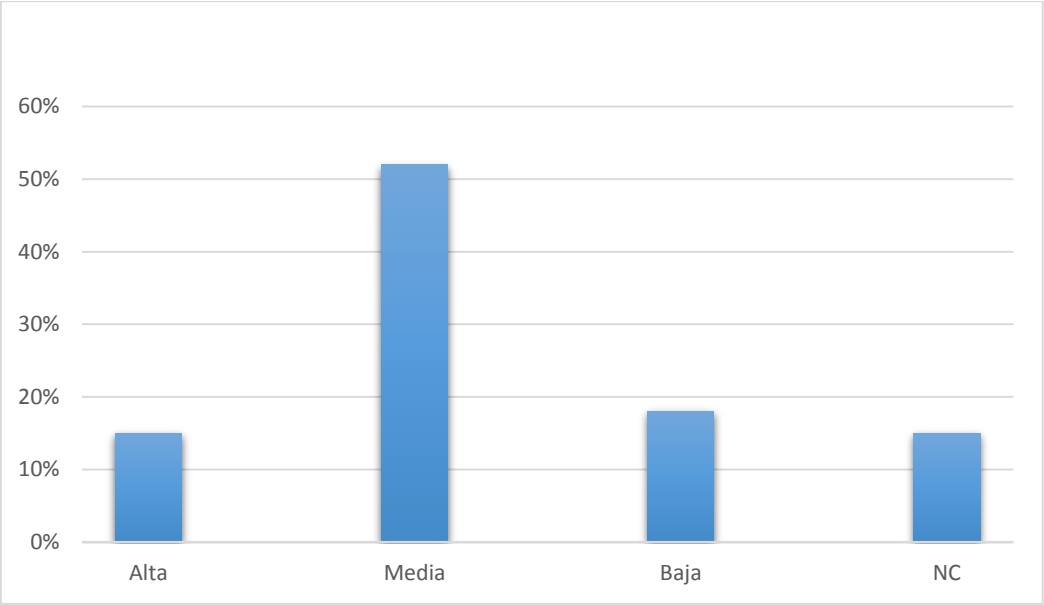


Figura 54: Valoración del factor "no se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio"
Fuente: Elaboración Propia

Factor 5: El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DELACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	8	0,16	16
MEDIA	24	0,49	49
BAJA	9	0,19	19
NO CONTESTA	8	0,16	16
TOTALES	N = 49	1,0	100

Tabla 28: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan" es de importancia MEDIA, para los estudiantes capacitados en seguridad informática y/o criptografía, como se observa en la figura 55, donde están representados en el 49%.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	12	0,20	20
MEDIA	22	0,36	36
BAJA	8	0,13	13
NO CONTESTA	19	0,31	31
TOTALES	N = 61	1,0	100

Tabla 29: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan" es de importancia MEDIA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, como se puede observar en la figura 55, representado con el 36 %.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	20	0,18	18
MEDIA	46	0,42	42
BAJA	17	0,15	15
NO CONTESTA	27	0,25	25
TOTALES	N = 110	1,0	100

Tabla 30: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "el sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan" es de importancia MEDIA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 55, en el 42 % del total.

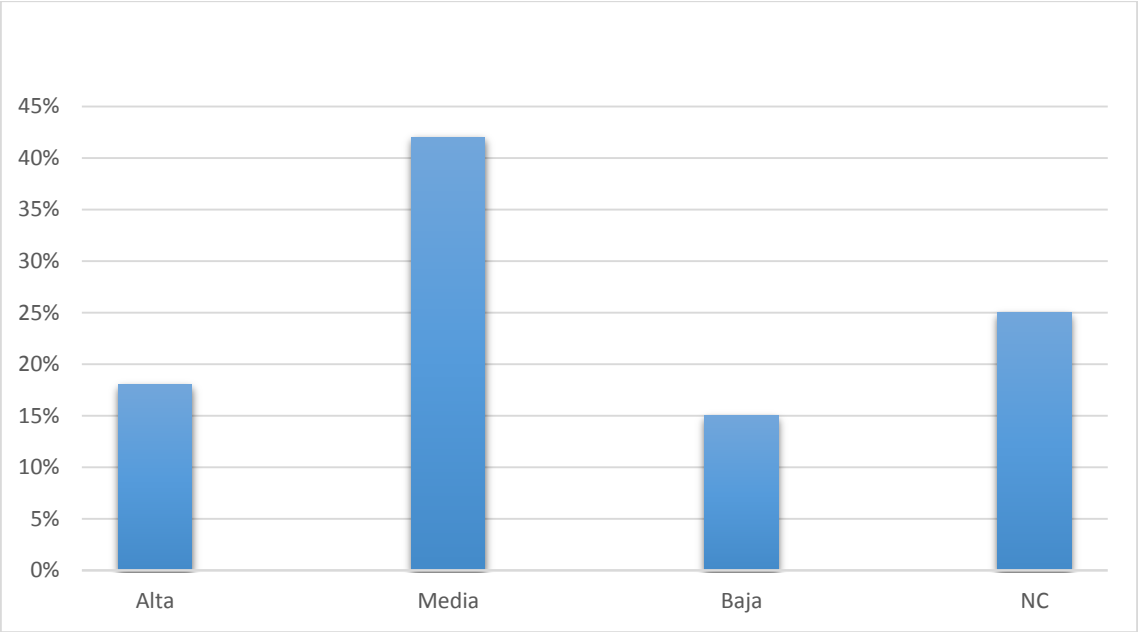


Figura 55: Valoración del factor "el sitio web no emplea P3P que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan
Fuente: Elaboración Propia

Clasificación de los factores que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionados con la implementación del sitio y la vinculación de éste con la red y los usuarios

.

Como se puede apreciar en la figura 56, el resultado de la encuesta determino que para la totalidad de los estudiantes los factores que tienen alta incidencia en la vulnerabilidad del sitio Web, en relación con las acciones del usuario cuando interactúa con el sitio, ordenados por nivel de importancia, se presentan como sigue:

Factores

1. El sitio web no tiene la certificación digital vigente avalada por una autoridad certificante

2. En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito.

3. En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio.

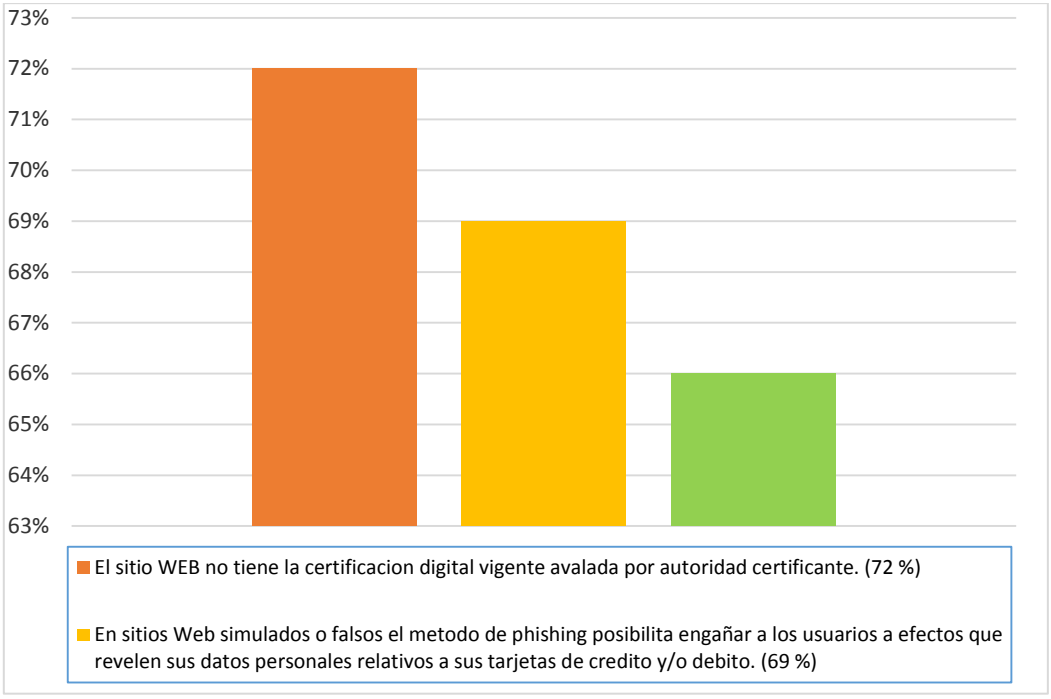


Figura 56: Clasificación de los factores determinantes que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionados con la implementación del sitio y la vinculación de éste con la red y los usuarios
Fuente: Elaboración Propia

Pregunta N° 8: Factores que generan vulnerabilidad en la seguridad del sitio web, relacionados con el mantenimiento y operación del sitio.

Asigne el orden de importancia: ALTA (A), MEDIA (M), BAJA (B) o NO CONTESTA (NC), a cada uno de los siguientes factores que afectan la vulnerabilidad del sitio web del vendedor y que están relacionados con el mantenimiento y operación del sitio.

Factor 1: Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	30	0,61	61
MEDIA	17	0,35	35
BAJA	2	0,04	4
NO CONTESTA	0	0,0	0
TOTALES	N = 49	1,0	100

Tabla 31: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.” es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía. Se puede observar en la figura 57, que el 61 % de ellos evaluó en ese sentido el mismo.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	44	0,72	75
MEDIA	15	0,24	24
BAJA	1	0,02	2
NO CONTESTA	1	0,02	2
TOTALES	N = 61	1,0	100

Tabla 32: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.” es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, como se puede observar en la figura 57, con el 75 %.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	74	0,67	67
MEDIA	32	0,29	29
BAJA	3	0,03	3
NO CONTESTA	1	0,01	1
TOTALES	N = 110	1,0	100

Tabla 33: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.” es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 57, que el 67 % indica en este sentido este factor.

Un software cuya eficacia es directamente proporcional a su grado de actualización son los antivirus.

Una vez que se carga un software de seguridad, su eficacia depende de la información disponible en el momento del desarrollo. Mientras tanto, los creadores de virus, los

piratas informáticos y otros individuos malintencionados generan continuamente nuevas e ingeniosas formas de atacar a sus objetivos. Esto tiene consecuencias críticas en lo que se refiere a vulnerabilidades. Por más que haya instalado un nuevo software antivirus hace unos meses, el usuario podría seguir siendo vulnerable a una gran cantidad de posibles ataques de virus nuevos (Norton by Symantec, 2017).

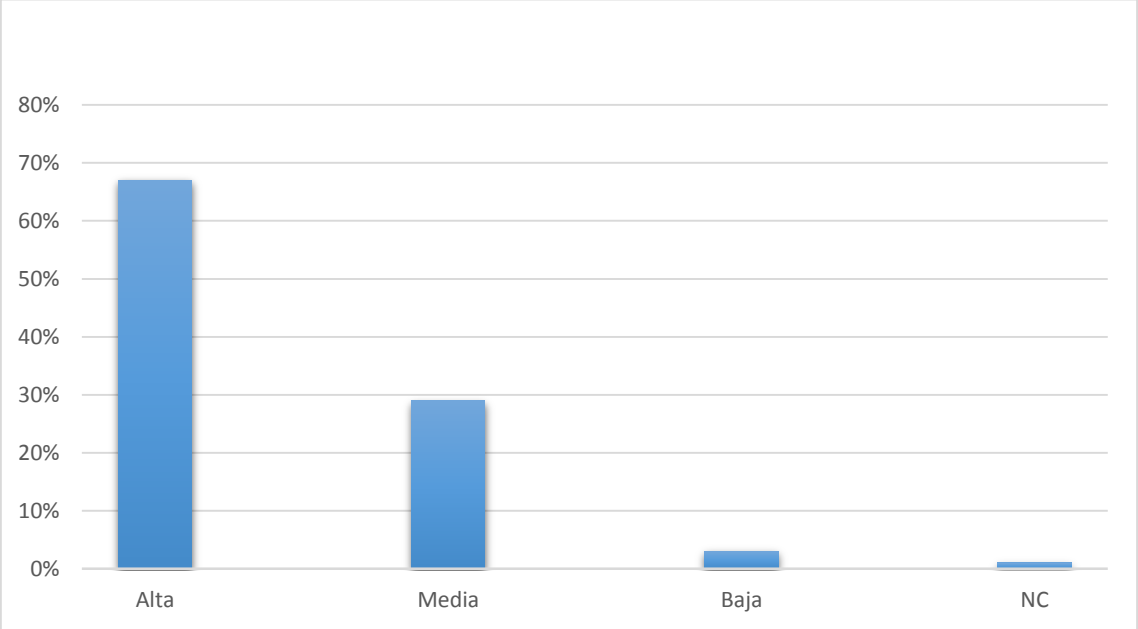


Figura 57: Valoración del factor "falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc."
Fuente: Elaboración Propia

Factor 2: Seguridad física del servidor deficiente

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	31	0,63	63
MEDIA	16	0,33	33
BAJA	2	0,04	4
NO CONTESTA	0	0,0	0
TOTALES	N = 49	1,0	100

Tabla 34: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “seguridad física del servidor deficiente” es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía, como se puede observar en la figura 58, con el 63 %.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	42	0,69	69
MEDIA	15	0,24	24
BAJA	3	0,05	5
NO CONTESTA	1	0,02	2
TOTALES	N = 61	1,0	100

Tabla 35: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “seguridad física del servidor deficiente” es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, como se puede observar en la figura 58, representado con el 69 %.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	73	0,66	66
MEDIA	31	0,28	28
BAJA	5	0,05	5
NO CONTESTA	1	0,01	1
TOTALES	N = 110	1,0	100

Tabla 36: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor “seguridad física del servidor deficiente” es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía, como se puede observar en la figura 58, representado con el 66 %.

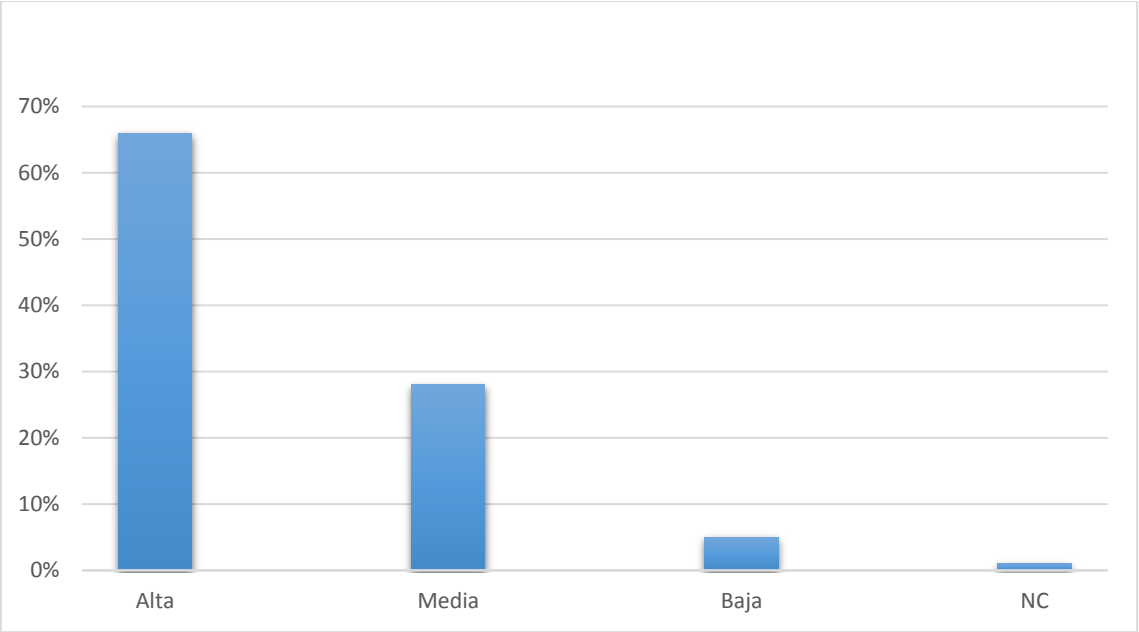


Figura 58: Valoración del factor "seguridad física del servidor deficiente"
Fuente: Elaboración Propia

Factor 3: Falta de realización periódica de pruebas de vulnerabilidad por personal idóneo

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	33	0,67	67
MEDIA	15	0,31	31
BAJA	1	0,02	2
NO CONTESTA	0	0,0	0
TOTALES	N = 49	1,0	100

Tabla 37: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de realización periódica de pruebas de vulnerabilidad por personal idóneo" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía, como se puede observar en la figura 59, representado con el 67 %.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	31	0,51	51
MEDIA	23	0,38	38
BAJA	3	0,05	5
NO CONTESTA	4	0,06	6
TOTALES	N = 61	1,0	100

Tabla 38: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de realización periódica de pruebas de vulnerabilidad por personal idóneo" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía, como se puede observar en la figura 59 representados con el 51 %.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	64	0,58	58
MEDIA	38	0,34	34
BAJA	4	0,04	4
NO CONTESTA	4	0,04	4
TOTALES	N = 110	1,0	100

Tabla 39: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de realización periódica de pruebas de vulnerabilidad por personal idóneo" es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía. Se puede observar en la figura 59 representados con el 58 %, indicando que afecta la vulnerabilidad del sitio web del vendedor y que está relacionado con el mantenimiento y operación del sitio.

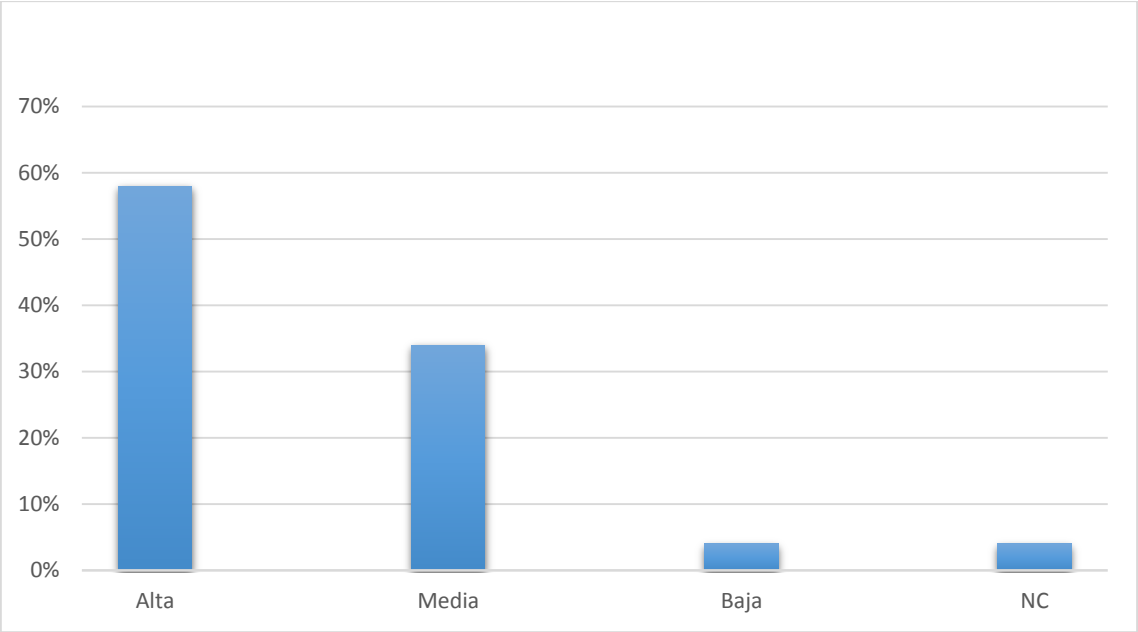


Figura 59: Valoración del factor "falta de realización periódica de pruebas de vulnerabilidad por personal idóneo"
Fuente: Elaboración Propia

Factor 4: Falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	10	0,21	21
MEDIA	24	0,49	49
BAJA	7	0,14	14
NO CONTESTA	8	0,16	16
TOTALES	N = 49	1,0	100

Tabla 40: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2" es de importancia MEDIA, para los estudiantes capacitados en seguridad informática y/o criptografía.

Se puede observar en la figura 60, que el 49 % de ellos le asignó ese valor y el 14 % baja importancia al factor. Por otro lado, el 16% de los estudiantes no respondió, presumiblemente por desconocer las normas estas normas PCI-DSS.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	19	0,31	31
MEDIA	18	0,30	30
BAJA	7	0,11	11
NO CONTESTA	17	0,28	28
TOTALES	N = 61	1,0	100

Tabla 41: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía como se puede observar en la figura 60, representados por el 31 %.

No obstante, se observa que el 28 % de los estudiantes no respondió respecto a la importancia de este factor debido presumiblemente al desconocimiento de la norma PCI-DSS.

c) Totalidad de los estudiantes encuestados (N = 110).

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	29	0,26	26
MEDIA	42	0,38	38
BAJA	14	0,13	13
NO CONTESTA	25	0,23	23
TOTALES	N = 110	1,0	100

Tabla 42: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2" es de importancia MEDIA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía.

Se puede observar en la figura 60, que el 38 % del total le asignó ese valor al factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2"**,** como vulnerabilidad del sitio Web relacionada con el mantenimiento y operación del sitio**.** No obstante, también es importante destacar que hubo un 23 % que desconoce del tema y otro 13 % que otorga un nivel de importancia bajo a este factor. Solo el 26 % del total de estudiantes encuestados considera que la importancia es alta. Como se mencionó en el punto 4.3.4 la actividad de implementación,

operación y mantenimiento de sitios web vinculados al comercio electrónico está estandarizada a través de normas, las más difundidas son las PCI DSS (*Payment Card Industry Data Security Standard* – Estándar de seguridad de datos de la industria de tarjetas de pago).

No obstante, el asignar a este factor una importancia media seguramente radica en el desconocimiento por parte de los estudiantes de esta norma que es específica del sistema de comercio electrónico. Al respecto recordemos que las entidades que operan en comercio electrónico deben cumplir como mínimo con estos estándares, a efectos de proteger los datos de los usuarios titulares de las tarjetas, como así también, no dañar la reputación comercial de la empresa y minimizar los riesgos financieros. El objetivo de las normas PCI DSS es garantizar que los datos privados y sensibles de los titulares de tarjeta estén siempre resguardados.

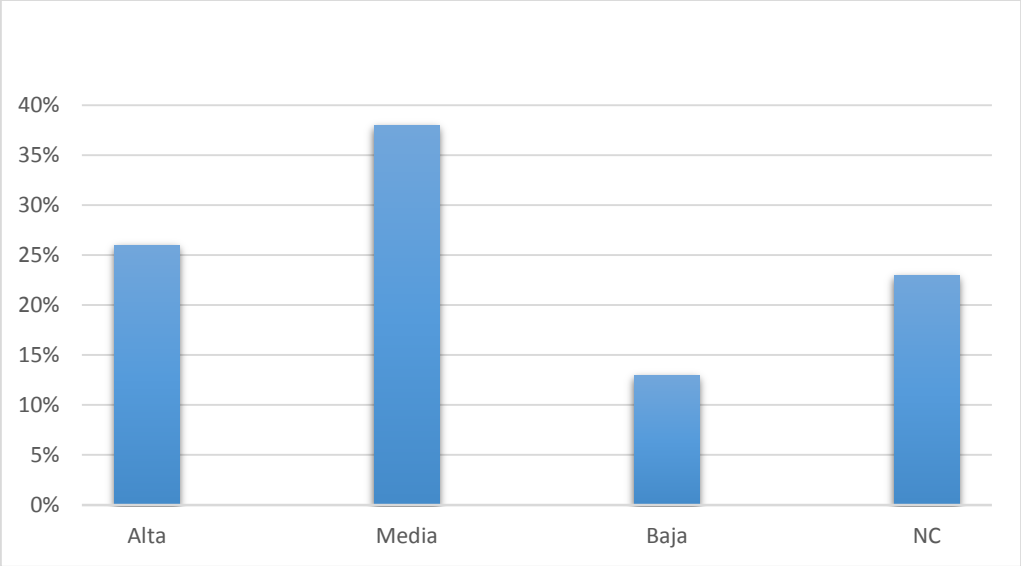


Figura 60: Valoración del factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2"
Fuente: Elaboración Propia

Factor 5: Deslealtad del personal que opera la plataforma de e-Commerce del sitio.

a) Estudiantes capacitados en seguridad informática y/o criptografía. (N = 49)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	33	0,67	67
MEDIA	12	0,25	25
BAJA	3	0,06	6
NO CONTESTA	1	0,02	2
TOTALES	N = 49	1,0	100

Tabla 43: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "deslealtad del personal que opera la plataforma de *e-Commerce* del sitio" es de importancia ALTA, para los estudiantes capacitados en seguridad informática y/o criptografía, como se puede observar en la figura 61, representados por el 67 %.

b) Estudiantes sin capacitación en seguridad informática y/o criptografía. (N = 61)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	41	0,67	67
MEDIA	12	0,20	20
BAJA	6	0,10	10
NO CONTESTA	2	0,03	3
TOTALES	N = 61	1,0	100

Tabla 44: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "deslealtad del personal que opera la plataforma de *e-Commerce* del sitio" es de importancia ALTA, para los estudiantes sin capacitación en seguridad informática y/o criptografía como se puede observar en la figura 61, representados por el 67 % de ellos.

c) Totalidad de los estudiantes encuestados (N = 110)

IMPORTANCIA DEL FACTOR	FRECUENCIA ABSOLUTA	FRECUENCIA RELATIVA	PORCENTAJE %
ALTA	74	0,67	67
MEDIA	24	0,22	22
BAJA	9	0,08	8
NO CONTESTA	3	0,03	3
TOTALES	N = 110	1,0	100

Tabla 45: Distribución de frecuencias absolutas y relativas para los datos cualitativos

La moda del factor "deslealtad del personal que opera la plataforma de *e-Commerce* del sitio" es de importancia ALTA, para la totalidad de los estudiantes encuestados de las dos submuestras; con y sin capacitación en seguridad informática y/o criptografía.

Se puede observar en la figura 61 que el 67 % del total de los estudiantes encuestados asignó importancia media al factor: deslealtad del personal que opera la plataforma de *e-Commerce* del sitio, que afecta la vulnerabilidad del sitio web del vendedor y que está relacionado con el mantenimiento y operación del sitio.

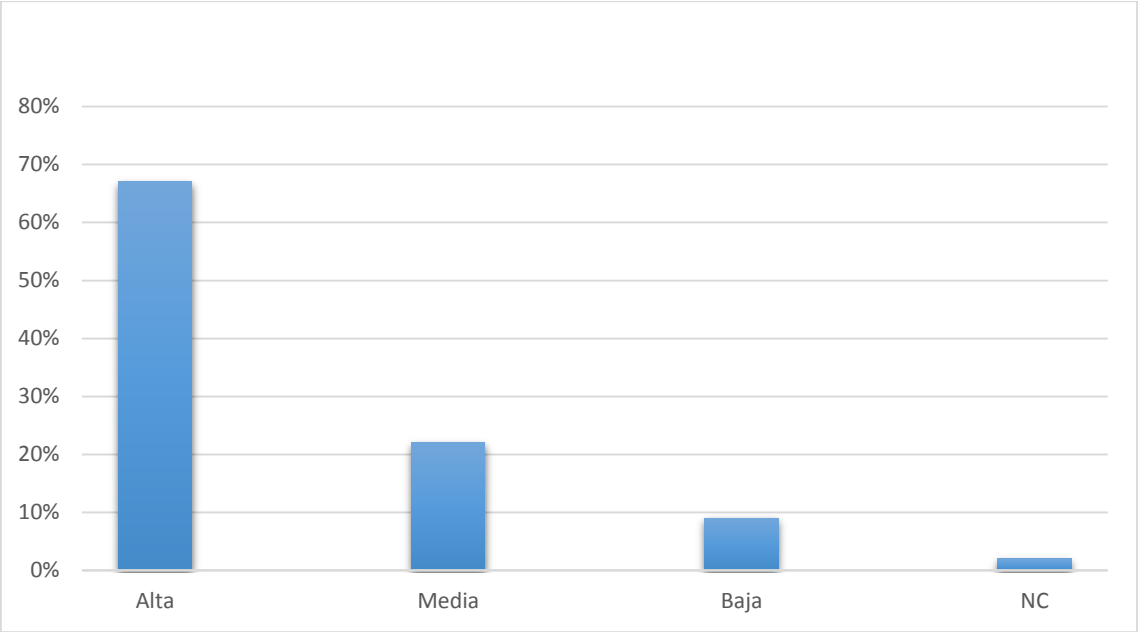


Figura 61: Valoración del factor "deslealtad del personal que opera la plataforma de *e-Commerce* del sitio"
Fuente: Elaboración Propia

Clasificación de los factores que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionados con el mantenimiento y operación del sitio.

En la figura 62 se grafican los resultados de la encuesta, que determino que para la totalidad de los estudiantes los factores que tienen alta incidencia ordenados por nivel de importancia, se presentan como sigue:

1. Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.
2. Deslealtad del personal que opera la plataforma de *e-commerce* del sitio
3. Seguridad física del servidor insuficiente
4. Falta de realización periódica de pruebas de vulnerabilidad por parte de personal idóneo

Para el factor "falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2", (factor N° 4), si bien hubo discrepancias entre la submuestra correspondiente a los estudiantes con capacitación que evaluó este factor con importancia media mientras aquellos sin capacitación que lo hizo como un factor de importancia alta, al considerar el total de los estudiantes, la evaluación final de este factor es de importancia media.

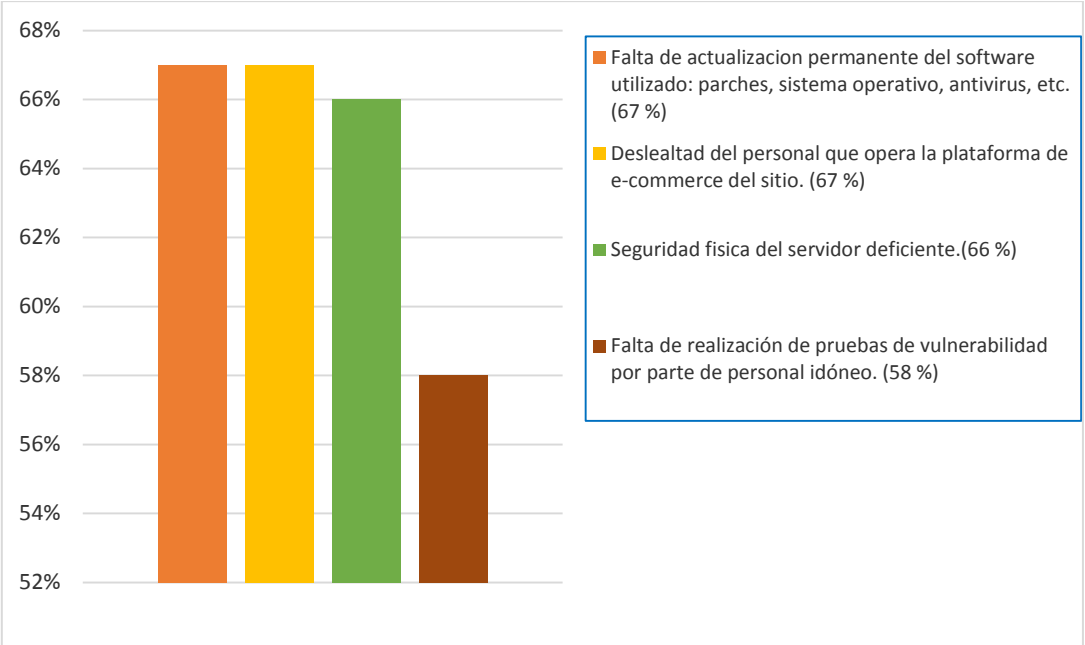


Figura 62: Clasificación de los factores que tienen mayor incidencia en las vulnerabilidades del sitio Web relacionados con el mantenimiento y operación del sitio
Fuente: Elaboración Propia

Orden de prioridad de los factores que generan vulnerabilidades en la seguridad del sitio web del proveedor

En la tabla 46 se han clasificado los factores que generan las vulnerabilidades en la seguridad del sitio web del proveedor en función del nivel de "importancia ALTA", adjudicado por la totalidad de los estudiantes, en función de la frecuencia absoluta obtenida en la encuesta. En caso de igual frecuencia absoluta para "importancia ALTA" el orden de los factores fue determinado por la frecuencia absoluta correspondiente a "importancia MEDIA" como fue el caso de los órdenes 4 y 5, como así también 8 y 9.6

Se observa que de los 15 factores incluidos en la encuesta, solo 10 han alcanzado el nivel de máxima importancia según la valoración de los futuros profesionales en TICs.

N° Orden	Descripción de la vulnerabilidad	Importancia ALTA	Importancia MEDIA	Importancia BAJA	NC
1	Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras	88	16	6	0
2	El sitio web no tiene la certificación vigente avalada por una autoridad certificante	79	24	6	0
3	En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito	76	24	3	7
4	Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.	74	32	3	1
5	Deslealtad del personal que opera la plataforma de *e-commerce* del sitio	74	24	9	3
6	Seguridad física del servidor deficiente	73	31	5	1
7	En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio	72	29	1	8
8	Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo	64	38	4	4
9	Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web	64	35	11	0
10	Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario	46	43	33	8

Tabla 46: Orden de prioridad de los factores que generan vulnerabilidades en la seguridad del sitio web del proveedor
Fuente: Elaboración Propia

Conclusiones del capítulo 3: L**a encuesta a futuros profesionales de TIC**

A lo largo de este capítulo se describe y analiza la instancia correspondiente al trabajo de campo, presentando el proceso que concluyó con la elaboración de una encuesta, realizada al universo muestral seleccionado, conformado por estudiantes de los dos últimos años de la carrera, en la Universidad de Buenos Aires, Facultad de Ciencias Económicas, carrera de Licenciatura en Sistemas de Información y en la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires, carrera de Ingeniería en Sistemas de Información.

Dada la amplia gama de alternativas de implementación del comercio electrónico, esta tesis se circunscribió - y en consecuencia la encuesta-, a evaluar solo el comercio electrónico trazable que opera con tarjetas de crédito. Como criterio de exclusión se estableció no considerar el análisis de las vulnerabilidades de la seguridad a la estación del usuario (computador y al navegador web), dado que las variables de configuración de los mismos son diversas y ameritan un estudio específico. Además, las falencias en la seguridad que pueda presentar la estación del usuario afectan a este último y no a todo el sistema de comercio electrónico, cuando este dispone de la protección de un firewall adecuado.

Para relevar la viabilidad de la herramienta de recolección se realizó el 18 de octubre del 2016 una encuesta piloto, que se efectuó en el curso correspondiente a la materia Tecnología de Comunicaciones, de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

En ella se solicitó la opinión escrita de los estudiantes respecto al contenido y formato de la encuesta propuesta. Como resultado de esta evaluación piloto se efectuaron modificaciones en la encuesta propuesta, que básicamente consistieron en la eliminación de tres preguntas y el agregado de aclaraciones correspondientes a términos empleados en el cuestionario.

La encuesta definitiva se efectuó en ambas universidades, en el mes de noviembre del 2016, sobre una muestra de 110 estudiantes y se obtuvieron los siguientes resultados, analizados para cada pregunta:

La primera pregunta de la encuesta se refería al nivel de capacitación técnica de los estudiantes en seguridad informática y/o criptografía, y buscaba conocer si habían recibido capacitación específica en esas temáticas, mediante seminarios, cursos o materias de grado.

Del total de 110 estudiantes encuestados, 49 estudiantes (submuestra 1) informaron que tuvieron capacitación en dichos temas, mientras que 61 estudiantes (submuestra 2) no tuvieron capacitación. Esta subdivisión de la muestra posibilitó analizar las respuestas de las siguientes preguntas para cada submuestra y para el total de la muestra.

La segunda pregunta se refería a los principales componentes del comercio electrónico. De los 110 estudiantes encuestados, el 77% opinó que efectivamente el comercio electrónico, desde el punto de vista del hardware y software, tiene como principales componentes: la estación del usuario compuesta por el host del cliente y su navegador web, la red Internet, los protocolos de comunicación y seguridad y el sitio web del vendedor (servidor y aplicaciones informáticas). No hubo diferencias significativas entre la submuestra 1 y 2, debido a que se trató de una pregunta básica sobre el comercio electrónico.

La tercera pregunta se refería a los requerimientos básicos de seguridad que son indispensables implementar para la transferencia segura de la información digital que tiene lugar en todo sistema de comercio electrónico. Del análisis de las respuestas, se observó que la divergencia de opinión entre los estudiantes que recibieron capacitación adicional (submuestra 1) y los que no la tuvieron (submuestra 2) fue mínima, menor al 1 %. Si bien la respuesta a esta pregunta requería de conocimientos más específicos sobre seguridad informática que la pregunta anterior, estos principios básicos se tratan en materias obligatorias de grado que ya cursaron los estudiantes de ambas submuestras. Si consideramos la totalidad de los estudiantes encuestados, el 89% de ellos acuerda con los conceptos básicos de la seguridad informática aplicados al comercio electrónico online, que son: la autenticación, la confidencialidad, la integridad, el no repudio y la disponibilidad de los datos y del sistema.

Las respuestas a las preguntas 2 y 3 están orientadas a medir el objetivo específico referido a: identificar los principales componentes que intervienen en una transferencia online de comercio electrónico trazable a través de la web y detallar los requerimientos mínimos de seguridad que debería tener la transferencia.

Las respuestas a la cuarta pregunta, relativa a los protocolos TCP y SSL/TSL revelo, en comparación con las otras preguntas, un mayor nivel de desconocimiento de los estudiantes sobre el tema. Al respecto, el 21 % de ellos desconoce el protocolo SSL/TLS y su función en la operatoria del comercio electrónico. Se observó un mayor nivel de

desconocimiento en el grupo de estudiantes sin capacitación adicional (submuestra 2) en seguridad informática que alcanzó al 25 %, mientras que el 54 % afirma que los protocolos consultados garantizan una comunicación confiable y segura.

El grupo de estudiantes capacitados (submuestra 1) tuvo menor porcentaje de desconocimiento del tema -solo el 16 %- y estuvo de acuerdo con lo afirmado en la pregunta respecto a que los protocolos TCP y SSL/TLS garantizan una comunicación confiable y segura el 63 % de los estudiantes.

Dado que del total de los 110 estudiantes, el 58 % está de acuerdo en afirmar que los protocolos TCP y SSL/TLS brindan confiabilidad (TCP) y seguridad (SSL/TLS) a la comunicación entre el sitio web del vendedor y el host del cliente pasando a través de las redes -específicamente, la insegura Internet- se pudo cumplir el objetivo planteado relativo a : determinar los protocolos que se emplean en las redes LAN, WAN e Internet para una comunicación confiable y segura entre el equipo del usuario y el sitio web.

La quinta pregunta tuvo como finalidad que los estudiantes identifiquen si el sitio web del proveedor es el componente del sistema de comercio electrónico trazable que presenta el mayor nivel de vulnerabilidad para la seguridad. Esta pregunta se encuentra directamente relacionada con la primera parte del objetivo principal de la tesis: identificar, según la evaluación efectuada por futuros profesionales de TIC, el componente del sistema de comercio electrónico trazable a través de la web, que presenta mayor nivel de vulnerabilidad para la seguridad del sistema.

Como respuesta, se obtuvo que el 62 % de los estudiantes sin capacitación adicional (submuestra 2) en seguridad informática está de acuerdo en considerar que en el sitio web se hallan las principales vulnerabilidades de la seguridad del comercio electrónico, mientras que para aquellos con capacitación (submuestra 1) ese porcentaje se eleva al 88%. Del total de los 110 estudiantes encuestados, el 74 % concuerda con la hipótesis en lo concerniente a ubicar el centro de la vulnerabilidad de la seguridad del comercio electrónico en el sitio web del proveedor y/o vendedor. Cabe mencionar también el bajo porcentaje de estudiantes que no respondieron a esta pregunta (8 %).

Podemos resumir hasta aquí, que los futuros profesionales de TIC consideraron que en el sistema de comercio electrónico, excluyendo del análisis la estación del usuario por las

razones mencionadas con anterioridad, la comunicación entre el usuario y el sitio web del vendedor no constituye un componente de riesgo para la seguridad del sistema, si se emplean los protocolos adecuados de comunicación y seguridad. En consecuencia, señalaron al último componente del sistema - el sitio web del vendedor- como el componente responsable de aportar la mayor vulnerabilidad al mismo.

Pero aquí surge una pregunta inevitable: ¿cuáles son los factores principales, en orden de importancia, que contribuyen a la inseguridad del sitio web y que, en definitiva, afectan la seguridad del sistema de comercio electrónico trazable?

Para responder a este interrogante, cuya respuesta contribuye a cumplir con la segunda parte del objetivo principal respecto a: determinar, para dicho componente, el orden de importancia de los factores que afectan la seguridad del mismo, se incluyeron las preguntas 6,7 y 8, relativas a los factores que afectan la seguridad del sitio WEB.

Estas tres últimas preguntas de la encuesta estuvieron referidas a la ponderación que los estudiantes efectuaron sobre la importancia de los factores presentados, en la generación de las vulnerabilidades en la seguridad del sitio web, agrupados según tres causas posibles:

- Las acciones del usuario relacionadas con el sitio web del vendedor
- La implementación del sitio web y su vinculación con la red y los usuarios
- El mantenimiento y operación del sitio web

Se incluyeron para cada causa de vulnerabilidad, cinco posibles factores que la generan o que contribuyen a ella, para los cuales, los estudiantes pudieron asignar el nivel de importancia que consideraron más adecuado según la escala ALTA, MEDIA, BAJA y en caso de no tener conocimiento podía seleccionar: NO RESPONDE.

Para la evaluación de las respuestas se utilizó la moda de cada nivel de importancia para cada factor. Por último, se clasificaron los factores según el siguiente criterio:

- Solo se consideraron los factores para los cuales la moda fue el nivel de importancia ALTA, adjudicado por la totalidad de los estudiantes.

- En caso de que dos o más factores obtuvieran igual frecuencia absoluta para importancia ALTA, el orden de los factores fue determinado por la frecuencia absoluta correspondiente a importancia MEDIA.

De los quince factores evaluados en la encuesta, sólo clasificaron según la consideración técnica de los estudiantes diez de ellos, considerados como factores determinantes que afectan directamente la vulnerabilidad de la seguridad del sitio web. Estos a su vez, se ordenaron según el valor decreciente de la moda alcanzado para importancia ALTA, obteniendo el siguiente resultado:

1. Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras
2. El sitio web no tiene la certificación vigente avalada por una autoridad certificante
3. En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito
4. Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.
5. Deslealtad del personal que opera la plataforma de *e-commerce* del sitio
6. Seguridad física del servidor deficiente
7. En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio
8. Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo
9. Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web
10. Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario

Por el contrario, los siguientes factores no fueron estimados por los estudiantes como de importancia ALTA:

- No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes
- No se emplea la facilidad “CAPTCHA” para el acceso de los usuarios al sitio web
- No se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio

- El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan
- Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS2

Se considera relevante la selección efectuada por los estudiantes universitarios de Sistemas de Información, dado que ellos ocuparán tareas tales como el desarrollo de aplicaciones informáticas, administración de redes, dirección de las áreas de sistemas, consultorías, seguridad informática, control de calidad, etc. y en consecuencia, entenderán en forma directa respecto a la evolución del sistema de comercio eléctrico y en relación a los principales factores que atenten contra su seguridad.

No obstante, cabe aclarar que la cantidad y el orden de importancia de los factores asignados por los futuros profesionales de TIC, no coincide con el considerado en la hipótesis de la tesis, que incluía los quince factores con importancia alta y según el siguiente orden:

1. El sitio web no tiene la certificación vigente avalada por una autoridad certificante
2. El acceso directo al sitio se efectúa sin el empleo de una contraseña segura ni se efectúa la prueba de *Turing* para diferenciar ordenadores de humanos (CAPTCHA)
3. No se emplean los servicios de un firewall para limitar e inspeccionar el tráfico entrante y saliente del sitio
4. Existencia de sitios web falsos que utilizan el método de *phishing* que posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito
5. Falta de actualización permanente del software utilizado en el sitio web
6. No se registran en el sitio las acciones de los usuarios en bitácoras adecuadas
7. Falta de realización periódica de pruebas de vulnerabilidad por personal idóneo
8. Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario
9. Falta de validación de los datos antes de almacenarlos en el servidor de la empresa
10. Seguridad física del servidor insuficiente
11. Deslealtad del personal que opera la plataforma de *e-commerce* del sitio
12. Falta de realización de pruebas de vulnerabilidad y de cumplimiento de las normas y estándares de la industria

13. El sitio web del vendedor no emplea el protocolo Plataforma de Preferencias de Privacidad (P3P) para el control, por parte de los usuarios, del uso que el sitio efectúa sobre sus datos personales
14. En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio
15. Falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas, como las normas PCI-DSS2

Conclusiones finales

El comercio electrónico es una actividad en permanente expansión que permite la entrega de bienes y servicios mediante el empleo de técnicas y herramientas electrónicas que, al efectuarse online, posibilitan automatizar el proceso de compra, reduciendo los costos y el tiempo de las operaciones comerciales.

Es necesario diferenciar entre comercio electrónico (*e-Commerce*) y los negocios en línea (*e-Business*). El primero incluye transacciones que trascienden las fronteras de la empresa, mientras que el segundo, se trata de tecnologías informáticas aplicadas a procesos que ocurren dentro de la empresa.

Un aspecto esencial del comercio electrónico es la confianza de los usuarios y proveedores para concretar las operaciones a través de dicho sistema. A su vez, esa confianza está basada en la ausencia de incidentes y estos últimos, ocurren cuando se presentan vulnerabilidades en la seguridad en uno o más componentes del sistema.

Con respecto a la inseguridad del sistema y en particular a la evolución del fraude en el comercio electrónico en América Latina, Souza (2017) a cargo del área "*Merchant Specialized Sales* Visa América Latina & Caribe" afirma:

> El rápido crecimiento posiciona a América Latina como una de las regiones más atractivas del mundo para el desarrollo del e-Commerce pero también para los ataques de los defraudadores. Hacia fines de 2016, en el marco de volumen de ventas, el *e-Commerce* en América Latina habrá representado un aproximado de US$ 66.700 millones. (pág. 3)

En consecuencia, dada la importancia a nivel mundial que representa el comercio electrónico y la influencia que el nivel de seguridad tiene en el desarrollo y expansión de esta actividad, se desarrolló el trabajo de tesis cuyo objetivo principal fue:

> Identificar, según la valoración efectuada por futuros profesionales de TICs, los factores determinantes, que, en el sistema de comercio electrónico trazable a través de la web, generan mayor nivel de vulnerabilidad en la seguridad del sistema y clasificar según el orden de importancia a dichos factores.

El trabajo de campo, se efectuó con estudiantes de los últimos años de la carrera (futuros profesionales de TIC) de dos universidades: en la Universidad de Buenos Aires, Facultad de Ciencias Económicas, carrera de Licenciatura en Sistemas de Información y en la Universidad Tecnológica Nacional, Facultad Regional Buenos Aires, carrera de Ingeniería en Sistemas de Información. En ambos casos, el universo lo integró estudiantes de los últimos años de las carreras.

Dada la amplia gama de posibilidades del comercio electrónico, el estudio de la tesis tomó en cuenta solo las operaciones trazables, que son aquellas realizadas mediante tarjetas de crédito, donde se pueden conocer con certeza los pasos ejecutados desde el origen hasta el destino final de la transacción comercial.

Se ha seleccionado este modelo por ser el más frecuentemente utilizado en el comercio electrónico. Asimismo, se excluyó del análisis de las vulnerabilidades en la seguridad, la estación del usuario (computador y navegador web), dado que las variables de configuración de los mismos son numerosas y ameritan un estudio específico aparte. Por otro lado, las falencias en la seguridad de la estación afectan a este último y no a todo el sistema de comercio electrónico, en especial cuando el sitio web del vendedor dispone de la protección de un firewall adecuado, situación que se verifica en la mayoría de ellos.

Para relevar la viabilidad y ajustar el contenido de la herramienta de recolección construida a tal efecto, se realizó una encuesta piloto en el curso correspondiente a la materia Tecnología de Comunicaciones, de la Licenciatura en Sistemas de Información de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

La encuesta definitiva se realizó en base a una muestra constituida por 110 estudiantes. Dado que la primera pregunta se refería al nivel de capacitación logrado por los estudiantes en seguridad informática y/o criptografía, mediante materias de grado (obligatorias y/o electivas), como así también, cursos y seminarios específicos, las respuestas a esta pregunta posibilitó dividir la muestra en dos submuestras, una constituida por 49 estudiantes que tuvieron capacitación en seguridad informática y/o criptografía, que denominamos submuestra 1, y la otra conformada por 61 estudiantes que no tuvieron capacitación en los temas mencionados, denominada submuestra 2.

Para poder alcanzar el objetivo principal de la tesis se tuvieron que establecer objetivos específicos, el primero de los cuales requería: identificar los principales componentes que intervienen en una transferencia online de comercio electrónico trazable a través de la web.

Las respuestas a esta pregunta, relativa a la composición del sistema de comercio electrónico, permitieron cumplir con el objetivo mencionado y corroborar la siguiente hipótesis específica:

> Se considera que el sistema de comercio electrónico trazable tiene como principales componentes: el host del cliente y su navegador web, las redes LAN e Internet, los protocolos de comunicaciones y de seguridad que brindan una conectividad confiable y segura, el sitio web del vendedor y entidades intermedias.

De los 110 estudiantes encuestados, el 77% opinó que efectivamente el comercio electrónico -desde el punto de vista del hardware y software- tiene los componentes detallados en la hipótesis. Para el grupo de estudiantes capacitados en seguridad informática el porcentaje fue del 90% y para el no capacitado fue del 67 %. Cabe aclarar, que a los componentes principales arriba indicados, en ciertas estructuras de comercio electrónico, se agregan también entidades intermedias y bancos.

En el capítulo 1 se presentaron los diferentes modelos de comercio electrónico. Sin embargo, el modelo B2C (*Business to Consumer*), entre el negocio o tienda virtual y los consumidores interesados en comprar productos o adquirir servicios, es el que frecuentemente se emplea por parte de los negocios y tiendas en línea para llegar a los consumidores individuales, por esta razón fue el considerado en este trabajo de tesis. Asimismo, se estimó como medio de pago la tarjeta de crédito, por ser el más difundido en el comercio electrónico, especialmente en el B2C que constituye nuestro caso.

Las siguientes preguntas de la encuesta se centraron en las vulnerabilidades, o también podríamos decir debilidades, del comercio electrónico. Entendemos como vulnerabilidades en dicho comercio a los aspectos técnicos, operativos y de procedimiento que pueden ocasionar la captura intencional de información confidencial por parte de terceros para ejecutar acciones - en tiempo real o diferidas- que afecten económicamente al comprador y/o al vendedor.

Los riesgos que tienen los usuarios cuando operan una transacción comercial son varios, entre los principales podemos citar: la suplantación de identidad, el robo de datos personales mediante el "*phishing*" u otros métodos, el fraude por parte de la empresa vendedora al no entregar los productos o servicios contratados, el ataque al sistema de

cómputos del usuario mediante malware, virus informáticos, troyanos, crackers, hackers, la divulgación de identidades y el ataque *ramsonware*.

Al analizar estos ataques al usuario, y a aquellos que pueden afectar al sitio web, se tuvieron en cuenta los conceptos básicos de seguridad informática que se consideran en toda operación que se realiza a través de la red Internet: la confidencialidad o privacidad, que consiste en la protección contra escuchas no autorizadas y que es especialmente importante en las transacciones con tarjetas de créditos evitando la difusión de sus datos; y la autenticación que abarca los conceptos de identificación, integridad y no repudio. La identificación del usuario brinda protección frente a la suplantación de personalidad; la integridad se refiere a la protección de los datos originales a efectos de evitar su modificación total o parcial; y el no repudio concierne a la protección frente a posteriores negaciones respecto del bien o servicio brindado por el vendedor y/o recibido por el comprador. También se agregó un concepto relevante para garantizar la operación en el comercio electrónico como es la disponibilidad de los datos, a efectos que la operación esté disponible en todo momento para las partes autorizadas.

Con respecto a estos conceptos básicos de seguridad informática, la respuesta de los estudiantes posibilitó cumplimentar el objetivo relativo a (…) detallar los requerimientos mínimos de seguridad que debería tener la transferencia y permitió en consecuencia, corroborar la siguiente hipótesis específica:

> Se considera que los requerimientos mínimos de seguridad de toda operación online de comercio electrónico deben ser: autenticación de las identidades de los participantes, la integridad de los datos implicados en las transacciones, la confidencialidad respecto de los datos intercambiados, la autorización que garantiza que la transacción es consentida por cada una de los participantes y la disponibilidad de los datos.

Si consideramos la totalidad de los estudiantes encuestados, el 89% de los mismos acuerda con los conceptos básicos de la seguridad informática aplicados al comercio electrónico online mencionados en la hipótesis anterior. Asimismo, se observó una divergencia menor al 1% entre en las respuestas de los estudiantes de la submuestra 1 (89,8%) y los de la submuestra 2 (88,5%). Esta circunstancia se originó presumiblemente en el hecho que la pregunta se refirió a conceptos básicos de seguridad informática como autenticación,

confidencialidad, integridad y no repudio, que se tratan normalmente cuando se analiza el tema de la transmisión de datos en el ámbito de las redes en asignaturas como Tecnología de Comunicaciones y Redes Informáticas (en la Facultad de Ciencias Económicas de la UBA), y en la asignatura Redes de Información en la UTN. Por lo cual, ambas submuestras demostraron poseer, al momento de la encuesta, un nivel similar de conocimiento sobre el tema.

Con respecto a la transmisión de datos a través de la red Internet entre el equipo del usuario y el sitio web del vendedor, se detalló en el capítulo 2, que puede realizarse con confiabilidad en la comunicación y con un nivel de seguridad satisfactorio, si se emplean los protocolos adecuados, actualizados e implementados según la normativa establecida para cada uno. En definitiva, se puede concretar con éxito la transferencia de datos de la operación de comercio electrónico, si se dispone de protocolos de comunicaciones confiables y protocolos de seguridad criptográficos.

Sobre este último punto, se analizó la confiabilidad de la comunicación en función del protocolo TCP, que es el que aporta confiabilidad en la comunicación entre el navegador web del usuario y la aplicación informática del vendedor. Éste es un protocolo orientado a la conexión y dispone de calidad de servicio, por lo cual brinda control de errores, control de flujo, control de congestión, administración de temporizadores, control activo de las retrasmisiones, evita la fragmentación a nivel IP y establece, en definitiva, en cada extremo de la comunicación, conexiones confiables en base a los sockets[190].

El TCP genera un paquete denominado segmento TCP que se transporta en el campo de carga del datagrama IP. Si bien, el protocolo IP no tiene calidad de servicio y no es orientado a conexión, estas funciones para la conexión las provee el TCP, con lo cual queda garantizada la realización de una comunicación confiable.

En el capítulo 1 también se analizaron las técnicas que posibilitan brindar seguridad a la transmisión de datos en la web. Las técnicas analizadas fueron la criptografía y la esteganografía. Para esta última, se concluyó que su factibilidad de empleo en el proceso de comercio electrónico trazable no resulta práctica, debido a que el objetivo de la misma es ocultar la transmisión de datos, y en el comercio electrónico analizado (B2C) se requiere la trazabilidad de la operación entre el usuario comprador y el sitio de venta.

[190] SOCKETS: Par de valores, constituidos por la dirección IP y el puerto, que identifican los extremos de una conexión TCP.

Con respecto a la criptografía se detallaron los tres métodos diferentes de encriptado: simétrico, asimétrico y *hashing* que, se pueden aplicar en forma aislada o combinada. Se emplean combinados para obtener seguridad en la transmisión de datos; con el cifrado simétrico se encriptan los datos y documentos debido a que es un método de cifrado rápido. No obstante, dada la dificultad en la distribución de la clave de sesión, ésta se transmite mediante encriptado asimétrico. Por otro lado, para acreditar la integridad de un documento se emplea el cifrado *hashing*. Para hacerlo, en el extremo transmisor, se cifra con el método *hashing* y se obtiene el *digest* que se trasmite conjuntamente con el documento; en el extremo receptor, se cifra el documento mediante el mismo método *hashing* obteniendo un nuevo *digest*. Por último, se comparan los dos *digest* y si son iguales no hubo ataques a la integridad del documento. Para autenticar y/o firmar un documento se emplean los cifrados *hashing* y asimétrico combinados.

Ahora bien, todos estos métodos de cifrado se combinan armónicamente para brindar seguridad en la transacción de comercio electrónico mediante el protocolo SSL/TLS que utiliza en el nivel de transporte al protocolo TCP ya mencionado. Cabe aclarar que si bien existen otros protocolos como IPsec, SSH, 3D *Secure*, iKP y SET que también brindan seguridad informática en la web, en el comercio electrónico trazable el protocolo SSL/TLS se halla presente en la mayoría de las implementaciones comerciales.

Podemos concluir que el protocolo SSL, desarrollado en la década de los 90 por la Empresa NETSCAPE para ser incluido en su navegador web, proporciona autenticación, integridad y confidencialidad en las comunicaciones a través de la red Internet, entre el navegador del cliente y la aplicación en el servidor del sitio web del proveedor, empleando los métodos criptográficos descriptos precedentemente.

La implementación de protocolos que brindan seguridad, como es el caso del SSL/TLS, protege las comunicaciones a través de la web del peligroso ataque denominado hombre en el medio (*man in the middle*), que consiste en alterar la información en tránsito, como así también suplantar la identidad de los extremos de la comunicación.

Como se desarrolló en el capítulo 2, si bien el protocolo SSL/TLS tiene un nivel de seguridad aceptable, éste depende de dos factores importantes: la versión del protocolo que se encuentra en servicio y el procedimiento empleado en la implementación del mismo. En el caso de tener en servicio una versión antigua no actualizada del protocolo y el

atacante tomar conocimiento de este hecho, podría utilizar las falencias en la seguridad que la versión vieja posee y que siguen vigentes en la instalación, dado que oportunamente no se actualizó.

Asimismo, si el servidor del sitio web está controlado por un troyano o posee una configuración deficiente del SSL/TLS, es muy probable que se reciban ataques tendientes a engañar a los usuarios conectados a dicho sitio. El ataque básico consiste en hacerle creer al usuario que se encuentra en una comunicación cifrada segura, cuando en realidad no lo está por ejemplo, simulando el candado que se observa en una página web segura. Otras alternativas son: forzar el uso de protocolos o algoritmos criptográficos con debilidades comprobadas, inducir a la aceptación de certificados digitales que no son válidos para el servidor al cual se desea conectar, etc.

Con referencia a la contribución de los protocolos TCP y SSL/TLS en el proceso de comercio electrónico podemos remitirnos a la pregunta número 4 de la encuesta, que se relaciona con el siguiente objetivo específico:

> Determinar los protocolos que se emplean en las redes LAN, WAN e Internet para una comunicación confiable y segura entre el equipo del usuario y el sitio web.

Allí se interroga a los estudiantes respecto a los protocolos TCP y SSL/TLS: ¿Considera que los protocolos TCP y SSL / TLS, empleados en las operaciones de comercio electrónico, garantiza una comunicación confiable y segura entre el equipo del usuario (navegador web) y el sitio Web del vendedor?

Las respuestas revelaron un nivel mayor de desconocimiento por parte de los estudiantes sobre el tema en comparación con las preguntas anteriores. Esto responde a la especificidad de la pregunta respecto de los protocolos TCP y SSL/TLS, sobre los cuales el 16,32% de la submuestra 1 y el 24,59 % de la submuestra 2 desconocen el alcance, características y participación en el proceso del comercio electrónico - especialmente para el caso del protocolo SSL/TLS-.

Se observó un mayor nivel de desconocimiento en la submuestra 2, correspondiente al grupo de estudiantes no capacitados en seguridad informática, respecto a la submuestra 1, conformada por los estudiantes capacitados en el tema. Del total de los estudiantes el 58 % está de acuerdo con afirmar que los protocolos TCP y SSL/TLS brindan confiabilidad y

seguridad a la comunicación entre el sitio web del vendedor y el host del cliente pasando a través de las redes - específicamente la insegura Internet-, el 21% desconoce el tema y el 21% no está de acuerdo.

La respuesta de los futuros profesionales de TICs que consideran al TCP y al SSL/TLS como garantía de confiabilidad y seguridad en la comunicación coincide con la siguiente hipótesis planteada:

> Se estima que, si se verifica que la transferencia de datos entre el host del usuario y el sitio web se efectúa a través de redes LAN e Internet mediante protocolos de comunicaciones con calidad de servicio como el Protocolo para el Control de las Transmisiones (TCP), que brinda confiabilidad; y también con protocolos que brindan seguridad como el protocolo Nivel de Puertos Seguros/Nivel de Transporte Seguro (SSL/TLS), que autentica y encripta la comunicación; la vulnerabilidad principal en la seguridad del comercio electrónico no se produce en el transporte de datos entre el usuario y el sitio web del vendedor.

No obstante los resultados que corroboran la hipótesis arriba indicada, cabe aclarar que el SSL/TLS garantiza un alto nivel de seguridad siempre que se cumplan las dos condiciones ya mencionadas y detalladas en el capítulo 2, relativas a la actualización permanente de la versión del protocolo y a una implementación adecuada del mismo.

Una vez definido que los protocolos TCP y SSL/TLS garantizan una transmisión confiable y segura entre la estación del usuario y el sitio web, la pregunta número 5 de la encuesta estuvo relacionada con el objetivo siguiente: determinar el componente en el cual reside la vulnerabilidad principal de la seguridad del comercio electrónico.

Esta pregunta requirió la opinión de los estudiantes excluyendo del análisis la estación del usuario y también el enlace entre ésta y el sitio web, en función del resultado de la pregunta anterior. Por lo expuesto, la pregunta número 5 centró el objetivo en el sitio web del vendedor: ¿considera que la vulnerabilidad principal de la seguridad del comercio electrónico reside principalmente en el sitio web del vendedor?

Al respecto, el 62 % de los estudiantes la submuestra 2 (estudiantes no capacitados en seguridad informática) estuvo de acuerdo en considerar que en el sitio web se hallan las principales vulnerabilidades de la seguridad del comercio electrónico, mientras que para

los estudiantes de la submuestra 1 (estudiantes con capacitación en seguridad informática) el porcentaje se eleva al 88 %. Del total de los 110 estudiantes encuestados, el 74 % acuerda con la hipótesis en lo concerniente a ubicar el centro de la vulnerabilidad de la seguridad del comercio electrónico en el sitio web del proveedor y/o vendedor. Cabe aclarar también que resulto bajo el porcentaje de estudiantes que no respondieron esta pregunta (8 %).

Podemos resumir hasta aquí que los futuros profesionales de TIC consideraron que, en el sistema de comercio electrónico, la comunicación entre el usuario y el sitio web del vendedor no constituye un componente de riesgo para la seguridad del sistema, si se emplean los protocolos adecuados de comunicación y seguridad. En consecuencia, señalaron al último componente del sistema -el sitio web del vendedor- como el componente responsable de aportar la mayor vulnerabilidad en la seguridad del sistema.

Para responder a este interrogante, cuya respuesta contribuye a cumplir la segunda parte del objetivo principal (…) determinar, para dicho componente (el sitio web del vendedor), el orden de importancia de los factores que afectan la seguridad del mismo-, se incluyeron las preguntas 6,7 y 8 relativas a los factores que afectan la seguridad del sitio WEB.

Estas preguntas estuvieron destinadas a determinar la ponderación que los estudiantes efectuaron sobre la importancia de los factores que generan las vulnerabilidades en la seguridad del sitio web, agrupadas según tres causas posibles:

- Las acciones del usuario relacionadas con el sitio web del vendedor
- La implementación del sitio web y su vinculación con la red y los usuarios
- El mantenimiento y operación del sitio web

Se incluyeron para cada causa los factores principales que generan la vulnerabilidad, donde los estudiantes asignaron el nivel de importancia que consideraron más conveniente según la escala de importancia: ALTA, MEDIA, BAJA, y en caso de no tener conocimiento podían seleccionar NO RESPONDE.

Para la evaluación de las respuestas se utilizó la moda estadística de cada nivel de importancia, para cada factor. Por último, se clasificaron los factores según el siguiente criterio:

- Sólo se consideraron los factores, adjudicado por la totalidad de los estudiantes, para los cuales la moda fue el nivel de importancia ALTA
- En caso de que dos o más factores obtuvieran igual frecuencia absoluta para importancia ALTA, el orden de los factores fue determinado por la frecuencia absoluta correspondiente a importancia MEDIA.

De los quince factores incluidos en la encuesta, según la evaluación técnica de los estudiantes, solo clasificaron diez como factores determinantes que afectan directamente la vulnerabilidad de la seguridad del sitio web. Estos a su vez, se ordenaron según el valor decreciente de la moda alcanzado para importancia ALTA, siendo el resultado el que sigue:

1. Acceso directo de los usuarios al servidor sin el empleo de contraseñas seguras
2. El sitio web no tiene la certificación vigente avalada por una autoridad certificante
3. En sitios Web simulados o falsos el método de *phishing* posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito
4. Falta de actualización permanente del software utilizado: parches, sistema operativo, antivirus, etc.
5. Deslealtad del personal que opera la plataforma de *e-commerce* del sitio
6. Seguridad física del servidor deficiente
7. En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio
8. Falta de realización periódica de "Pruebas de Vulnerabilidad" por personal idóneo
9. Falta de validación de los datos del usuario antes de almacenarlos en el servidor del sitio web
10. Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario

Por el contrario, los siguientes factores no fueron estimados por los estudiantes como de importancia alta:

- No se registran en el servidor web las acciones de los usuarios en las bitácoras correspondientes.

- No se emplea la facilidad “CAPTCHA” para el acceso de los usuarios al sitio web
- No se emplean *proxies* en la conexión entre la red Internet y el entorno de la aplicación del sitio
- El sitio web no emplea P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan
- Falta de observancia y/o actualización de los estándares de la industria que dictan "mejores prácticas" como las normas PCI-DSS2

Del análisis de los diez factores determinantes seleccionados por los estudiantes surge que no coinciden con los considerados en la hipótesis de la tesis, que incluía quince factores, en el siguiente orden:

1. El sitio web no tiene la certificación vigente avalada por una autoridad certificante
2. El acceso directo al sitio se efectúa sin el empleo de una contraseña segura ni se efectúa la prueba de *Turing* para diferenciar ordenadores de humanos (CAPTCHA)
3. No se emplean los servicios de un firewall para limitar e inspeccionar el tráfico entrante y saliente del sitio
4. Existencia de sitios web falsos que utilizan el método de *phishing* que posibilita engañar a los usuarios a efectos que revelen datos personales relativos a sus tarjetas de crédito y/o débito
5. Falta de actualización permanente del software utilizado en el sitio web
6. No se registran en el sitio las acciones de los usuarios en bitácoras adecuadas
7. Falta de realización periódica de pruebas de vulnerabilidad por personal idóneo
8. Falta de códigos de control en formularios y de controles en el sitio sobre las cadenas de caracteres ingresadas por el usuario
9. Falta de validación de los datos antes de almacenarlos en el servidor de la empresa.
10. Seguridad física del servidor insuficiente
11. Deslealtad del personal que opera la plataforma de *e-commerce* del sitio.
12. Falta de realización de pruebas de vulnerabilidad y de cumplimiento de las normas y estándares de la industria.
13. El sitio web del vendedor no emplea el protocolo Plataforma de Preferencias de Privacidad (P3P) para el control, por parte de los usuarios, del uso que el sitio efectúa sobre sus datos personales

14. En el servidor no se ha prohibido todo el tráfico entrante y saliente, excepto el estrictamente necesario para la operación del servicio del sitio
15. Falta de observancia y/o actualización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2

Por lo tanto, como resultado de la tesis podemos concluir que en el sistema de comercio electrónico trazable B2C que opera preferentemente con tarjetas de crédito, según la opinión técnica de estudiantes universitarios de las carreras de Licenciatura e Ingeniería en Sistemas de Información, futuros profesionales de TIC, la vulnerabilidad principal de la seguridad reside en el sitio web del vendedor o proveedor y no en la comunicación entre la estación del usuario y el mencionado sitio. Asimismo, los estudiantes determinaron los diez factores, mencionados precedentemente, que inciden en la vulnerabilidad de la seguridad del sitio, que se han ordenados según un orden de importancia decreciente.

Se considera relevante la determinación realizada por estudiantes universitarios de Sistemas de Información sobre el componente de mayor incidencia en la vulnerabilidad de la seguridad del sistema de comercio electrónico, como así también, en la selección de los factores más importantes para la seguridad del sitio web. Estos estudiantes serán futuros profesionales de TIC, los cuales, en el desarrollo de sus actividades se ocuparán de tareas tales como la implementación de aplicaciones informáticas, administración de redes, dirección de áreas de sistemas, consultorías, seguridad informática, control de calidad, etc. y en consecuencia, tendrán participación directa respecto a la evolución del sistema de comercio eléctrico en relación a la problemática de la seguridad del mismo.

En consecuencia, esta tesis proporciona un enfoque diferente sobre la seguridad del sistema de comercio electrónico, que si bien es evaluado frecuentemente por instituciones y entidades en función de numerosas encuestas realizadas a usuarios, comerciantes y empresarios, tienden a reflejar la percepción subjetiva que dichos agentes tienen respecto a la inseguridad de este sistema, basada en experiencias personales y/o ajenas, exitosas o no. Estas apreciaciones no están basadas en un análisis profesional fundado en los factores determinantes que condicionan la seguridad del sistema, ni son evaluados por futuros profesionales de TIC como en el caso desarrollado.

Por otro lado, la identificación del componente de mayor vulnerabilidad para la seguridad del sistema de comercio electrónico trazable, y la determinación de los factores de mayor incidencia en la vulnerabilidad del sitio web, constituyen un aporte para la planificación de

la estrategia a seguir por empresas, consultoras, entidades y organismos involucrados en la evolución, desarrollo y mantenimiento de sistemas de comercio electrónico.

Desde el punto de vista académico, las conclusiones de la tesis posibilitarán que los programas de estudio de las asignaturas relacionadas con seguridad informática aplicada a los sistemas de comercio electrónico, profundicen en el análisis de los factores que los estudiantes evaluaron de alta prioridad para la seguridad.

Asimismo, sería conveniente continuar con la línea investigativa de esta tesis profundizando en fundamentos técnicos y operativos que originaron la alteración del orden de importancia de los factores por parte de los estudiantes, respecto al establecido en la hipótesis. En particular, se debería investigar la incidencia en la vulnerabilidad de la seguridad del sitio web los siguientes factores a los que los estudiantes no se asignaron nivel de importancia ALTA:

- Registro en el servidor web de las acciones de los usuarios en las bitácoras correspondientes
- Empleo de la facilidad “CAPTCHA” para el acceso de los usuarios al sitio web
- Utilización de programas *proxies* para la conexión entre la red Internet y el entorno de la aplicación del sitio
- Utilización en el sitio web del protocolo P3P (Plataforma de Preferencias de Privacidad) que ofrece a los usuarios una forma automatizada de controlar el uso que se hace de su información personal en los sitios Web que visitan
- Utilización de los estándares de la industria que dictan mejores prácticas como las normas PCI-DSS2

Por último, la línea de investigación llevada a cabo en la presente tesis debería ampliarse incorporando la estación del usuario. Asimismo, en una etapa posterior se debería considerar continuar con variantes de comercio electrónico no trazable, que utilicen la denominada moneda electrónica.

Referencias Bibliográficas

Acebey, J., & Terrazas , D. (diciembre de 2006). *UV.ES*. Obtenido de http://www.uv.es/. ~sto/articulos/BEI-2003-11/certificados_digitales.html. [14] Wagner D.

Ackoff, R. (2001). *Differences that make a difference.* Triarchy Press.

Administrador de G Suite. (10 de Febrero de 2017). *G Suite*. Obtenido de https://support.google.com/a/answer/1217728?hl=es

Agnew. (2003). Secure electronic transactions: Overview, capabilities and current status. *Payment Technologies for e-commerce*, Springer-Verlag, Berlin, pp. 211-226.

Aguirre, J. R. (Octubre de 2014). *Cripto Red*. Obtenido de http://www.criptored.upm.es/thoth/material/texto/pildora007.pdf

APWG News. (23 de Febrero de 2017). *APWG*. Obtenido de http://www.antiphishing.org/apwg-news-center/

Arabia, C. (Abril de 22 de 2017). *Infobae Economico*. Obtenido de http://www.infobae.com/economia/2017/04/22/dinero-electronico-5-mecanismos-del-bcra-para-reducir-la-utilizacion-del-dinero-fisico-y-el-costo-de-las-transacciones/

Arielmcorg. (15 de septiembre de 2016). *INFOSERTEC*. Obtenido de https://infosertec.com.ar

Bae Negocios (16 de Febrero de 2017) *El comercio electronico local sigue creciendo en el ultimo año movió 100.000 millones*. Obtenido de www.diariobae.com

Banco Bilbao Vizcaya Argentina. (29 de Diciembre de 2015). *BBVA Que significan los numeros de las tarjetas de credito*? Obtenido de https://www.bbva.com/es/noticias/economia/bancos/tarjetas/significan-los-numeros-las-tarjetas-credito-debito/

Barba Marti, A. (2001). *Gestion de red.* Mexico: Alfaomega.

Black, U. (1997). *Redes de Computadores, protocolos, normas e interfaces.* Mexico: Rama.

Black, U. (1999). *Tecnologias emergentes para redes de computadoras.* Mexico: Prentice Hall.

Bustamante, A. J. (1999). *Sistemas de clave publica*. *IEEE*, 3.

Caballero, P. (2002). *Introducción a la Criptografía, 2ª Edición.* Madrid: Ra-Ma .

Callegari, O. (15 de Febrero de 2017). *RDNS Net Report*. Obtenido de http://www.rnds.com.ar/articulos/069/RDNS_116w.pdf

Camara Argentina de Comercio Electronico. (11 de Marzo de 2017). *CACE*. Obtenido de www.cace.org.ar

Cano, J. (2013). *Inseguridad de la informacion.* Colombia: Alfaomega.

Carlson, B., Crilly, P., & Rutledge, J. (2007). *Sistemas de comunicacion.* Mexico: McGraw Hill.

CCM. (19 de Marzo de 2017). *CCM*. Obtenido de http://es.ccm.net/contents/745-registradores-de-pulsaciones-de-teclas

Centro de respuestas a incidentes de seguridad informatica de Uruguay. (5 de Marzo de 2013). *CERTuy*. Obtenido de https://www.cert.uy/inicio/incidentes/que_es-un-incidente/

Centro de Seguridad de Norton. (19 de Marzo de 2017). *Norton by Symantec*. Obtenido de https://ar.norton.com/vital-security/article

Chapra, S., & Canale , R. (1999). *Metodos numericos para ingenieros.* Mexico: McGraw Hill.

Chou, W. (2002). Inside SSL: the secure sockets layer protocol. *IEEE Computer Society*, vol. 4, p. 4, pp. 47-52.

Clarin Negocios. (2 de Mayo de 2017). Obtenido de https://www.clarin.com/

Comer, D. (1996). *Redes globales de informacion con Internet y TCP/IP.* Mexico: Prentice Hall.

Comercio electronico. (25 de Febrero de 2017). *Medios de Pagos en Comercio electronico*. Obtenido de https://karencanoshirlissaenz.wordpress.com/medios-de-pago-comercio-electronico/

Cornejo, M. A. (22 de Mayo de 2015). *Seguridad Informatica 365*. Obtenido de http://bellapadula.blogspot.com.ar/2015/05/esteganografia.html

Dolder, H. (29 de Abril de 1999). La Economía en Red, la Sociedad en Red y el Ciberespacio. *IEEE*, 10.

Drew , G. (1999). *Using Set for Secure Electronic Commerce.* New york: Prentice Hall.

EcuRed. (19 de Marzo de 2017). *EcuRed*. Obtenido de https://www.ecured.cu/Prueba_de_penetraci%C3%B3n

Encuesta Global sobre Delitos Económicos 2016. (20 de febrero de 2017). *PWC Argentina*. Obtenido de https://www.pwc.com.ar/es/publicaciones/assets/encuesta-delitos-economicos-2016.pdf

Engst, A., & Fleishman, G. (2003). *Introduccion a las redes inalambricas, 802.11a, 802.11b, AirPort y AirPort Extreme de Apple.* España: Anaya.

Estudio de situacion del comercio electronico en España. (1 de Enero de 1999). *CIPRES - UPM*. Obtenido de http://www.dit.upm.es/~enrique/ce/sec3/par325.html

Estudio especial de la OMC sobre Comercio Electronico. (16 de Julio de 2012). *Organizacion Mundial del Comercio*. Obtenido de http://www.wto.org/spanish/tratop s/ecom s/special study s.pdf

Feit, S. (1998). *Arquitectura, protocolos e implementacion con IPv6 y seguridad IP*. España: Mc Graw Hill.

Finanzas por iprofesional. (18 de Junio de 2013). *iprofesional*. Obtenido de www.iprofesional.com

Forouzan, B. (2006). *Transmision de datos y redes de comunicaciones.* Madrid: Mc Graw Hill.

Forrester Research. (2010). *The value of corporate secrets.How compliance and collaboration affect enterprise perceptions of risk.* EEUU: Forrester Research.

Freund, J., Miller, I., & Miller, M. (2001). *Estadistica Matematica con aplicaciones.* Mexico: Prentice Hall.

Fusario, R. (2006). *Tecnicas de transmision banda base aplicadas a redes LAN y WAN.* Buenos Aires: INET.

Gallardo, C. (2004). *Seguridad en redes telematicas.* Madrid: Mc Graw Hill.

Gomez, J. (2011). *Matematicos, espias y piratas informaticos.* España: RBA .

Gomez, V. (10 de Abril de 2015). *Desarrollo Geek*. Obtenido de https://desarrollo-geek.net/sistemas-operativos/linux/soft-linux/los-mejores-8-scanners-de-vulnerabilidades-web/

Guasch, J. (20 de Diciembre de 2013). *Security by default.* Madrid: RootedCON.

Halsall, F. (1998). *Comunicacion de datos,redes de computadores y sistemas abiertos.* Wilmington Delaware: Addison Wesley.

Halsall, F. (2006). *Redes de Comoputadores e Internet.* Madrid: Pearson.

Harris, P., Rethie, R., & Kuan, C. (2005). Adoption and Usage of M-Commerce: A CrossCultural Comparison of Hong Kong and the United Kingdom. *Journal of Electronic Commerce Research, Vol. 6 (3)*, 210-224.

Hurtado, I. L., & Toro, J. G. (2001). *Paradigmas y metodos de investigacion en tiempos de cambios.* Valencia: Episteme.

IBM. (2 de Marzo de 2017). *IBM Appscan*. Obtenido de http://avnet360.com/seguridad/appscan

ITInsecurity . (12 de noviembre de 2010). *ITInsecurity* . Obtenido de https://xombra.com/index.php?do/noticias/nota/5167/op/4/t/bases-datos---insegu

Jacoby, J., & Kaplan, L. (1972). The components of perceived risk. *Proceedings of the 3rd Annual Conference of the Association for Consumer Research*, 382-393.

JC Mouse. (29 de Enero de 2017). *JC Mouse*. Obtenido de : http://jc-mouse.blogspot.com.ar/2011/05/esteganografia-lsb-en-java-proyecto.html

Koosis , D. (1972). *Introduccion a la inferencia estadistica para administracion y economia.* Mexico: Limusa.

Kroll. (Mayo de 2011). *Global Fraud Report*. Obtenido de Http://www.krollconsulting.com/media/pdfs/kroll_global_Fraud_Report_May_2011_spanish_final.pdf

Kuper, P. (2005). The state of security. *IEEE Security & Privacy*.

Laudon, K., & Traver, C. (2013). *E-commer 2013.* Mexico: Pearson.

Lechtaler, A. C., & Fusario, R. (1999). *Teleinformatica para ingenieros en sistemas de informacion.* Madrid: Reverte.

Lechtaler, A. C., & Fusario, R. (2015). *Comunicaciones y Redes para profesionales en sistemas de informacion.* Buenos Aires: Alfaomega.

Leinwand, A., & Pinsky, B. (2001). *Configuracion de routers Cisco.* España: Cisco Press.

Leon, I. H., & Garrido, J. T. (2001). *Paradigmas y metodos de investigacion en tiempos de cambios.* Valencia: Episteme.

Li, Z.-N., & Drew, M. (2004). *Fundamentals of Multimedia.* EEUU: Pearson.

Lopez lopez, J. (27 de Febrero de 2014). *El economista*. Obtenido de http://www.eleconomista.es/tecnologia/noticias/5578707/02/14/La-moda-del-Big-Data-En-que-consiste-en-realidad.html

Lorena, R. (4 de julio de 2016). *Rankia.com*. Obtenido de https://www.rankia.com/blog/mejores-tarjetas/2824096-que-cvv-cvc-significan-numeros-tarjetas-credito-debito

Lussato, B. (1982). *El desafio informatico.* Madrid: Planeta.

Martínez López, L., Mata Mata , F., & Rodríguez Domínguez, R. (2009). SISTEMAS DE PAGO SEGURO. SEGURIDAD EN EL COMERCIO ELECTRÓNICO . *Revista de Estudios Empresariales. Segunda época*, 63 - 76 .

Merkow , M., & Breithaupt, J. (1998). *Building SET Applications for Secure Transaction.* EEUU: John Wiley & Sons.

Mifsud, E. (26 de Marzo de 2012). *Observatorio tecnologico*. Obtenido de http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3

Modelo Consumer To Business. (11 de Noviembre de 2015). *Modelos de Comercio Electronico*. Obtenido de www.comercioelectgronicopaitoc.blogspot.com.ar

Montañana, R. (20 de Febrero de 2017). *SlidePlayer*. Obtenido de (http://slideplayer.es/slide/106539/

Movistar. (23 de Septiembre de 2013). *Movistar*. Obtenido de http://comunidad.movistar.es/t5/Software-y-Sistemas-Operativos/Tecnolog%C3%ADa-4G-Qu%C3%A9-es-y-para-qu%C3%A9-sirve/td-p/1444770

Moya, J. (2006). *Redes y servicios de comunicaciones.* España: Paraninfo.

Negocios. (2 de Mayo de 2017). *Clarin*. Obtenido de https://www.clarin.com/

negocios@diariobae.com. (16 de Febrero de 2017). El comercio electronico local sigue creciendo: en el ultimo año movio mas de $ 100.000 millones. *BAE Negocios*, pág. 16.

Nombela, J. (1997). *Seguridad Informatica.* España: Paraninfo.

Noriega, S. (22 de Octubre de 2014). *Certsuperior*. Obtenido de https://www.certsuperior.com/Blog/por-que-un-certificado-ssl-hace-mi-empresa-mas-productiva

Norton by Symantec. (19 de Marzo de 2017). *Symantec Corporation*. Obtenido de https://ar.norton.com/virus-first-written/article

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

Orellana, L. (2001). *Estadistica descriptiva.* Buenos Aires.: UBA.

Pacheco, F. (2014). *Criptografia.* Buenso Aires: Redusers.

PCI Security Standards Council . (Noviembre de 2013). *PCI Security Standards* . Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Rayport, J., & Jaworski, B. (2003). *Introduction to E-commerce.* Nueva York: Mc Graw Hill.

Requisitos y procedimientos de evaluación de seguridad. (Noviembre de 2013). *PCI(Industrias de trajetas de Pago)*. Obtenido de https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

Rescorla, E. (2000). *SSL and TL. Designing and Building Secure Systems.* EEUU: Addison Wesley.

Rivero, M. (7 de Febrero de 2017). *Info Spyware*. Obtenido de https://www.infospyware.com/articulos/que-es-el-phishing/

Ropero, A. (16 de Febrero de 2017). *Hispasec*. Obtenido de Denegacion de servicio en Open SSL: (http://unaaldia.hispasec.com/2017/02/denegacion-de-servicio-en-openssl.html

Rouse, M. (Septiembre de 2005). *TechTarget*. Obtenido de http://searchsecurity.techtarget.com/definition/PUP

Rubalcaba, L. (2010). *La Innovacion en servicios en España.* Madrid: Rooter.

Sabater, A. F., Martinez, D., Hernandez, E., Montoya, V., & Muñoz, M. (2001). *Tecnicas Criptograficas de Proteccion de Datos.* Madrid: Alfaomega.

Saquete, R. (3 de Septiembre de 2013). *Human Level Communications*.

Saravia, M. (2007). *Los metodos cuantitativos y cualitativos en la evaluacion de impactos en proyectos de investigacion social.* Guatemala: Universidad Mariano Galvez.

Scolnik, H. (2014). *Que es la seguridad informatica.* Buenos Aires: Paidos.

Senn, J. (1992). *Analisis y diseño de sistemas de informacion.* Mexico: Mc Graw Hill.

Sierra, G. (5 de Abril de 2015). *Clarin*. Obtenido de http://www.clarin.com/mundo/Ciberguerra-Estados_Unidos-China-Gran_Bretana-NSA-SnowdenGCHQ_0_1333067115.html

Souza, F. (20 de Febrero de 2017). *Cybersource Corporation*. Obtenido de https://www.cybersource.com/content/dam/cybersource/es-lac/documents/Online_Fraud_Report_2016.pdf

Stallings, W. (2004). *Comunicaciones y Redes de Computadoras.* España: Pearson.

Stallings, W. (2004). *Fundamentos de seguridad en redes. Aplicaciones y estandares.* . Madrid: Pearson.

Sumanjeet. (2009). Emergence of payment systems in the age of electronic commerce. *The state of art. Global Journal of International Business research.*, 17.

Suplantacion de identidad Phishing. (1 de Marzo de 2017). *CCM Comunidad Informatica*. Obtenido de http://es.ccm.net/contents/35-suplantacion-de-identidad-phishing

Tanenbaum, A. (2003). *Redes de Computadoras.* Maxico: Pearson.

TECNO. (22 de Febrero de 2012). *INFOBAE*. Obtenido de http://www.infobae.com/2012/02/22/633461-microsoft-omitio-informacion-importante-su-acusacion-contra-google/.

Tirante, J. (2006). *Delitos Informaticos.* Buenos Aires: CEIT.

Tomasi, W. (2003). *Sistemas de comunicaciones electronicas.* Mexico: Pearson.

Traver, L. (2014). *E-commerce, Negocios, tecnologia, sociedad.* Mexico: Pearson.

Tulloch, M. (2003). *Microsoft Encyclopedia of segcurity.* EEUU: Microsoft Press.

Universidad Politecnica de Valencia. (20 de Fecbrero de 2017). *Universidad Politecnica de Valencia*. Obtenido de http://www.upv.es/contenidos/CD/info/711545normalc.html

Urbano, S. M. (26 de Febrero de 2017). *ACTUALIDADECOMMERCE*. Obtenido de www.actualidadecommerce.com

Valles, J. P. (2002). Sistemas de Pagos Electronicos. *Buran*, 40.

Velasco, R. (7 de Agosto de 2015). *RedesZone*. Obtenido de https://www.redeszone.net/2015/08/07/sha-3-nuevo-estandar-hash-aprobado-nist/

Viega, j., Messier, M., & Chandra, P. (2002). *Network Security with OpenSSL, Cryptography for Secure Communications.* EEUU: O'Really.

VISA INTERNATIONAL. (20 de Febrero de 2017). *Estandar de seguridad tarjetas de pago*. Obtenido de https://www.visaeurope.es/estandar-de-seguridad-tarjetas-de-pago

vulnerabilidades, A. y. (16 de Marzo de 2017). *Red y Seguridad (UNAM)*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html

Wang, J. (2006). *Computer Network Security: Theory and Practice.* Beijing: Higher Education Press. .

Wright. (2002). Comparative Evaluation of Electronic Payment Systems. *Information Systems and Operational Research* , 71.

Tabla de Acrónimos

AES: Advanced Encription Standard

APWG: Anti Phishing Working Group

ARP: Address Resolution Protocol

AS: Autonomous System

ARPANET: Advanced Research Projects Agency Network..

ATM: Asynchronous Transfer Mode.

B2B: Business To Business

B2C: Business To Consumer.

B2E: Business To Employee.

BMP: BitMaP.

CA: Certification Authority.

C2B: Consumer To Business

C2C: Consumer To Consumer.

C2G: Consumer To Government.

CAPTCHA: Completely Automated Public Turing, Computers and Humans Apart.

CNP: Card No Present

CRM: Customer Relationship Management.

CSS: Cascading Style Sheets.

DCT: Discrete Cosine Transform

DoS: Denial of Service.

DDoS: Distributed Denial of Service.

DEA: Data Encription Algorithm

DES: Data Encription Standard

DNS: Domain Name System

DoS: Denial of Service

EoF: End Of File.

EPS: Electronic Pay Systems.

FCS: Frame Check Sequency.

FFT: Fast Fourier Transform

FTP: File Transfer Protocol.

GAN: Global Area Network.

GIF: Graphic Interchange Format

GPRS: General Packet Radio Service

HTTPS: Hipertext Transfer Protocol Secure

ICMP: Internet Control Message protocol

IDEA: International Data Encription Algorithm

IEEE: Institute of Electrical and Electronics Engineers

ikP: Internet Keyed Payment Protocols

IOUG: Independent Oracle Users Group's

IP/MPLS: Internet Protocol/Multiple Protocols Lavels Swiching

IP: Internet Protocol.

IPSEC: Internet Protocol Security

ISO/IEC: International Estandar Organization/ International Electrotechnical Commision.

ISP: Internet Service Provider.

JPEG: Joint Photographic Experts Group

LAN: Local Area Network.

LSB: Last significative Bit

M2B: Movil To Business

MAC: Message Authentication Code

MD5: Message Digest Algorithm 5

MIT: Massachusetts Institute of Technology de EEUU

MSS: Maximun Segment Size

NAT: Network Address Translation

NIST: National Institute of Standards and Technology

OCSP: On line Certificate Status Protocol

OSI: Open Systems Inteconnection.

OWASP: The Open Web Application Security Proyect

P3P: Platform for Privacy Preferences.

PCI DSS: Payment Card Industry Data Security Standard

PCI DSS: Payment Card Industry Data Security Standard

PDF: Portable Document Format.

PDU: Unit Data Protocol

PHP: Hypertext Preprocessor.

PING: Packet Internet Groper

PKI: Public Key Infraestructure.

PNG: Portable Network Graphics

PPP: Point To Point Protocol

PUPs: Potentially Unwanted Programs

QoS: Quality of Service

RC2: Ron's Code 2.

RC4: Ron's Code 4

RC5: Ron's Code 5

RFC: Request For Comments.

RGB: Red Green Blue.

RP: Routing Protocols

SAFER: Secure And Fast Encription Routine

SCADA: Supervisory Control And Data Acquisition

SET: Secure Electronic Transaction

SHA: Segure Hash Algorithm

SMS: Short Message Service

SMTP: Simple Mail Transfer Protocol

SNMP: Simple Network Management Protocol

SQL: Structured Query Language.Lenguaje.

SSH: Secure Shell

SSL/TLS: Secure Sockets Layer/ Transport Layer Security

STEGFS: Steganographic File System

TCP/IP: Transmission Control Protocol / Internet Protocol.

TCP: Transmission Control Protocol.

TELNET: Telecommunication Network.

TRIPLE DES: Triple Data Encription Standard

UBA FCE: Universidad de Buenos Aires – Facultad de Ciencias Económicas

UDP: User Datagram Protocol

UMTS: Universal Mobile Telecommunications System

URL: Uniform Resource Locator,

UTN FRBA: Universidad Tecnológica Nacional – Facultad Regional Buenos Aires.

VPN: Virtual Private Network

W3C: World Wide Web Consortium

WAN: Wide Area Network.

WAP: Wireless Application Protocol

WIFI: Wireless Fidelity.